Jahresbericht 1998/99 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 1998 und 1999. 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-Management Gesellschaft betreuten Instituts für Telematik e.V. Nähere Informationen hierzu können der Homepage

`http://www.ti-fgh.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 Anstöße zu möglichen Kooperationsprojekten in Forschung und Lehre sehr freuen.

Christoph Meinel Trier, im April 2000

Inhaltsverzeichnis

1 Personelle Zusammensetzung

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

- **Wissenschaftliche Assistenten**
  Dr. rer. nat. Martin Mundhenk

- **Wissenschaftliche Mitarbeiter**
  Dipl. WiMath. Jochen Bern
  Dr. rer. nat. Carsten Damm (bis 30.11.1998)
  Dr. rer. nat. Frank Recker (ab 15.04.1998)
  Dipl. Inform. Harald Sack (ab 01.03.1999)
  RNDr. Anna Slobodova CSc. (bis 31.07.1998)

- **Wissenschaftliche Angestellte in Drittmittelprojekten**
  Dr. rer. nat. Stasys Jukna (bis 31.10.1999)
  Dr. rer. nat. Carsten Damm (ab 01.03.1999)

- **Wissenschaftliche Praktikanten**
  Dipl. Inform. Harald Sack (bis 28.02.1999)

- **Sekretärinnen**
  Ingeborg Weitzel (bis 30.04.98)
  Lilo Helbig (ab 01.05.98)

- **Stipendiaten**
  Dipl. Inform. Christian Stangier (bis 30.11.1999)
  Dipl. Inform. Klaus Schwettmann (bis 31.05.1998)
  Stipendiaten des Graduiertenkollegs „Mathematische Optimierung".

- **Praktikanten**
  Khaldoon Moosa Ahmed Mhaidat, University of Science and Technology, Irbid (Jordanien)
  (01.07.1998 - 31.08.1998)
  Anderson Luiz de Arujo Lima, Faculdades Positivo, Curitiba (Brasilien)
  (01.09.1998 - 30.10.1998)
  Edith Maria Teixeira Moraes, Faculdade de Administracao e Informatica, Florianopolis (Brasilien)
  (01.09.1999 - 30.11.1999)
  Maja Milicic, Faculty of Mathematics, Belgrad (Jugoslawien)
  (20.10.1999 - 23.12.1999)

- **Wissenschaftliche Hilfskräfte**
  Gerstenmayer, Thomas (ab 01.11.1998)
  Leiß, Knut (01.05. bis 31.07.1998)
  Licht, Wolfgang (bis 21.02.1998)
  Sander, Marietta (01.05. bis 31.07.1999)
  Schommer, Michael (ab 01.10.1998)
  Dipl. Inform. Christian Stangier (ab 01.12.1999)

2 Mit dem Lehrstuhl personell verbundene Einrichtungen

2.1 Zentrum für Wissenschaftliches Elektronisches Publizieren - WEP

Das neue Zentrum für Wissenschaftliches Elektronisches Publizieren an der Universität Trier ist eine fachübergreifende Einrichtung, die als Informationsbasis und Koordinationszentrum für 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. Darüberhinaus 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

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, e.V.

Das zum 01.01.1998 gegründete Forschungs- und Entwicklungsinstitut für Telematik ist aus dem Trierer Bereich des Instituts für Techno- und Wirtschaftsmathematik, dem ITWM-Trier, hervorgegangen. Es hat die Rechtsform eines eingetragenen, gemeinnützigen Vereins und wird von der Fraunhofer Management Gesellschaft in München betreut, über die auch eine enge Verbindung zu den Instituten der Fraunhofer-Gesellschaft besteht. Leiter des Instituts ist Univ.-Prof. Dr. sc. 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. Zur Zeit werden Projekte im Auftrag weltbekannter Konzerne, wie zum Beispiel Siemens und Dresdner Bank, bearbeitet, aber auch für kleine und mittelständische Firmen, Krankenhäuser und Banken in Rheinland-Pfalz und im benachbarten Luxemburg wird geforscht und entwickelt.

Die am Institut für Telematik bearbeiteten Forschungs- und Entwicklungsaufträge sind im Schnittbereich von *Tele*kommunikation und Infor*matik* angesiedelt. Hier kommt, neben dem Ausbau der Telekommunikation und der Bereitstellung von leistungsfähigen Übertragungskapazitäten, der Schaffung telematischer Systeme eine besondere Schlüsselstellung zu. Ohne leistungsfähige Redaktionssysteme zur multimedialen Aufbereitung vorhandener Informationen und ohne Navigationssysteme zur Erschließung des in den Datennetzen verfügbaren Wissens können die Herausforderungen der Zukunft beim Übergang von der Industriegesellschaft zur Wissensgesellschaft nicht gemeistert werden. 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 beschäftigt sich mit folgenden Kompetenzbereichen, in denen eine Reihe von Projektfeldern bearbeitet werden:

- Internet / Intranet
- Elektronisches Publizieren
- Telemedizin
- Sicherheit in offenen Datennetzen
- Systementwurf und -analyse

Weitere Informationen können im WWW gefunden werden unter der URL

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

3 Aktivitäten in der Lehre: Vorlesungen, Übungen und Seminare

Sommersemester 1998

Diskrete Strukturen und Logik II (2+2 SWS)
Vorlesung: Martin Mundhenk
Übung: Frank Recker

siehe Wintersemester 1999/2000

Algorithmen und Datenstrukturen (Informatik II) (2+2 SWS)
Übung: Frank Recker

Ihre zentrale Bedeutung lassen Algorithmen zum Hauptuntersuchungsgegenstand und zum einigenden Konzept der Informatik werden. Insbesondere werden Algorithmen unter den folgenden Gesichtspunkten studiert:

- Wie entwirft man gute Algorithmen?
- Wie werden Algorithmen beschrieben?
- Welchen Zeit- und Speicherplatzbedarf benötigt die Abarbeitung eines Algorithmus?

Die Vorlesung ist diesen und den damit zusammenhängenden Fragen gewidmet. Sie will in das Gebiet des Entwurfs und der Analyse von effizienten Algorithmen und Datenstruktur einführen und zu fundierten eigenen Aktivitäten befähigen. Insbesondere das letztgenannte Anliegen gebietet mathematische Strenge in der Darstellung, ohne die das Ausgeführte nicht nachvollziehbar wäre.

Randomisierte Algorithmen (2+2 SWS)
Vorlesung und Übung: Carsten Damm

Ein randomisierter Algorithmus ist ein Algorithmus, der bei der Abarbeitung „würfeln darf“. Ein Beispiel soll die grundlegende Idee erläutern:

Es ist mühsam, allein durch elementare algebraische Umformungen nachzuweisen, daß zwei Polynomausdrücke $P(x_1,\dots,x_n)$ und $Q(x_1,\dots,x_n)$ sehr hohen Grades identisch sind. Ein probabilistischer Ansatz führt jedoch sehr schnell zum Ziel: es werden die Werte der Polynome $P(x_1,\dots,x_n)$ und $Q(x_1,\dots,x_n)$ an einer *zufällig geratenen* Stelle $(a_1,\dots,a_n)$ berechnet. Ist $P(a_1,\dots,a_n) \neq Q(a_1,\dots,a_n)$, so gilt natürlich $P \not\equiv Q$. Anderenfalls ist entweder $P \equiv Q$ oder es wurde zufällig eine Nullstelle des Polynoms $R = P - Q$ geraten, was jedoch unwahrscheinlich ist, denn Nullstellen sind „selten“. Wenn bei wiederholten unabhängigen Versuchen nach diesem Prinzip stets gleiche Ergebnisse entstehen, so kann man davon ausgehen, daß tatsächlich $P \equiv Q$ gilt: Die Fehlerwahrscheinlichkeit kann (je nach Anzahl der Versuche) beliebig klein gemacht werden, z.B. kleiner als die Wahrscheinlichkeit, daß ein Hardwarefehler ein falsches Ergebnis verursacht.

Probabilistische Algorithmen zeichnen sich durch Effizienz, Einfachheit und mathematische Eleganz aus. Daß das Herangehen keineswegs nur theoretischer Natur ist, beweist die erfolgreiche Anwendung derartiger Verfahren beim Testen digitaler Schaltkreise. Auch bei der Implementation von Public-Key-Kryptosystemen sind probabilistische Algorithmen unerläßlich.

Neben Verfahren zum Entwurf und zur Analyse probabilistischer Algorithmen, sowie der Diskussion verschiedenster Anwendungen, werden auch Derandomisierungsmethoden vorgestellt.

Kryptographie mit Java (4 SWS)
Praktikum: Carsten Damm, Frank Recker

Die mathematischen Grundlagen der Kryptographie sind ein faszinierendes Forschungs- und Lehrgebiet. Die Schwierigkeiten der praktischen Umsetzung beginnen dann, wenn man die Algorithmen zuverlässig, flexibel und benutzerfreundlich implementieren will. Die Programmiersprache Java mit ihren zahlreichen Bibliotheken bietet Möglichkeiten dies sehr elegant zu tun. Genau dieses Vorhaben wollen wir im Praktikum angehen. Idealziel ist die Schaffung eines erweiterbaren *Krypto-Kit* zum Erproben kryptographischer und einfacher kryptanalytischer Algorithmen über das Netzwerk.

Gleichberechtigte Ziele des Praktikums sind:

- Vertiefung kryptographischer Kenntnisse,
- Erwerb von Team-Programmierfähigkeiten,
- Bearbeitung eines größeren Projekts mit Java und
- Kennenlernen der Netzwerkfähigkeiten und der Sicherheitsphilosophie von Java.

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.

Sequentielle Verifikation digitaler Schaltkreise (2SWS)
Seminar: Harald Sack

Digitale Schaltkreise sind mittlerweile zu einem allgegenwärtigen und unverzichtbaren Bestandteil unseres täglichen Lebens geworden. Vom Toaster, dem Anrufbeantworter, über das Auto, das z.B. 1995 bereits durchschnittlich mit ca. 50 Mikroprozessoren ausgestattet war, über den PC bis hin zur Grußpostkarte. Dabei wächst die Komplexität der Schaltkreise kontinuierlich von Jahr zu Jahr und immer schwieriger wird die mithin lebenswichtige Aufgabe, deren Korrektheit zu garantieren. In das Bewußtsein der Öffentlichkeit gerückt ist dieses Problem spätestens 1995 mit dem *Pentium-Bug*: Eine Tabelle des seit vielen Jahren bekannten SRT-Divisionsschaltkreises (benannt nach den Initialen der drei Erfinder) enthielt im Fall der Pentium-Implementation inkorrekte Einträge. Der öffentliche Druck nach Bekanntwerden dieses Fehlers veranlaßte Intel zu der bis dahin größten Rücknahmeaktion in der Geschichte der Halbleiterindustrie, deren Kosten sich auf schätzungsweise 475 Millionen Dollar beliefen. Diese hohen Folgekosten haben das Gebiet der Hardwareverifikation zu einem der wesentlichen Schritte innerhalb des Entwurfsprozesses werden lassen. Von besonderer Bedeutung ist dabei die Verifikation sequentieller Systeme. Die meisten Schaltungen lassen sich auf logischer Ebene durch ein sequentielles System beschreiben. Das Seminar behandelt dabei folgende Themen:

- Werkzeuge zur effizienten Analyse von sequentiellen Systemen:
  Ordered Binary Decision Diagrams (OBDDs) *effiziente Manipulation von Finite State Machines* (FSMs).
- Erreichbarkeitsanalyse:
  Transitionsrelationen, Partitionierte Transitionsrelationen, State-of-the-art Techniken zur Effiziensssteigerung.
- Symbolic Model Checking:
  Computational Tree Logic (CTL), Implementierungen.

Theorie-AG (2 SWS)
Seminar: Martin Mundhenk

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 1998/99

Diskrete Strukturen und Logik I (2+2 SWS)
Vorlesung: Christoph Meinel
Übung: Frank Recker

siehe Wintersemester 1999/2000

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

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.

CAD-Logiksynthese und -optimierung (4+2 SWS)
Vorlesung: Christoph Meinel
Übung: Frank Recker

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.

Mehrwertige Logik (2+2 SWS)
Vorlesung und Übung: Harald Sack

Die Ursprünge der mehrwertigen Logik lassen sich bis zurück in die Antike verfolgen. Schon die griechische Philosophie beschäftigte sich mit Fragen der Erfüllbarkeit logischer Aussagen, wobei die Diskussion dieser Fragen das Problem aufwarf, ob die Antwort notwendigerweise auf eine der beiden Alternativen *wahr* oder *falsch* zu beschränken sei. Die klassische, zweiwertige Logik schließt diese Möglichkeit über das Gesetz des ausgeschlossenen Dritten - *Tertium non datur* - aus und läßt somit die Aussage $(a+\overline{a})$ als Tautologie gelten. *Jan Lukasiewicz* (1878 - 1956) führte das erste nicht-klassische logische Kalkül ein und aufbauend auf seine Arbeit über *dreiwertige Logik* entstanden weitere nicht-klassische Logiken, wie *modale Logik, probabilistische Logik*, oder auch *Fuzzy Logik*. Diese Vorlesung beschäftigt sich nach einer kurzen, formalen Einführung in die Theorie der mehrwertigen Logiken in der Hauptsache mit aktuellen Anwendungen derselben, insbesondere in den Bereichen *Logic Design* und *Logic Synthesis*, wie z.B.*Symbolic Model Checking* und *Computational Tree Logic* (CTL), *Multi-Valued Decision Diagrams* (MDDs) und deren Anwendung, Datenbanken, Wissensrepräsentation, sowie Anwendungen aus dem Bereich der Fuzzy Logik.

