SCHLOSS DAGSTUHL

INTERNATIONAL
CONFERENCE AND
RESEARCH CENTER
FOR COMPUTER SCIENCE

Informatics
10 Years Back, 10 Years Ahead

Conference at the Occasion of the
10th Anniversary of Schloss Dagstuhl

Saarbrücken, August 27 - 31, 2000

Program

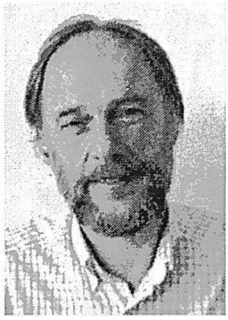
Contents

Address:
IBFI Schloss Dagstuhl, D-66687 Wadern, Germany
Tel.: +49-6871-9050

Information:
Dagstuhl Office, Universität des Saarlandes,
Postfach 15 11 50, D-66041 Saarbrücken, Germany
Tel: +49-681-302-4398, E-Mail: office@dagstuhl.de

Conference Web Page:
http://www.dagstuhl.de/10Years/

Welcome



Welcome to the Conference *"Informatics - 10 Years Back, 10 Years Ahead"* at the occasion of the 10th anniversary of the International Conference and Research Center in Schloss Dagstuhl. Internationally renowned scientists and engineers from different areas of Informatics and neighbouring disciplines will present their views of the state of our field, of past contributions, and of remaining challenges. Stimulating discussions (almost) in the style known and appreciated from Dagstuhl may clarify and push ahead some of the visions. We hope that this conference will have a strong impact on our field. When we discussed how to celebrate Dagstuhl's anniversary the idea of such a conference was quite compelling as it could concentrate in one week the efforts we do all across Informatics over the whole year. Exploiting the feelings of gratitude towards Dagstuhl of frequent guests allowed us to come up with this interesting program. We are very grateful to the speakers who were willing to lean back for a while, employ their visionary talents, travel to Saarbrücken, and share the results of their thinking process with us.

Fresh Informatics doctors or doctors to be from Dagstuhl's member universities and the German dissertation award competition have the chance to present posters about their work.

An evening discussion (in German) will discuss Virtualization, "How Images Change Reality". It is organized together with Saarland Radio.

Proceedings of the talks will be produced after the conference by Springer Verlag as *"Lecture Notes in Computer Science, Vol. 2000"* and will be distributed to the conference participants.

We are grateful to Saarland University for hosting this conference. It is a pleasure to acknowledge the support our sponsors provided through their generous contributions.

Saarbrücken, August 27, 2000 *Reinhard Wilhelm*

Talks

Monday, August 28

The Web

The Web in 2010: Challenges and Opportunities for Database Research

Gerhard Weikum, Universität des Saarlandes, Germany

The impressive advances in global networking and information technology provide great opportunities for all kinds of Web-based information services, ranging from digital libraries and information discovery to virtual-enterprise workflows and electronic commerce.

However, many of these services still exhibit rather poor quality in terms of unacceptable performance during load peaks, frequent and long outages, and unsatisfactory search results. For the next decade, the overriding goal of database research should be to provide means for building zero-administration, self-tuning information services with predictable response time, virtually continuous availability, and, ultimately, "money-back" service-quality guarantees.

A particularly challenging aspect of this theme is the quality of search results in digital libraries, scientific data repositories, and on the Web. To aim for more intelligent search that can truly find needles in haystacks, classical information retrieval methods should be integrated with querying capabilities for structurally richer Web data, most notably XML data, automatic classification methods based on standardized ontologies and statistical machine learning, and more aggressive caching and prefetching for efficiency.

The talk gives an overview of promising research directions along these lines.

Ubiquitous Data Access Michael Franklin, University of California, Berkeley, USA The Asilomar Report on Database Re-

search cites ubiquitous "information appliances" as a major driver for database systems research over the next ten years. For the present, however, the use of mobile devices is mostly restricted to Personal Information Management (PIM) applications. In order to fully realize the potential of ubiquitous data access, such devices must be allowed to serve as an extension to the Web and to enterprise data management infrastructures. Furthermore, while some pundits claim that human attention is becoming the primary bottleneck, recent commercial failures and an explosion in the global demand for data storage indicate that old fashioned performance issues still matter.

Data management technology must be adapted to deal with the limitations as well as the tremendous opportunities of large-scale ubiquitous data access. Challenges exist in core database areas such as system architecture, query processing, and transaction management, as well as in emerging areas such as data dissemination and user-centered, context-aware data delivery. In this talk I will outline several of these challenges and describe approaches that have been proposed to meet them.

Ubiquitous Data Access

Michael Franklin, University of California, Berkeley, USA

The Asilomar Report on Database Research cites ubiquitous "information appliances" as a major driver for database systems research over the next ten years. For the present, however, the use of mobile devices is mostly restricted to Personal Information Management (PIM) applications. In order to fully realize the potential of ubiquitous data access, such devices must be allowed to serve as an extension to the Web and to enterprise data management infrastructures. Furthermore, while some pundits claim that human attention is becoming the primary bottleneck, recent commercial failures and an explosion in the global demand for data storage indicate that old fashioned performance issues still matter.

