Jahresbericht 2000/2001 des Lehrstuhls

„Theoretische Konzepte und neue Anwendungen der Informatik“

(Univ.-Prof. Dr. sc. Christoph Meinel)

Fachbereich IV – Informatik
Universität Trier
D-54286 Trier, Germany

Vorwort

Der vorliegende Bericht gibt Auskunft über die Aktivitäten am Lehrstuhls "Theoretische Konzepte und neue Anwendungen der Informatik" der Universität Trier in den Jahren 2000 und 2001. Weitere Details finden Sie auf unserer Homepage

`http://www.informatik.uni-trier.de/TI`

Der Bericht gibt keine Auskunft über die Aktivitäten des unter meiner Leitung stehende, von der Fraunhofer-Gesellschaft betreuten Instituts für Telematik. Nähere Informationen hierzu können der Homepage

`http://www.ti.fhg.de/`

und den Jahresberichten des Instituts für Telematik entnommen werden. Die Mitarbeiter des Lehrstuhls und ich hoffen auf Ihr Interesse an unserer Arbeit und würden uns über Kontakte und Anstöße zu möglichen Kooperationsprojekten in Forschung und Lehre sehr freuen.

Christoph Meinel Trier, im Mai 2002

Inhaltsverzeichnis

1 Personelle Zusammensetzung

- **Professor**
  Prof. Dr. sc. Christoph Meinel

- **Wissenschaftliche Assistenten**
  PD Dr. rer. nat. Martin Mundhenk (bis 16.04.2001)

- **Wissenschaftliche Mitarbeiter**
  Dipl. WiMath. Jochen Bern (bis 30.09.2000)
  Dr. rer. nat. Frank Recker (bis 28.02.2001)
  Dr. rer. nat. Harald Sack
  Dr. rer. nat. Rustam Mubarakzjanov (ab 01.04.2000)
  Dipl. Inform. Gennadij Umanskij (ab 01.04.2001)
  Dipl. Inform. Volker Schillings (ab 01.11.2001)

- **Wissenschaftliche Angestellte in Drittmittelprojekten**
  PD Dr. rer. nat. Carsten Damm (bis 29.02.2000)

- **Sekretärin**
  Agnes Jacoby (ab 01.04.2000)

- **Stipendiaten**
  Dr. rer. nat. Rustam Mubarakzjanov (01.01.2000-31.03.2000)
  Stipendiat des Graduiertenkollegs „Mathematische Optimierung“.

- **Praktikanten**
  Sergej Schischkin, Kazan State University, (Russia)
  (01.02.2000 - 30.04.2000)
  Maja Milicic, Faculty of Mathematics, Belgrad (Yugoslavia)
  (16.10.2000 - 22.12.2000)
  Suchada Wachirapraditporn, Sirindhorn International Institute of Technology,
  Thammasat University (Thailand)
  (04.10.2000 - 22.12.2000)
  Herbert Kwasi Twumasi, University of Science and Technology,
  Kumasi (Ghana)
  (04.10.2000 - 22.12.2000)
  Wang Kee Steve Poon, Polytechnic University, (China)
  (01.06.2001 - 31.08.2001)

- **Wissenschaftliche Hilfskräfte**
  Dipl. Inform. Christian Stangier
  Gennadij Umanskij (bis 31.01.2001)
  Volker Schillings (bis 31.03.2001)
  Andreas Reinhart (02.05.2000 - 31.07.2000)
  Holger Hink (01.11.2000 - 28.02.2001)
  Thomas Gerstenmayer 01.11.2000 - 28.02.2001)
  Lothar Jost (01.11.2000 - 28.02.2001)
  Raphael Heege (01.05. - 31.07.2001)
  Michael Bahra (01.05. - 31.07.2001)
  Marc Kalle (01.05. - 31.07.2001)
  Thomas Henke (01.05. - 31.07.2001)

2 Mit dem Lehrstuhl personell verbundene Einrichtungen

2.1 Zentrum für Wissenschaftliches Elektronisches Publizieren - WEP

Das Zentrum für Wissenschaftliches Elektronisches Publizieren an der Universität Trier ist eine fachübergreifende Einrichtung, die als Informationsbasis und Koordinationszentrum für alle universitären Aktivitäten auf dem Gebiet des wissenschaftlichen elektronischen Publizierens dienen soll.

Unter anderem stehen dabei die Erprobung und die Evaluation neuer Möglichkeiten wissenschaftlicher Kommunikation durch Rechnernetze und weltweit verfügbare Informationssysteme im Vordergrund. Darüber hinaus stellen die Förderung des interdisziplinären Erfahrungsaustausches, sowie die Initiierung von Projekten auf dem Gebiet des wissenschaftlichen elektronischen Publizierens einen weiteren Aufgabenschwerpunkt dar. Das WEP soll dabei interessierte Stellen in Wirtschaft und Gesellschaft beraten und dadurch die Zusammenarbeit mit außeruniversitären Kooperationspartnern fördern.

Aufgaben des WEP:

- Initiierung, Verwaltung und Betrieb von online-Journalen
- Zugang zu fachspezifischen online-Recherche-Systemen
- Verwaltung von Bibliographiedatenbeständen
- Unterstützung bei der Konzeption von Internet-Präsenzen
- Hypertext- und Multimedia-Anwendungen
- Organisation von universitären Kolloquien

Das Zentrum für Wissenschaftliches Elektronisches Publizieren steht unter der Leitung von Univ.-Prof. Dr. sc. Christoph Meinel (Direktor), die Geschäftsführung liegt in den Händen von Dipl.-Inform. Harald Sack.

Weitere Informationen können im WWW gefunden werden unter der URL

`http://www.wep.uni-trier.de/`

2.2 Institut für Telematik

Das am 1.1.1998 gegründete Forschungs- und Entwicklungsinstitut für Telematik betreibt Hightech-Forschung rund ums Internet. Das Institut hat die Rechtsform eines eingetragenen, gemeinnützigen Vereins und wird von der Fraunhofer-Gesellschaft in München betreut, über die eine enge Verbindung zu den Instituten der Fraunhofer-Gesellschaft besteht. Leiter des Instituts ist Univ.-Prof. Dr. sc. nat. Christoph Meinel.

Die wissenschaftliche Arbeit des Instituts für Telematik ist ausgerichtet am Fraunhofer-Forschungsideal, das vom Erfolg angewandter Forschung und Entwicklung im Kontext konkreter Projektaufträge aus Wirtschaft und Gesellschaft ausgeht. Das Institut finanziert sich zum überwiegenden Teil durch Auftragsforschung. Die Leistungsbilanz des Instituts nach den ersten vier Jahren seiner Tätigkeit verzeichnet zum Beispiel zwei Patente, vier Promotionen und mehr als 80 Beiträge zu internationalen Konferenzen. Im Jahr 2001 wurde das Institut als Mitglied der Initiative D21 aufgenommen und bekam den Erfinderpreis 2001 des Landes Rheinland-Pfalz verliehen für seine Internet-Sicherheitsschleusenlösung „Lock-Keeper“. Die Aktivitäten des Instituts im Jahr 2001 stießen auch auf starke Resonanz in den Medien.

Zur Zeit werden Projekte im Auftrag bekannter Konzerne (zum Beispiel Dresdner Bank) bearbeitet, aber auch für kleine und mittelständische Unternehmen, Institutionen und Behörden in Rheinland-Pfalz, Baden-Württemberg und im benachbarten Luxemburg wird geforscht und entwickelt. Zudem bietet das Institut Consulting an und unterstützt bei der Realisierung konkreter Praxis-Lösungen.

Die am Institut für Telematik bearbeiteten Forschungs- und Entwicklungsaufträge sind im Schnittbereich von Telekommunikation und Informatik angesiedelt. Ziel sind anwenderfreundliche und praxisgerechte telematische Hightech-Lösungen. Ein besondere Schwerpunkt der Arbeit des Instituts liegt im Bereich der IT-Sicherheit. Das Institut für Telematik will sich mit Forschungs- und Entwicklungsbeiträgen den Herausforderungen dieses Wandels zur Wissensgesellschaft stellen und im Rahmen konkreter Projekte Beiträge zur Umsetzung dieser visionären Ziele leisten.

Das Institut weist derzeit folgende Kompetenzbereiche auf, in denen eine Reihe von Projektfeldern bearbeitet werden:

- @security
- @banking
- @knowledge
- @government
- @publishing
- @learning
- @health

Detaillierte Informationen sind unter der URL

`http://www.ti.fhg.de/`

zu finden.

3 Aktivitäten in der Lehre: Vorlesungen, Übungen und Seminare

Sommersemester 2000

Automatentheorie und formale Sprachen (2 SWS)
Vorlesung: Christoph Meinel
Übung: Frank Recker

Die Vorlesung gibt eine kompakte Einführung in das Gebiet der Automatentheorie und formalen Sprachen, das sowohl für die theoretische Informatik (Berechenbarkeitstheorie, Komplexitätstheorie, formale Systeme und Semantik) als auch für die praktische Informatik (Programmiersprachen, Syntaxanalyse, Compilerbau usw.) von grundlegender Bedeutung ist.

Dabei nennen wir eine Menge von Wörtern über einem vorgegebenen Alphabet eine formale Sprache, wenn es ein Regelsystem gibt, das alle Wörter dieser Menge generieren kann (und nur diese). Die Chomsky-Hierarchie teilt die Menge der formalen Sprachen ein in vier Klassen: Die regulären Sprachen, die kontextfreien Sprachen, die kontextsensitiven Sprachen, und schließlich sonstige formale Sprachen. Wir folgen dieser Einteilung und arbeiten für jede dieser vier Klassen die wichtigsten Eigenschaften und Darstellungen heraus. Die Vorlesung gehört zum Kanon der Grundvorlesungen. Die aktive Teilnahme an der angebotenen zweistündigen ist notwendig zum Scheinerwerb.

Komplexitätstheorie (4 SWS)
Vorlesung: Christoph Meinel
Übung: Rustam Mubarakzjanov

Ziel der Komplexitätstheorie ist die Quantifizierung von Computerressourcen (Zeit, Speicherplatz, Hardwareaufwand ...), die zur algorithmischen Lösung konkreter Probleme bzw. von Problemklassen benötigt werden. In der Vorlesung, die sich an Studenten des Informatik- bzw. Mathematikhauptstudiums wendet und Kernvorlesung für den Bereich der theoretischen Informatik ist, sollen schwerpunktmäßig die folgenden Themenkomplexe behandelt werden:

- Komplexitätsklassen und ihre Beziehungen
- Reduktionskonzepte
- NP-vollständige Probleme
- Randomisierte Berechnungen
- Approximationstheorie

Elektronisches Publizieren (4 SWS)
Praktikum: Christoph Meinel, Jochen Bern, Harald Sack

Mit der zunehmenden Verbreitung von Computern und Computernetzen zum Zweck des Information Retrieval wird auch der Teilbereich des Electronic Publishing - d.h. der angemessenen Verfügbarmachung von Informationen von einem Anbieter an möglichst viele Interessenten mit geringem Aufwand an dedizierter Hardware - weiterentwickelt. Sowohl in der Professur Meinel als auch am Institut für Telematik werden theoretische wie praktische Arbeiten besonders im Hinblick auf internetgestützte Dienste durchgeführt, die in einem gewissen Maß auch als Modell für andere Formen des Electronic Publishing (wie Verbreitung von Information auf maschinellen Datenträgern) dienen können.

Im Rahmen dieser Zielsetzung sind Teilprojekte durchzuführen, die beispielsweise die Themen Autorenunterstützung (wie kann man einem Autor bei der Aufgabe helfen, Informationen, vor allem Querverweise, aktuell zu halten?), Informationsstrukturierung (welches System zur Informationsauswahl ist für welche Datensammlung geeignet/optimal?), Softwarebau (Modifikation oder Generierung der Software zur Bereitstellung spezieller Netzwerkservices), Datenbank-Interfacing (wie kann man Informationen, die bereits in einer Datenbank existieren, kontrolliert veröffentlichen, ohne sie auszugsweise duplizieren zu müssen?) oder Sicherheitsmechanismen (wie gewährt man nur registrierten Benutzern Zugang, wie rechnet man die Leistung mit ihnen ab, wie schützt man eine erlaubte Transaktion gegen Manipulation und Mithören?) haben können.

VLSI-Design (4 SWS)
Praktikum: Christoph Meinel, Jochen Bern

Im Anwendungsschwerpunkt *VLSI-Design* des Informatik-Hauptstudiums ist ein Praktikum zu absolvieren. Im Rahmen dieses Praktikums sollen Kenntnisse und Techniken aus dem Bereich des computerunterstützten Entwurfs und Tests von hochintegrierten Schaltkreisen durch praktische Arbeiten anwendungsorientiert vermittelt bzw. gefestigt werden.

Gegenstand des Praktikums ist die Mitarbeit an bzw. Weiterentwicklung der vom Lehrstuhl benutzten Software zur Forschung an BDDs. Die dabei anfallenden Aufgaben reichen von der Programmierung neuer Funktionalität für die Benutzeroberfläche z.B. `vis` über die Implementation neuer Ansätze in den zugrundeliegenden Softwarebibliotheken (CUDD u.a.) bis hin zu Entwurf und Analyse neuer Heuristiken für die verwendeten Typen und Ordnungen. Der Besuch der Vorlesung *Binäre Entscheidungsgraphen* ist nicht Voraussetzung für die Teilnahme.

Theoretische Informatik (2 SWS)
Forschungsseminar: Christoph Meinel

Seminar am Lehrstuhl Meinel (2 SWS)
Christoph Meinel

Informatik-Kolloquium
D. Baum, Ch. Meinel, B. Walter

Oberseminar-Informatik
D. Baum, Ch. Meinel, B. Walter

Wintersemester 2000/2001

Diskrete Strukturen und Logik I (4 SWS)
Vorlesung: Christoph Meinel
Übung: Frank Recker

Die Grundstudiumsvorlesung *Diskrete Strukturen und Logik* führt in die für das Informatikstudium im Hauptfach bzw. im Nebenfach grundlegenden Begriffe und Methoden der diskreten Mathematik und der mathematischen Logik ein. Die Vorlesung ist in die drei Komplexe *Grundlagen*, *Techniken* und *Diskrete Strukturen* gegliedert und behandelt folgende Themenkomplexe:

1. *Grundlagen*: Aussagenlogik; Mengen und Mengenoperationen; Relationen und Funktionen; Folgen und Summen; Algorithmen,

2. *Techniken*: Mathematisches Schließen; Zählen,

3. *Wichtige diskrete Strukturen*: Boolesche Algebra; Aussagen-und Prädikatenlogik, Graphen und Bäume; Endliche Gruppen.