Kombinatorik für Informatiker (2+2 SWS)
Vorlesung und Übung: Stasys Jukna

Die Vorlesung ist als Einführung in die Extremale Kombinatorik gedacht. In allgemeinen fragt man, wie viele Teile ein Objekt (Graph, Matrix, geometrische Figur, usw.) haben muß oder kann, um (ohne irgendetwas mehr über diese Menge zu wissen!) sicherzustellen, daß das Objekt eine spezielle Konfiguration enthält oder vermeidet. Zum Beispiel:

- Wie viele Kanten kann ein Graph ohne Dreiecke höchstens haben?
- Wir färben die 0,1-Vektorenlänge n und wollen, daß jedes Paar von Vektoren mit Hamming'scher Distanz d verschiedene Farben bekommt. Wie viele Farben brauchen wir dann mindestens?

Solche und ähnliche Fragen treten in verschiedenen Gebieten der Informatik (Analyse von Algorithmen, Kodierungstheorie, Komplexitäatstheorie, usw.) und der Diskreten Mathematik oft auf. In der Vorlesung werden die wichtigsten Methoden und Ideen behandelt, die solche Probleme lösen:

1. Klassische Methoden: Pigeonhole-Prinzip, Inklusion-Exklusion, Counting Tricks, usw.
2. Lineare-Algebra-Methode: Unabhängigkeits- Prinzip, Dimensions-Argumente, usw.
3. Probabilistische Methode: Zerstörungs-Methode, Lovasz-Sieb, Entropie, usw.

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

siehe Sommersemester 1998.

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

siehe Sommersemester 1998.

Theorie-AG (2SWS)
Martin Mundhenk

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 1999

Diskrete Strukturen und Logik II (2+4 SWS)
Vorlesung: Christoph Meinel
Übung: Frank Recker

siehe Wintersemester 1999/2000

Technische Grundlagen des elektronischen Publizierens (4+2 SWS)
Vorlesung: Christoph Meinel
Übung: Harald Sack

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, CSS, XML, HTTP-Server*). Eine Vermittlung dieser Grundlagen ist das Ziel dieser Vorlesung.

Graphen: Theorie und Algorithmen(4+2 SWS)
Vorlesung: Martin Mundhenk
Übung: Frank Recker

Graphentheorie ist ein schöner Spielplatz zur Entdeckung von Beweistechniken in der diskreten Mathematik. In dieser Vorlesung werden Teile der Graphentheorie vorgestellt, die für Informatiker von besonderem Interesse sind. Das ist einerseits die algorithmische Graphentheorie. Dort können aus Beweisen zur Eigenschaft von Problemen recht direkt Algorithmen zur Problemlösung gewonnen werden. Dazu werden im wesentlichen effiziente Graph-Algorithmen vorgestellt. Andererseits wird auf Graphenprobleme eingegangen, für die keine effizienten Lösungen bekannt sind und die in der Komplexitätstheorie eine wichtige Rolle spielen. Ein Schwerpunkt wird die Approximation von Lösungen solcher Probleme sein.

Bei den algorithmisch betrachteten Problemen geht es u.a. um Durchlaufverfahren in Graphen, das Finden von Wegen und aufspannenden Bäumen, Matchings, Flußprobleme, Zusammenhangsprobleme, planare Graphen, Rundreiseprobleme, Färbungsprobleme und Cliquenprobleme.

Komplexität Boolescher Funktionen (2+2 SWS)
Vorlesung und Übung: Stasys Jukna

Jeder Algorithmus hat seine Komplexität (Laufzeit, Anzahl von Befehlen order Gattern, Speicherplatz, usw.). In der Praxis will (oder sogar muss) man einen Algorithmus für eine vorgegebene Funktion von möglichst geringer Komplexität entwerfen. Leider geht es nicht immer (oder schlimmer: fast nie), und man fragt dann – warum? Bin ich nicht klug genug, um ein guten Algorithmus zu finden, oder ist die Funktion selbst daran Schuld, d.h. ist sie selbst inhärent schwer? Um dies zu beantworten, muss man beweisen, dass es überhaubt keinen guten Algorithmus für die gegebene Funktion gibt.

Das sind die Kernfragen des *Untere-Schranken Problems*, das eines der Grundprobleme der Informatik und - weil es um Beweise der inhärenten Schwierigkeit von Funktionen geht - auch eine der zentralen Fragen der gesamten Mathematik ist. Die berühmte Frage, ob $\mathbf{P} = \mathbf{NP}$, ist nur ein Teil dieses Problems. Auch für praktische Anwendungen sind untere Schranken von großer Bedeutung. In der Vorlesung werden die wichtigsten Berechnungsmodelle (decision trees, branching programs, combinational circuits, Boolean formulas, communication protocols) untersucht. Das Hauptziel der Vorlesung aber ist, die neuesten Untere-Schranken-Methoden kennenzulernen.

Evolutionäre Algorithmen (2 SWS)
Seminar: Harald Sack

Im Prozeß des VLSI-CAD fallen schwierige Optimierungsprobleme zur Lösung an, die bislang unter Einsatz vielfältiger Methoden bearbeitet wurden. Während einige dieser Methoden mittlerweile zum Standard gehören wurden andere, wie z.B. auch die evolutionären Algorithmen lange Zeit ignoriert. Seit einiger Zeit jedoch erfahren diesen Methoden, deren Strategien sich an der Natur orientieren, gesteigerte Aufmerksamkeit. Das Seminar soll einen Überblick über die Anwendung evolutionärer Strategien zur Optimierung des IC-Design und IC-Verifikationsprozesses geben, wobei auf einzelne Verfahrensschritte wie *Logiksynthese, Boolean Mapping* oder *Testing* speziell eingegangen wird. Die Komplexität evolutionärer Optimierungsstrategien soll dabei mit herkömmlichen Methoden in Vergleich gesetzt werden, wobei ihr Einsatz in Verbindung mit Binären Entscheidungsdiagrammen (OBDDs) besondere Berücksichtigung finden soll.

Theorie-AG (2SWS)
Martin Mundhenk

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

Winterersemester 1999/2000

Diskrete Strukturen und Logik (4+2 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.

Binäre Entscheidungsgraphen (4+2 SWS)
Vorlesung: Christoph Meinel
Übung: Harald Sack

Binäre Entscheidungsdiagramme haben eine große Bedeutung erlangt als Datenstruktur für Boolesche Funktionen (bekannt auch als logische Funktionen oder Schaltfunktionen). Ursache für diese Bedeutung ist der relativ gute *Trade–off* zwischen speichereffizienter Repräsentation und zeiteffizienter Ausführbarkeit wichtiger Grundoperationen wie Komposition und Äquivalenztest. Binäre Entscheidungsdiagramme haben sehr zahlreiche Anwendung, z.B. in verschienenden Gebieten des computerunterstützten Schaltkreisentwurfs, der kombinatorischen Optimierung oder der Verifikation logischer Systeme.

Die Vorlesung soll eine systematische Einführung der Datenstruktur der binären Entscheidungsdiagramme und eine breite Übersicht über die verschiedenen Anwendungen bieten. Dabei wird besonderer Wert auf eine theoretisch fundierte Analyse der Komplexität der einzelnen Grundaufgaben der Booleschen Manipulation sowie auf mathematisch fundierte Aussagen zur Repräsentationskomplexität gelegt.

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

siehe Wintersemester 1998/1999.

Technische Grundlagen des Elektronischen Publizierens II (2+2 SWS)
Vorlesung und Übung: Harald Sack

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, CSS, XML, HTTP-Server). Eine Vermittlung dieser Grundlagen ist das Ziel dieser Vorlesung, die an die Einführungsveranstaltung *Technische Grundlagen des Elektronischen Publizierens im Internet* im Sommersemester 1999 nahtlos anschließt. Neben einer ausführlichen Behandlung von Dokumentenkonzepten im WWW, wie *HTML*, *XML*, und *cgi* wird sich die Vorlesung mit dem Betrieb von HTTP-Servern und als zweitem Schwerpunkt dem wissenschaftlichen elektronischen Publizieren im Internet zuwenden. Themen sind dabei u.a. Möglichkeiten, Fachpublikationen über das WWW verfügbar zu machen, sowie die elektronische Einreichung und Evaluierung von Konferenz- und Zeitschriftenbeiträgen.

Authentifizierung und digitale Signaturen (2 SWS)
Seminar: Frank Recker

In dem Seminar werden zwei Gebiete der moderneren Kryptographie untersucht:

- *Authentifizierung*: Authentifizierung bedeutet, die Identität einer Person (oder eines Computers) zweifelsfrei festzustellen. Dies geschieht häufig dadurch, daß die Person ein Geheimnis präsentiert, das nur ihr bekannt ist. Dies kann zum Beispiel ein Passwort sein. Die Sicherheit dieses Systems beruht auf der Annahme, daß das Geheimnis nur dem rechtmässigen Besitzer bekannt ist. Das zur Zeit sicherste Konzept hierfür bieten die *Zero-Knowledge Proof Systems.* Mit ihrer Hilfe kann eine Person beweisen, daß sie ein Geheimnis kennt, ohne das Geheimnis selbst zu verraten.

- *Digitale Signaturen*: Elektronisch gespeicherte Daten können häufig mit geringem Aufwand verändert werden. Daher werden Verträge zwar auf einem Computer erstellt, aber dann ausgedruckt und *auf dem Papier* unterschrieben. Dieser Umweg ist bei Verträgen, die auf rein elektronischem Weg abgeschlossen werden, nicht mehr möglich. *Digitale Signaturen* bieten eine Lösung für dieses Problem. Wir werden im Seminar sowohl die dafür notwendigen kryptographischen Grundlagen, als auch die bereits vorhandenen Anwendungen besprechen.

Theorie-AG (2 SWS)
Martin Mundhenk

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

4 Dissertationen und Habilitationen

4.1 Dissertationen

Dipl. Inform. Thorsten Theobald

Transformation Techniques for Decision Diagrams in Computer-Aided Design

Betreuer:

- Prof. Dr. Christoph Meinel, Universität Trier

Gutachter:

- Prof. Dr. B. Becker, Universität Freiburg
- Prof. Dr. Ch. Meinel, Universität Trier
- Prof. Dr. H. Seidl, Universität Trier

Datum der Disputation: 19. Dezember 1997

Abstract: Ordered binary decision diagrams (OBDDs), which have been introduced in 1986, provide the state-of-the-art data structure for representing Boolean functions. Within the last decade, they have found numerous applications, in particular in computer-aided design of integrated circuits (CAD for VLSI) and in formal verification. OBDDs represent Boolean functions by means of a decision process in a rooted directed acyclic graph.

As the running times of all algorithms on OBDDs are correlated to the size of the input graphs and of the resulting graphs, it is an important task to optimize the size of these graphs. This topic has become even more serious by the observation that for a substantial number of OBDD-based applications the choice of the optimization technique is the deciding factor whether a computation succeeds or not. The main optimization parameter of OBDDs is the underlying variable order. Hence, many research efforts have been spent to efficient optimization algorithms for constructing good variable orders. Unfortunately, there are many important applications, in particular in the analysis of finite automata/finite state machines, where this optimization technique reaches its limits.

In this thesis, we propose and discuss new optimization approaches for decision diagrams. Our central topic is the use of transformation techniques to reduce the size of OBDDs. In particular, we focus on two concepts that are related to each other.

Encoding transformations: We systematically analyze and exploit the fact that in the context of finite state machines the state encoding can be used as an additional optimization parameter.

Domain transformations: Recently, the concept of domain transformations has been proposed to enlarge the optimization space of variable ordering. We characterize suitable classes of transformations and show how these constructions can be well integrated into existing algorithms for finding good variable orders. Here, it turns out that the class of linear transformations is of particular importance.

Within this framework, we cover a variety of aspects: from theoretical investigations over optimization algorithms, fully automated techniques, implementation issues of efficient realizations, up to applications in VLSI design. Our presentation shows that the proposed transformation techniques significantly enrich the tool set of Boolean manipulation in computer-aided circuit design.

4.2 Habilitationen

Dr. Stasys Jukna

Combinatorics of Finite Computations - The Lower Bounds Problem

Gutachter:

- Prof. Dr. D. Baum, Universität Trier
- Prof. Dr. Ch. Meinel, Universität Trier
- Prof. Dr. I. Wegener, Universität Dortmund

Datum des Habilitationsvortrages: 07. Juli 1999

Abstract: In this thesis we explore a central theme of the theory of computing: the study of the inherent complexity of computational tasks via combinatorial models such as decision trees, branching programs, Boolean circuits and communication games. The basic question is to discover those combinatorial properties of Boolean functions which make them hard for a particular model. This is known as *Lower Bounds Problem*, and lies on the core of the whole Theory of Computational Complexity, the famous P versus NP problem being its special case. Despite of great efforts of many mathematicians for now more that 30 years, the solution is not even in sight. This shows that our understanding a *computation* as such is still very limited.