Data management technology must be adapted to deal with the limitations as well as the tremendous opportunities of large-scale ubiquitous data access. Challenges exist in core data-

base areas such as system architecture, query processing, and transaction management, as well as in emerging areas such as data dissemination and user-centered, context-aware data delivery. In this talk I will outline several of these challenges and describe approaches that have been proposed to meet them.

Programmable Networks

Andrew T. Campbell, Columbia University, USA

Recent advances in active network technology, open signaling and control, distributed systems, service creation, resource allocation and transportable software are driving a reexamination of existing network architectures, middleware and the evolution of control and management systems away from traditional constrained solutions. The ability to dynamically create, deploy and manage new network architectures, protocols and services in response to user demands is creating a paradigm shift in telecommunications. Network researchers are exploring new ways in which network switches, routers and base stations can be dynamically programmed by network applications, users, operators and third parties to accelerate network innovation.

This trend reflects the acceptance of computing and middleware paradigms in telecommunication networks. Programmable networks seek to exploit advanced software techniques and technologies in order to make network infrastructure more flexible, thereby allowing users and service providers to customize network elements to meet their own specific needs. Customizing routing, signaling, resource allocation and accelerating information processing in this manner raises a number of significant security, reliability and performance issues. In this talk we will discuss the state of the art in programmable networks. We will discuss a number of important innovations that are creating a paradigm shift in networking leading to higher levels of network programmability.

Technologies for Multilateral Security

Andreas Pfitzmann, TU Dresden, Germany

After pointing out some basic facts about security technology in general, a structured overview of technologies for multilateral security is given. An evaluation of the maturity and effectiveness of these technologies shows that some should be applied immediately, while others need quite a bit of further research and development.

Cryptography

Ueli Maurer, ETH Zürich, Switzerland

Information is becoming a crucial if not the most important resource of the economy and the society at large. The protection of this new resource and of intellectual property in general is vital for the development of the envisaged information society. While some basic security requirements such as confidentiality, authenticity, and availability of information are quite well understood, new applications like voting over the Internet, digital payment systems, the protection of personal privacy, distributed databases and many more lead to new and more complex security requirements. Many of them still remain to be identified, understood, and solved.

This talk reviews the primary role that cryptography plays in information security. We summarize the most important achievements in cryptography in the past years, demonstrate the beauty of some of these results, take a look at the hot current research areas, and discuss some of the major challenges for future research in cryptography.

The Case for Language-Based Security

Fred B. Schneider, Cornell University, USA

The flexibility provided by today's extensible system architectures is also a source of vulnerability. Extensible systems must therefore have security mechanisms to protect against malicious actions by foreign code—whether that code is provided locally or downloaded across the network. The security mechanisms we seek must support the Principle of Least Privilege instantiated with application-level abstractions, in addition to exhibiting only modest run-time overheads. This talk will discuss a search for those mechanisms, describing how program translation and analysis techniques help.

Thank to the sponsor of the conference banquet

COMPAQ

Immersion into Other Disciplines

Bioinformatics - From Genomic Data to New Drugs

Thomas Lengauer, GMD - St. Augustin, Germany

Life's processes are composed of complex biochemical reaction networks. Within these networks matter (metabolic networks) as well as information (regulatory networks) are processed. Many diseases arise from imbalances within the network. Medical therapy is aimed bringing the network back to balance. Today this is mostly done by breaking cycles within the network that drive the disease.

The identification of a location within the network, at which a cycle is to be broken, amounts to the selection of a "target" protein that catalyzes the respective reaction. Blocking the function of the target protein by tightly binding a drug molecule to it can then effectively break the cycle. Today all drugs used over the world target only about 500 proteins. In contrast, at least several thousand of the estimated 50 000 proteins of man are presumed to be viable targets for drugs. In the past few years new screening methods of molecular biology have afforded a comprehensive search for protein targets. The respective experiments generate voluminous data from with a few promising proteins have to be selected for further experimental study. Bioinformatics methods are an essential aid in this selection.

Once the target protein has been identified, we have to search for a drug molecule that blocks the target protein. Systematic search for drug molecules has also been made possible only a few years ago, with high-throughput screening methods that measure binding affinities and combinatorial chemistry methods with which one can synthesize a large variety of new drug candidates. Here again, preselection can be greatly improved with the help of bioinformatics methods.

We summarize research activities that have been conducted at GMD in the past few years and resulted in effective bioinformatics software contributing to these goals. We use discrete algorithmic and statistical methods in order to quickly come up with viable molecular hypotheses on computers such as PCs or workstations.

Computer Science in Physics

Peter Young, Physics Department, University of California - Santa Cruz, USA

There is a great deal of interest in the physics community in problems where determination of the ground state is non-trivial because of conflicts (called "frustration") between different terms in the energy. The most commonly studied such example is the "spin glass".