CAD-Logiksynthese und -optimierung (4 SWS)
Vorlesung: Christoph Meinel
Übung: Dr. Rustam Mubarakzjanov

Beim Entwurf und der Optimierung hochintegrierter mikroelektronischer Schaltkreise kommt es auf eine Realisierung der spezifizierten Schaltfunktion ("Logik") mit einem geringstmöglichen Ressourcenaufwand (z.B. Zahl der elektronischen Gatter, Verbindungsleitungen etc.) an. Aufgrund der Komplexität der Schaltfunktionen werden dazu effiziente Datenstrukturen und schnelle Algorithmen benötigt. Da komplexitätstheoretische Untersuchungen zeigen, daß bei vielen der relevanten Probleme nicht mit effizienten Lösungen gerechnet werden kann, kommt heuristischen Verfahren eine große Bedeutung zu. Die Vorlesung stellt eine Reihe von Repräsentationsschemata für Schaltfunktionen (auch Boolesche oder logische Funktionen genannt) vor und gibt einige komplexitätstheoretische Charakteristiken. Motiviert durch die weitverbreiteten und technisch gut beherrschten PLA-basierten Chiprealisierungen werden vor allem Verfahren und Heuristiken zur zweistufigen Logikminimierung besprochen.

Die Vorlesung wendet sich vornehmlich an Studenten der Informatik und der Mathematik im Hauptstudium. Sie ist Kernvorlesung im Schwerpunkt VLSI-Design.

Berechenbarkeit und Komplexität (2 SWS)
Vorlesung: Martin Mundhenk
Übung: Martin Mundhenk und Rustam Mubarakzjanov

Die Theorie der Berechenbarkeit ist die älteste Disziplin der Informatik – sie existierte schon lange, bevor man überhaupt von Informatik sprach und bevor es Computer gab. Der Inhalt dieser Theorie ist die Frage, was ein Algorithmus leisten kann, insbesondere auch die Definition des Begriffs *Algorithmus*. Wir werden mehrere Konkretisierungen des intuitiven Algorithmenbegriffs einführen und beweisen, daß diese im wesentlichen alle dieselbe Leistungsfähigkeit besitzen. Der Höhepunkt dieses Teils der Vorlesung wird der Nachweis sein, daß es Probleme (und zwar praktisch relevante Probleme) gibt, die algorithmisch nicht lösbar sind.
Im zweiten Teil der Vorlesung beschäftigen wir uns mit der Frage, welche Probleme nicht nur prinzipiell lösbar sind, sondern auch unter Berücksichtigung der realistischen Forderung, daß nur ein bestimmter vorgegebener Aufwand betrieben werden kann (etwa beschränkte Rechenzeit oder fest vorgegebener Speicherplatz oder beides). Wir werden Komplexitätsklassen einführen, an erster Stelle die Klassen **P** und **NP**, und werden untersuchen, welche Probleme zu den schwersten in einer gegebenen Klasse zu zählen sind.

Informationsdesign im WWW (2 SWS)
Seminar: Harald Sack

Kaum 10 Jahre sind vergangen, seit Tim Berners-Lee und Robert Cailliau das World Wide Web ins Leben riefen. Was als einfaches Dokumentenaustauschsystem für das Forschungsinstitut CERN begann löste die wohl folgenschwerste Revolution der Informationsindustrie aus: Das Internet fand Zutritt in die Welt außerhalb von Universitäten und Forschungseinrichtungen. Ein Netz von Millionen von miteinander verbundenen dezentral gelagerten Dokumenten, so stellt sich die Hypertextarchitektur des Wissensraumes WWW heute dar.

Doch diese Unmengen von Information machen einen gezielten Zugriff auf die gerade benötigten Daten immer schwieriger. Daher gilt es, über Strukturierung und Indizierung Ordnung in das Chaos von Dokumenten zu bringen. Prinzipien die für das gesamte WWW gelten haben natürlich auch für die einzelne Web-Seite ihre Gültigkeit. Die angebotene Information soll effizient dargeboten werden und - in Zeiten des stetig wachsenden E-Commerce - Anreiz bieten, eine einmal angesprungene Seite erneut zu besuchen.

Dieses Seminar befaßt sich mit der effizienten und informationsgerechten Darstellung von Web-Seiten, sowie der dazu notwendigen Techniken.

Theorie-AG (2 SWS)
Martin Mundhenk

Die Theoretische Informatik umfasst viele interessante Gebiete, von denen in den Grundstudiumsveranstaltungen grundlegende Begriffe vorgestellt wurden. In dieser Arbeitsgemeinschaft sollen Themen aus den Gebieten der Berechenbarkeits- und Komplexitätstheorie sowie der Logik behandelt werden. Das Thema in diesem Semester lautet Aussagenlogische Beweissysteme und ihre Komplexität. Das Beweissystem Resolution ist ja bereits aus der Vorlesung "Diskrete Strukturen ..." bekannt. Zusätzlich werden wir noch Tableau-Beweise und Schnittebenen-Beweise kennenlernen. Die Komplexität eines Beweissystems wird in der Länge der Beweise gemessen. Wir werden betrachten, wie sich die drei Beweissysteme hinsichtlich ihrer Komplexität miteinander vergleichen lassen. Grundlage dazu ist die Arbeit The Complexity of Propositional Proofs von Alasdair Urquhart.

Eine recht weitläufige Übersicht über das Themengebiet findet man in der Arbeit Propositional Proof Complexity: Past, Present, and Future von Paul Beame und Toniann Pitassi (lokale Kopie). Als Skript zur Veranstaltung dienen die Notizen meiner Vorlesung auf der European Summerschool for Logic, Language, and Information 1999.

VLSI-Design (4 SWS)
Praktikum: Christoph Meinel, Rustam Mubarakzjanov
siehe Sommersemester 2000.

Elektronisches Publizieren (4 SWS)
Praktikum: Christoph Meinel, Harald Sack
siehe Sommersemester 2000.

Forschungsseminar Theoretische Informatik (2 SWS)
Christoph Meinel

Seminar am Lehrstuhl Meinel (2 SWS)
Christoph Meinel

Informatik-Kolloquium
D. Baum, Ch. Meinel, B. Walter

Oberseminar-Informatik
D. Baum, Ch. Meinel, B. Walter

Sommersemester 2001

Automatentheorie und Formale Sprachen (2 SWS)
Vorlesung: Christoph Meinel
Übung: Rustam Mubarakzjanov
siehe Sommersemester 2000

Sicherheit im Internet - Schwachstellen und Angriffspunkte (4 SWS)
Vorlesung: Christoph Meinel
Übung: Harald Sack

In der Vorlesung werden Fragen rund um die Informationssicherheit im Internet behandelt. Nach einer einführenden Risikoanalyse werden Funktionsweise und Architektur von Internets und Intranets detailliert besprochen. Aufbauend auf einem fundierten Verständnis der TCP/IP-Protokollwelt werden dann Schwachstellen und Angriffspunkte behandelt, wie z.B.

- menschliches Versagen
- Beschaffung von Systeminformationen
- Account- und Passwortangriffe
- Design- und Programmierfehler in Applikationen
- Schwachstellen in UNIX/Linus bzw. in Windows NT/2000 sowie
- Angriffspunkte im WWW

Elektronisches Publizieren (2 SWS)
Proseminar: Harald Sack

Im diesem Proseminar werden grundlegende Themen des Elektronischen Publizierens näher behandelt. So bildet der Themenbereich *Markup-Sprachen*, neben den *technischen Grundlagen* der Internet-Technologie und *Sicherheitsmechanismen* einen der Schwerpunkte des Proseminars, die durch *Praxisaspekte* abgerundet werden.

Elektronisches Publizieren (4 SWS)
Praktikum: Christoph Meinel, Harald Sack
siehe Sommersemester 2000

VLSI-Design (4 SWS)
Praktikum: Christoph Meinel, Rustam Mubarakzjanov
siehe Sommersemester 2000

Forschungsseminar Theoretische Informatik (2 SWS)
Christoph Meinel

Seminar am Lehrstuhl Meinel (2 SWS)
Christoph Meinel

Informatik-Kolloquium
D. Baum, Ch. Meinel, B. Walter

Oberseminar-Informatik
D. Baum, Ch. Meinel, B. Walter

Wintersemester 2001/2002

Technische Grundlagen des elektronischen Publizierens im WWW
(4 SWS)
Vorlesung: Christoph Meinel
Übung: Harald Sack

Die komplette Vorlesung wurde live im Internet übertragen. Jeder Interessierte konnte oder kann diese Veranstaltung bei sich zu Hause auf einem PC mit geeignetem Internetanschluß live und on-demand verfolgen. Es werden dabei sowohl die in der Vorlesung präsentierten Folien sowie der Vortragende in Bild und Ton auf den heimischen Rechner übermittelt. Die Veranstaltungen sollen aufgezeichnet und archiviert werden, um eine spätere Wiederholung zur Nachbereitung und Prüfungsvorbereitung zu ermöglichen. Die zur Teilnahme benötigte Software, Zugangsdaten, Sendezeiten udn weitere Informationen sind unter der folgenden Internetseite abrufbar:

http://www.informatik.uni-trier.de/TI/teleteaching.html

Neue Medien, Internet und WWW sind in aller Munde. Neue, z.T. ungeahnte Möglichkeiten tun sich auf, wenn es darum geht, Inhalte multimedial und vielfältig verlinkt weltweit verfügbar zu machen, also elektronisch zu publizieren. Um diese vielfältigen Potentiale und Möglichkeiten des Elektronischen Publizierens richtig einschätzen und ausschöpfen zu können, bedarf es eines vertieften Verständnisses der technischen Grundlagen der Internet Technologie und der Konzepte des World Wide Web (WWW) (z.B. URI, HTTP, SGML, HTML...). Eine Vermittlung dieser Grundlagen ist das Ziel dieser Vorlesung.

Die Vorlesung wendet sich zunächst an Studenten der Informatik im Hauptstudium und ist dort Kernvorlesung im Schwerpunkt Elektronisches Publizieren. Da die Vorlesung so konzipiert ist, dass Grundkenntnisse der Informatik ausreichen, um folgen zu können, sind auch Hörer anderer Fächer und Fachbereiche mit Interesse für die neue Grundtechnologie der Wissensgesellschaft, das Elektronische Publizieren, eingeladen.

Die Vorlesung wird im Folgesemester fortgesetzt, wobei im zweiten Teil Markupsprachen (HTML, CSS, XHTML, XML) neben technischen Aspekten der Konfiguration von Web-Servern (HTTxpP, SSL) und der Programmierung von Web-Applikationen (javascript, dynamisches HTML, cgi) Schwerpunkte bilden.

Diskrete Strukturen und Logik I (4 SWS)
Vorlesung: Christoph Meinel
Übung: Rustam Mubarakzjanov
siehe Wintersemester 2000/2001

Informationsdesign im WWW (2 SWS)
Seminar: Harald Sack
siehe Wintersemester 2000/2001

Sicherheit in offenen Netzen (4 SWS)
Praktikum: Christoph Meinel, Harald Sack, Gennadij Umanskij

Wie kann Sicherheit in einem heterogenen LAN, das an das Internet angebunden ist hinreichend und unter vertretbarem Aufwand gesichert werden?

Unter dem Motto dieser zentralen Fragestellung soll im Praktikum auf die nachfolgenden Teilprojekte näher eingegangen werden:

(1) IDS-Konfiguration Konkret sollen hier mögliche Angriffe aus dem Internet erkannt und abgewehrt werden. Dies kann mit Hilfe eines Intrusion Detection Systems (IDS) bewerkstelligt werden. Zwar sind diese Systeme bereits weit verbreitet und sogar frei erhältlich, jedoch können sie nur dann von Nutzen sein, wenn sie gewissenhaft entsprechend der Topologie und der Besonderheiten des jeweiligen lokalen Netzwerks mit Hilfe eines komplexen Regelwerkes angepaßt sind. Einem bereits vorhandenen IDS soll hier ein adäquates www-basiertes Front-End hinzugefügt werden, das eine effiziente und anschauliche Anpassung dieses Regelwerkes gestattet.

(2) Logfile-Analyse Neben der Anpassung des IDS-Regelwerks ist eine effiziente Analyse der Log-Files, die sämtliche sicherheitsrelevanten Netzwerk-Events beinhalten von besonderer Bedeutung. Dazu soll ein www-basiertes flexibles Werkzeug entwickelt werden, das eine grafische Aufbereitung nach Maßgaben des Benutzers unter variablen Parametersätzen gestattet. Oft können Einbruchsversuche nur durch eine entsprechende grafische Aufbereitung der Log-Datensätze überhaupt erst entdeckt werden.

(3) IDS Konfiguration - Teil 2 Mit Hilfe der Teilprojekte (1) und (2) soll eine effiziente Anpassung des lokal installierten IDS-Systems vorgenommen werden.

Elektronisches Publizieren (4 SWS)
Praktikum: Christoph Meinel, Harald Sack
siehe Sommersemester 2000

VLSI-Design (4 SWS)
Praktikum: Christoph Meinel, Rustam Mubarakzjanov
siehe Sommersemester 2000

Theoretische Informatik (2 SWS)
Forschungsseminar: Christoph Meinel

Seminar am Lehrstuhl Meinel (2 SWS)
Christoph Meinel

Informatik-Kolloquium
D. Baum, Ch. Meinel, B. Walter

Oberseminar-Informatik
D. Baum, Ch. Meinel, B. Walter

4 Dissertationen und Habilitationen

4.1 Habilitationen

Dr. Carsten Damm

"Boolean and Arithmetic Computations"
Habilitationsschrift, Universität Trier, 1999

Gutachter:

- Prof. Dr. H. Seidl, Universität Trier
- Prof. Dr. Ch. Meinel, Universität Trier
- Prof. Dr. Eric Allender, Rutgers University, New York

Datum des Habilitationsvortrages: 05.07.2000

Abstract: This thesis represents part of my research work over in the last few years. Part of the results where published in conference proceedings or in journals. Others are under review. A few of the results were obtained in co-operation with other researchers and are clearly marked as such. Where I included techniques and results from other authors, I cited the original references.