A new direction in the 1980's brought on a burst of activity. By placing sufficiently strong restrictions on the class of circuits it became possible to prove strong lower bounds. The first results of this kind were obtained by Tseitin (1967) for the size of regular resolution proofs, by Pulatov (1977) for contact schemes without null-chains, by Tkachev (1980), Furst, Saxe and Sipser (1981) and Ajtai (1983) for the bounded depth circuits, by Wegener (1984) and Žák (1984) for read-once branching programs, by Razborov (1985a) and Andreev (1985) for monotone circuits, by Haken (1985) for the resolution proofs. Thank these (and other) results our mathematical equipment to attack the unrestricted case was enriched by several new proof techniques, like the *method of random restrictions* (for bounded depth circuits), the *method of approximations* (for monotone circuits), different realizations of *cut-and-paste principle* (for branching programs), the *bottlenecks counting* argument (for resolution), the *fusion method* (for monotone circuits and span programs), the *method of finite limits* (for small depth circuits and monotone circuits), the *entropic approach* (for branching programs), and others.

In this thesis we summarise the contribution of the author to this line of research and, in particular – to the development of the last five proof techniques, mentioned above. We consider several basic models of computation – decision trees, restricted branching programs, monotone circuits, depth-3 circuits, resolution, one-way communication protocols – and prove exponential lower bounds for them. In these proofs we introduce several new arguments and isolate some (previously hidden) combinatorial properties of Boolean functions, which make them hard to compute. These properties give us some tractable lower bounds *criteria* for a particular model.

Shortly, our main results are the following.

1. Proof that NP$\neq$co–NP in the context of decision trees and read-once branching programs. This resolves a long–standing problem about the connection between decision tree, CNF and DNF *size*, and contrasts with the well-known fact (established independently by several groups of authors 10 years ago) that if we consider the *depth* instead of the size, then NP=co–NP

2. Combinatorial lower bounds *criteria* for different types of ordinary branching programs (b.p.) – read-once b.p., $(1,+s)$-b.p., syntactic read-k times b.p. – as well as for some of their semantic counterparts corresponding to *corrupting* Turing machines. Proof that the characteristic functions of some explicit linear codes are hard in all these models of b.p. At present, these results are the best for reading-restricted branching programs and lie exactly at the border of our current knowledge about branching programs.

3. New *information-theoretic* approach to proving lower bounds on the size of branching programs, based on measuring the entropy (or uncertainty about the output) at different stages of individual computations. Proof of Kraft-McMillan type inequalities for the average entropy of computations.

The approach is demonstrated by the proof that some explicit Boolean functions (including the Clique and the Pointer functions) cannot be computed by small branching programs in a "gentle" way. This contrasts with the (also proved in the thesis) fact that some Boolean functions – like the characteristic functions of linear codes – which are hard for all previously considered restricted models of branching programs, can be easily computed in a gentle way. These results imply that our (entropic) lower bounds argument can (at least in principle) capture those combinatorial characteristics of Boolean functions, which were missed by the previous arguments.

4. First general combinatorial lower bounds criterion for *monotone circuits* with large fanin Boolean and real-valued gates. This resolves the problem raised by Razborov at the Congress of Mathematicians (Berkeley, 1986). Despite its extreme simplicity, the criterion yields (in a uniform and easy way) *new* exponential lower bounds. In particular, we use it to prove a (somewhat surprising) fact that – unlike for the Boolean case, where monotone circuits are exponentially weaker than non-monotone ones – the power of monotone real circuits and non-monotone Boolean circuits is *incomparable.*

5. A *top-down* lower bounds method for depth-3 circuits (with AND, OR, NOT and threshold gates) based on finite limits. Optimal lower bounds for Parity and Majority functions via simple combinatorial arguments. First exponential gap between Σ_3 and Π_3 circuits.

6. Exponential lower bounds on the size of *semantic Resolution* proofs. This system (introduced by Krajiček) essentially extends the standard Resolution, and no lower bounds were known for it. Our bound is quite general and applies to different combinatorial principles, including the generalized pigeonhole principle PHP_n^m and well-known blocking set principles for finite projective and affine planes.

7. Observation that optimal circuits are instable not only w.r.t. *deletion* but also w.r.t. *renaming* of gates (the size in this case remains the same!). Proof that for some explicit function, their optimal circuits either must be large or must have very short null chains. This, in particular, has led to exponential bounds for formulas without null chains computing, so-called, *semi-slice* functions – a case where previous known arguments have failed.

8. Easy lower bounds argument for best partition 2-party communication games, based on the *term-rank* of communication matrices. This argument was published already in 1987, but remained unknown for researchers in West.

9. Matching upper and lower bounds on the conservative one-way *multiparty* communication complexity of Pointer Jumping function. Although "conservativeness" is rather severe restriction, these results first braked down the mysterious barrier of $k = \log n$ players in the seminal lower bound $\Omega(n/2^k)$ due to Babai, Nisan and Szegedy: our bound is non-trivial up to $k = n^{1/3-\epsilon}$ players.

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 logische 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 darüberhinaus 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 logische Funktionen** wurden Datenstrukturen für die Repräsentation und Bearbeitung von logischen (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 NP^{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. 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 bei den *Web-Seiten* des *WWW* kommen im Vergleich zu papierbasierten Publikationen 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.

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, die Abwicklung der STACS 2001 ist in Vorbereitung.

3.) Das im November 1997 offiziell eröffnete *Zentrum für Wissenschaftliches Elektronisches Publizieren (WEP)* (`http://www.wep.uni-trier.de/`) hat 1998 eine Reihe von Vorträgen und Kolloquien veranstaltet und auch erste fachbereichsübergreifende Projekte initiiert.

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.

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 Drittmittelprojekte am Lehrstuhl

Mitträger des Graduiertenkollegs
„Mathematische Optimierung" an der Universität Trier
Förderer: Deutsche Forschungsgemeinschaft – DFG
Förderzeitraum: seit 01.04.1995

Entwicklung und Anwendung der Fusionsmethode für die Ableitung unterer Schranken in der Berechnungskomplexität

Förderer: Deutsche Forschungsgemeinschaft – DFG
Förderzeitraum: 1995 - 1999

Efficient Data Structures for Computer Aided Design

Förderer: Deutscher Akademischer Austauschdienst, NSF-Programm – DAAD
Förderzeitraum: 1997 - 1999

High-level Beschreibung und Verifikation komplexer digitaler Systeme

Förderer: Deutscher Akademischer Austauschdienst, Vigoni-Programm – DAAD
Förderzeitraum: 1997 1998

Control in Stochastic Domains: Complexity and Solutions

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

Betriebsumgebung für ECCC

Förderer: Institut für Telematik
Förderzeitraum: 1998 - 02/1999

Linear-Algebraische Berechnungsmodelle für Boolesche Funktionen und ihre Anwendung

Förderer: Deutsche Forschungsgemeinschaft – DFG
Förderzeitraum: 1999 - 2001

7 Herausgeberschaft

7.1 "Electronic Colloquium on Computational Complexity — ECCC"

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

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

7.2 WWW–Site der STACS Symposium on Theoretical Aspects of Computer Science

Im Frühjahr 1999 fand in Trier das *Symposium on Theoretical Aspects of Computer Science*, die alljährlich stattfindende größte europäische Konferenz im Bereich der Theoretischen Informatik statt. Eine Website mit allen Informationen rund um diese Konferenz, sowie Software, die die Abwicklung und das Management der Veranstaltung unterstützt, angefangen von der Einreichung wissenschaftlicher Arbeiten, der Begutachtung von Arbeitung durch das Programm-Komitee, bis hin zur Buchung von Hotelzimmern wurde vom Lehrstuhl entwickelt und gepflegt. Die Software wird auch in Zukunft von nachfolgenden Konferenzen genutzt werden.

`http://stacs.uni-trier.de/STACS99/`

7.3 WWW–Site der GI–Fachgruppe 0.1.4 „Komplexität"

Regelmäßig werden von Christoph Meinel, dem Sprecher der GI-Fachgruppe 0.1.4 „Komplexität", und Jochen Bern aktualisierte WWW–Seiten mit Informationen zu Konferenzen, Theorietagen, Graduiertenkollegs, Sommerschulen, Stellenangeboten etc. veröffentlicht.

`http://www.informatik.uni-trier.de/GI/FG-014/`

8 Veröffentlichungen

8.1 Bücher

Ch. Meinel, M. Morvan, D. Krob:
15th Annual Symposium on Theoretical Aspects of Computer Science, STACS'98
Conference proceedings (Februar 1998, Paris),
LNCS 1373, ISBN Nr. 3-540-64230-7

Abstract: STACS has become one of the most important annual meetings in Europe for the theoretical computer science community. It covers a wide range of topics in the area of foundations of computer science. For STACS'98, 155 submissions from all over the world and most European countries were received, almost all in electronic form, thanks to *Jochen Bern* in Trier, who made the electronic procedure possible and so efficient. The submitted papers address basic problems from many areas of computer science: algorithms and data structures, automata and formal languages, complexity, and logic. The sessions of the conference have been chosen to represent these main topics.

Ch. Meinel, T. Theobald:
Algorithms and Data Structures in VLSI Design:
OBDD - Foundations and Applications
Springer-Verlag, Heidelberg, 1998, ISBN Nr. 3-540-64486-5

Abstract: One of the main problems in chip design is the huge number of possible combinations of individual chip elements, leading to a combinatorial explosion as chips become more complex. New key results in theoretical computer science and in the design of data structures and efficient algorithms can be applied fruitfully here. The application of ordered binary decision diagrams (OBDDs) has led to dramatic performance improvements in many computer-aided design projects. This textbook provides an introduction to the foundations of this interdisciplinary research area with an emphasis on applications in computer-aided circuit design and formal verification.

Ch. Meinel, T. Theobald:
Algorithmen und Datenstrukturen im VLSI-Design: OBDD, Grundlagen und Anwendungen
Springer-Verlag, Heidelberg, 1998, ISBN Nr. 3-540-63869-5

Abstract: Eines der Hauptprobleme beim Chipentwurf besteht darin, daß die Anzahl der zu bewältigenden Kombinationen der einzelnen Chipbausteine ins Unermeßliche steigt. Hier hat sich eine sehr fruchtbare Verbindung zu einem Kerngebiet der Theoretischen Informatik, dem Gebiet des Entwurfs von Datenstrukturen und effizienten Algorithmen, herstellen lassen: Die Verbindung besteht im Konzept der geordneten binären Entscheidungsgraphen, das in zahlreichen CAD-Projekten zu einer beträchtlichen Leistungssteigerung geführt hat. Die Autoren stellen die Grundlagen dieses interdisziplinären Forschungsgebiets dar und behandeln wichtige Anwendungen aus dem rechnergestützten Schaltkreisentwurf.

8.2 Buchbeiträge

Martin Mundhenk, Anna Slobodová:
Optimal non-approximability of Max-Clique.
In: Mayr, Prömel, Steger (eds.): Lectures on proof verification and approximation algorithms, Mayr, Prömel, Steger (Hrsg.) (LNCS 1365: 235–248, Springer Verlag 1998)

Abstract: We present a proof of Håstad (1996) about the non-approximability of the Max-Clique problem.

8.3 Veröffentlichungen in Zeitschriften

C. Damm, S. Jukna, J. Sgall:
Some Bounds on Multiparty Communication Complexity of Pointer Jumping.
Computational Complexity 7, 109–127, 1998

Abstract: We introduce the model of *conservative one-way* multiparty complexity and prove lower and upper bounds on the complexity of *pointer jumping*.
The pointer jumping function takes as its input a directed layered graph with a starting node and k layers of n nodes, and a single edge from each node to one node from the next layer. The output is the node reached by following k edges from the starting node. In a conservative protocol the ith player can see only the node reached by following the first $i-1$ edges and the edges on the jth layer for each $j > i$. This is a restriction of the general model where the ith player sees edges of all layers except for the ith one. In a one-way protocol, each player communicates only once in a prescribed order: first Player 1 writes a message on the blackboard, then Player 2, etc., until the last player gives the answer. The cost is the total number of bits written on the blackboard.
Our main results are the following bounds on k-party conservative one-way communication complexity of pointer jumping with k layers:

(1) A lower bound of order $\Omega(n/k^2)$ for any $k = O(n^{1/3-\varepsilon})$.

(2) Matching upper and lower bounds of order $\Theta(n \log^{(k-1)} n)$ for $k \leq \log^* n$.

C. Damm:
Depth-efficient Simulation of Boolean Semi-unbounded Circuits by Arithmetic Ones.
Information Processing Letters, 69 , 175-179, 1999

Abstract: We prove by a randomized construction that depth d semi-unbounded *Boolean* circuits can be simulated by depth $2d + O(\log d + \log n)$ semi-unbounded *arithmetic* circuits, regardless of the size. This is an improvement on a similar construction by Gál that achieves depth $3d + O(\log s + \log n)$, where s is the size of the original circuit.

S. Jukna and A. Razborov:
Neither reading few bits twice nor reading illegally helps much, Discrete Applied Mathematics, **85**:3, pp. 223–238, 1998.