In this talk I will discuss some of the advances that have been made in understanding spin glasses and related systems through the application of optimization techniques from computer science, which enable one to determine exact ground states for quite large systems.

Actually, the physics community is frequently less interested in the ground state than in the behavior of the system at low but finite temperature. As an example, one might like to know whether a finite temperature phase transition occurs in a spin glass system. Low temperature properties are controlled by excitations out of the ground state, and I will show that optimization techniques can usefully study them by determining how the ground state changes in response to various types of perturbation.

We thank our sponsor

DaimlerChrysler

Tuesday, August 29

Software

Software Engineering - Future Challenges

H. Dieter Rombach, Universität Kaiserslautern
& Fraunhofer IESE Kaiserslautern, Germany

The role of software will change dramatically in the near future from *adding value and optimizing* existing products and business processes to *enabling* new products and business processes. This foreseeable trend does not only change the economic view on software from cost to revenue generator, but also requires competencies in innovative technologies and sound engineering.

This presentation paints some future scenarios of software, derives key requirements for *engineering practices* suitable for such software, and defines major scientific, engineering, and educational challenges.

Formal Methods

Clifford B. Jones, University of Newcastle, United Kingdom

The idea that some formally-based notation should be used is common to most engineering disciplines. The essence of formality is not to things difficult but just to ensure that "calculations" based on an abstract model will not result in inconsistencies. The extent to which interesting properties of reality can be captured in such abstractions is of course another question. This talk will try to take a broad look at some of the attempts to use formalism in the design of computer systems. While basically positive, it will look at failures and genuine open problems as well as obvious successes. Since other speakers will cover some interesting areas such as model checking and abstract interpretation, the main focus will be on formalism in specification and development methods.

Software Engineering - The Avionics Case

Famanta Randimbivololona, Aerospatiale Matra Airbus, Toulouse, France

Avionics are mostly based on embedded-computers where functions - and hence safety goals - are implemented partly by electronics and partly by software. Software solutions and engineering have to comply with explicit safety requirements as defined by the assigned criticality levels and systems safety analyses. Currently, major trends are the ever-increasing part and the ever-growing volume of the software due to the conjunction of basic technologies opportunities and needs for new functions : evolution in software solutions and engineering are expected to cope with this situation.

The Gap between Software Research and Practice

James R Larus, Microsoft Research - Redmond, USA

Software development, of course, is an old and nagging problem that has been, at various times, the focus of considerable academic attention. Nevertheless, this research (and computer science education, for that matter) has had little positive impact on commercial software development. The problems in this area are obviously difficult and improvement slow, but progress is impeded by a large gap between academic research and education and actual development problems and constraints. This gap has many aspects, ranging from a lack of understanding, choice of problems, issues of scale, to education. Given the ever growing importance of software to the world economy, it is time to renew attempts to bridge these two worlds and form a joint resolve to improve software development and software quality. This talk is a first step that briefly identifies some dimensions of this gap and, even more briefly, proposes solutions to a few problems.

Progress on Abstract Interpretation Based Formal Methods and Future Challenges

Patrick Cousot, École normale supérieure, Paris, France

Abstract Interpretation is a theory of approximation of the behavior of dynamic discrete systems such as the formal semantics of programs. Since such behaviors can be characterized by fixpoints, the theory essentially provides constructive and effective methods for fixpoint approximation and checking by abstraction.

Non-conventional *applications* of abstract interpretation include the design of hierarchies of semantics at different levels of observation of program execution, the generation of heuristics for search problems in artificial intelligence, program watermarking, etc.

The origin and most well-known application of abstract interpretation is *program analysis* that is the automatic static determination of dynamic run-time properties of programs. Formally, this subsumes and includes data flow analysis, set or constraint based analysis, type inference, etc. Program analysis techniques are used for compile-time program optimization, partial evaluation, program abstract model-checking, abstract program debugging and testing and more generally *semantic-based software verification and manipulation.*

In the past ten years, program analysis by abstract interpretation moved from an intensive research area to its first industrial applications leading to the emergence of innovative startups.

The impressive evolution of hardware by a factor of 10^6 over the past 25 years has lead to a similar explosion of the size of programs. The size, complexity and scope of application of large programs is likely to continue expanding rapidly in the next decade. These big programs will have to be modified and maintained during their whole lifetime which often exceeds 20 years. The size and efficiency of the programming and maintenance teams in charge of their design and follow-up cannot grow up in similar proportions. At a not so uncommon rate of one bug per thousand lines such huge programs might rapidly become hardly manageable in particular for safety critical systems.

Therefore in the next 10 years, the *software reliability* problem is likely to become a major concern to modern computer-dependent societies.

In this context, we will discuss why, in comparison with other empirical and formal methods, program analysis is likely to shortly become a dependable, inescapable and cost-effective software verification method. We will take a prospective look at a number of future challenges for research and development in abstract interpretation based formal methods, including program analysis.