Many computational models appear in a Boolean and an arithmetic variant. The most obvious examples are Boolean and arithmetic circuits. Another example are nondeterministic Turing machines with acceptance defined by Boolean or numeric conditions on the set of accepting computations. Often, moreover, the Boolean version has an obvious arithmetic counterpart obtained by simply replacing the Boolean (semiring) operations by arithmetic operations in a field. While the former is adapted to model the logics of human thinking, the latter seems to be appropriate for the study of arithmetic computations. How is the computational power of the models influenced by the type of the underlying algebraic structure?

There has long been the feeling that arithmetic computations are more powerful than traditional Boolean models and we know that this indeed true for some restricted models. But, for unrestricted models, like polynomial time Turing machines, up to now we have only weak evidence: arithmetic computations are not less powerful than Boolean computations (if some kind of "advice" is allowed). Although this is great progress, we do not really understand the strength of arithmetic computations. This motivates our research.

We compare Boolean and arithmetic models in the following situations:

- Restricted computations: What is the relation between computational powers of Boolean and arithmetic "low-level" models (i.e., in an area, where we have lower bound methods)?
- Characterizations: To which types of problems are the Boolean or arithmetic models especially adapted?
- Simulations: Which resources are needed to simulate Boolean by arithmetic simulations?

We contribute in a sequence of results to the following answers: (1) The powers of Boolean and arithmetic *restricted* computational models are incomparable, but the arithmetic variant can at least approximate the outcome of the Boolean one. (2) The powers of Turing machine based Boolean and arithmetic computational models are characterized by the complexity of graduations of natural algebraic problems over different algebraic structures. (3) There exist efficient simulations of late(unrestricted) Boolean computational models by corresponding arithmetic models with advice.

A more detailed description of our contributions is given in the introductory chapter.

Dr. Martin Mundhenk

"The Complexity of Planning with Partially-Observable Markov Decision Processes"
Habilitationsschrift, Universität Trier, 2000

Gutachter:

- Prof. Dr. H. Seidl, Universität Trier
- Prof. Dr. Ch. Meinel, Universität Trier
- Prof. Dr. J. Goldsmith, University of Kentucky

Datum des Habilitationsvortrages: 17.01.2001

Abstract: This work surveys results on the complexity of planning under uncertainty. The planning model considered is the partially-observable Markov decision process. The general planning problems are, given such a process, (a) to calculate its performance under a given control policy, (b) to find an optimal or approximate optimal control policy, and (c) to decide whether a good policy exists. The complexity of this and related problems depend on a variety of factors, including the observability of the process state, the compactness of the process representation, the type of policy, or even the number of actions relative to the number of states. In most cases, the problem can be shown to be complete for some known complexity class.

5 Kurzbeschreibung der Forschungsbereiche

Die Forschungsarbeiten am Lehrstuhl für Theoretische Konzepte und neue Anwendungen der Informatik konzentrierten sich im genannten Zeitraum auf die folgenden drei Schwerpunkte:

- *BDD-basierte Datenstrukturen für boolesche Funktionen*
- *Komplexität von Berechnungen*
- *Elektronisches Publizieren*

Die erzielten Forschungsergebnisse wurden auf ausgewiesenen internationalen Tagungen vorgestellt und in den einschlägigen wissenschaftlichen Journalen veröffentlicht bzw. zur Veröffentlichung eingereicht. Sie sind darüber hinaus in Form von Forschungsberichten und Softwaretools weitgehend über World Wide Web

URL: http://www.informatik.uni-trier/~meinel/

bzw.

URL: http://www.informatik.uni-trier/TI/

abrufbar.

5.1 BDD-basierte Datenstrukturen

Im Forschungsschwerpunkt **BDD-basierte Datenstrukturen für boolesche Funktionen** wurden Datenstrukturen für die Repräsentation und Bearbeitung von booleschen (also 0-1-wertigen) Funktionen entworfen und analysiert. Der vielgestaltige praktische Einsatz dieser Datenstrukturen z.B. in CAD-Systemen zum Schaltkreisentwurf oder in Tools zur Verifikation von sequentiellen Systemen, elektronischen Schaltkreisen oder Kommunikationsprotokollen machte Bemühungen zur Optimierung und Kompaktifizierung solcher Strukturen zu einem sehr lohnenden Forschungsziel. Im einzelnen lassen sich die in diesem Forschungsschwerpunkt behandelten Fragestellungen folgendermaßen zusammenfassen:

1.) Der einzige Weg, die BDD-Größe zu verringern, liegt in der Bestimmung einer geeigneteren Variablenordnung. Als wirkungsvollste Methode hat sich hierzu das dynamische Umordnen der Variablen erwiesen. Problematisch ist dabei lediglich das oftmals sehr schlechte und für den praktischen Einsatz nicht darstellbare Zeitverhalten. Daher wurde intensiv an Techniken zur Beschleunigung des dynamischen Umordnens gearbeitet. Die entwickelten Methoden und Heuristiken basieren jeweils auf der Auswertung struktureller oder semantischer Informationen.

Die Heuristiken wurden erfolgreich in der *kombinatorischen Verifikation* eingesetzt. Um einen Einsatz auf den sehr anspruchsvollen Gebieten der *Erreichbarkeitsanalyse* und des *symbolisches Model Checking* zu ermöglichen wurden die Heuristiken auf die speziellen Erfordernisse dieser Gebiete angepasst und erweitert.

2.) Eine weitere Steigerung der Effizienz der BDD-Datenstrukturen stellt die Erweiterung durch Relaxation von Strukturrestriktionen der BDDs und Einbringung zusätzlicher Funktionalelemente dar. In Free-BDDs kann auf jedem Berechnungspfad von der Wurzel zur Senke eine andere Ordnung der Eingabevariablen vorliegen. $\oplus$-OBDDs hingegen stellen eine Erweiterung der OBDD-Datenstruktur hinsichtlich der Funktionalität der einzelnen Knoten innerhalb des Entscheidungsdiagrammes dar. Zusätzlich zu den bekannten Entscheidungsknoten werden Operatorknoten eingeführt, die im Falle von $\oplus$-OBDDs die Parität der beiden Vorgängerknoten berechnen und in vielen Fällen zu einer kompakteren Darstellung führen. Am Lehrstuhl wurden Programmbibliotheken zur effizienten Manipulation von Free-BDDs und $\oplus$-OBDDs entwickelt und gepflegt.

3.) Nach Anwendung einer geeigneten linearen Transformation auf den Definitionsbereich einer Booleschen Funktion kann diese oft sehr viel kompakter als OBDD dargestellt werden, als dies ohne Transformation möglich wäre. Von besonderem Interesse bei dieser Herangehensweise ist, daß der grundlegende Vorteil der guten algorithmischen Handhabbarkeit von OBDDs nicht verloren geht. Bestehende BDD-Programmpakete wurden hinsichtlich dieser Funktionalität erweitert und finden nun Einsatz in der formalen Verifikation.

4.) Der praktische Umgang mit BDDs zeigt, daß für die jeweils darzustellenden Funktionen oft sehr stark unterschiedliche Variablenordnungen geeignet sind. Es wurde deshalb ein Programmpaket zur Synthese von BDDs entwickelt, das OBDDs mit unterschiedlichen Variablenordnungen bearbeiten kann. Erklärtes Ziel ist es, Heuristiken zu entwerfen, die - jeweils im Kontext einer Anwendung in der formalen Verifikation - gut geeignete gemeinsame Variablenordnungen ermitteln.

5.) Der Kern jeglicher formaler sequentieller Verifikation ist die Berechnung der erreichbaren Zustände. Problematisch bei der OBDD-basierten Erreichbarkeitsanalyse ist die Repräsentation der Transitionsrelation, die meistens partitioniert wird. Nur eine gute Partitionierung erlaubt eine effiziente Berechnung. Es wurden Heuristiken entwickelt, die die Qualität der Partitionierung erheblich verbessern und so die Analyse von industriellen Protokollen vereinfachen bzw. erst ermöglichen.

6.) Wenn formale Verifikation in einem industriellen Umfeld nicht angewendet wird, liegt das oft daran, daß sie nicht in den Entwicklungszyklus passt, am Lehrstuhl wurde eine Methodik entwickelt, die formale Verifikation von Protokollen in den Entwicklungszyklus integriert. Die daraus resultierenden gestiegenen Anforderungen an die BDD-Technologie werden ebenfalls untersucht.

5.2 Komplexität von Berechnungen

Im Forschungsschwerpunkt **Komplexität von Berechnungen** ging es um zentrale Fragestellungen aus dem Kernbereich der Forschung in der theoretischen Informatik, nämlich um die Charakterisierung des Ressourcenbedarfs – insbesondere des Ressourcenmindestbedarfs – für konkrete Berechnungen. Im einzelnen waren die in diesem Forschungsschwerpunkt angesiedelten Arbeiten vornehmlich der Untersuchung folgender Fragestellungen gewidmet:

1.) Untersuchung der *Schaltkreiskomplexität.* Hier wurden Ressourcenbedarfsgrenzen (sogenannte untere und obere Schranken) für die Berechnung konkreter Probleme durch Schaltkreise und verwandte Berechnungsmodelle untersucht. Es wurden:

- Zusammenhänge zwischen Booleschen und algebraischen Berechnungen untersucht und Komplexitätsklassen durch algebraische Probleme charakterisiert;
- untere Schranken für zahlentheoretische Probleme mit Fourier-analytischen Methoden nachgewiesen;
- untere Schranken für die mittlere Sensitivität zahlentheoretischer Funktionen nachgewiesen und untere Schranken für Entscheidungsbäume und Formeln abgeleitet;
- ein einfaches *kombinatorisches* Untere-Schranken-*Kriterium* für monotone Schaltkreise gefunden und damit ein vor 15 Jahren von A. Razborov gestelltes Problem gelöst;
- ein Entropie-Ansatz zur Ableitung unterer Schranken für Verzweigungsprogramme gefunden. Dies hat exponentielle untere Schranken sogenannter "gentle programs" geliefert, wo alle bisher bekannte Methoden versagt haben.

2.) Untersuchung der *Kommunikationskomplexität.* Es konnte gezeigt werden, daß arithmetische Varianten von verteilten Berechnungen die üblichen nichtdeterministischen Varianten approximieren können, obwohl im Sinne der Simulierbarkeit arithmetische und Boolesche Kommunikationskomplexität unvergleichbar sind. Dieses Resultat konnte noch erweitert werden auf alternierende Kommunikationskomplexität.

3.) Untersuchung der *Instanzen-Komplexität.* Es wurde ein Begriff angegeben, mit dem “harte Instanzen” – d.h. Instanzen, die ein Problem zu schwierig für Berechnungen unter bestimmten Ressourcenbeschränkungen machen – bestimmt werden können. Dieser Begriff basiert auf dem Vergleich von Instanzen- und Kolmogoroff-Komplexität. Daraus ergeben sich Charakterisierungen der Klassen der semi-entscheidbaren, entscheidbaren und effizient entscheidbaren Probleme.

4.) Untersuchung der *Komplexität Markoff'scher Entscheidungsprozesse.* Abhängig von verschiedenen Parametern betreffend die Sichtbarkeit, Darstellung und Steuerungsmöglichkeit wurden Markoff'sche Entscheidungsprozesse bezüglich ihrer strukturellen Komplexität untersucht. Dabei ergaben sich Vollständigkeitsresultate für bekannte Komplexitätsklassen wie NL, P, NP und PSPACE, aber auch für interessante Zählklassen wie PL, PP, P^{PP} und $\mathrm{NP}^{\mathrm{PP}}$. Darüberhinaus wird die Approximierbarkeit der Probleme betrachtet.

5.3 Elektronisches Publizieren

Im Forschungsschwerpunkt **Elektronisches Publizieren** wird schwerpunktmäßig an der Erschließung der Möglichkeiten der neuen elektronischen Kommunikationsmedien in *Intranets* und dem *Internet* gearbeitet. Anders als der traditionelle Weg der Publikation ermöglicht das Elektronische Publizieren die Verfügbarmachung von Dokumenten weitgehend unabhängig vom bestehenden Verlagswesen. Dabei ist unter „Verfügbarmachung“ weniger die Bereitstellung für einen gezielten Abruf *dieses Dokuments* zu verstehen als vielmehr die Schaffung von Möglichkeiten, das Dokument anhand von Thema, Stichworten, Zitatketten etc. etc. aufzufinden. Für die Erstellung der Dokumente wiederum sind die besonderen Möglichkeiten, die die verwendeten *neuen Medien* bieten, von besonderem Interesse. Speziell in den *Web-Seiten* des *WWW* kommen im Vergleich zu papierbasierten Publikationen multimediale Funktionalitäten wie *Hyperlinks,* bewegte Bilder, Töne etc. hinzu. An konkreten Projekten wurden verfolgt:

1.) Herausgabe und Weiterentwicklung des *“Electronic Colloquium on Computational Complexity” (ECCC).* In diesem internationalen elektronischen Forschungsarchiv, das im WWW unter der URL `http://www.eccc.uni-trier.de/eccc/` zu erreichen ist, veröffentlichen die Forscher auf dem Gebiet der *Computational Complexity* konzentriert ihre aktuellen Forschungsergebnisse. Die Erfahrungen mit diesem bereits seit 1994 erfolgreich betriebenen Projekt wurden wissenschaftlich aufbereitet und unter anderem auf der Konferenz SIGDOC '98 vorgestellt. Das vorhandene Archiv wird zusätzlich seit 2000 jährlich in Form einer CDROM publiziert.