Abstract We first consider so-called $(1, +s)$-*branching programs* in which along every consistent path at most s variables are tested more than once. We prove that any such program computing a characteristic function of a linear code C has size at least $2^{\Omega(\min\{d_1,\ d_2/s\})}$, where d_1 and d_2 are the minimum distances of C and its dual $C^{\perp}$. We apply this criterion to explicit linear codes and obtain a super-polynomial lower bound for $s = o(n/\log n)$.
Then we introduce a natural generalization of read-k-times and $(1, +s)$-branching programs that we call *semantic branching programs*. These programs correspond to *corrupting* Turing machines which, unlike eraser machines, are allowed to read input bits even *illegally*, i.e. in excess of their quota on multiple readings, but in that case they receive in response an unpredictably corrupted value. We generalize the above mentioned bound to the semantic case, and also prove exponential lower bounds for semantic read-once nondeterministic branching programs.

S. Jukna:
Exponential Lower bounds for semantic resolution.
In: Feasible Arithmetics and Length of Proofs, P. Beame and S. Buss, Eds., DIMACS-AMS Series in Discrete Mathematics and Theoretical Comput. Sci., vol. 39 (1998) pp. 63-172.

Abstract: In a semantic resolution proof we operate with clauses only but allow *arbitrary* rules of inference: consistency is the only requirement. We prove a very simple exponential lower bound for the size of bounded fanin semantic resolution proofs of a general *Hitting Set Principle* stating that, for any set system with hit-

ting set number τ, no set of size less than τ can be a hitting set. The pigeonhole principle and known blocking principles for finite (affine and projective) planes are special cases of this general principle.

Ch. Meinel:
Elektronisches Publizieren im World Wide Web - Eine neue Dimension in der wissenschaftlichen Kommunikation.
Forschung & Lehre. No. 3, 1998, pp.122-125.

Abstract: Das World Wide Web ist ein sehr erfolgreiches Medium zur einfachen weltweiten Kommunikation. Ist der eigene Rechner mit dem Internet verbunden, dann kann über diesen Rechner auf sämtliche über das Internet verfügbare multimediale Dokumente zugegriffen werden. Wie kann es intensiver für Forschung und Lehre genutzt werden?

Ch. Meinel, T. Engel:
Institut für Telematik (Trier) - angewandte Forschung nach Fraunhofer Ideal.
Informatik - Forschung und Entwicklung, Bd. 13, Heft 2, 1998, pp. 97-101.

Abstract: Das Institut für Telematik ist ein von der Fraunhofer Management Gesellschaft betreutes Institut, das Forschungsprojekte und Entwicklungsaufträge im Schnittpunkt von Telekommunikation und Informatik, dem jungen Wissenschaftsgebiet der Telematik, bearbeitet. Tatsächlich liegt die zentrale Herausforderung beim Wandel von der Industriegesellschaft zur Wissensgesellschaft im effektiven Umgang mit den auf Datennetzen verfügbaren Informationen und deren Umwandlung in einsatzfähiges Wissen. Neben der Sicherung der Infrastruktur kommt dabei der Bereitstellung telematischer Systeme eine besondere Schlüsselstellung zu. Die Tätigkeit des Instituts für Telematik reicht von der anwendungsorientierten Grundlagenforschung in ausgewählten Teilgebieten der Telematik bis hin zur Entwicklung maßgeschneiderter Problemlösungen und Pilotsysteme. Die projektbezogene Finanzierung sichert die Erfolgskontrolle durch den Anwender. Kooperationspartner des Instituts für Telematik sind neben der Universität Trier sowohl High-Tech-Unternehmen mit Problemen von der Forschungsfront als auch kleinere und mittlere Unternehmen, bei denen wissenschaftliche Ergebnisse im Bereich der Computertechnik und Optimierung in den letzten Jahren mit Macht zum Einsatz drängen.

H.-J. Görg, Ch. Meinel:
Digitale Signaturen schaffen Sicherheit auf der Datenautobahn - Public-Key-Verfahren als Ausgangspunkt für gesetzgeberische Initiativen.
Management und Krankenhaus, Heft 10/98, pp.8-9.

Abstract: Die Sicherheit medizinischen Datenmaterials bei der Übertragung in offenen Netzen wie dem Internet, hängt maßgeblich davon ab, daß Unberechtigten die Einsicht in die übertragenen Dokumente verwehrt wird (Geheimhaltung), daß die übertragenen Dokumente verwehrt und eindeutig von dem ausgewiesenen Absender stammen (Authentizität) und daß sie auf dem Übertragungswege keine inhaltliche Veränderung erfahren haben (Integrität). Der Beitrag beschäftigte sich mit den Sicherheitsaspekten einer den Anforderungen des Signaturgesetzes und der Signaturverordnung entsprechenden elektronischen Datenübertragung, insbesondere im Hinblick auf die Schaffung gesetzeskonformer Zertifizierungsstellen, die auch im medizinischen Bereich eine vertrauenswürdige und rechtssichere Grundlage für das Arbeiten mit elektronischen Unterschriften schaffen und damit Sicherheit sowohl bezüglich der Urheberschaft, als auch der Unverfälschtheit des versendeten Materials garantieren.

H.-J. Görg, Ch. Meinel:
Digitale Signaturen schaffen Sicherheit auf der Datenautobahn - Sicherheitsaspekte im Organisationsablauf von Trust Center Dienstleistungen.
Management und Krankenhaus, Heft 11/98, pp. 77-78

Abstract: siehe oben

Michael L. Littman, Judy Goldsmith, Martin Mundhenk:
The Computational Complexity of Probabilistic Planning.
Journal on Artificial Intelligence Research, Vol.9, pp. 1-36, 1998.

Abstract: We examine the computational complexity of testing and finding small plans in probabilistic planning domains with both flat and propositional representations. The complexity of plan evaluation and existence varies with the plan type sought; we examine totally ordered plans, acyclic plans, and looping plans, and partially ordered plans under three natural definitions of plan value. We show that problems of interest are complete for a variety of complexity classes: PL, P, NP, coNP, PP, NP(PP), coNP(PP), and PSPACE. In the process of proving that certain planning problems are complete for NP(PP), we introduce a new basic NP(PP)-complete problem, E-MAXSAT, which generalizes the standard Boolean satisfiability problem to computations involving probabilistic quantities; our results suggest that the development of good heuristics for E-MAXSAT could be important for the creation of efficient algorithms for a wide variety of problems.

8.4 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 1998 und 1999 entnommen werden.*

J. Bern, Ch. Meinel, H. Sack:
Electronic Colloquia: Idea and Practice
in: Proc. of the Int. Symp. of SIGDOC'98, Quebec (Kanada), 1998.

Abstract: The scientific community, especially the more computer related fields of science like computer science and mathematics, have not only been doing research in information technology, they have simultaneously begun to exploit its advantages for their own purposes. However, scientific publishing is distinct from other application areas of information technology in that it requires publications to be not only fast, but also comparable to traditional media in terms of quality control and long-term availability. Peer reviewing and paper-based publishing are still the methods of choice to achieve the latter, restricting electronic means to more or less "inofficial" communications.
Within the field of scientific communication, we find a number of types of communication with slightly different goal and character: From scientific journals with their extensive and, consequently, slow reviewing mechanisms over conference papers to — nowadays usually electronic — forms of publication by the author. On the other hand, and in spite of the delay incurred, peer review is advantageous in that the remaining publications are reasonably filtered for quality, making the series, resp. conference proceedings, worthwhile to read and use to the recipients.
The department for computer science at the University of Trier (Trèves), Germany, has taken part in research on and implementation of information technology in this area. In this paper, we will present two of the three main projects. Meanwhile, the university has created the *Center for Scientific Electronic Publishing (WEP),* which serves as an institution for the exchange of know-how on information technology and its applications between the departments of the university.
The two projects we are going to present are the *Electronic Colloquium on Computational Complexity (ECCC)* and the *STACS Electronic Submission Service.* For both, we will introduce the specific situations they were developed for, present the specific problems of interest and the chosen solutions, and conclude with a report of current status and use. Finally, we will outline our view of the future both for the

field as a whole and for the specific projects.

C. Damm:
On Boolean vs. Modular Arithmetic for Circuits and Communication Protocols.
In: Mathematical Foundations of Computer Science, August 1998. LNCS 1450, Springer, pp. 780-788, 1998

Abstract: We compare two computational models that appeared in the literature in a Boolean setting and in an analog setting based on modular arithmetic. We prove that in both cases the arithmetic version can to some extend simulate the Boolean version. Although the models are very different, the proofs rely on the same idea based on the Schwartz-Zippel-Theorem.
In the first part we give a new simulation of semi-unbounded Boolean circuits by semiunbounded circuits with unbounded parity gates. Our simulation is simpler and more efficient with respect to depth than the original simulation of (Gál and Wigderson (1996). In the second part we prove, that two-party parity communication protocols can approximate nondeterministic communication protocols. A strict simulation of one by the other is impossible as was shown in Damm et al. (1994).

A. Bernasconi, C. Damm, I. Shparlinski: *On the Average Sensitivity of Testing Square-Free Numbers.*
In: Proc. of the 5th Ann. Intern. Computing and Combinatorics Conference, Tokyo (Japan), LNCS 1627, 291-299, Springer-Verlag 1999.

Abstract: We study combinatorial complexity characteristics of a Boolean function related to a natural number theoretic problem. In particular we obtain a linear lower bound on the average sensitivity of the Boolean function deciding whether a given integer is square-free. This result allows us to derive a quadratic lower bound for the formula size complexity of testing square-free numbers and a linear lower bound on the average decision tree depth. We also obtain lower bounds on the degrees of exact and approximative polynomial representations of this function.

C. Damm, K-H. Kim, F. Roush: *On covering and rank problems for matrices and their applications.*
In: Proc. of the 5th Ann. Intern. Computing and Combinatorics Conference, Tokyo (Japan), LNCS 1627, 123-133, Springer-Verlag 1999.

Abstract: We consider combinatorial properties of Boolean matrices and their application to two-party communication complexity. Let A be a binary $n \times n$ matrix and let K be a field. *Rectangles* are sets of entries defined by collections of rows and columns. We denote by $\mathrm{rank}_B A$ ($\mathrm{rank}_K A$, resp.) the least size of a family of

rectangles whose union (sum, resp.) equals A.

We prove the following:

- With probability approaching 1, for a random Boolean matrix A the following holds:
$$\mathrm{rank}_B A \geq n(1 - o(1)).$$
- For finite K and fixed $\varepsilon > 0$ the following holds: If A is a Boolean matrix with $\mathrm{rank}_B A \leq t$ then there is some matrix $A' \leq A$ such that $A - A'$ has at most $\varepsilon \cdot n^2$ non-zero entries and $\mathrm{rank}_K A' \leq t^{O(1)}$.

As applications we mention some improvements of earlier results: (1) With probability approaching 1 a random n-variable Boolean function has nondeterministic communication complexity n, (2) functions with *nondeterministic* communication complexity l can be *approximated* by functions with *parity* communication complexity $O(l)$. The latter complements a result saying that nondeterministic and parity communication protocols cannot efficiently *simulate* each other. Another consequence is: (3) matrices with small Boolean rank have small matrix rigidity over any field.

Judy Goldsmith and Martin Mundhenk:
Complexity issues in Markov decision processes.
Proceedings of the 13th Conference on Computational Complexity, pp. 272–280, IEEE Press, 1998.

Abstract: We survey the complexity of computational problems about Markov decision processes: evaluating policies, finding good and best policies, approximating best policies, and related decision problems.

S. Jukna and S. Žák:
On branching programs with bounded uncertainty
In: *Proceedings of ICALP'98* (Aalborg, Denmark, July 1998), Volume 1443 of Lecture Notes in Computer Science, pp. 259–270. Springer Verlag, 1998.

Abstract: We propose an information-theoretic approach to proving lower bounds on the size of branching programs (b.p.). The argument is based on Kraft-McMillan type inequalities for the average amount of uncertainty about (or entropy of) a given input during various stages of the computation. We first demonstrate the approach for read-once b.p. Then we introduce a strictly larger class of so-called 'gentle' b.p. and, using the suggested approach, prove that some explicit Boolean functions, including the Clique function and a particular Pointer function (which belongs to AC^0), cannot be computed by gentle program of polynomial size. These lower bounds are

new since explicit functions, which are known to be hard for *all* previously considered reading-restricted classes of b.p. (such as $(1, +s)$-b.p. or syntactic read-k-times b.p.) can be easily computed by gentle b.p. of polynomial size.

Ch. Meinel, Ch. Stangier:
Speeding Up Symbolic Model Checking
5th International Conference on Advanced Computer Systems (ACS'98), Szczecin, Polen, 1998, pp. 548 -554

Abstract: Model checking is a widely used technique in verification of sequential circuits, reactive systems, protocols, etc. Ordered Binary Decision Diagrams (OBDDs) allow a symbolic representation of the model that may bypass the state space explosion problem of larger systems. As the size of OBDDs and also the computation time depends on the order of the input variables, the verification may only succeed if a well suited variable order is chosen. Since the characteristics of the 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.
We present a technique that substantially accelerates the reordering process by using easily computable structural information about the represented function without increasing OBDD sizes significantly.

Ch. Meinel, A. Slobodová:
Sample Method for Minimization of OBDDs
In: *Proceedings of SOFSEM'98* (Jasna, Slowakia), 1998, pp. 419 - 428.