Program Checking

K. Rustan M. Leino, Compaq SRC - Palo Alto CA, USA

A powerful approach to finding errors in computer software is to translate a given program into a verification condition, a logical formula that is true if and only if the program is free of the classes of errors under consideration. Finding errors in the program is then done by mechanically searching for counterexamples to the verification condition.

This talk gives an overview of the technology that goes into such program checkers, reports on some of the progress and lessons learned in the past ten years, and identifies some remaining challenges.

We thank our sponsor

SAP AG

Progress on the State Explosion Problem in Model Checking

Edmund M. Clarke, Carnegie Mellon University - Pittsburgh, USA

Model checking is an automatic verification technique for finite state concurrent systems. In this approach to verification, temporal logic specifications are checked by an exhaustive search of the state space of the concurrent system. Since the size of the state space grows exponentially with the number of processes, model checking techniques based on explicit state enumeration can only handle relatively small examples. This phenomenon is commonly called the "State Explosion Problem".

Over the past ten years considerable progress has been made on this problem by

1. representing the state space symbolically using BDDs and by
2. using abstraction to reduce the size of the state space that must be searched.

As a result model checking has been used successfully to find extremely subtle errors in hardware controllers and communication protocols.

In spite of these successes, however, additional research is needed to handle large designs of industrial complexity. In this talk, we will focus on recent advances in the two directions mentioned above. We show how LTL model checking can be efficiently reduced to propositional satisfiability (SAT). As a result, powerful new SAT procedures like GRASP and Stalmarck's method can be used instead of BDDs for model checking. We will also describe an automatic abstraction methodology that exploits information obtained form spurious counterexamples to obtain increasingly more accurate abstractions.

From Research Software to Open Source

Susan L. Graham, University of California, Berkeley, USA

It is a longstanding practice that software researchers share their source code with the research community, allowing other researchers to inspect their work and to build on it. Many widely-used software systems originated as code distributions from research projects. Early examples include Berkeley Unix, sendmail, TeX, Emacs, and many others. The distribution practices of the research community evolved into the free software movement initiated by Richard Stallman, and the more recent open source and libre software movements. Eric Raymond has argued eloquently in The Cathedral and the Bazaar that the development processes that stem from these approaches to software development and distribution lead to higher quality software than the traditional proprietary approaches. There is much talk about open source in the commercial arena.

In this talk I will review the issues that surround the open source approach to software development. What are the problems and the benefits? Is open source still the right approach for the research community? What is its role in the commercial world? Will the Bazaar crowd out the Cathedral?

We thank our sponsor

Microsoft® Research

Wednesday, August 30

Architecture

Microprocessors: 10 Years Back, 10 Years Ahead

Gurindar S. Sohi, Univ. Wisconsin - Madison, USA

The past decade has seen a tremendous improvement in microprocessor performance brought on by two factors: faster transistors, and many more transistors. A 30-fold increase in the number of transistors on a microprocessor chip has allowed microprocessor architects to use a horde of techniques to improve performance: multiple instruction issue, out-of-order execution, speculative execution. Starting with single-issue, in-order execution processors at the beginning of the decade, we now routinely have four-issue, out-of-order execution processors. The next decade promises to be equally exciting for computer architects, as another 30-fold increase in the transistor budget will enable even more opportunities. New opportunities, however, will bring new constraints, such as wire speeds and power budgets. Microprocessor architects are expected to use these new opportunities to continue to improve the exploitation of instruction-level parallelism (ILP), as well as moving towards to the exploitation of thread-level parallelism.

This talk will attempt to put the past and (likely) future evolution of microprocessors into context. We will discuss the research successes of the past that have successfully influenced modern microprocessors (e.g., ILP, out-of-order execution, speculative execution), current research issues that are likely to impact next-decade microprocessors (e.g., multithreading, speculative multithreading), as well as future research issues that are likely to be successful in influencing future-generation microprocessors.

The Quantum Computing Challenge

Paul Vitanyi, CWI - Amsterdam, The Netherlands

New computation devices increasingly depend on particular physical properties rather than on logical organization alone as used to be the case in conventional technologies. The laws of physics impose limits on increases in computing power. Two of these limits are interconnect wires in multicomputers and thermodynamic limits to energy dissipation in all computers.

Quantum computing is a novel computational paradigm and technology that promises to eliminate problems of latency and wiring associated with parallel computers and the rapidly approaching ultimate limits to computing power imposed by the fundamental thermodynamics. The prospect of quantum computing has created excitement both among researchers and in the popular press by its algorithmic improvements over classical computing: integer factorization in square time (Shor), searching unstructured lists in square root time (Grover), improved communication complexity (Buhrman, Cleve).