2.) Weiterentwicklung und Betrieb des *„Konferenz-Servers“*, angewandt u.a. bei den STACS-Konferenzen. Es handelt sich hierbei um einen Mechanismus, der die Organisatoren einer wissenschaftlichen Konferenz bei der Entgegennahme der eingereichten Konferenzbeiträge unterstützt. Nach der auf Email basierenden Version, die bei den Konferenzen STACS'97 und STACS'98 zum Einsatz kam, wurde für die STACS 1999 (`http://stacs.uni-trier.de/STACS99/`) in Trier eine überarbeitete, auf dem WWW basierende Version erstellt. Neben den eigentlichen Einreichungen unterstützt diese weitere Teile des Arbeitsablaufs der Organisatoren, insbesondere im Prozeß der Begutachtung und Auswahl der eingereichten Arbeiten. Für die STACS'2000 in Lille wurde die Software weiterentwickelt und mit großem Erfolg erneut verwendet, sowie auch für die STACS 2001 in Dresden und die MFCS 2001.

3.) Das im November 1997 eröffnete *Zentrum für Wissenschaftliches Elektronisches Publizieren (WEP)* (`http://www.wep.uni-trier.de/`) veranstaltete eine Reihe von Gastorträgen und Kolloquien und ist beratend an fächerübergreifenden Projekten, wie z.B. mit der Germanistik, der Lusitanistik oder der Politikwissenschaft beteiligt. Die Aktivitäten des WEP wurden im März 2001 mit großem Erfolg auf der CeBit 2001 vorgestellt, auf der das WEP als Aussteller präsent war.

4.) Ein im Jahr 1998 neu begonnenes Projekt ist MOPS, eine speziell auf das Erschließen von im WWW veröffentlichten Forschungsarbeiten zugeschnittene *Suchmaschine.* MOPS spürt solche Dokumente im WWW auf, extrahiert aus ihnen die textuellen Bestandteile und führt einen entsprechenden Index. Benutzer von MOPS werden dadurch in die Lage versetzt, Dokumente durch eine Volltextsuche zu erfassen, die als *PostScript-Dateien* vorliegen und herkömmlichen Web-Suchmaschinen unzugänglich sind. Mittlerweile existieren verschiedene spezielle Versionen dieses Services für unterschiedliche Themengebiete, wie Komplexitätstheorie und OBDDs.

5.) Ein weiteres Projekt *OBDD Heuristics Online (OHO)*, das die Forschungsschwerpunkte elektronisches Publizieren und BDD-basierte Datenstrukturen miteinander verbindet, sucht einen neuralgischen Punkt bei der Forschung zu BDDs zu überwinden, nämlich den, daß die Hersteller von integrierten Schaltkreisen nur äußerst ungern Schaltkreisentwürfe, die Stand der Technik sind, nach außen geben — die Entwerfer von Algorithmen und Datenstrukturen benötigen aber genau solche Entwürfe als *Benchmarks,* um die Anwendbarkeit ihrer Neuerungen beurteilen zu können. Bei OHO werden nun Implementationen dieser Neuerungen einerseits und Benchmarks andererseits auf einem zentralen Server zusammengeführt mit einem WWW-Interface für die Einspeisung der Benchmarks. Auf diese Weise müssen die Benchmarks nicht mehr uneingeschränkt veröffentlicht, sondern nur noch bei Bedarf an eine einzelne vertrauenswürdige Stelle übermittelt werden.

6.) Ein weiteres Projekt beschäftigt sich mit der Visualisierung komplexer Algorithmen und Strukturen. Die Visualisierung soll dazu dienen, sowohl Studenten als auch Praktikern das Verständnis und das Begreifen der visualisierten Sachverhalte zu erleichtern. Neben der Visualisierung von Kommunikationsabläufen im Intra- und Internet, die mit Hilfe von Studenten in die Tat umgesetzt worden sind, wurde in dem Projekt *visBDD* der Versuch unternommen, den komplexen OBDD-Synthese-Algorithmus in geeigneter Form graphisch und in multimedialer Form umzusetzen.

7.) Eingebettet in die durch den Lehrstuhl betriebene WWW-Portalsite

`http://www.bdd-portal.org/`

befindet sich neben den bereits genannten *OHO* und *visBDD* ein aktuelles Link-Archiv, das Forscher, Forschungsgruppen, Publikationen, sowie Programmpakete und einen Konferenzkalender aus allen Bereichen der BDD-Forschung unterhält. Auf der Konferenz DAC 2000 in Los Angeles war dieses Projekt im Rahmen einer Panel-Diskussion präsent.

8.) Der Bereich *Teleteaching* zu dem bereits auch das bereits angesprochene Projekt *visBDD*, sowie die bereits realisierten Visualisierungen zählen gewann im Wintersemester 2001 große Aufmerksamkeit, als erstmals eine Informatikvorlesung *Technische Grundlagen des Elektronischen Publizierens* sowohl live online, als auch später in archivierter Form über das Internet angeboten werden konnte. Neben einem Videobild des Dozenten wurde das Tafelbild in hoher Qualität sowie natürlich der Ton übertragen. Die Bemühungen in diesem Bereich zielen darauf ab, eine technisch möglichst einfache Umgebung für den Teilnehmer zu schaffen, die ihn ohne große Mühe dazu in die Lage versetzen, das Teleteaching-Angebot zu nutzen, sowie in einer Reduktion der dazu notwendigen Bandbreite.

6 Drittmittelprojekte am Lehrstuhl

Mitträger des Graduiertenkollegs „Mathematische Optimierung" an der Universität Trier

Förderer: Deutsche Forschungsgemeinschaft – DFG
Förderzeitraum: 01.04.1995 bis 31.03.2001

Linear-Algebraische Berechnungsmodelle für Boolesche Funktionen und ihre Anwendung

Förderer: Deutsche Forschungsgemeinschaft – DFG

Förderzeitraum: 1999 - 2001

Control in Stochastic Domains: Complexity and Solutions

Förderer: Deutscher Akademischer Austauschdienst, NSF-Programm – DAAD
Förderzeitraum: 1999 - 2000

Über die zahlreichen Drittmittelprojekte, die am Institut für Telematik bearbeitet werden, wird an anderer Stelle berichtet, z.B. im Tätigkeitsbericht des TI.

7 Bücher und Buchbeiträge

7.1 Bücher

Christoph Meinel, Martin Mundhenk
Mathematische Grundlagen der Informatik
Mathematisches Denken und Beweisen - Eine Einführung
B.G. Teubner (Stuttgart, Leipzig), 2000, ISBN 3-519-02949-9

Abstract: Konzepte und Anwendungen der Informatik durchdringen in immer stärkerem Maße alle Bereiche der Wirtschaft und Gesellschaft; ohne ihr Grundverständnis ist deshalb ein erfolgreiches Wirken dort zunehmend unmöglich. Das daraus resultierende große Interesse auch bei Nichtinformatikern an der Informatik und ihren intellektuellen Grundlagen macht eine Einführung auch in die mathematischen Grundlagen der Informatik immer dringlicher, eine Einführung, die auch ohne eine traditionell vorausgesetzte mathematische Grundausbildung auskommt und trotzdem sachkundig in die für die Informatik typischen und grundlegenden mathematischen Denkweisen und Formalisierungen einführt. Das vorliegende Buch hat sich diese Aufgabe zum Ziel gestellt. Es führt den interessierten Leser ein in das für die Informatik typische Vorgehen, zunächst noch vage Ideen und Konzepte schrittweise zu formalisieren und damit einer Bearbeitung durch den Computer zugänglich zu machen.

7.2 Buchbeiträge

Randy Bryant, Christoph Meinel
Ordered Binary Decision Diagrams in Electronic Design Automation. Foundations, Applications and Innovations
In: Logic Synthesis and Verifications, Ed. S. Hassoun and T. Sasao, Kluwer Academic Publishers, Dordrecht/Netherlands, pp. 285-307, 2001

Abstract: Ordered Binary Decision Diagrams (OBDDs) play a key role in the automated synthesis and formal verification of digital systems. They are the state-of-the-art data structure representing switching functions in various branches of electronic design automation. In the following we discuss the properties of this data structure, characterize its algorithmic behaviour and describe some prominent applications.

Christoph Meinel, Christian Stangier
Data Structures for Boolean Functions. BDDs-Foundation and Applications
In: Festschrift des Graduiertenkollegs Berlin, H. Alt, ed. appears in LNCS, Springer-Verlag, pp. 61-78, 2000

Abstract: This article gives a lecture about ordered binary decision diagrams (OBDDs). Introduced in 1986, OBDDs still are the state-of-the-art data structure for representation of Boolean functions. An overview is given about the data structure, its properties, algorithmic behaviour, and the most important applications.

8 Herausgeberschaft

8.1 Proceedingsbände

Christoph Meinel, Lutz Gollan (Eds)
Digitale Signaturen
Proceedings Trierer Symposium Digitale Signaturen, Trier, Germany, 2001,
Institut für Telematik, ISSN 1433-8106, 2001

Christoph Meinel, Bernd Dusemund (Eds)
Mobile Commerce
Proceedings Trierer Symposium Mobile Commerce, Trier, Germany, 2001
Institut für Telematik, ISSN 1433-8106, 2001

M. Suilmann, Christoph Meinel, F. Veit, W. Schneider (Eds)
Security u. Public Key Infrastrukturen
Proceedings Online 2001 - Congress IV ONLINE-Verlag, ISBN 3-89077-222-6, 2001

Christoph Meinel, Michael Düro (Eds.)
Virtuelle Hochschule
Proceedings Trierer Symposium Virtuelle Hochschule, Trier, Germany, 2000, Institut für Telematik, ISSN 1433-8106, 2000

Christoph Meinel, Lutz Gollan (Eds.)
Smart Cards
Proceedings Trierer Symposium Smart Cards, Trier, Germany, 2000 Institut für Telematik, ISSN 1433-8106, 2000.

Christoph Meinel, M. Lawo, F. Veit, M. Suilmann (Eds.)
Telekommunikations-Sicherheit & Security Management
Proceedings ONLINE' 2000, Congress IV, Düsseldorf, Germany, ONLINE-Verlag, Velbert, ISBN 3-89077-209-9, 2000

8.2 Web-Sites

„ECCC.uni-trier.de"

Seit Ende 1994 wird am Lehrstuhl „Theoretische Konzepte und neue Anwendungen der Informatik" das „Electronic Colloquium on Computational Complexity — ECCC" herausgegeben.

„STACS.uni-trier.de"

Am Lehrstuhl für Theoretische Konzepte und neue Anwendungen der Informatik wird die Website des Symposium on Theoretical Aspects of Computer Science mit allen Informationen rund um diese Konferenz geführt. Darüber hinaus wird Software zur Verfügung gestellt, die die Abwicklung und das Management der Veranstaltung unterstützt, angefangen von der Einreichung wissenschaftlicher Arbeiten, der Begutachtung von Arbeiten durch das Programm-Komitee, bis hin zur Buchung von Hotelzimmern. Diese Software wurde am Lehrstuhl entwickelt und gepflegt.

„www.bdd-portal.org“

Eine WWW-Portalsite mit umfassendendem Informationsangebot und Link-Archiv zu allen Themengebieten rund um die Datenstruktur OBDD. Zusätzlich wird eine standardisierte Testumgebung für BDD-Experimente mit dem System *OHO* bereitgestellt.

„www.informatik.uni-trier.de/GI/FG-014/“

Regelmäßig werden von Christoph Meinel, dem Sprecher der GI-Fachgruppe 0.1.4 „Komplexität“, Jochen Bern (bis zum 31.09.2000) und Rustam Mubarakzjanov (ab 01.10.2000) aktualisierte WWW–Seiten mit Informationen zu Konferenzen, Theorietagen, Graduiertenkollegs, Sommerschulen, Stellenangeboten etc. für die Mitglieder der Fachgruppe „Komplexität der deutschen Gesellschaft für Informatik (GI)“ veröffentlicht.

9 Veröffentlichungen

9.1 Veröffentlichungen in Zeitschriften

L. Gollan, Ch. Meinel
Elektronischer Notar
Kommune 21, Heft 7, pp. 12-13, 2001

Abstract: Die Anwendungen im Bereich der elektronischen Unterschrift sind aufgrund fehlender Standards oft inkompatibel. Kann die Ausgabe digitaler Signaturen der Wirtschaft überlassen werden oder trägt der Staat hier die Verantwortung?

Christopher Lusena, Judy Goldsmith, Martin Mundhenk
Nonapproximability Results for Partially Observable Markov Decision Processes
Journal of Artificial Intelligence Research 14, pp. 83–113, 2001

Abstract: We show that for several variations of partially observable Markov decision processes, polynomial-time algorithms for finding control policies are unlikely to or simply don't have guarantees of finding policies within a constant factor or a constant summand of optimal. Here “unlikely” means “unless some complexity classes collapse,” where the collapses considered are P=NP, P=PSPACE, or P=EXP. Until or unless these collapses are shown to hold, any control-policy designer must

choose between such performance guarantees and efficient computation.

Christoph Meinel, Stefan Waack
The "Log Rank" Conjecture for Modular Communication Complexity
Computational Complexity 10, pp. 70-91, 2001

Abstract: The "log rank" conjecture involves the question of how precisely the deterministic communication complexity of a problem can be described in terms of algebraic invariants of the communication matrix of this problem. We answer this question in the context of modular communication complexity. We show that the modular communication complexity can be exactly characterised in terms of the logarithm of a certain rigidity function of the communication matrix. Thus, we are able to exactly determine the modular communication complexity of several problems, such as, e.g., set disjointness, comparability, and undirected graph connectivity. From the bounds obtained for the modular communication complexity we deduce exponential lower bounds on the size of depth-two circuits having arbitrary symmetric gates at the bottom level and a MOD m-gate at the top.