Abstract: This paper contributes to the solution of the minimization problem of Ordered Binary Decision Diagrams by means of variable reordering. We suggest a new heuristic that is based on sampling. A small OBDD sample is chosen from the OBDDs that are considered for minimization. Solving the problem for this small sample, we obtain a variable order that is adapted for the entire OBDDs. We present first experimental results with the Sample Reordering targeted at combinatorial verification. The suggested heuristic is substantially faster than Sifting.

J. Bern, Ch. Meinel:
One Step Further - Extending Electronic Submission Into the Reviewingr Process
in: Proc. of the Int. Symp. of SIGDOC'99, New Orleans, 1999.

Abstract: In the academic environment, two prime examples of the use of information technology for document processing are scientific journals and conference proceedings. In addition to being genuinely multi-authored documents, the authors

contributing to these collections are usually distributed across a significant part of the globe. As a result, academia has eagerly adopted, over the last years, the developing means of electronic communication in general, and electronic document exchange in particular. Journals and conferences in "computer intensive" fields, like mathematics and computer science, basically all use electronic document exchange. In this paper, we focus onto our work in the area of support for editorial processes with such electronic systems.

In one of our projects — the Electronic Colloquium on Computational Complexity (ECCC), operative since the end of 1994 — the decision process for selection of contributions to include was radically simplified in comparison to traditional journals. As a result, ECCC has a guaranteed limit on the delay between submission and decision of two months; many electronic journals use the same decision mechanism as paper journals, and suffer the same delays of sometimes over a year because of the time spent for communication between reviewers and editors.

Another project of ours is software for electronic submission of and editorial work on conference papers. The basic difference to the ECCC, where we designed an improved workflow, is that the workflow of a conference usually must be supported as-is. In 1999, we performed electronic submissions to the Symposium on Theoretical Aspects of Computer Science (STACS), and since the conference was hosted in Trier, we were able to "co-develop" certain changes in the decision process and a software implementing support for the entire process.

J. Bern, Ch. Meinel:
Electronic Colloquia in the WWW - a New Form of Scientific Publications
in: Proc. of SCI/ISAS'99, Orlando, 1999.

Abstract: The scientific community, especially the more computer related fields of science like computer science and mathematics, have not only been doing research in information technology, they have simultaneously begun to exploit its advantages for their own purposes. However, scientific publishing is different from other areas where information technology has been applied in that it requires publications to be not only fast, but also comparable to traditional media in terms of quality control and long-term availability. Peer reviewing and paper-based publishing are still the methods of choice to achieve the latter goals, restricting electronic means to more or less "inofficial" communications.

Within the field of scientific communication, we find a number of types of communication with slightly different goal and character: From scientific journals with their extensive and, consequently, slow reviewing mechanisms over conference papers to — nowadays usually electronic — forms of publication by the author. On the other hand, and in spite of the delay incurred, peer review is advantageous: The remaining publications are reasonably filtered for quality, making the series worthwhile to read.

The department for computer science at the University of Trier (Trèves), Germany, is researching and implementing solutions in the area of information technology. In this paper, we will present one of our three main projects, the *Electronic Colloquium on Computational Complexity (ECCC)* We will introduce the specific situations it was developed for, present the specific problems of interest and the chosen solutions, and conclude with a report of current status and use. Finally, we will outline our view of the future both for the field as a whole and for the specific projects.

Ch. Meinel, A. Slobodová: *Sample Method for Minimization of OBDDs*
In: *Proceedings of IWLS'98, Granlibakken Resort, Lake Tahoe (Kalifornien, USA), 1998, pp. 311 - 316.*

Abstract: siehe oben.

Ch. Meinel, F. Somenzi, T. Theobald: *Function Decomposition and Synthesis Using Linear Sifting*
In: *Proceedings of ASP-DAC'98, Yokohama (Japan), 1998, pp. 81-86.*

Abstract: In order to simplify a synthesis task for particularly hard functions it is sometimes inevitable to decompose the function in a preprocessing step. We propose a new algorithm for automatically decomposing a target function by extracting a linear filter within the synthesis process. The algorithm is an application of the Linear Sifting algorithm which has been proposed in [6]. Using this method we were able to synthesize functions with standard tools which fail otherwise.

Ch. Meinel, H. Sack:
$\oplus$-OBDDs - a BDD Structure for Probabilistic Verification
In:*Proc. of the 1998 IEEE/ACM Int. Workshop on Logic Synthesis (IWLS98)* (Lake Tahoe, Cal, June 1998).

Abstract: Ordered Binary Decision Diagrams (OBDDs) have already proved usefull in the verification of combinational and sequential circuits. Due to limitations of the descriptive power of OBDDs several 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.

G. Cabodi, S. Quer, Ch. Meinel, H. Sack, A. Slobodova, Ch. Stangier:
Binary Decision Diagrams and the Multiple Variable Order Problem
In: *Proc. of the 1998 IEEE/ACM Int. Workshop on Logic Synthesis (IWLS98)* (Lake

Tahoe, Cal, June 1998).

Abstract: Ordered Binary Decision Diagrams (OBDDs) are the first choice in manipulating and representing Boolean functions in CAD. Since the size of an OBDD heavily depends on the chosen variable order, much effort is spent in finding good and improving existing variable orders. If these optimizing techniques are used in OBDD applications, one has to cope with OBDDs of different variable orders very often (e.g., representing the transition relation and the reachable state set in sequential verification). For an efficient manipulation and represention of OBDDs as a multi rooted OBDD, a common variable order is desired.

Ch. Meinel, H. Sack:
$\oplus$-OBDDs - a BDD Structure for Probabilistic Verification
In: *Proc. of the 1998 Workshop on Probabilistic Methods in Verification (PROB-MIV'98)* (Indianapolis, IN, USA, 1998).

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 several 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.

M. Mundhenk:
Propositional Proofs and Their Complexity
In: 11*th European Summerschool in Logic, Language and Information*, 1999.

Abstract: The first part of this course notes is devoted to recall the basics of propositional logic, and to introduce basic concepts from computational complexity theory. A main goal is to show the connection between proof lengths and open questions in complexity theory. In the second part, the three proof systems analytic tableaux, resolution, and cutting-plane proof systems are introduced. Our goal is to give a complexity taxonomy of the proof systems. For this, we show how proofs can be transformed from the one to the other system without increasing the proof length, and we exhibit formulas which have exponentially long proofs in the one system and short proofs in the other one. The background of these lower bound proofs will be illuminated.

M. Mundhenk:
Instance Complexity of NP-hard Sets

In *Proceedings Journées de l'Informatique Messine 1999.*

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 (i.e. the inherent complexity of a string), 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, 1996) proved that NP-hard sets have p-hard instances, unless P=NP. The unbounded version of the conjecture was proven wrong by Kummer (1995), and therefore it cannot be used to characterize e.g. the class recursive sets.

We introduced a slightly weaker notion of hard instances. In the unbounded version, we used it to characterize the classes of recursively enumerable resp. recursive sets. In time-bounded versions, we characterized the class P. Hard instances are shown to be stronger than complexity cores (introduced by Lynch (JACM, 1975)). Nevertheless, NP-hard sets must have both: super-polynomially dense hard instances and super-polynomially dense non-hard instances, unless P=NP.

Ch. Meinel, H. Sack:
Algorithmic Considerations for Parity-OBDD Reordering
In *Proceedings of the 1999 IEEE/ACM Int. Workshop on Logic Synthesis (IWLS99), Lake Tahoe, Cal, 1999.*

Abstract: Ordered Binary Decision Diagrams (OBDDs) have already proved useful in the proce ss 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, we address $\oplus$-OBDDs and introduce algorithms for improving their efficiency by reordering of variables and functional nodes.

Ch. Meinel, A. Wagner:
Evaluation of OBDD-Heuristics via the Internet
In *Proceedings of the 1999 IEEE/ACM Int. Workshop on Logic Synthesis (IWLS99), Lake Tahoe, Cal, 1999.*

Abstract: In EDA algorithm research, an important question is how to publish performance data. Tables listing benchmark computation results are useful but limited in their information content. Specifically in the field of OBDD heuristics, there seems to be a need for an additional better mechanism. This paper discusses the limitation of traditional approaches and stresses the need for solutions using the Internet. After developing requirements, we describe a system that allows the online comparison and evaluation of OBDD heuristics. We also describe technical ascpects

of our actual implementation and give a short overview of related work.

Ch. Meinel, H. Sack, C. Stangier:
Overcoming Ordering Restrictions for Synthesizing Binary Decision Diagrams
In *Proceedings of NORCHIP '99, Oslo, Norway 1999.*

Abstract: Many problems in computer-aided design of highly integrated circuits (CAD for VL SI) can be transformed to the task of manipulating objects over finite domains. The efficiency of these operations depends substantially on the chosen data structures. In the last years, ordered Binary Decision Diagrams (OBDDs) have proved to be very efficient in this context. One restriction for the efficient synthesis of two or more OBDDs is that they must share a common variable order. We address the problem of efficiently synthesizing OBDDs that have different variable orders by adapting a reordering based synthesis technique. In particular, we apply this technique to the basic operation of the irredundant cover problem, i.e. testing functional containment of two OBDDs.

Ch. Meinel, Ch. Stangier:
Increasing efficiency of symbolic model checking by accelerating dynamic variable reordering In *Proceedings of the on Design, automation and test in Europe 99, München,Germany,1999*

Abstract: Model checking is a widely used technique in verification of sequential circuits, reactive systems, protocols, etc.. Ordered Binary Decision Diagrams (OBDDs) allow a symbolic representation of the model that may bypass the state space explosion problem of larger systems. As the size of OBDDs and also the computation time depends on the order of the input variables, the verification may only succeed if a well suited variable order is chosen. Since the characteristics of the 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.

We present techniques that substantially accelerate the reordering process by using either easily computable structural or implicit semantical information about the represented function without increasing OBDD sizes significantly.

Ch. Meinel, K. Schwettmann, A. Slobodová *Application Driven Variable Reordering and an Example Implementation in Reachability Analysis* In *Proceedings of ASP-DAC'99, Hongkong, 1999*

Abstract: Variable reordering is the main approach to minimize the size of Ordered Binary Decision Diagrams. But despite the huge effort spent, up to now, to design different reordering heuristics, their performance often does not meet the needs of

the applications. In many OBDD-based computations, the time cost for reordering dominates the time spent by the computation itself. There are some known approaches for accelerating the reordering by taking advantage of structural properties of OBDDs and functions represented. In this paper, we propose a reordering method that exploits application specific information. The main idea is to drive the reordering process by the computation. This effects an acceleration of the whole computation rather than of the reordering only. The power of the approach is illustrated on hand of speeding up forward traversal of finite state machines.

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

S. Jukna:
Combinatorics of Monotone Computations
Nr. TR98-041

Abstract: We consider a general model of monotone circuits, which we call *d-local*. In these circuits we allow as gates: (i) arbitrary monotone Boolean functions whose minterms or maxterms (or both) have length $\leq d$, and (ii) arbitrary real-valued non-decreasing functions on $\leq d$ variables. Our main result is a general combinatorial lower bounds criterion for such circuits. This resolves a problem, raised by Razborov in 1986, and yields, in a uniform and easy way, non-trivial lower bounds for circuits computing explicit functions even when $d \to \infty$. The proof is relatively simple and direct, and combines the bottlenecks counting method of Haken with the idea of finite limit due to Sipser.
We demonstrate the criterion by super-polynomial lower bounds for explicit Boolean functions, associated with bipartite Paley graphs and partial t-designs. We then derive exponential lower bounds for clique-like graph functions of Tardos, thus establishing an exponential gap between the monotone real and non-monotone Boolean circuit complexities. Since we allow real gates, the criterion also implies corresponding lower bounds for the length of cutting planes proof in the propositional calculus.

S. Jukna and S. Žák:
On branching programs with bounded uncertainty
Nr. TR98-030

Abstract: siehe Abschnitt 8.4

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

Ch. Meinel, Th. Theobald:
Ordered Binary Decision Diagrams and Their Significance in Computer-Aided Design of VLSI Circuits Forschungsbericht Nr. 98-01.

Abstract:
Many problems in computer-aided design of highly integrated circuits (CAD for VLSI) can be transformed to the task of manipulating objects over finite domains. The efficiency of these operations depends substantially on the chosen data structures. In the last years, ordered binary decision diagrams (OBDDs) have proven to be a very efficient data structure in this context. Here, we give a survey on these developments and stress the deep interactions between basic research and practically relevant applied research with its immediate impact on the performance improvement of modern CAD design and verification tools.

C. Damm:
On Boolean vs. Modular Arithmetic for Circuits and Communication Protocols
Forschungsbericht Nr. 98-06.

Abstract: siehe Abschnitt 8.4

C. Damm:
On Alternating vs. Parity Communication Complexity
Forschungsbericht Nr. 98-20.

Abstract: We prove that for any $O(1)$-alternating communication protocol of length L computing a function f and for $0 < \delta$ there is a parity communication protocol of length $O((L - \log\delta)^{O(1)})$ computing a function differing from f in at most a δ-fraction of the inputs. This can be generalized to computations based on arithmetic over any finite field.
A consequence is a new proof and improvement of a connection between matrix rigidity over finite fields and alternating communication complexity that was first observed by Razborov (1998).
As a side result we prove upper bounds on the rigidity over any field of a 0-1-matrix A in terms of the numbers of constant submatrices required to cover A.