For some other problems (like binary search) quantum computation gives no super-linear speed-up over classical computing. While fast factoring will break almost all public key cryptosystems in use today, compromising almost all secure (financial, government, commerce) e-transactions, quantum cryptography (Bennett, Brassard) may possibly come to the rescue. Superiority of quantum computing over classical probabilistic computing are due to the exploitation of interference in parallel quantum superposition and quantum entanglement. The actual realization of quantum computers is a formidable technological and theoretical challenge. Part of this challenge involves quantum information and communication theory (compression, fault-tolerance and error-correcting codes).

The great algorithmic challenge is to find more quantum algorithms that improve classical ones (or show that none exist), and to more precisely determine the complexity of quantum computations compared to the classical complexity classes.

(Joint work with Harry Buhrman and Ronald de Wolf.)

Parallelism: Considering Software and Hardware Concurrently

Lawrence Snyder, University of Washington, USA

The promises and frustrations of parallelism have been part of computing since the very beginning. The Eniac applied parallelism and opportunities to use concurrency abound. Yet, parallel computer architecture continually changes and parallel programs have proved very difficult to write, debug and maintain. Why has this powerful idea yielded results so grudgingly?

Both the hardware and software aspects of concurrency must be considered. In the parallel architecture domain, the last decade began with SIMD computers still very much thought to be realistic architectures. But the consequences of Moore's Law quickly pushed MIMD to the fore, and the battle shifted from the program counter to the memory model. Both shared and distributed memory models vied for the hearts and minds of users, and both can claim some degree of success. Though it is becoming clearer which will win, victory is not yet guaranteed. Will there by a "standard" parallel architecture, or will experimentation go on forever?

In the parallel software domain the last decade dawned with dozens of proposed programming systems based on extending a sequential language in some way that accommodated parallelism. Though many considerations motivated this idea — there exist programs, programmers, tools and "brand recognition" — virtually all of them have failed. The survivor, the overwhelming method of choice of production programmers, is message passing added to some existing language (Fortran, C, C++). It is brutally difficult to use effectively, and scares potential users away from parallelism. Much has been learned about parallel languages and programming in the past decade, which portends many opportunities for the next decade.

Theory

Complexity

Juris Hartmanis, Cornell University, USA

This talk will illustrate how computational complexity contributes to deeper understanding of computation, leads to practical results and reveals new insights about the fundamental nature of mathematics.

Types in Language Design and Implementation

Robert Harper, Carnegie Mellon University - Pittsburgh, USA

Over the last two decades type theory has emerged as the central organizing principle in the theory of programming languages. More recently type theory has emerged as a fundamental tool for their implementation as well. These developments have not only increased the expressiveness of programming languages, but have also led to radically new concepts such as certified object code that may be easily verified to satisfy a range of safety properties. In this talk I will illustrate some of these advances by discussing the role of type theory in the design of type-based certifying compilers for type-safe languages.

We thank our sponsor

Dresdner Bank

Die Beraterbank

Logic for Computer Science: An Engineering Discipline?

Wolfgang Thomas, RWTH Aachen, Germany

This talk is a reflection on the roles which logic played and can play in the development of computer science. The past is well known: Mathematical logic has enormous merits as a parent of computer science, for example by providing the idea of formal system, the clarification of the notion of algorithm, and a clear picture of the limits of the algorithmic method. But is this enough justification today, in particular for logic as a subject in the computer science curriculum? We claim that its focus is too narrow and discuss some bright perspectives which logic could have if it not only restricted itself to be a foundational science, but developed into an applied and even engineering discipline. Such a tradition of logic existed well before Hilbert and Goedel; its most prominent representative was Leibniz.

Why Theory can also be Dangerous

Hermann Maurer, TU Graz, Austria

In this talk I will demonstrate using a number of examples that theoretical result may sometimes stifle progress, lead in the wrong direction, or actually can be counter-productive since they may destroy healthy intuition or lead to wrong intuitive ideas. More specifically, we will show that some results proven to be undecidable can indeed (for all practical purposes) be solved in O(1) time; that problems known to be NP complete but approximations can be done fast lead to dangerous (wrong) intuitions and, most surprising of all, that the way and order in which proofs, results and definitions are digested by learners can have a startling influence on how effective the learners are able to apply their knowledge in concrete situations. In this connection we analyze a number of aspects of the learning process that should be kept in mind when communicating theory so as to avoid some of the pitfalls pointed out earlier.

Algorithms: Theory, Implementations, and Libraries

Kurt Mehlhorn, MPI - Saarbrücken, Germany

In the past 10 years, the area of algorithms has broadened its scope by also addressing implementation, experimentation, and libraries. The effect was two-fold. A rich source of new problem was opened and the area has gained direct impact through systems (the area has always had impact through concepts: think of NP-completeness and/or B-trees). I will discuss the development and the difficulties encountered and will outline some of the solutions found.

We thank our sponsor

Sun microsystems

We're the dot in .com™

Internet Access during the Conference

The conference sponsor Sun Microsystems offers a Sun Ray 1 Enterprise Appliance with 6 desktop boxes to the use of the conference participants. All participants will have a personal account on this system with internet connectivity.

The computers are located in room 015 in building 45.