Christoph Meinel, Fabio Somenzi, Thorsten Theobald
Linear Sifting of Decision Diagrams and its Application in Synthesis
IEEE Transactions on CAD, Vol. 19, No. 5, pp. 521-533, 2000

Abstract: We propose a new algorithm, called *linear sifting*, for the optimization of decision diagrams that combines the efficiency of sifting and the power of linear transformations. The new algorithm is applicable to large examples, and in many cases leads to substantially more compact diagrams when compared to simple variable reordering. We also show in what sense linear transformations complement variable reordering and how the technique can be applied to verification issues. Going a step further, we discuss a synthesis scenario where – due to the complexity of the target function – it is inevitable to decompose the function in a preprocessing step. By using linear sifting it is possible to extract al inear filter and, hence, to achieve the necessary decomposition. Using this method we were able to synthesize functions with standard tools which fail otherwise.

Christoph Meinel, Thorsten Theobald
Local Encoding Transformations for Optimizing OBDD-Representations of Finite State Machines
Formal Methods in System Design, 18, pp. 285-301, 2001

Abstract: Ordered binary decision diagrams are the state-of-the-art representation of switching functions. In order to keep the sizes of OBDDs tractable, heuristics and dynamic reordering algorithms are applied to optimize the underlying variable order. When finite state machins are represented by OBDDs the state encoding can be used as an additional optimization parameter. In this papers, we analyze local encoding transformations which can be applied dynamically. First, we investigate the potential of r-encoding techniques. We then propose the use of an XOR-transformation and show why this transformation is most suitable among the set of all encoding transformations. The presented theoretical framework establishes a new optimization technique for OBDDs.

Christoph Meinel, Harald Sack
Mod2OBDDs - a BDD Structure for Probabilistic Verification
Electronic Notes in Theoretical Computer Science, Vol. 22, 2000

Abstract: Ordered Binary Decision Diagrams (OBDDs) have already proved useful in the verification of combinational and sequential circuits. Due to limitations of the descriptive power of OBDDs serveral more general models of Binary Decision Diagrams have been studied. In this paper $\oplus$-OBDDs - also known as Mod2OBDDs in respect to their ability to serve as a tool for combinational verification are considered. Besides the application of $\oplus$-OBDDs, the more general problem of how to exploit the inherent potential of $\oplus$-OBDDs more efficiently is addressed.

Rustam Mubarakzjanov
On Complexity classes defined by branching programs of bounded width
Discretnyi analys i issledovanie operacii, S.1, V.7, 1, 2000

Abstract: Read-once ordered branching programs (or OBDDs) having a constant width are studied. The relationship between the complexity classes $P, BPP, NP, coNP$ in the context of OBDDs of constant width and of OBDDs with other restrictions are proven. A new function computable by probabilistic unbounded error OBDD of constant width is presented. This function is hard for non-deterministic OBDDs and for bounded error OBDDs.

Martin Mundhenk
On hard instances
Theoretical Computer Science 242 (1-2), pp. 301-311, 2000

Abstract: Instance complexity was introduced by Orponen, Ko, Schöning, and Watanabe (JACM 1994)as a measure of the complexity of individual instances of a decision problem. Comparing instance complexity to Kolmogorov complexity, they

introduced the notion of p-hard instances, and conjectured that every set not in P has p-hard instances. Whereas this conjecture is still unsettled, Fortnow and Kummer (TCS 1995) proved that NP-hard sets have p-hard instances, unless P=NP. The unbounded version of the conjecture was proven wrong by Kummer (Structures 1995). We introduce a slightly weaker notion of hard instances. In the unbounded version, we characterize the classes of recursive enumerable resp. recursive sets by hard instances. In bounded versions, we characterize the class P.Hard instances are shown to be stronger than complexity cores (introduced by Lynch (JACM 1975)). Nevertheless, NP-hard sets must have super-polynomially dense hard instances and cannot consist of hard instances only, unless P=NP.

Martin Mundhenk
The complexity of optimal small policies
Mathematics of Operations Research 25(1), pp. 118-129, 2000

Abstract: We investigate the complexity of problems concerned with partially-observable Markov decision processes which are run for a finite number of steps under small policies. The calculation of the expected sum of rewards of a process under a small policy is shown to be complete for the complexity class PP, a class which lies intermediate between NP and PSPACE. Optimal small policy computation is shown to be complete for NP(PP). The latter contrasts results of Papadimitriou and Tsitsiklis (1987) who showed that this problem is PSPACE-complete, if no assumptions about the representability of the policy are made, and that it is P-complete for fully-observable processes.

Martin Mundhenk, Judy Goldsmith, Christopher Lusena, Eric Allender
Complexity of finite-horizon Markov decision process problems
Journal of the ACM 47(4), pp. 681-720, 2000

Abstract: Controlled stochastic systems occur in science, engineering, manufacturing, social sciences, and many other contexts. If the system is modeled as a Markov decision process (MDP) and will run *ad infinitum*, the optimal control policy can be computed in polynomial time using linear programming. The problems considered here assume that the time that the process will run is finite, and based on the size of the input. There are many factors that compound the complexity of computing the optimal policy. For instance there are many factors that compound the complexity of this computation. For instance, if the controller does not have complete information about the state of the system, or if the system is represented in some very succinct manner, the optimal policy is provably not computable in time polynomial in the size of the input. We analyze the computational complexity

of evaluating policies and of determining whether a sufficiently good policy exists for a MDP, based on a number of confounding factors, including the observability of the system state; the succinctness of the representation; the type of policy; even the number of actions relative to the number of states. In almost every case, we show that the decision problem is complete for some known complexity class. Some of these results are familiar from work by Papadimitriou and Tsitsiklis and others, but some, such as our PL-completeness proofs, are surprising. We include proofs of completeness for natural problems in the as yet little-studied classes $\mathrm{NP}^{\mathrm{NP}}$.

9.2 Veröffentlichungen in Tagungsbänden

Anmerkung: *Die folgende Auflistung beschränkt sich auf diejenigen Veröffentlichungen in Tagungsbänden von Mitarbeitern des Lehrstuhls, die im Rahmen von Forschungsprojekten am Lehrstuhl für Theoretische Konzepte und neue Anwendungen der Informatik an der Universität Trier erstellt wurden. Tagungsbeiträge, die von Angehörigen des Lehrstuhls im Zusammenhang mit Projekten am Institut für Telematik entstanden sind, können den Tätigkeitsberichten des Instituts für Telematik für die Jahre 2000 und 2001 entnommen werden.*

V. Arvind, J. Köbler, M. Mundhenk, J. Toràn
Nondeterministic instance complexity and hard-to-prove tautologies
In. Proc. of Symposium on Theoretical Aspects of Computer Science 2000 Lecture Notes in Computer Science, 1770:313–323, Springer Verlag 2000

Abstract: In this note we first formalize the notion of hard tautologies using a nondeterministic generalization of instance complexity. We then show, under reasonable complexity-theoretic assumptions, that there are infinitely many propositional tautologies that are hard to prove in any sound propositional proof system.

Elena Dubrova, Harald Sack
Probabilistic Verification of Multiple-Valued Functions
In: Proc. 30th IEEE International Symposium on Multiple-Valued-Logic (ISMVL 2000), Portland, Oregon, USA, pp. 460-466, 2000

Abstract: This paper describes a probalistic method for verifying the equivalence of two multiple-valued functions. Each function is hashed to an integer code by transforming it to an integer-valued polynomial and the equivalence of two polynomials is checked probabilistically. The hash codes for two equivalent functions are always the same. Thus, the equivalence of two functions can be verified with a known

probability of error, arising from collisions between inequivalent functions. Such a probalistic verification can be an attractive alternative for verifying functions that are too large to be handled by deterministic verification methods.

Christoph Meinel, Harald Sack
Improving XOR-node Placement for Mod2-OBDD Minimzation
In: Proc. Reed-Muller' 2001, Starkville (Mississippi,USA), pp. 51-56, 2001

Abstract: Ordered Binary Decision Diagrams (OBDDs) have already proved useful in the process of electronic design automation. Due to limitations of the descriptive power of OBDDs more general models of Binary Decision Diagrams have been studied. In this paper, $\oplus$-OBDDs as a true extension of the OBDD data structure are addressed. One important factor for the representation size of $\oplus$-OBDDs is determined by the number and the position of the introduced $\oplus$-nodes. Based on a simple greedy strategy that switches between different function decompositions, it is shown how to introduce $\oplus$-nodes during $\oplus$-OBDD synthesis just at the right place. The efficiency of the approach is proven by symbolic simulation of standard benchmarks.

Christoph Meinel, Harald Sack
A Simple Heuristic for Mod2-OBDD Minimization
In: Proc. IWLS' 2001, Lake Tahoe (California, USA), pp. 304-309, 2001

Abstract: Ordered Binary Decision Diagrams (OBDDs) have already proved useful in the process of electronic design automation. Due to limitations of the descriptive power of OBDDs more general models of Binary Decision Diagrams have been studied. In this paper, $\oplus$-OBDDs as a true extension of the OBDD data structure are addressed. One important factor for the representation size of $\oplus$-OBDDs is determined by the number and the position of the introduced $\oplus$-nodes. Based on a greedy strategy a heuristic for improving the representation size of $\oplus$-OBDDs is developed and its efficiency is proven by symbolic simulation of a standard benchmark set.

Christoph Meinel, Harald Sack, Volker Schillings
IDDS: An Interactive Decentralized Documentation System
In: Proc. ACM SIGDOG 2001, Santa Fe (USA), 2001

Abstract: The paper describes the design and the application of an Interactive Decentralized Documentation System (IDDS). IDDS is a web-based, interacitve documentation system that is especially designed for the support of working groups distributed over many places. It enables the creation of „just-in-time"-documentation and provides authoring tools for multimedia documents supporting multiple authors

per document including a versioning system. IDDS provides an HTML-frontend for being accessible anywhere with a standard webbrowser for creating, reading, or commenting on the provided documentation. The workflow of IDDS includes an interacitive and guided reviewing process of the documentation including security mechanisms that are designed to maintain a high quality of the created documentation. Furthermore, first experiences of the application of IDDS in a system and network-administration environment are given.

Christoph Meinel, Christian Stangier
Hierarchical Image Computation with Dynamic Conjunction Scheduling
In: Proc. ICCD' 2001, Austin (Texas, USA), pp. 354-359, 2001

Abstract: Image computation is the core operation for optimization and formal verification of sequential systems like controllers or protocols. State exploration techniques based on OBDDs use a partitioned representation of the transition relation to keep the OBDD-sizes manageable. This paper presents algorithms for building a hierarchically partitioned transition relation and conjunction scheduling based on this partitioning. The conjunction scheduling algorithm allows to dynamically reorder partitions and is targeted to improve the AndExist operation. Model checking experiments prove the effectiveness of the new algorithms.

Christoph Meinel, Christian Stangier
Hierarchical Image Computation with Dynamic Conjunction Scheduling
In: Proc. IWLS' 2001, Lake Tahoe (California, USA), pp. 316-321, 2001

Abstract: Image computation is the core operation for optimization and formal verification of sequential systems like controllers or protocols. State exploration techniques based on OBDDs use a partitioned representation of the transition relation to keep the OBDD-sizes manageable. This paper presents algorithms for building a hierarchically partitioned transition relation and conjunction scheduling based on this partitioning. The conjunction scheduling algorithm allows to dynamically reorder partitions and is targeted to improve the AndExist operation. Model checking experiments prove the effectiveness of the new algorithms.

Christoph Meinel, Christian Stangier
A new Partitioning Scheme for Improvement of Image Computation
In: Proc. ASP-DAC' 2001, Yokohama (Japan), pp. 97-102, 2001

Abstract: Image computation is the core operation for optimization and formal verification of sequential systems like controllers or protocols. State exploration techniques based on OBDDs use a partitioned representation of the transition relation to keep the OBDD-sizes manageable.This paper presents a new approach that significantly increases the quality of the partitioning of the transition relation of finite state machines. The heuristic has been successfully applied to reachability analysis and symbolic model checking of real life designs, resulting in a significant reduction in CPU time as well as in memory consumption.

Christoph Meinel, Christian Stangier
Speeding Up Symbolic Model Checking by Accelerating Dynamic Variable Reordering
In: Proc. of 10th GLS-VLSI, Chicago, USA, pp. 39-42, 2000

Abstract: Symbolic Model checking is a widely used technique in sequential verification. As the size of the OBDDs and also the computation time depends on the order of the input variables, the verification may only succeed if a well suited represented functions are changing, the variable order has to be adapted dynamically. Unfortunately, dynamic reordering strategies are often very time consuming and sometimes do not provide any improvement of the OBDD representation. This paper presents adaptions of reordering techniques originally intended for combinatorial verification to the specific requirements of symbolic model checking. The techniques are orthogonal in the way that they use either structural information about the OBDDs or semantical information about the represented functions. The application of there techniques substantially accelerates the reordering process and makes it possible to finish computations, that are too time consuming, otherwise.

Christoph Meinel, Christian Stangier
Accelerating Techniques for OBDD-based Formal Verification of Sequential Systems
In: Proc. of FMTOOLS' 2000, Reisenburg (Germany), pp. 129-134, 2000

Abstract: Model checking has been proven to be a powerful tool in formal verification of sequential circiuts, reactive systems, protocols, etc. The model checking of systems with huge state spaces is possible only if there is an efficient representation of the model. Recuded Odered Binary Decision Diagrams (shortly: OBDDs) [1] allow an efficient *symbolic* representation of the model [8].

In the following we present techniques that attack two major problems of symbolic model checking:

- Finding a good partitioning of the transition relation of the system under consideration.
- Efficient dynamic variable reordering during the computation.

All techniques have in common that *high level information* is utilized. For the first problem RTL information is used to improve the quality of the partitioning. While, for the second problem detailed knowledge about themodel checking process is used to accelerate variable reordering.

Christoph Meinel, Christian Stangier
Speeding Up Image Computation by Using RTL Information
In: Proc. of Formal Methods in CAD' 2000 (FMCAD 00, LNCS 1954), Austin, USA, pp. 443-454, 2000

Abstract: Image computation is the core operation for optimization and formal verification of sequential systems like controllers or protocols. State exploration techniques based on OBDDs use a partitioned representation of the transition relation to keep the OBDD-sizes manageable. This paper presents a new approach that significantly increases the quality of the partitioning of the transition relation of controllers given in the hardware description language Verilog. The heuristic has been successfully applied to reachability analysis and symbolic model checking of real life designs, resulting in a significant reduction both in CPU time and memory consumption.