A. Bernasconi, C. Damm, I. Shparlinski
Circuit and Decision Tree Complexity of Some Number Theoretic Problems
Forschungsbericht Nr 98-21.

Abstract: We extend the area of applications of the Abstract Harmonic Analysis

to lower bounds on the circuit and decision tree complexity of Boolean functions related to some number theoretic problems. In particular, we prove that deciding if a given integer is square-free and testing co-primality of two integers by unbounded fan-in circuits of bounded depth requires superpolynomial size.

G. Cabodi, S. Quer, Ch. Meinel, H. Sack, A. Slobodova, C. Stangier:
Binary Decision Diagrams and the Multiple Variable Order Problem
Forschungsbericht 98-22.

Abstract: siehe Abschnitt 8.4

Ch. Meinel, Chr. Stangier:
Increasing Efficiency of Symbolic Model Checking by Accelerating Dynamic Variable Reordering Forschungsbericht 98-23.

Abstract: siehe Abschnitt 8.4

Ch. Meinel, A. Slobodová:
Accelerating OBDD-Minimization by Means of Structural and Semantical Properties
Forschungsbericht 98-25. **Abstract:** siehe Abschnitt 8.4

Ch. Meinel, A. Wagner:
The WWW meets EDA: Usability Evaluation of OBDD-Heuristics Via the Internet
Forschungsbericht 98-27.

Abstract: We present an approach for the evaluation of OBDD-heuristics over the Internet. We explain why there is a genuine need for the possibility of evaluating the power of new methods (e.g. heuristics) independently, and why an Internet-based solution is superior. The case of OBDD heuristics is used as an example of practical relevance. Desirable characteristics of an Internet based approach are developed and aspects of security are discussed. Our system, featuring a couple of innovative new OBDD heuristics is presented.

Ch. Meinel, H. Sack:
Mod2OBDDs - a BDD Structure for Probabilistic Verification
Forschungsbericht 98-28.

Abstract: siehe Abschnitt 8.4

Ch. Meinel, H. Sack, C. Stangier, A. Wagner:
Do We Really Need Common Variable Orders for Synthesizing OBDDs?
Forschungsbericht 98-29.

Abstract: Ordered Binary Decision Diagrams (OBDDs) have already proved useful in the verification of combinational and sequential circuits. But for the synthesis of two or more OBDDs it is usually necessary that they have a common variable order. We address the problem of synthesizing OBDDs that have different variable orders. We do this by applying a reordering based synthesis technique. In particular, we apply this technique to the basic operation of the irredundant cover problem, i.e. testing functional containment of two OBDDs.

Ch. Meinel, H. Sack:
Algorithmic Considerations for Parity-OBDD Reordering
Forschungsbericht 99-19.

Abstract: siehe Abschnitt 8.4

C. Damm:
On the Complexity of Tensor Formulae
Forschungsbericht Mathematik/Informatik Nr. 99-20, Universität Trier, 1999.

Abstract: We consider three propositional proof systems under the aspect of proof length: analytic tableaux, resolution, and cutting-plane proof systems. All of them are widely used in automatic theorem proving.

The first part is devoted to recall the basics of propositional logic, and to introduce basic concepts from computational complexity theory. A main goal is to show the above mentioned connection between proof lengths and open questions in complexity theory. In the second part, the three above proof systems will be introduced. Our goal is to give a complexity taxonomy of the proof systems. For this, we show how proofs can be transformed from the one to the other system without increasing the proof length, and we exhibit formulas which have exponentially long proofs in the one system and short proofs in the other one. The background of these lower bound proofs will be illuminated.

M. Mundhenk:
The Complexity of Optimal Small Policies
Forschungsbericht Nr. 99-22.

Abstract: We investigate the complexity of problems concerned with partially-observable Markov decision processes which are run for a finite number of steps un-

der 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 Tstitsiklis (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.

E. Dubrova, H. Sack:
Probabilistic Verification of Multiple-Valued Functions
Forschungsbericht Nr. 99-23.

Abstract: This paper describes a probabilistic 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 probabilistic verification can be an attractive alternative for verifying functions that are too large to be handled by deterministic verification methods.

M. Mundhenk, J. Goldsmith, C. Lusena, E.Allender:
Complexity of Finite-Horizon Markov Decision Process Problems.
Forschungsbericht Nr. 99-25.

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 NP(PP).

G. Hoff, M. Mundhenk:
Finding Scientific Papers with HPSearch and MOPS
Forschungsbericht Nr. 99-26.

Abstract: The fast dissemination of new research results on the world-wide web poses new challenges for search engines. In this paper we describe a new approach to seek scientific papers relevant to a pre-defined research area. Different from other approaches, we do not search for web pages which contain certain keywords, but we search for web pages which are created by scientists who are active in the research area under consideration. The names of these scientists are obtained from the DBLP server. The HPSearchsystem finds the Home Pages according to the names, and MOPS finds research papers close to the Home Pages. It creates an index of these papers and makes it accessible on the web. We conclude that such a focused crawling is very effective for building high-quality collections and indices of scientific papers, using ordinary desktop hardware.

H. Sack, E. Dubrova, Ch. Meinel:
Mod-p Decision Diagrams: A Data Structure for Multiple-Valued Functions
Forschungsbericht Nr. 99-27.

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 thatn the variables obtained by a binary encoding. Several types of MDDs, employing different multiple-valued decompositions have been already introduced. We present a more general class of multiple-valued decision diagrams containing not only branching nodes but also functional nodes, labeled by addition modulo p operation, 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 require time linear in the number of nodes.

Ch. Meinel, Chr. Stangier:
Speeding Up Symbolic Model Checking by Accelerating Dynamic Variable Reordering
Forschungsbericht Nr. 99-28.

Abstract: Symbolic Model checking based on OBDDs is a widely used technique in verification of sequential circuits, reactive systems or protocols.

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 variable order is chosen. Since the characteristics of the 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 these techniques substantially accelerates the reordering process and makes it possible to finish computations, that are too time consuming, otherwise.

Chr. Stangier, U. Holtmann:
Applying Formal Verification with Protocol Compiler Forschungsbericht Nr. 99-29.

Abstract: This paper gives two examples how to verify designs with 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.

We find that assertion checking fits well into the design flow and is easy to use within Protocol Compiler.

8.7 Vorabveröffentlichungen außerhalb der Universität Trier

C. Damm:
A Note on Spectral Lower Bound Arguments for Decision Trees.
Bulletin of the EATCS, 65 (1998), 136–138.

Abstract: Let $\mathsf{DT}(f)$ and $\overline{\mathsf{depth}}(f)$ be the minimal size and the minimal average depth of decision trees that compute a given Boolean function $f : \{0,1\}^n \to \{+1,-1\}$. Based on geometric arguments we give a very simple proof for the following lower bounds due to Brandman, Orlitsky, and Hennessy (1990):

$$\mathsf{DT}(f) \geq \sum_{S\subseteq[n]} 2^{|S|} \cdot \hat{f}(S)^2, \overline{\mathsf{depth}}(f) \geq \sum_{S\subseteq[n]} |S| \cdot \hat{f}(S)^2,$$

where the $\hat{f}(S)$ are the Fourier coefficients of f.

Ch. Meinel, T. Theobald:
Ordered Binary Decision Diagrams and Their Significance in Computer-Aided Design of VLSI Ciruits.
Bulletin of EATCS, 64 (1998), 171–187.

Abstract: Many problems in computer-aided design of highly integrated circuits (CAD for VLSI) can be transformed to the task of manipulating objects over finite domains. The efficiency of these operations depends substantially on the chosen data structures. In the last years, ordered binary decision diagrams (OBBDs) have proven to be a very efficient data structure in this context. Here, we give a survey on these developments and stress the deep interactions between basic research and practically relevant applied research with its immediate impact on the performance improvement of modern CAD design and verification tools.

J. Goldsmith, Ch. Lusena, M. Mundhenk:
Nonapproximability Results for Markov Decision Processes.
University of Kentucky Computer Science Department TR 275-98.

Abstract: We show that for several variations of partially observable Markov decision processes, polynomial-time algorithms for finding control policies are unlikely or impossible to 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 or P=PSPACE. Until or unless these collapses are shown to hold, any control-policy designer must choose between such performance guarantees and efficient computation.

Technische Berichte 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/frame/pubtech.html/`

abgerufen werden.

Ch. Meinel:
Elektronisches Publizieren im World Wide Web - Eine neue Dimension in der wissenschaftlichen Kommunikation.
Techn. Bericht Nr. 98-01.

J. Bern, C. Damm, Ch. Meinel:
The Electronic Colloquium on Computational Complexity (ECCC): A Digital Library in Use.
Techn. Bericht Nr. 98-02.

S. Hludov, C. Schröter, Ch. Meinel:
Adaptive Komprimierung von DICOM-Bildern.
Techn. Bericht Nr. 98-03.

A. Heuer, K. Siemonsen, Th. Engel, Ch. Meinel:
Web-basierte Navigationssysteme für Datenbanken.
Techn. Bericht Nr. 98-04.

S. Hludov, Ch. Meinel:
JAVA-DICOM-Viewer.
Techn. Bericht Nr. 98-05.

S. Müller, H.-J. Görg, Th. Engel, Ch. Meinel:
CryptoPay-Sicheres Bezahlen im Internet.
Techn. Bericht Nr. 98-06.

C. Schröter, Th. Engel, Ch. Meinel:
Internetbasiertes Arztbriefsystem.
Techn. Bericht Nr. 98-07.

S. Hludov, L. Köhler, Ch. Meinel, Th. Engel:
PACS für Radiologie.
Techn. Bericht Nr. 98-08.

H.-J. Görg, Th. Engel, Ch. Meinel:
TI-Trust Center - Eröffnung einer Zertifizierungsstelle in Anlehnung an das Signaturgesetz und die Signaturverordnung.
Techn. Bericht Nr. 98-09.

Ch. Meinel, S. Müller:
Trierer Telemedizin Symposium, Internet-Technologie in der Medizin (Hrsg.).
Techn. Bericht Nr. 98-10.

Ch. Meinel, S. Müller:
Trierer Telemedizin Symposium - Internet-Technologie in der Medizin, Proceedings.
Techn. Bericht Nr. 98-11.

Ch. Meinel, A. Wagner:
The WWW meets EDA: Usability Evaluation of OBDD-Heuristics via the Internet
Techn. Bericht Nr. 98-12.

F. Losemann, Ch. Meinel:
Warum Zertifikate?
Techn. Bericht Nr. 98-13.

U. Roth, E.G. Haffner, Th. Engel, Ch. Meinel:
Smart Data Server (SDS) - Modularer Aufbau und verteilte Funktionalität
Techn. Bericht Nr. 98-14.

E.G. Haffner, Th. Engel, Ch. Meinel:
Flood-Gates statt Firewall - eine „High-Society"-Lösung zum sicheren Datenaustausch zwischen Internet und Intranet.
Techn. Bericht Nr. 98-15.

M. Hastenteufel, Ch. Meinel:
Digitale Zertifikate - Standards und Anwendungen.
Techn. Bericht Nr. 99-01.

E. G. Haffner, U. Roth, Th. Engel, Ch. Meinel:
Vorhersage von Benutzeranforderungen im Internet.
Techn. Bericht Nr. 99-02.

Z. Zhang, A. Heuer, Th. Engel, Ch. Meinel:
DAPHNE - A Tool for Distributed Web Authoring and Publishing.
Techn. Bericht Nr. 99-03.

Ch. Meinel, A. Wagner:
Ein Decision Diagram Portal im World Wide Web.
Techn. Bericht Nr. 99-04.

Uwe Roth, Ernst-Georg Haffner, Andreas Heuer, Thomas Engel, Christoph Meinel
Hyperlink Management System - HLM.
Techn. Bericht Nr. 99-05.

9 Vorträge

9.1 Vorträge außerhalb der Universität Trier

Jochen Bern:

ACM SIGDOC '99, 13.–15.09.1999, New Orleans

Carsten Damm: *„Über die Simulation Boolescher durch Arithmetische Schaltkreise"* ADiMMO'98: Workshop über algorithmische und diskrete Mathematik und mathematische Optimierung, (April 1998, Trier)

„Boolesche vs. modulare Arithmetik für Schaltkreise und Kommunikationsprotokolle",
35. Workshop über Komplexitätstheorie, Datenstrukturen und Effiziente Algorithmen (Juni 1998, Paderborn).