Thursday, August 31

Artificial Intelligence

Pervasive Speech and Language Technology

Wolfgang Wahlster, Universität des Saarlandes & DFKI, Germany

Advances in human language technology offer the promise of pervasive access to on-line information and electronic services. Since almost everyone speaks and understands a language, the development of natural language systems will allow the average person to interact with computers anytime and anywhere without special skills or training, using common devices such as a mobile telephone. This talk surveys the state of the art in human language technology, discusses current challenges for speech and language technology, and concludes with a presentation of open problems and future research directions.

The latest results and component technologies for multilingual and robust speech processing, prosodic analysis, parsing, semantic analysis, discourse understanding, translation, and speech synthesis are reviewed using the Verbmobil system as an example. Verbmobil is a speaker-independent and bidirectional speech-to-speech translation system for spontaneous dialogs in mobile situations. It recognizes spoken input, analyses and translates it, and finally utters the translation. The multilingual system handles dialogs in three business-oriented domains, with context-sensitive translation between three languages (German, English, and Japanese).

We will show that the most successful current systems are based on hybrid architectures incorporating both deep and shallow processing schemes. They integrate a broad spectrum of statistical and rule-based methods and combine the results of machine learning from large corpora with linguists' handcrafted knowledge sources to achieve an adequate level of robustness and accuracy. We argue that packed representations together with formalisms for underspecification capture the

uncertainties in each processing phase, so that these uncertainties can be reduced by linguistic, discourse and domain constraints as soon as they become applicable.

We show that the current core technologies for natural language and speech processing enable us to create the next generation of information extraction and summarization systems for the Web, speech-based Internet access and multimodal communication assistants combining speech and gesture.

More details can be found in:

- Cole, R. (ed.): Survey of the State of the Art in Human Language Technology, Cambridge Univ. Press, 1998
- Maybury, M, Wahlster, W. (eds.): Readings in Intelligent User Interfaces. San Francisco: Morgan Kaufmann, 1998
- Wahlster, W. (ed.): Verbmobil: Foundations of Speech-to-Speech Translation. Berlin, Heidelberg, New York: Springer, 2000

Embodied Artificial Intelligence

Rolf Pfeifer, University of Zurich, Switzerland

The field of artificial intelligence has dramatically changed during the past 15 years-or-so. Initially, starting in the fifties, intelligence was essentially considered to be synonymous with thinking, i.e. with problem solving, reasoning, and logical deduction. Thinking in turn could naturally be conceptualized as a sequence of steps, as algorithms, which is why artificial intelligence was mostly viewed as a sub-discipline of computer science. During the 1980s, as many people started building robots, the limitations of viewing intelligence as a computational phenomenon exclusively became obvious: the idea of mapping sensory stimulation such as camera images onto internal representations, generating plans of action by logical reasoning, and finally executing them, simply did not work in the real world. It was clear that a radically new approach would be required. Rodney Brooks of the MIT Artificial Intelligence Laboratory sug-

gested that we forget about logic and problem solving, that we do away with thinking and with what people call high-level cognition and focus on the interaction with the real world. This interaction is, of course, always mediated by a body, i.e. the proposal was that intelligence needs to be "embodied". What originally seemed nothing more than yet another buzzword turned out to have profound ramifications and rapidly changed the research disciplines of artificial intelligence and cognitive science - a new research field had emerged. It is currently beginning to exert its influence on psychology, neurobiology, and ethology, as well as engineering.

Embodiment has two main types of implications, physical and information theoretic. The former are concerned with physical forces, inertia, friction, vibrations, and energy dissipation, i.e. anything concerned with the (physical) dynamics of the system, the latter with the relation between sensory signals, motor control and neural substrate. Rather than focusing on the neural substrate only, the focus is now on the complete organism which includes morphology (shape, distribution and physical characteristics of sensors and actuators, limbs, etc.) and materials. Often, problems (e.g. learning problems) that seem intractable if viewed from a purely computational perspective, turn out to be easy if the embodiment and the interaction with the environment are appropriately taken into account. For example, given a particular task environment, if the morphology is right, the amount of neural processing required may be dramatically reduced. Because of this perspective on embodiment, entirely new issues are raised and need to be taken into account which go well beyond computer science proper. An important issue concerns the so-called "ecological balance", i.e. the interplay between the sensory system, the motor system, the neural substrate, and the materials used. Ten years of research in this new field have generated a large number of fascinating results and surprising insights.

In the presentation I will discuss the developments that have lead to these new ideas, present examples illustrating some of the results and novel insights, talk about a number of the big challenges for the years to come such as the role of sensory-motor coupling and morphology in development and learning, concept acquisition and object invariance, and computational

properties of materials. I will also outline a few application scenarios.