Christoph Meinel, Arno Wagner
WWW.BDD-PORTAL.ORG
In: Proc. of IEEE IWLS' 2000, Dana Point (California, USA), pp. 349-353, 2000

Abstract: There is a need for specialized World Wide Web portal sites to facilitate access to resources for specific research communities. We present the portal for the Decision Diagram research community we have built, featuring links to important resources, a powerful literature search and a sophisticated system that allows use and evaluation of Decision Diagram heuristics online via the Internet. A discussion of the difficulties involved in such a project is given and our solutions are presented.

Christoph Meinel, Arno Wagner
WWW.BDD-PORTAL.ORG - An Electronical Basis for Cooperative Research in EDA
In: Proc.of CRIS 2000, Helsinki (Finland), 2000

Abstract: There is a need for specialized World Wide Web portal sites to facilitate access to resources for specific research communities. We present the portal for the Decision Diagram research community we have built, featuring links to important resources, a powerful literature search and a sophisticated system that allows use

and evaluation of Decision Diagram heuristics online via the Internet. A discussion of the difficulties involved in such a project is given and our solutions are presented.

Rustam Mubarakzjanov
On Probabilistic OBDDs with Constant Width
In: Proc. of the Workshop on Computer Science and Information Technologies CSIT' 2000, Ufa, Russia, September 18-23, V. 2, pp. 62-68, 2000

Abstract: One of central open problems in the complexity theory is the question: $NC^1 \stackrel{?}{=} LOGSPACE$. It is known that $LOGSPACE/poly(n)$ and $NC^1/poly(n)$ are equal respectively to the class of all Boolean functions computable by branching programs of the polynomial size and to the class of all Boolean functions computable by polynomial size branching programs of a constant width. Read-once ordered branching programs (or OBDDs) having a constant width (cwOBDD for short) are studied in this work. An other restriction for a cwOBDD is a requirement that the connections between neighboring levels of the cwOBDD are the same for all such pairs of levels . We use the notation fixOBDDs for such programs.

We present a new function computable by probabilistic (without bounded error) fixOBDD. There is no polynomial non-deterministic OBDD and no polynomial randomized OBDD computing this function. It is known that the complexity classes $P, BPP, NP, coNP$ in the context of OBDDs are different. We show that these classes are equal in the context of cwOBDDs and in the context of fixOBDDs as well.

Harald Sack, Christoph Meinel
Functional Extension of Decision Diagrams in Practice
In: Proc. FMTOOLS' 2000, Reisenburg (Germany), pp. 195-196, 2000

Abstract: In computer aided design of very large scale integrated circuits (CAD for VLSI) Ordered Binary Decision Diagrams (0BDDs) [1] have been established as the state-of-the-art data structure. They are applied in synthesis as well as in formal verification of combinatorial or sequential designs.This is due to the fact that almost every design step can be mapped to the task of manipulating Boolean functions. For performing these tasks efficiently in an automated way with a computer, OBDDs are very well suited, because they are compact, efficiently to manipulate, and canonical, i.e. there exists a unique OBDD for every Boolean function. The compactness property of OBDDs holds for most Boolean functions that are used in practice, but unfortunately not for all. The multiplication of two binary encoded numbers can only be represented with an OBDD of exponential size related to the number of inputs. This restriction is responsible for the research and development of more general data structures, based on extensions of OBDDs.

Besides relaxing the ordering restriction [2], easing the read-once property of the input variables,or the usage of different decomposition types for Boolean functions, we are focusing on the extension of OBDDs with functional operator nodes, esp. Parity-OBDDs (POBDDs), i.e. OBDDs with additional operator nodes computing the Boolean parity of their successors [3]. By introducing parity nodes the representation has the potential of being mor compact [3]. By introducing parity nodes the representation has the potential of being more compact while on the other hand giving up canonicity. Therefore, the identification of two POBDDs representing the same Boolean function becomes an essential operation. We present an efficient probabilistic equivalence test for POBDDs that admits working with POBDDs in an professional environment [4]. Due to the fact that the size of Decision Diagrams curcially depends on the order of the input variables we show how to apply heuristics for POBDD minimization based on dynamic changes in the variable order and the relocation of parity operator nodes inside the data structure.

Many problems in practice require the transformation of symbolic variables to a binary encoding for getting accessible with OBDDs or POBDDs. Extending the OBDD data structure from the binary domain to a finite domain results in so called Multi-valued Decision Diagrams (MDDs) [5] and a binary encoding of symbolic variables is not necessary anymore. The already introduced POBDDs can no be extended towards Mod-p-Decision Diagrams (Mod-p-DDs), i.e. MDDs with additional operator nodes, representing an integer addition modulo p, p-prime. Such decision diagrams have a potential of being more space-efficient than MDDs. However, they are not a canonical representation and thus, the equivalence test of two Mod-p-DDs is more difficult than the test of two MDDs. To overcome this problem, we design a fast probabilistic equivalence test for Mod-p-DDs based on the transformation of integer functions, represtented by Mod-p-OBDDs to polynomials over a finite domain [6] and show how to apply heuristics for their minimization.

Harald Sack, Elena Dubrova, Christoph Meinel
Representation of Multiple-Valued Functions with Mod-p-Decision Diagrams
In: Proc. of IEEE/ACM Int. Workshop of Logic Synthesis (IWLS 2000), Dana Point, CA, USA, pp. 341-348, 2000

Abstract: Multiple-valued logic allows us to formulate problems by using symbolic variables which are often more naturally associated with the problem specification than the variables obtained by a binary encoding. In this paper we present a data structure for representation and manipulation of multiple-valued functions - Mod-p Decision Diagrams(Mod-p-DDs). Mod-p-DDs differ from conventional Multiple-Valued Dicision Diagrams (MDDs) in that they contain not only branching nodes but also functional nodes, labeled by addition modulo p operation, p prime. Mod-p-DDs are potentially much more space-efficient than MDDs. However, they are not a canonical representation and thus, the equivalence test of two Mod- p-DDs is more difficult than the test of two MDDs. To overcome this problem, we design a fast probalistic equivalence test for Mod- p-DDs that requires time linear in the number of nodes.

Harald Sack, Elena Dubrova, Christoph Meinel
Mod-p Decision Diagrams: A Data-Structure for Multiple-Valued Functions
In: Proc. of 30th IEEE International Symposium on Multiple-Valued-Logic (ISMVL, 2000), Portland, Oregon, USA, pp. 233-238, 2000

Abstract: Multiple-valued decision diagrams (MDDs) give a way of approaching problems by using symbolic variables which are often more naturally associated with the problem statement than the variables obtained by a binary encoding. We present a more general class of MDDs, containing not only branching nodes but also functional nodes, labeled by addition modulo p prime, and give algorithms for their manipulation. Such decision diagrams have a potential of being more space-efficient than MDDs. However, they are not a canonical representation of multiple-valued functions and thus the equivalence test of two Mod-p-DDs is more difficult than the test of two MDDs. To overcome this problem, we design a fast probabilistic equivalence test for Mod-p-DDs that requires time linear in the number of nodes.

Christian Stangier, Ulrich Holtmann
Applying Formal Verification with Protocol Compiler
In: Proc. of EUROMICRO Digital System Design' 2001 (DSD'01), Warsaw (Poland), 2001

Abstract: This paper presents a practical methodology for the application of formal verification to the industrial design environment "Protocol Compiler". Our verification flow is to first create a testbench and simulate the design. Then we modify the testbench and perform a formal verification technique called assertion checking. The examples are taken from the networking arena. The first is a simplified RS232 transceiver, the second a pipelined FIFO-like buffer written in Verilog. We show that assertion checking fits well into the design flow and is easy to use within Protocol Compiler.

Christian Stangier, Ulrich Holtmann, Christoph Meinel
Optimization of Transition Relations by Using High-Level Information
In: Proc. of the 2000 IEEE/ACM Int. Workshop on Logic Synthesis (IWLS 00), Dana Point, USA, 2000

Abstract: The computation of the reachable state set is a core task of optimization and formal verification of sequential systems like controllers or protocols. State exploration techniques based on OBDDs use a partitioned representation of the transition relation to keep the OBDD-sizes manageable. This paper presents a new approach that significantly increases the quality of the partitioning of the transition relation of controllers given in the high-level description language Protocol Compiler, resulting in a much more efficient reachable states computation.

9.3 Veröffentlichungen im "Electronic Colloquium on Computational Complexity — ECCC"

Rustam Mubarakzjanov
Bounded-Width Probabilistic OBDDs and Read-Once Branching Programs are incomparable
ECCC-Report Nr. TR01-037 (ISSN 1433-8092)

Since the problem of proving exponential lower bounds on the complexity for general probabilistic OBDDs is open so far, it is interesting to study this problem in a restricted setting. For this reason we deal in this work with probabilistic OBDDs whose width is bounded. We prove in this work that probabilistic OBDDs of width bounded by a constant can be more powerful than even non-deterministic read-once branching programs. To do it we present a probabilistic OBDD of constant width computing the known function PERM. We prove for several known functions that they cannot be computed by probabilistic OBDDs of constant width. To show it we present a new method allowing to obtain lower bound Omega(n) on the width of corresponding OBDDs (n is the number of variables).

Rustam Mubarakzjanov
Probabilistic OBDDs: On Bound of Width versus Bound of Error
ECCC-Report Nr. TR00-085, (ISSN 1433-8092)

Abstract: Ordered binary decision diagrams (OBDDs) are well established tools to represent Boolean functions. There are a lot of results concerning different types of generalizations of OBDDs. The same time, the power of the most general form

of OBDD, namely probabilistic (without bounded error) OBDDs, is not studied enough. In order to compare probabilistic OBDDs with other kinds of branching programs, we consider such OBDDs bounding their width by a constant. We show this computation model can be more powerful than polynomial size non-deterministic, probabilistic with bounded error OBDDs and non-deterministic read-once branching programs. We discuss also the possibilities to find functions being hard for probabilistic OBDDs with constant width. Keywords: Probabilistic branching programs "Boolean functions" complexity classes

9.4 Vorabveröffentlichungen in der Reihe Forschungsberichte Mathematik/Informatik der Universität Trier

Christoph Meinel, Martin Mundhenk
6. Berlin-München-Trierer Workshop zur Algorithmischen Diskreten Mathematik und Mathematischen Optimierung (ADiMMO 2001)
Forschungsbericht Nr. 01-04

Abstract: Zum sechsten Mal wurde der schon traditionelle ADiMMO Workshop veranstaltet. Teilnehmen werden Wissenschaftler des Europäischen Graduiertenkollegs *Combinatorics, Geometry, Computation* in Berlin und Zürich, des Trierer Graduiertenkollegs *Mathematische Optimierung*, des Münchner Graduiertenkollegs *Angewandte algorithmische Mathematik*, sowie Dozenten und Studenten der Abteilungen Mathematik und Informatik der Universität Trier und auswärtige Gäste.

Die Vorträge decken ein weites Gebiet der Diskreten Mathematik, der Algorithmischen Geometrie und der Theoretischen Informatik ab. Neben Vorträgen von Angehörigen der Graduiertenkollegs freuen wir uns, dass Susanne Albers und Wolfgang Paul unsere Einladung angenommen haben und in ihren Vorträgen Forschungsgebiete außerhalb der Themen der Graduiertenkollegs vorstellen.

Martin Mundhenk
43. Workshop für Komplexitätstheorie, Datenstrukturen und effiziente Algorithmen (Theorietag)
Forschungsbericht Nr. 01-05

Christoph Meinel, Harald Sack
A Heuristic for (+)-OBDD Minimization
Forschungsbericht Nr. 01-06

Abstract: Ordered Binary Decision Diagrams (OBDDs) have already proved useful in the process of electronic design automation. Due to limitations of the descriptive power of OBDDs more general models of Binary Decision Diagrams have been studied. In this paper, $\oplus$-OBDDs as a true extension of the OBDD data structure are addressed. One important factor for the representation size of $\oplus$-OBDDs is determined by the number and the position of the introduced $\oplus$-nodes. Based on a greedy strategy a heuristic for improving the representation size of $\oplus$-OBDDs is developed and its efficiency is proven by symbolic simulation of standard benchmarks.

Christoph Meinel, Harald Sack
Improving XOR-Node Placement for (+)-OBDDs
Forschungsbericht Nr. 01-07

Abstract: Ordered Binary Decision Diagrams (OBDDs) have already proved useful in the process of electronic design automation. Due to limitations of the destriptive power of OBDDs more general models of Binary Decision Diagrams have been studied. In this paper, $\oplus$-OBDDs as a true extension of the OBDD data structure are addressed. One important factor for the representation size of $\oplus$-OBDDs is determined by the number and the position of the introduced $\oplus$-nodes. Based on a simple greedy strategy that switches between different function decompositions, it is shown how to introduce $\oplus$-nodes during $\oplus$–OBDD synthesis just at the right place. The efficiency of the approach is proven by symbolic simulation of standard benchmarks.

Christoph Meinel, Harald Sack
WWW.BDD-PORTAL.ORG: An Experimentation Platform for Binary Decision Diagram Algorithms
Forschungsbericht Nr. 01-09

Abstract: There is an upcoming need for World Wide Web portal sites to facilitate access to resources for specific research communities. The portal site described in this paper provides a testbed functionality besides additional information resources that are of interest in the research in Binary Decision Diagrams (BDDs). In the last decade, BDDs have proven to be the state-of-the-art structure in computer aided design of integrated digital circuits. To assess the strengths and weaknesses of manipulation algorithms for BDDs, benchmark calculation is one of the most important methods in BDD-research. Due to the inherent high sensitivity of these algorithms to the particular experimental setup it is rather difficult or even impossible to reproduce benchmark results for comparison or for independent result verification. We have designed and implemented a WWW based BDD-testbed that overcomes these problems and greatly facilitates BDD algorithm comparison.