„On Boolean vs. Modular Arithmetic for Circuits and Communication Protocols",
Mathematical Foundations of Computer Science (August 1998, Brno)

Überdeckungs und Rang-Probleme für 0-1-Matrizen,
ADiMMO-Workshop, FU Berlin (29.-30.03.1999, Berlin)

On the complexitiy of tensor formulae,
DIMACS Worksshop on Arithmetic Circuits and Algebraic Methods in Complexity Theory (02.06.1999, New Brunswick/USA)

On Covering and Rank Problems for 0/1-Matrices,
COCOON'99 (26.07.1999, Tokyo/Japan)

On the Average Sensitivity of Testing Square-Free Numbers,
COCOON'99 (27.07.1999, Tokyo/Japan)

On the Complexity of Tensor Calculus,
Departément d'I.R.O., Université de Montréal (12.10.1999, Montreal/Canada)

A constructive upper bound on matrix rigidity,
19th Colloquium on Combinatorics (12.11.1999, Braunschweig)

The complexity of tensor calculus,
39. Workshop über Komplexitätstheorie, Datenstrukturen und Effiziente Algorithmen (30.11.1999, Düsseldorf)

Christoph Meinel:

„Vorstellung des Instituts für Telematik"
Universität Trier, Veranstaltung „Uni und Handwerk" (Januar 1998, Trier)

„BDD's - a new BDD-based Data Structure for Manipulating Boolean Functions"
Kyushu Institute of Technology (Februar 1998, Japan)

„Ordered Binary Decision Diagrams - Data Structure for Switching Functions"
Kyushu University (Februar 1998, Japan)

„Perspektiven der Internet-Technologie"
Sparkasse (März 1998, Trier)

„Sicherheitskonzepte in offenen Netzen"
Deutsches Luft- und Raumfahrtzentrum (März 1998, Bonn)

„Konzept eines Intranet-basieren Arztbriefsystems"
Mutterhaus der Borromäerinnen (März 1998, Trier)

„Abschlußbericht zu den Projekten Nutzernavigationsinterface und Intranet-Redaktionssystem"
Dresdner Bank (April 1998, Frankfurt)

„Potential der Internet/Intranet-Technologie in der Bank"
DG-Bank (April 1998, Luxembourg)

„Telematik im Gesundheitswesen"
Deutsche Krankenhausgesellschaft (Mai 1998, Düsseldorf)

„Telematik und ihre Leistungspotentiale für die Wirtschaft“
Industrieausschuß der Region Trier im Institut für Telematik (Juni 1998, Trier)

„Vorstellung des Instituts für Telematik in Trier“
Forschungszentrum von Daimler-Benz (Juni 1998, Berlin)

„ECCC - das an der Universität Trier beheimatete elektronische Kolloquium“
Freundeskreis der Universität Trier (Juli 1998, Trier)

„Digitale Signaturen und die Aufgaben eines Trust-Centers“
Bezirksregierung (Juli 1998, Trier)

„Potential der Internet-Technologie in Wirtschaft und Gesellschaft“
Medienausschuß des Landtags von Rheinland-Pfalz im Institut für Telematik (Juli 1998, Trier)

„Konzept zur Realisierung eines leistungsfähigen Web-Auftritts“
DG-Bank (Juli 1998, Luxembourg)

„Bedeutung des WWW für mittelständische Unternehmen“
ZDF-Kongreßzentrum (September 1998, Mainz)

„Telematik im Gesundheitswesen“
Deutsche Krankenhausgesellschaft (September 1998, Düsseldorf)

„Telematik - Schrittmacher auf dem Weg in die Wissensgesellschaft“
Feierliche Eröffnung des Instituts für Telematik (September 1998, Trier)

„ECCC - an Electronic Colloquium“
SIGDOC'98, Quebec (September 1998, Kanada)

„Vorstellung des Instituts für Telematik“
Luxemburger Bankenverein (Oktober 1998, Luxembourg)

„Leistungspotentiale und Projekte des Instituts für Telematik“
Kuratorium des Instituts für Telematik (Oktober 1998, Trier)

„Potentiale der Internet-Technologie in der Telemedizin"
Trierer Telemedizin-Symposium (Oktober 1998, Trier)

„Projekte des Instituts für Telematik in Trier in der Finanzindustrie"
Zentralbank von Südafrika, Johannisburg (Oktober 1998, Südafrika)

„Konzepte und Bedeutung der Internet-Technologie in der Medizin"
Internationaler Luxemburger Chirurgenkongreß AECV (Dezember 1998, München)

„Digitale Signaturen in der Medizin"
Internationaler Luxemburger Chirurgenkongreß AECV (Dezember 1998, München)

„Bedeutung des World Wide Web für die Medizin"
Ärztekammer Trier (Januar 1999, Trier)

„Application Driven Variable Reordering in Reachability Analysis"
ASP-DAC'99 (Janaur 1999, Hongkong)

„Konzept eines Unternehmerbüros"
Rathaus Trier (Februar 1999, Trier)

„Using BDDs in Reachability Analysis"
DAAD-Projekt, Technische Universität Turin (Februar 1999, Turin)

„Vorstellung der CeBit-Projekte des Instituts für Telematik"
Landespresekonferenz Rheinland-Pfalz (März 1999, Mainz)

„Eröffnung des Symposiums Elektronisches Publizieren des Instituts für Telematik"
Institut für Telematik (März 1999, Trier)

„Sicherheit im elektronischen Geschäftsverkehr"
rlp-inform, Landeskonferenz (Mai 1999, Burg Lahnstein)

„Vorstellung des Instituts für Telematik"
Institutsleitertreffen der Fraunhofer Management-Gesellschaft (Juni 1999, München)

„DICOM - Image Compressions“
12th IEEE CBMS (Juni 1999, Stamford, USA)

„PACS for Teleradiology“
12th IEEE CBMS (Juni 1999, Stamford, USA)

„Compression of Medical Images“
IASTED SIP'99 (Oktober 1999, Nassau, Bahamas)

„Vorstellung des Instituts für Telematik“
IT-Vorstand der Allianz Versicherungs AG (Juli 1999, München)

„Electronic Colloquia in the WWW - a New Form of Scientific Publication“
SCI'99 / ISAS'99 (August 1999, Orlando, USA)

„Vorstellung der Projekte des Instituts für Telematik“
Kuratorium und Mitgleiderversammlung des Instituts für Telematik e.V. (September 1999, Trier)

„Neue Formen des elektronischen Publizierens“
EU-Bibliothekskonferenz Eisenstadt (September 1999, Eisenstadt, Österreich)

„Efficient Manipulation of Boolean Functions with OBDDs“
Universität Groningen (Oktober 1999, Groningen, Niederlande)

„Vorstellung des Instituts für Telematik“
Treffen der Humboldt-Stipendiaten des südwestdeutschen Raumes (November 1999, Trier)

„Eröffnung des Televerwaltungs-Symposiums des Instituts für Telematik“
Institut für Telematik (November 1999, Trier)

„Vorstellung des Instituts für Telematik“
Institutsbesichtigung durch TelekomForum (November 1999, Trier)

„Neue Formen des elektronischen Publizierens“
Ringvorlesung Medienwissenschaften (November 1999, Trier)

“Efficient Manipulation of Boolean Function with OBDDs“
Königliche Technische Universität Stockholm (Dezember 1999, Stockholm)

“Using OBDDs for Formal Verification“
Technologisches Institut Stockholm (Dezember 1999, Stockholm)

Martin Mundhenk:

Harte Instanzen
35. Workshop über Komplexitätstheorie, Datenstrukturen und Effiziente Algorithmen (Juni 1998, Paderborn).

Hard instances for NP-hard sets
35. Workshop über Komplexitätstheorie, effiziente Algorithmen und Datenstrukturen, Metz (Frankreich), 23. Mai 1999

Harte Instanzen
Oberseminar Informatik, Universität Würzburg, 1. Juli 1999.

Propositional proofs and their complexity
11th European Summerschool in Logic, Language and Information, Utrecht (Niederlande), 9.–13. August 1999.

Hard-to-prove tautologies
Midwest Theory Day, University of Chicago, 4. Dezember 1999.

Frank Recker:

The Search Complexity in Trees with a Lying Oracle
Colloquium on Combinatorics, Braunschweig, 12.–13. November 1999.

Harald Sack:

$\oplus$-OBDDs - a BDD Structure for Probabilistic Verification
3. Berlin-Trierer Workshop zur Algorithmischen Diskreten Mathematik und Mathematischen Optimierung (ADiMMO'98), (April 1998).

$\oplus$-OBDDs - a BDD Structure for Probabilistic Verification
1998 IEEE/ACM Int. Workshop on Logic Synthesis (IWLS98), Lake Tahoe, Cal, (Juni 1998)

$\oplus$-OBDDs - a BDD Structure for Probabilistic Verification
1998 Workshop on Probabilistic Methods in Verification (PROBMIV'98) Indianapolis, IN, USA , (Juni 1998)

Sample Method for Minimization of OBDDs
25th Annual Conference on Current Trends in Theory and Practice of Informatics, (SOFSEM'98), Jasna, Slovakia, (November 1998)

Algorithmic Considerations for Parity-OBDD Reordering
1999 IEEE/ACM Int. Workshop on Logic Synthesis (IWLS99), Lake Tahoe, Cal, (Juni 1999)

Algorithmic Considerations for Parity-OBDD Reordering
4th International Workshop on Applications of the Reed-Müller Expansion in Circuit Design (Reed-Müller 99), Victoria, B.C., Canada, (August 1999)

Christian Stangier:

OBDD-based Verification of Communication Protocols,
34. Workshop über Komplexitätstheorie, Datenstrukturen und Effiziente Algorithmen (März 1998, Chemnitz).

OBDD-based Verification of Communication Protocols
3. Berlin-Trierer Workshop zur Algorithmischen Diskreten Mathematik und Mathematischen Optimierung (ADiMMO'98), (April 1998).

Speeding Up Model Checking,
5th International Conference on Advanced Computer Systems (ACS'98), Szczecin, Polen, (November 1998).

Effiziente Methoden für die OBDD Minimierung
DFG-Schwerpunktkolloquium ALGORITHMEN 1998, Köln, (November 1998).

Accelerating Variable Reordering
Dagstuhl Seminar: Computer-Aided Design and Test '99, Dagstuhl Februar 99).

Arno Wagner:

OHO - OBDD Heuristics Online
Dagstuhl Seminar: Computer-Aided Design and Test '99, Dagstuhl Februar 99).

9.2 Vorträge im Informatik–Oberseminar

30.11.99 **Arno Wagner**:
Firewalls - Struktur, Einsatz, Attacken

06.07.99 **Martin Mundhenk**:
Die Komplexität von Entscheidungsprozessen

22.06.99 **Frank Recker**:
Ein beweisbar sicheres Verschlüsselungsverfahren

15.06.99 **Carsten Damm**:
Boolesche und Arithmetische Berechnungen - Ein vergleichender Überblick

30.06.98 **Frank Recker**:
Kombinatorische Suche

19.05.98 **Carsten Damm**:
Uber die Simulation Boolescher durch Arithmetische Schaltkreise

9.3 Vorträge im Forschungsseminar

21.12.99	**Jochen Bern**: *Computer Aided Conference STACS 2000 - Demonstration und Erfahrungsbericht*
14.12.99	**Christian Stangier**: *A High Level Heuristic for Partitioning of Transition Relations*
07.12.99	**Arno Wagner**: *Watermarking im Electronic Design: Stand der Dinge*
30.11.99	**Harald Sack**: *Reordering of Parity OBDDs - How To ?*
23.11.99	**Staffan Ulfberg**: *On Lower Bounds for Median Selection*
16.11.99	**Frank Recker**: *Die Suchkomplexität bei einem lügenden Orakel*
09.11.99	**Martin Mundhenk**: *Ein kurzer Beweis für lange Resolutionsbeweise (nach einer Arbeit von Beame und Pitassi)*
16.09.99	**Frank Recker**: *Verwaltung von verschiedenen Softwareversionen mit CVS*
14.09.99	**Christian Stangier**: *Erfahrungsbericht Synopsys: Protokolldesign und Verifikation in der Praxis*
06.07.99	**Anca Muscholl**: *Quantencomputing*
29.06.99	**Frank Recker**: *Ein Secret Sharing Verfahren für Dateien*
22.06.99	**Arno Wagner und Harald Sack**: *Obdd Heuristics Online: Kurzvortrag vor der IWLS*
15.06.99	**Martin Mundhenk**: *Das Leerheitsproblem für probabilistische endliche Automaten (mit einer Anwendung für POMDPs)*
01.06.99	**Jochen Bern**: *BIND, ntp, sendmail - Typische Aufgaben der Systemadministration*
25.05.99	**Carsten Damm**: *Komplexität von Tensorformeln*
09.02.99	**Christian Stangier**: *Mulvar - multiple Variablenordnungen - einige theoretische Aspekte*
02.02.99	**Michael Schommer**: *Private Simultaneous Messages (über eine Arbeit von Ishai und Kushilevitz)*
01.12.98	**Jordan Gergov**: *Compile-Time Memory Optimization and Interval Coloring of Intersection Graphs*

24.11.98	**Stanislav Žák** (Prague): *Inert branching programs and other problems*
10.11.98	**Christian Stangier**: *Speeding up symbolic model checking*
05.10.98	**Christoph Meinel**: *Kurzbericht über die SIGDOC-Konferenz*
08.09.98	**Harald Sack**: *Design mapping for large scale combinational and sequential circuits*
07.07.98	**Christian Stangier**: *BDD's und das Problem multipler Variablenordnungen (IWLS'98)*
30.06.98	**Martin Mundhenk**: PP*- und* NP^{PP}*-vollständige Planungsprobleme*
02.06.98	**Stasys Jukna**: *Monotone span programs (the best of 1995-97)*
19.05.98	**Carsten Damm**: *Über Boolesche und Parity-Überdeckungen*
28.04.98	**Frank Recker**: *Kombinatorische Suche in Bäumen (Zusammenfassung)*
31.03.98	**Jens Doppelhamer**: *Bericht über das ECCC-Projekt*
19.03.98	**Arno Wagner**: *Perl-Seminar I (Zusatzliteratur: Perl-Reference-Guide)*
17.03.98	**S. Blank, H. Frieden, T. Frieden**: *VLSI-Praktikum (Bericht)*
03.03.98	**Masohiro Fujita** (Fujitsu Labs): *Boolean Comparison Techniques for Two Similar Circuits*
17.02.98	**Carsten Damm**: *On semi-unbounded circuits*
10.02.98	**Martin Mundhenk**: *Interaktive Beweissysteme*
03.02.98	**Jens Doppelhamer / Johannes Lehnert**: *Optimale Sokoban-Strategien* *mit OBDD's*
27.01.98	**Stasys Jukna**: *On Gentle Branching Programs*
20.01.98	**Anna Slobodová**: *Canonical TBDD's and Their Application to Combinatorial Verification* *(Goldberg et al.)*