More details can be found in:

- Pfeifer, R., and Scheier, C. (1999). *Understanding intelligence.* Cambridge, Mass.: MIT Press.
- Pfeifer, R. (1999). Dynamics, morphology, and materials in the emergence of cognition. *Proc. KI-99, Lecture Notes in Computer Science.* Berlin: Springer, 27-44.
- Pfeifer R. (2000). On the role of morphology in adaptive behavior. To appear in SAB-2000, *Proc. of the 6th International Conference on the Simulation of Adaptive Behavior.* Cambridge, Mass.: MIT Press.

We thank our sponsor

SIEMENS

Graphics and Vision

Scientific Visualization

Hans Hagen, Universität Kaiserslautern & DFKI, Germany

Scientific Visualization is currently a very active and vital area of research, teaching and development. The success of Scientific Visualization is mainly due to the soundness of the basic premise behind it, that is, the basic idea of using computer-generated pictures to gain information and understanding from data (geometry) and relationships (topology). This is an extremely intuitive and very important concept which is having a profound and wide spread impact on the methodology of science and engineering.

Scientific Visualization is a new approach in the area of simulation. It allows researchers to observe the results of simulations using complex graphical representations. Visualization provides methods for seeing what is normally not visible, e.g. torsion forces inside a body, wind against a wall, heat conduction, flows, plasmas, earthquake mechanisms, molecules, etc.

Since vision dominates our sensory input, strong efforts have been made to bring the power of mathematical abstraction and modelling to our eyes through the mediation of computer graphics. This interplay between various application areas and their specific problem solving visualization techniques is emphasized in this talk.

Computer Vision: Past and Future

Jan-Olof Eklundh, NADA - KTH Stockholm, Sweden

In 1950 John von Neumann suggested that images could be analyzed by computers by representing them as matrices of grey levels and comparing adjacent elements of these matrices. About 10 years later Roberts in his dissertation (1963) described a system for interpreting images of 3D scenes containing objects consisting of toy blocks. Initial techniques for recognizing patterns in images in the form of characters, cells and chromo-

Monday Aug 28

8 am Registration

9 am Opening

The Web

...how make the best use of it

- G. Weikum
- M. Franklin

...what's underneath

- A. Campbell

Lunch

The Web

...how to still feel secure

- A. Pfitzmann
- U. Maurer
- F. Schneider

Immersion into Other Disciplines

- T. Lengauer
- P. Young

Tuesday Aug 29

9 am Software

...the right engineering

- H. D. Rombach
- C. Jones
- F. Randimbivololona
- J. Larus

Lunch

Software

...the right tooling

- P. Cousot
- R. Leino
- E. Clarke

...open source?

- S. L. Graham

...the right process

- Discussion

Wednesday Aug 30

9 am Architecture

...still silicon computing?

- G. Sohi
- P. Vitanyi
- L. Snyder

Lunch

Theory

...why it is needed

- J. Hartmanis
- R. Harper
- W. Thomas

...why it can be dangerous

- H. Maurer

...how it becomes practice

- K. Mehlhorn

7 pm Podiumsdiskussion

„Schöne virtuelle Welt" -
Wie Abbilder die Wirklichkeit verändern

HS 001

Thursday Aug 31

9 am Artificial Intelligence

...verbal, symbolic, subsymbolic

- W. Wahlster
- R. Pfeifer

Graphics and Vision

- H. Hagen
- J.-O. Eklundh
- K. Grebner

Lunch

1:30 pm bus shuttle to Wadern

3 pm Birthday Party

...at Schloss Dagstuhl

- official addresses
- "Search for the Important Problems in Informatics", *J. Hartmanis*
- concert and exhibition
- 6 pm barbecue

8:30 pm and 9:30 pm bus shuttle back to Saarbrücken

somes had also been appearing then. One felt promise that computers could be made to "see".

This turned out to be a difficult and ill-defined task. Even though well functioning methods for mail sorting and bar code reading were developed, they didn't generalize to generic problems on visual understanding. Analogously, methods suited for the blocks world provided only limited insight into the analysis of real-world scenes. In the 1970's and 80's Marr and others tried to put the field that was now called computer vision on a firm scientific ground. With influence from biological vision science the interest was shifted towards how one can reconstruct the 3-dimensional world from images of it. Computational and mathematical problems capturing the physical and geometrical aspects of the world came in focus, and although Marr had pointed to the importance of both representational problems and to the understanding of high level qualities such as shape, these issues attracted far less attention for years to come.

During the past 10 years computer vision has evolved along several different paths, in many cases going back to earlier considered methods, but with a more elaborate theoretical basis. The main path has been that of developing increasingly sophisticated methods for deriving scene characteristics from images, including local properties, scene geometry, motion, and complete scene structure. This has involved applying advanced mathematical and statistical methods and careful physical modeling. Computational problems have mainly concerned treating uncertainties and obtaining convergence and efficiency.

One of the driving forces behind this development is that cameras today are common input devices to computers and that interpreting and visualizing this input has become a ubiquitous problem. In this context reconstruction of the depicted scene with limited knowledge about camera location is a relevant issue. Recognizing objects and actions, especially humans (human faces) and human action, also becomes essential. Indeed, these topics have attracted considerable attention.