Christoph Meinel, Harald Sack, Volker Schillings
IDDS: An Interactive Decentralized Documentation System
Forschungsbericht Nr. 01-15

Abstract: The paper describes the design and the application of an Interactive Decentralized Documentation System (IDDS). IDDs is a web-based, interactive documentation system that is especially designed for the support of working groups distributed over many places. It enables the creation of „just-in-time“-documentation and provides authoring tools for multimedia documents supporting multiple authors per document including a versioning system. IDDs provides an HTML-frontend for being accessible anywhere with a standard webbrowser for creating, reading, or commenting on the provided documentation. The workflow of IDDS includes an interactive and guided reviewing process of the documentation including security mechanisms that are designed to maintain a high quality of the created documentation. Furthermore, first experiences of the application of IDDs in a system and networkadministration environment are given.

Christoph Meinel, Christian Stangier
Modular Partitioning for Improvement of Image Computation
Forschungsbericht Nr. 01-16

Abstract: Image computation is the core operation for optimization and formal verification of sequential systems like controllers or protocols. State exploration techniques based on OBDDs use a partitioned representation of the transition relation to keep the OBDD-sizes manageable. This paper presents new approaches that significantly increase the quality of the partitioning of the transition relation of finite state machines. The heuristics have been successfully applied to reachability analysis and symbolic model checking of real life designs written in Verilog, resulting in a significant reduction in CPU time as well as in memory consumption.

Christoph Meinel, Harald Sack, Volker Schillings
VisBDD - A Web-based Visualization Framework for OBDD Algorithms
Forschungsbericht Nr. 01-21

Abstract: This paper presents a web-based visualization framework visBDD, intended for learning and understanding basic algorithms related to Ordered Binary Decision Diagrams (OBDDs). With visBDD the key algorithm for OBDD-synthesis, the ITE-algorithm can be explored in depth and step-by-step by the user, while all involved data structures can be made visible at different levels of abstraction. The framework is intended as well as for professionals as also for students, who want to gain more insight into the powerful OBDD data structure that is used in many verification and synthesis tools, for a better understanding of the underlying mecha-

nisms and the problem complexity, without being dependent on reading textbooks.

Christopher Lusena, Judy Goldsmith, Martin Mundhenk
Nonapproximability Results for Partially Observable Markov Decision Processes
Forschungsbericht Nr. 00-12

Abstract: We show that for several variations of partially observable Markov decision processes, polynomial-time algorithms for finding control policies are unlikely to or simply don't have guarantees of finding policies within a constant factor or a constant summand of optimal. Here "unlikely" means "unless some complexity classes collapse," where the collapses considered are P=NP, P=PSPACE, or P=EXP. Until or unless these collapses are shown to hold, any control-policy designer must choose between such performance guarantees and efficient computation.

Rustam Mubarakzjanov
Lower Bounds for Randomized Branching Programs with a Big OBDD Part
Forschungsbericht Nr. 00-13

Abstract: There are exponential lower bounds on the complexity of randomized *OBDD*s with bounded error. For more general model of read-once branching programs (*BP1*), no such bound is known for an arbitrary computation error. We investigate in this work such *BP1*s on n variables that for some assignment of $O(\log n)$ variables the subprogram on the rest variables is an *OBDD*. We show that polynomial size randomized *BP1*s with this restriction are more powerful than polynomial size randomized *OBDD*s and less powerful than polynomial size *BP1*s. Furthermore, we show that the integer multiplication can not be computed by such restricted randomized *BP1*s of polynomial size.

9.5 Vorabveröffentlichungen in den Berichten des Instituts für Telematik

Sämtliche Technische Berichte des Instituts für Telematik können über das Institut bezogen oder unter der URL

`http://www.ti.fhg.de/publikationen/technische-berichte/index.html/`

abgerufen werden.

Paul Ferring, Thomas Engel, Christoph Meinel
Computer-Telefonie-Integration und Packet-Bases-Communication Systems
TR-Nr. 01-01

Bernd Dusemund, Christoph Meinel
Trierer Symposium Mobile Commerce Abstracts
TR-Nr. 01-02

Ernst-Georg Haffner, Thomas Engel, Christoph Meinel
Schleusentechnologie "Lock-Keeper" und ihre Integration in moderne Sicherheitsarchitekturen
TR-Nr. 01-03

Bernd Dusemund, Christoph Meinel
Trierer Symposium Mobile Commerce Proceedings
TR-Nr. 01-04

Uwe Becker, Thomas Engel, Christoph Meinel
IT-Sicherheitszertifikate
TR-Nr. 01-05

Lutz Vorwerk, Christoph Meinel
Die Bedeutung des DICOM Standards für das europäische Gesundheitswesen
TR-Nr. 01-06

Lutz Gollan, Lutz Vorwerk, Ulf Birkel, Christoph Meinel
Studie Teleradiologie: Umfrage unter Akut-Krankenhäusern in Baden-Württemberg 2000/2001
TR-Nr. 01-07

Uwe Roth, Christoph Meinel
SDS in der öffentlichen Verwaltung
TR-Nr. 01-08

Lutz Gollan, Christoph Meinel
Trierer Symposium Digitale Signaturen Abstracts
TR-Nr. 01-09

Uwe Roth, Frank Losemann, Thomas Engel, Christoph Meinel
Anforderungsprofil für den "sicheren"Betrieb eines WLAN
TR-Nr. 01-10

Lutz Gollan, Christoph Meinel
Trierer Symposien Digitale Signaturen Proceedings
TR-Nr. 01-11

Zhongdong Zhang, Andreas Heuer, Xiaoping Zuo, Thomas Engel, Christoph Meinel
Redaktionssystem DAPHNE
TR-Nr. 00-01

Ernst-Georg Haffner, Thomas Engel, Christoph Meinel
Die Lock-Keeper Architektur. Sicherer Schutz gegen Online-Attacken aus dem Internet
TR-Nr. 00-02

Ernst-Georg Haffner, Thomas Engel, Christoph Meinel
Techniques for Securing Networks against Criminal Attacks
TR-Nr. 00-03

Uwe Roth, Christoph Meinel
Was Sie noch nie über Spam wissen wollten, aber gezwungen waren zu erfahren
TR-Nr. 00-04

Christoph Meinel, Michael Düro
Trierer Symposium Virtuelle Hochschule, Proceedings
TR-Nr. 00-05

Christoph Meinel, Michael Düro
Trierer Symposium Virtuelle Hochschule, Abstracts
TR-Nr. 00-06

Christoph Meinel, Lutz Gollan
Trierer Symposium Smart Cards
TR-Nr. 00-07

Lutz Gollan, Christoph Meinel
Electronic Signatures. An American and European Perspective
TR-Nr. 00-08

Lutz Vorwerk, Burkhard Lüpken, Frank Losemann, Thomas Engel, Christoph Meinel
Modell für den Einsatz von Java Cards im Gesundheitswesen
TR-Nr. 00-09

Ali Mabrouk, Kais Louizi, Lutz Gollan, Christoph Meinel, Thomas Engel
Mobile Commerce
TR-Nr. 00-10

Sergej Hludov, Christoph Meinel, Mihail Gevantmakher, Thomas Engel
Das Patienten CD-System, Sicherheitsaspekte der mobilen Technologien
TR-Nr. 00-11

Christoph Meinel, Lutz Gollan
Trierer Symposium Smart Cards
TR-Nr. 00-12

Mariana Podesta, Christoph Meinel
The Necessity of a Public Key Infrastructure for a Virtual University
TR-Nr. 00-13

Ernst-Georg Haffner, Thomas Engel, Christoph Meinel
Integration der Schleusentechnologie Lock-Keeper in moderne Sicherheitsarchitekturen
TR-Nr. 00-14

Bernd Dusemund, Thorsten Becker, Lutz Gollan, Thomas Engel, Christoph Meinel
Security in Open Networks, The Functionality of a Public Key Infrastructure

TR-Nr. 00-15

9.6 Sonstige Vorabveröffentlichungen

Martin Mundhenk
The Complexity of Planning with Partially-Observable Markov Decision Processes
Dartmouth College, Dept. of Computer Science TR 2000-376

Abstract: This work surveys results on the complexity of planning under uncertaintly. The planning model considered is the partially-observable Markov decision process. The general planning problems are, given such a process, (a) to calculate its performance under a given control policy, (b) to find an optimal or approximate optimal control policy, and (c) to decide whether a good policy exists. The complexity of this and related problems depend on a variety of factors, including the observability of the process state, the compactness of the process representation, the type of policy, or even the number of actions relative to the number of states. In most cases, the problem can be shown to be complete for some known complexity class.

10 Vorträge

10.1 Vorträge außerhalb der Universität Trier

Christoph Meinel:

„Security and Public Key Infrastrukturen"
Online' 2001, Düsseldorf, 29.01.2001

„Telematik - junge Disziplin mit grenzenlosen Anwendungen"
Jubiläum European Medialab, Heidelberg, 12.02.2001

„Telemedizin - Telematik im Gesundheitswesen"
Informatikkolloquium, Universität Berlin, 05.03. - 06.03.2001

„Aktuelle Telematikforschung und das Problem der Sicherheit in offenen Netzen“
Universität Leipzig, 19.03.2001

„Telematik - junge Disziplin mit grenzenlosen Anwendungen“
„Telemedizin - Telematik im Gesundheitswesen“
„Sicherheit in offenen Netzen“
„Elektronisches Publizieren, Portal-Sites und virtuelle Universitäten“
Donau-Universität Krems, 20.03. - 22.03.2001

„Telematik - junge Disziplin mit grenzenlosen Anwendungen“
GT-BIK Tübingen, 04.04. - 05.04.2001

„Telematik - anwendungsgetriebene Forschung und Enwicklung“
Universität Linz, 20.04.2001

„Gesundheitsportal für Trier“
Regionale Gesundheitskonferenz, Trier, 13.07.2001

„ACERT - eine Konzeption für ein unternehmungsinternes CERT“
Workshop der Allianzgruppe, Hamburg, 24.07.2001

„IT-Security and Digital Signatures“
Polytechnical University, Peking, 18.09. - 28.09.2001

„Actual BDD-Research in Trier“
Universität Rom, 03.10. - 07.10.2001

„Sicherheit in offenen Netzen - Digitale Signaturen“
Mannheimer IT-Tage, Mannheim, 05.11.2001

„Perspektiven im Elektronischen Publizieren“
„Perspektiven im IT-Sicherheit“
Perspektivenseminar Dagstuhl, 21.11. - 23.11.2001

„Vorstellung des Instituts für Telematik“
InMit, Trier, 19.01.2000

„Trustcenter und Multifunktionskarten“
Online' 2000, Düsseldorf, 31.01.2000

„Telematik - eine junge Wissenschaftsdisziplin“
DResearch, Berlin, 18.02.2000

„BDDs - State-of-the-Art Data Structures for Boolean Functions“
Universität Barcelona, Spanien, 17.03.2000

„Institut für Telematik - Forschungs- und Entwicklungsprojekte“
ADiMMO 2000, TU München, 30.03.2000

„Notwendigkeit und Aufgaben eines Luxembourger Trust Centers“
ABBL, Luxembourg, 18.04.2000

„Eröffnungsvortrag“
Trierer Symposium "Virtuelle Hochschule", Trier, 04.05.2000

„BDD-basierte Datenstrukturen im Schaltkreisentwurf“
Informatikkolloquium, ETH Zürich/Schweiz, 22.05.2000

„WWW.BDD-Portal.Org - An Electronical Basis for Cooperative Research in EDA“
CRIS 2000, Helsinki/Finnland, 26.05.2000

„WWW.BDD-Portal.Org“
DAC 2000, Los Angeles, 08.06.2000

„Rechenschaftsbericht Institut für Telematik“
Kuratoriumssitzung, Trier, 21.06.2000

„Internet-Orientated Medical Information System for DICOM-Data Transfer, Visualization and Revision“
13th IEEE CBMS' 2000, Houston/USA, Juni 2000

„A Multimedia-Editor for Making Findings in Radiology“
13th IEEE CBMS' 2000, Houston/USA, Juni 2000

„Smart Cards - The Personal Safe in an E-Commerce World“
1th IC' 2000, Las Vegas, Juni 2000

„Vorstellung des Instituts für Telematik“
Besuch einer koreanischen Wissenschaftlerdelegation, Trier, 08.08.2000

„BDD-based Data Structures in VLSI“
Dagstuhl-Seminar "Experimentelle Algorithmen", 12.09.2000

„Institut of Telematics - Research and Development Activities“
Polytechnical University, Peking/China, 03.10.2000

„Rechenschaftsbericht des Instituts für Telematik“
Kuratoriumssitzung, Trier, 10.11.2000

„Implementation of a Document Management System Based on WebDAV Protocol“
ICMIT' 2000, Singapore, 15.11.2000

„Einführungsvortrag“
Trierer Symposium "Smart Cards", Trier, 23.11.2000

„BDD-basierte Datenstrukturen für sequentielle Schaltkreise“
Abschlusskolloquium des DFG-Schwerpunktprogramm "Effiziente Algorithmen", Universität Karlsruhe, 28.11.2000

„Trust Center-Infrastructure, Specifications and Standards“
ABBL, Luxembourg, 20.12.2000

Rustam Mubarakzjanov:

„Lower Bounds on Complexity of Probabilistic Branching Programs“
„Computer Aided Design and Test - BDD versus SAT“, Schloss Dagstuhl, 29.01.-02.02.2001

„On Functions Being Hard for Probabilistic Branching Programs“
6th Berlin-München-Trierer Workshop zur Algorithmischen Diskreten Mathematik und Mathematischen Optimierung (ADiMMO 2001), Universität Trier, 16.03.2001

„Probabilistische OBDDs mit konstaner Breite vs. read-once Branching Programme“
Workshop Komplexitaetstheorie, Datenstrukturen und Effiziente Algorithmen (Theorietag), Trier, 03.04.2001

„Bounded-width probabilistic OBDD versus read-once branching programs“
Workshop "Optimal Discrete Structures and Algorithms",
Rostock, 11.09.-13.09.2000

„On Probabilistic OBDDs with Constant Width“
Workshop des Graduiertenkollegs A^3DiM^3O 2000, München, 30.03.-31.03.2000

Martin Mundhenk:

„The hardness of planning“
6th Berlin-München-Trierer Workshop zur Algorithmischen Diskreten Mathematik und Mathematischen Optimierung (ADiMMO 2001), Universität Trier, 15.03.2001