9.4 Gäste und Gastvorträge

28.01.98	**Priv.-Doz. Dr. med. Sigmund**, Chefarzt der Radiologie des Mutterhauses der Borromäerinnen, Trier *Telemedizin aus klinischer Sicht*
26. – 27.03.98	**Gianpiero Cabodi, Stefano Quer, Politechnico Torino**, Italien (Forschungsbesuch)
02.03.98	**Masohiro Fujita** , Fujitsu Labs, Santa Clara , USA *Model Checking: Its Basics and Reality*
06. – 07.04.98	**Kurt Mehlhorn**, MPI Saarbrücken *Vom Algorithmus zum Programm*
	Gerd Tinhofer, TU München *Kombinatorische Kompaktheit*
	Peter Widmayer, ETH Zürich *Eins–zwei–drei – wie zählt man in einem verteilten System?*
16.06.98	**Dr. Christel Baier**, Universität Mannheim *Probabilistisches Model Checking: ein Resume der automatischen Verifikation randomisierter Prozesse*
01.07.98	**Prof. Dr. Klaus Merle**, Zentrum für DV, Universität Mainz *Internet-Telefonie - eine echte Alternative zum klassischen Telefon?*
22.07.98	**Dr. Wolfgang Knappe** *Überblick zu den gewerblichen Schutzrechten Wichtige Bestimmungen und Überlegungen*
04.11.98	**Anderson Luiz de Araujo Lima**, Faculdades Positivo-Curitaba, Brasilien *Development of Generic Internet-based Managemend Tools*
01.–10.11.98	**Stanislav Žák**, Institute for Computer Science, Czech Academy of Sciences *Branching Programs - contemporary trends*
13.11.98	**Dr. Jutta Thielen** *Einfluß atmosphärischer Prozesse auf industrielle Abläufe: Zwei Beispiele aus der Medizin- und Hydrometeorologie*
18.11.98	**Dr. Angela Requate**, Universität Bergen *Das Wittgensteinarchiv der Universität Bergen – Bericht über die elektronische Ausgabe des Nachlasses Ludwig Wittgensteins*

16.12.98	**Dr.-Ing. G. Deuster**, Fraunhofer Management GmbH, München *Mechanismen und Rahmenbedingungen von Technologietransfer- und Innovationsprozessen unter besonderer Berücksichtigung junger innovativer Unternehmen*
18.01.99	**Prof. Dr. Shparlinski**, Macquarie University, Sidney/Australia *On Fourier Coefficients of Functions Deciding Quadratic Residuacity* (Graduiertenkolleg)
05.–16.07.99	**Prof. Dr. Judy Goldsmith**, University of Kentucky, Lexington/USA *Counting Sets*
05.–16.07.99	**Christopher Lusena**, University of Kentucky, Lexington/USA
09.–16.10.99	**Dr. Elena Dubrova**, Royal Institute of Technology, Kista/Sweden *Multiple-Valued Logic in VLSI: Challenges and Opportunities* (Graduiertenkolleg) *Three-Level Minimization of Boolean Functions* (Forschungsseminar)
05.–14.11.99	**Dr. Stanislav Žák**, Institute for Computer Science, Czech Academy of Sciences, Prague
22.–25.11.99	**Staffan Ulfberg**, University of Stockholm/Sweden *Lower Bounds for Median Selection* (Forschungsseminar) *Lower Bounds for Bounded Depth Perceptrons* (Graduiertenkolleg)
16.–19.11.99	**Prof. Dr. Stephan Waack**, Universität Göttingen
29.11.–03.12.99	**Dr. Elena Dubrova**, Royal Institute of Technology, Kista/Sweden
30.11.–02.12.99	**Prof. Dr. Shparlinski**, Macquarie University, Sidney/Australia *Pseudorandom Number Generators in Cryptography and Monte Carlo Methods* (Graduiertenkolleg)

10 Mitgliedschaften in Programmkomitees und Aufsichtsräten, Gutachtertätigkeiten

Carsten Damm:

Gutachtertätigkeiten

- Conference on Computational Complexity 1998
- International Workshop on Boolean Problems 1998
- Symposium on Theoretical Aspects of Computer Science 1999
- Zentralblatt für Mathematik
- IEE Proceedings on Computer and Digital Techniques 1999
- Informatik-Spektrum 1999
- Journal of Computer and Systems Sciences 1999
- IEEE Transactions on Computer Aided Design 1999
- ICALP'99
- MFCS'99
- STACS2000

Stasys Jukna:

Gutachtertätigkeiten

- SIAM Journal on Computing
- Symposium on Theoretical Aspects of Computer Science, STACS'99
- ICALP'99
- RAIRO Journal on Theoretical Informatics
- Theoretical Computer Science
- Computational Complexity 98 (CCC'98)

Christoph Meinel:

Veranstaltung von Tagungen und Symposien

- Veranstalter des Trierer ADiMMO Workshops der DFG Graduiertenkollegs Algorithmische Diskrete Mathematik (Berlin) und Mathematische Optimierung (Trier) 6. und 7. April, 1998
- Veranstalter des Trierer Telemedizin Symposiums 8./9.10.98
- Chairman von STACS'99, 4.-6.03.1999, Trier
- Veranstalter des Trierer Symposiums *Elektronisches Publizieren* 25./26.03.99
- Veranstalter des Trierer Symposiums *Televerwaltung* 11./12.11.99

Mitglied im Programm-Komitees nationaler und internationaler Tagungen

- 5th International Luxembourg Congress on New Technology in Surgery, 09. - 12.12.98, München,
- Trierer Telemedizin Symposium 8./9.10.98,
- 3rd International Workshop on Boolean Problems 17./18.09.98, Freiberg (Sachsen),
- 1. Sächsisches Telemedizinsymposium 26./27.06.98, Dresden,
- STACS'98 - Symposium on Theoretical Aspects of Computer Science 25.-27.02.98, Paris
- Date'99 - Design, Automation and Test in Europa, 09.-12.03.99, München
- ICALP'99 - Internatical Colloquium on Automata, Languages and Programming, 11.-15.06.99, Prag

Weitere Funktionen

- Sprecher der GI-Fachgruppe 0.1.4 „Komplexität"
- Direktor des Zentrums für Wissenschaftliches Elektronisches Publizieren (WEP)
- Mitglied des wissenschaftlichen Direktoriums (bis April 1998) und des Aufsichtsrates des IBFI Schloss Dagstuhl (ab Mai 1998)
- Mitglied des Technologiebeirats Rheinland-Pfalz
- Mitglied der Arbeitsgruppe Gesundheit des Forums Info 2000 von BMBF
- Vertrauensdozent der Gesellschaft für Informatik an der Universität Trier

Gutachtertätigkeiten

- STACS'99
- ICALP'99
- DAC´99
- DATE´99
- ICCAD¸98
- Information Processing Letter
- Formal Methode in CAD
- IEEE Journal on CAD
- IEEE Journal on Computers

- Zentralblatt für Mathematik
- Deutsche Forschungsgemeinschaft DFG
- Stiftung Innovation Rheinland-Pfalz

Martin Mundhenk:

Gutachtertätigkeiten

- Conference on Computational Complexity 1998
- Symposium on Theoretical Aspects of Computer Science 1999

Frank Recker:

Gutachtertätigkeiten

- Symposium on Theoretical Aspects of Computer Science 1999

Harald Sack:

Veranstaltung von Tagungen und Symposien

- Veranstalter des Trierer Symposiums *Elektronisches Publizieren* 25./26.03.99

Weitere Funktionen

- Geschäftsführer des Zentrums für Wissenschaftliches Elektronisches Publizieren (WEP) an der Universität Trier

Gutachtertätigkeiten

- DAC 1998
- IWLS 1998
- DAC 1999
- DATE 1999
- ICALP 1999
- MFCS 1999
- IWLS 1999
- IEEE Transactions on Computers
- IEEE Transactions on CAD

Christian Stangier:

Gutachtertätigkeiten

- DAC 1998
- IWLS 1998
- DAC 1999
- DATE 1999
- ICALP 1999
- MFCS 1999
- IEEE Transactions on CAD

Arno Wagner:

Gutachtertätigkeiten

- DAC 1999
- DATE 1999
- IWLS 1999

11 Rechnerausstattung

Im Laufe des Jahres 1999 konnte ein im September 1997 eingereichter WAP-Antrag abgewickelt und so die Ausstattung der Professur mit Arbeitsplatzrechnern sichergestellt werden. Damit ging insbesondere auch eine Umorientierung vom Betriebssystem SunOS auf Linux einher. Gegen Ende des Jahres wurde nur noch ein Arbeitsplatz — der des Verwalters der SUNs — sowie Server für solche Dienste, die benötigt wurden und nur auf der SUN-Plattform verfügbar sind, auf SUN-Basis betrieben.

Derzeit sind insgesamt 15 Pentium-PCs und drei SUNs 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, seltener Windows, meist bibootable auf derselben Maschine, für die PCs. Auch die Drucker wurden erneuert, anstelle der beiden SPARCprinter (die nur an eine SUN angeschlossen arbeiteten) und des allmählich unzuverlässig werdenden HP IIIsi sind nun zwei HP LaserJet der 4000er Reihe im Einsatz. Des weiteren konnten Peripheriegeräte zur Unterstützung von Multimedia-Anwendungen beschafft werden.

Zum Jahreswechsel 1999/2000 rückte insbesondere die Vorbereitung auf mögliche Y2K-Probleme in den Mittelpunkt der Systemadministration. Während die Linux-Rechner neuwertig und weitestgehend von entsprechenden Zusagen abgedeckt waren, mußte davon ausgegangen werden, daß die SUNs nach dem Jahreswechsel nicht mehr betriebsbereit sein würden. Für diejenigen Dienste, die noch auf SUNs angesiedelt waren — wie gesagt nur solche, die nicht in äquivalenter Form auf anderen Rechnern zur Verfügung stehen —, wurden deswegen entsprechende Ausweichplanungen angestellt und die betroffenen SUNs mit den verfügbaren Y2K Patches bestückt. Tatsächlich stellte sich heraus, daß Y2K-Probleme auch auf diesen als anfällig einzustufenden Maschinen äußerst selten und dort, wo sie auftraten, harmlos bis vernachlässigbar waren.

Zur Netzwerkinstallation ist anzumerken, daß das V-Gebäude in 1998 — im Rahmen des schon seit längerem laufenden Hochschulbauantrages — vollständig von *10Base2 Ethernet* (Bus-Struktur) mit *EAD-Anschlußdosen* auf eine modulare Vernetzung auf der Basis von *10BaseT / 100BaseTX Ethernet* (Stern-Struktur) mit *RJ45-Anschlußdosen* in neu installierten Brüstungskanälen umgestellt wurde. Da die Finanzierung vollständig aus dem erwähnten Antrag erfolgte und keine nennenswerten technischen Probleme beim Anschluß alter Hardware an das neue Netzwerk auftraten, hatte dies keinen Effekt auf die eigentliche Rechnersituation der Professur.

Ebenfalls in 1998 wurden erste Pläne für einen Umzug der Informatik in das (noch umzubauende) *Hospital* vorgelegt. Das Netzwerk dort ist für die von der Informatik belegten Räume auf Glasfaserbasis projektiert *(10BaseF / 100BaseFX Ethernet).* Es ist nicht davon auszugehen, daß die neuerliche Umstellung mehr Probleme bereitet als die oben erwähnte.

Im Jahr 1999 wurden die aktiven Netzwerkkomponenten — bis dahin eine Mischung von Switches und Hubs, Informatik-eigenen und vom Rechenzentrum bereitgestellten, mit Port-Zahlen bis hinauf zu zwei Dutzend — durch einen einzelnen, vom Rechenzentrum betriebenen Gigabit Ethernet Switch von Cisco ersetzt. Verbunden damit ist eine Umstellung des „Backbone", an das die Informatik angeschlossen ist, vom früheren FDDI-Ring mit festem Routing auf das neue Gigabit Ethernet mit VLANs. Zu den Vorteilen dieses neuen Aufbaus gehört neben der erhöhten Bandbreite für jede Netzwerkdose ("dedicated full duplex 100 Mbps on desk") insbesondere die VLAN-typische Fähigkeit, kurz- (Vorführrechner in einem Hörsaal) oder langfristig (z.B. Professur Näher im Drittmittelgebäude) Rechner an Stellen zu betreiben, an denen sie bei statischem Routing ohne neu zugewiesene Adresse nicht betriebsfähig wären.