„Guter Plan ist teuer“
Schloss Dagstuhl, 11.04.2001

„Woran erkennt man harte Nüsse“
Informatik-Kolloquium, Universität Göttingen, 28.11.2000

„Guter Plan ist teuer“
Workshop über Komplexitätstheorie, effiziente Algorithmen und Datenstrukturen, Göttingen, 14.11.2000

„Ein Konzept für die Informatikausbildung von Nichtnaturwissenschaftlern“
Universität Jena, 19.05.2000

„Hard tautologies for propositional proof systems“
Boston University, 05.05.2000

„Nondeterministic instance complexity and hard-to-prove tautologies“
Symposium on Theoretical Aspects of Computer Science 2000, Lille, 18.02.2000

„Why is it so hard to prove theorems“
Universität de Metz, 27.01.2000

Frank Recker:

„Parallel Searching in Trees“
Workshop on Search, Sorting and Coding, Universität Bielefeld, 10.10.2000

Harald Sack:

„Heuristics for Mod2-OBDD Minimization“
„Computer Aided Design and Test - BDD versus SAT“, Schloss Dagstuhl, 29.01.-02.02.2001

„Minimization of Mod2-OBDDs
6th Berlin-München-Trierer Workshop zur Algorithmischen Diskreten Mathematik und Mathematischen Optimierung (ADiMMO 2001), Universität Trier, 15.03.2001

„A Simple Heuristics for Mod2-OBDD Minimization“
Int. Workshop on Logic and Synthesis (IWLS 2001), Granlibakken, CA., USA, 12.06.-15.06.2001

„Improving XOR-Node Placement for Mod2-OBDD“
5th International Workshop on Applications of the Reed Muller Expansion in Circuit Design (Reed-Muller 2001), Starkville, (Mississippi, USA) 10.08.-11.08.2001

„Implementation of a WebDAV-based Collaborative Distance Learning Environment“
SIGUCCS‘ 2000, Richmond,Virginia, 28.10.-02.11.2000 USA

„Development of an Mod2-OBDD package/Accelerating OBDD minimization by Sampling/Iterative Synthesis with OBDDs of Different Variable Orders“
Fujitsu Labs of America, Sunnyvale, CA, USA, 18.07.2000

„Functional Extension of Decision Diagrams in Practice“
4th Workshop on Tools for System Design and Verification (FM-Tools), Reisenburg Castle, 10.07.-13.07.2000

„ECCC - Ein elektronisches Kolloquium“
"Hochschulentwicklung durch neue Medien", Ludwig-Maximilians-Universität München, 06.07.2000

„Mod-p-Decision Diagrams: A Data Structure for Multi-Valued Functions“
International Workshop on Logic Synthesis (IWLS 2000), Dana Point, CA, USA, 31.05.-02.06.2000

„ECCC - Eine digitale Bibliothek im Einsatz“
Trierer Symposium „Virtuelle Hochschule“, Institut für Telematik, Trier, 04.05.-05.05.2000

„Representing discrete functions with Mod-p-Decision Diagrams“
Dagstuhl Seminar on "Probabilistic Methods in Verification", Internationales Begegnungs- und Forschungszentrum Informatik, Schloß Dagstuhl, 30.04.-05.05.2000

„Funktionale Erweiterungen von BDDs in der Praxis“
A^3DiM^3O 2000, Munich, 30.03.-31.03.2000

Christian Stangier:

„A new Partitioning Scheme for Improvement of Image Computation“
ASPDAC 2001, Yokohama/Japan, 29.01.-02.02.2001

„RTL-based Partitioning Schemes for Improvement of Image Computation“
6th Berlin-München-Trierer Workshop zur Algorithmischen Diskreten Mathematik und Mathematischen Optimierung (ADiMMO 2001), Universität Trier, 16.03.2001

„Speeding Up Image Computation by using RTL Information“
FMCAD 2000, Austin/USA, 31.10.-07.11.2000

„Speeding Up Symbolic Model Checking by Accelerating Dynamic Variable Reordering“
10th ACM Great Lakes Symposium on VLSI (GLS-VLSI), Chicago/USA, Nov. 2000

10.2 Vorträge im Informatik–Oberseminar

04.07.00	Arno Wagner: *WWW.BDD-Portal.Org - Ein BDD-Portal im World Wide Web*
18.01.00	Martin Mundhenk: *Komplexität von Planungsproblemen*
11.01.00	Martin Mundhenk: *Schwer beweisbare Formeln*

10.3 Vorträge im Forschungsseminar

27.11.01	Rustam Mubarakzjanov: *Local Encoding Transformation of OBDDs by a Conjunction of 2 Variables*
20.11.01	Harald Sack: *Dynamic Variable Reordering for $\oplus$-OBDDs*
13.11.01	Christian Stangier: *OBDD Variablen Reordering - revisited*
06.11.01	Volker Schillings: *Multimediales Lernen - Visualisierung von Algorithmen und Datenstrukturen am Beispiel des OBDD ITE Algorithmus*
17.07.01	Harald Sack: *Efficient Placement of XOR-Nodes in Mod2OBDDs*
10.07.01	Rustam Mubarakzjanov: *Linear (Exponential) Lower Bounds on the Probabilistic Communication (OBDD) Complexity*
03.07.01	Gennadij Umanskij: *Verteiltes Filesystem mit variablem Aktualisierungsgranulat für den mobilen Einsatz*
17.07.01	Harald Sack: *Heuristics for $\oplus$-OBDD Minimization*

29.05.01	*Christian Stangier*: *Hierarchical Image Computation with Dynamic Conjunction Scheduling*
15.05.01	Rustam Mubarakzjanov: *Satisfiability for Probabilistic Ordered Branching Programs*
23.01.01	Christian Stangier: *A new Partitioning Scheme for Improvement of Image Computation*
21.11.00	Harald Sack: *Implementation of WebDAV based Collaborative Distributed Learning Environment*
14.11.00	Farid Ablayev: *On the Lower Bounds for One-way Quantum Automata*
24.10.00	Christian Stangier: *Speeding Up Image Computation by using RTL-Information*
17.10.00	Rustam Mubarakzjanov: *Restricted Randomized Read-Once Branching Program and an Exponential Lower Bound for Integer Multiplication*
04.07.00	Jochen Bern: *Get Organized! - Sinn und Zweck des Palm Top*
27.06.00	Frank Recker: *Resenttable Zero-Knowledge* (nach einer Arbeit von Canetti, Goldreich, Goldwasser und Micali)
20.06.00	Rustam Mubarakzjanov: *Über Funktionen, die hart für beschränkte probabilistische OBDD sind*
23.05.00	Arno Wagner: *Freenet, Gnutella, Napster: Neue Wege der Informationsspeicherung und -verbreitung*
16.05.00	Harald Sack: *Representation of Multiple Valued Functions with Mod-p DDs*
29.02.00	Arno Wagner: *Projekt BDD-Portal: Statusbericht*
15.02.00	Jochen Bern: *Konferenzmanagement Software STACS 2000 - Demonstration und Erfahrungsbericht*
01.02.00	Rustam Mubarakzjanov: *Probabilistische OBDDs mit konstanter Breite*
25.01.00	Carsten Damm: *Zero-Knowledge Proofs of Knowledge*
11.01.00	Frank Recker: *über "Clueless Agents" von Bruce Schneier et al*

10.4 Gäste und Gastvorträge

04.12.01	Prof. Dr. Dima Grigoriev, Université de Rennes, France *Complexity of algebraic proofs*
19.08. - 20.08.01	Prof. Dr. Fabio Somenzi, University of Colorado at Boulder, USA *Divide and Compose: SCC Refinement for Language Emptiness*
20.12.00	Roderick Bloem, University of Colorado at Boulder/USA *Efficient Buechi Automata from LTL Formula*
12.12. - 15.12.00	Dr. Elena Dubrova, Electronic System Design Lab, Department of Electronics, Royal Institute of Technology, Stockholm/Sweden *Multiple Valued Surprices*
11.11. - 18.11.00	Prof. Dr. Farid Ablayev, Dpt. of Theoretical Cybernetics, State University, Kazan *On the lower bounds for one-way Quantum*(Forschungsseminar) *The Complexity of General and Restricted Programs: A Communication Complexity Approach* (Graduiertenkolleg)
10.10.00	Dr. Thorsten Theobald, TU München *Kugeln im Computer: Algorithmische Fragen und geometrische Antworten*
28.03.00	Prof. Dr. Farid Ablayev, Dpt. of Theoretical Cybernetics, State University, Kazan *On the Power of Quantum and Probabilistic Computations*

11 Mitgliedschaften in Programmkomitees und Aufsichtsräten, Gutachtertätigkeiten

Christoph Meinel:

Veranstaltung von Tagungen und Symposien

- Veranstalter des Trierer ADiMMO Workshops der DFG, Graduiertenkolleg Algorithmische Diskrete Mathematik (Berlin) und Mathematische Optimierung (Trier) 15. und 16. März 2001
- Veranstalter des Trierer Symposiums "Mobile Commerce", 07. - 08. Juni 2001
- Veranstalter des Trierer Symposiums "Digital Signatures", 15. - 16. November 2001
- Veranstalter des Trierer Symposiums "Virtuelle Hochschule", 04. - 05. Mai 2000
- Veranstalter des Trierer Symposiums "Smart Cards", 23. - 24. November 2000

Mitglied in Programm-Komitees nationaler und internationaler Tagungen

- Online' 2001 - Symposium IV-1: Telekommunikations - Sicherheit und Security-Management, 31.01.2001 Düsseldorf (Germany), Chair
- IEEE/CBMS 2001 - International Symposium on Computer Based Medical Systems, June, 2001, Washington D.C. (USA),
- IEEE/ACM/IWLS 2001 - International Workshop on Logic Synthesis, 12.06. - 15.06.2001, Granlibaken (California, USA)
- 2001 Reed-Muller Workshop, 10.-11.08.2001, Mississippi State University (USA)
- FCT 2001 - Fundamentals of Computation Theory, 22.-24.08.2001, Riga, (Latvia)
- Online' 2000 - Symposium IV-1: Telekommunikations-Sicherheit und Security-Management, 31.01.2000, Düsseldorf,
- "Probabilistic Methods in Verification", Dagstuhl-Seminar, 30.04.-05.05.2000, IBFI Dagstuhl (Germany),
- Trierer Symposium "Virtuelle Hochschule", 04.-05.05.2000, Trier (Germany), Chair
- IEEE/ACM/IWLS 2000 International Workshop on Logic Synthesis, 31.05.-02.06.2000, Dana Point (California, USA)
- 4th International Workshop on Boolean Problems, 17.-18.09.2000, Freiberg (Germany)

Weitere Funktionen

- Sprecher der GI-Fachgruppe 01.1.4 „Komplexität“
- Direktor des Zentrums für Wissenschaftliches Elektronisches Publizieren (WEP)
- Mitglied des Aufsichtsrates des IBFI Schloss Dagstuhl

Gutachtertätigkeiten

- IWLS 2001
- STACS 2001
- Reed-Muller 2001
- DAC 2000
- DATE 2000
- IWLS 2000
- MFCS 2000
- Computational Complexity
- Formal Methode in CAD
- IEEE Transactions on CAD
- IEEE Transactions on Computers
- ACM Reviews
- Zentralblatt für Mathematik

Rustam Mubarakzjanov:

Gutachtertätigkeiten:

- IWLS 2001
- Journal of Computer and System Sciences
- Journal Theory of Computer Systems
- IWLS 2000
- MFCS 2000

Martin Mundhenk:

Veranstaltung von Tagungen und Symposien

- Veranstalter des Trierer ADiMMO Workshops der DFG Graduiertenkollegs Algorithmische Diskrete Mathematik (Berlin) und Mathematische Optimierung (Trier), 15. und 16. März 2001
- Veranstalter des 43. Workshop über Komplexitätstheorie, Datenstrukturen und Effiziente Algorithmen (Theorietag), 03. April 2001

Gutachtertätigkeiten

- Artificial Intelligence Journal
- SIAM Journal on Computing
- RAIRO Theoretical Informatics and Applications
- ICALP 2000
- MFCS 2000

Harald Sack:

Weitere Funktionen

- Geschäftsführer des Zentrums für Wissenschaftliches Elektronisches Publizieren (WEP)

Gutachtertätigkeiten

- IWLS 2001
- REED MULLER 2001
- ISMVL 2001
- IEEE Transactions on CAD
- IWLS 2000
- MFCS 2000
- DAC 2000
- MVL 2000
- STTT - Springer's Int. Journal on Software Tools for Technology Transfer
- ToC - IEEE Transactions on Computing
- TCAD - IEEE Transactions on CAD

Christian Stangier:

Gutachtertätigkeiten

- IWLS 2000
- MFCS 2000

Arno Wagner:

Gutachtertätigkeiten

- IWLS 2000
- MFCS 2000

12 Rechnerausstattung

Derzeit sind insgesamt 15 Pentium II/III -PCs und eine SUN in Betrieb, sowie eine kleinere Zahl von SUNs als Notfallreserve verfügbar. Die benutzten Betriebssysteme sind SunOS 4.1.3 U1B auf SUN-Seite sowie SuSE Linux 6.1/6.4/7.1, seltener Windows9x/2k/XP, meist bi-bootable auf derselben Maschine, für die PCs. Ein Toshiba-Notebook unterstützt die Vorführungen in Hörsälen. Als Drucker sind nun zwei HP LaserJet der 4000er Reihe sowie zwei Farbdrucker HP DeskJet 970cxi im Einsatz. Zur Unterstützung von Multimedia-Anwendungen stehen ein Multimedia-PC sowie eine WebCam, ein DVD-Laufwerk mit einer MPEG-Dekoder-Karte und ein Scanner zur Verfügung.

Zur Netzwerkinstallation ist anzumerken, daß die Professur eine modulare Vernetzung auf der Basis von *100BaseTX Ethernet* (Stern-Struktur) mit *RJ45-Anschlußdosen* aufweist. Ein Funk-LAN Access Point ELSA LANCOM Wireless IL-11 unterstützt die Funk-LAN Anbindung der Professur nach der IEEE 802.11b Norm.