These issues largely relate to pictorial vision, i.e. to what information one or more pictures convey about the scene they depict. The role of the observer, the one who "sees" is not explicit. In many applications it may of course be perfectly valid to omit that, but if the intention is to develop computers that

"see", such questions inevitably arise. Another research path in the past 10 years, that on active or animate vision, addressed issues of that sort. Techniques for including the observer in the form of oculomotor systems, were developed and are today applied for e.g. people tracking. The general view was that by considering perception and action in conjunction, which is natural from a biological perspective, many of the hard problems of computer vision could be formulated in ways that would allow robust and efficient solutions. Robust oculomotor control was indeed achieved, but the results did not extend much beyond that. Two reasons for that are obvious. One was that the necessary computing power to make these active systems solve higher level visual problems was lacking. The other one that such problem formulations shifted the focus towards problems of process control and systems integration, and that there theories for these were not at hand.

So with this perspective one can ask what the challenges of the field are for the coming 10 years. To begin with one can note that information in visual form today pervades our computer world. Hence, the need to perform computations and analysis on such data is greater than ever. A number of issues must be addressed to provide us with techniques by which we can process visual information appropriately, enabling us to develop "seeing systems":

- Bringing existing theoretically well-founded tools for extracting properties and scene characteristics from images should be brought to work ROBUSTLY on real applications. This work will likely follow the route we already are on, with an emphasis on mathematical, statistical and physical aspects.
- Developing systems that can "see", including the drives, tasks and actions of the observer. Apart from a number of basic vision science problems we have here a number of difficult systems problems, e.g. on asynchronous, distributed computations, control and scheduling, trade-offs between top-down and bottom-up computations, scalable architectures, and also on how to program such systems.

In addition, aspects of embodiment and non-visual information have to be included.

- Understanding visual recognition and categorization. This forms part of learning using vision in a more general sense and is then closely related to the second point above. The capabilities of visual recognition, categorization and learning will be crucial for the application of computer vision. To achieve them many problems on memory representation and learning need to be solved. Although it is well-known how they are realized in neurophysiological terms, computational models working on real data are still missing.

In the presentation we will discuss these topics, elaborating on the development in recent years and the challenges for the future.

Virtual Reality in Car Design. Real-time Simulation of Classical Mechanics for Virtual Packaging Applications

Klaus Grebner, DaimlerChrysler Research - Ulm, Germany

Virtual reality (VR) is a man-machine interface, which enables us to perceive a computer-generated environment as reality by addressing several senses.

It is the intuitively correct man machine interface to all stages of the product design process and an unbelievably fast and efficient method to recognize design errors instantly. It is used along the whole product development cycle (styling, design, production, sales, service) to reduce errors in the early phases of development and by that shorten cycle times and save development costs.

One main objective of Mercedes-Benz is to have a so called DMU, a Digital Mockup. This means that the product should be digitally available during the whole development process. Based on this digital product questions concerning

constructability, maintenance etc. can be answered without building a physical model.

To perceive a computer-generated environment as reality - the key message of the definition above is tightly connected to the notion of *immersion*. Immersion is the user's feeling of psycho-physical integration into the virtual world and is a kind of measure for the degree of realism of the virtual environment. VR is technologically based on three fundamental concepts:

1. real-time 3D-computergraphics with stereoscopic viewing,
2. real-time intuitive interaction in and with the virtual worlds, and
3. online real-time simulations.

In computer aided mechanical engineering, virtual reality techniques help to interactively simulate an assembly of mechanical parts. To lend enough realism to such a virtual environment, collisions between objects have to be detected and realistic reactions to these collisions to be determined. Contact and friction forces facilitate the interactive handling of virtual objects.

The simulation of rigid body dynamics according to classical mechanics supports the user in his interaction with the virtual world. Collision detection guarantees the most fundamental physical property of rigid objects; they cannot interpenetrate. Based on the spatial and kinetic configurations of the objects at the moment of collision, contact forces can be computed. They enable a more intuitive and realistic handling of objects particularly if they are interactively moved along the boundaries of other virtual objects in the virtual world. These virtual objects should behave physically plausible.

But not only rigid objects, also flexible objects like cables should be regarded in packaging simulations. Further on contacts must not be unilateral only. We are now interested in arbitrary kinematic structures. One crucial question for the packaging engineer is to determine the space of reachable points for a given kinematic structure. These are two main directions we are working on at the moment. Another focus is to bring force feedback devices into our applications.

Poster Session - Abstracts

Cutting Planes and the Elementary Closure of Polyhedra

Fritz Eisenbrand, Max-Planck-Institut für Informatik, Saarbrücken

Integer programming is concerned with the optimization of a linear function over the integer points in a polyhedron P. Among the most successful methods for solving integer programming problems is the cutting plane method in combination with branch-and-bound. A Gomory-Chvátal cutting plane [2, 1] for P is an inequality $c^T x \leq \lfloor \delta \rfloor$, where c is an integral vector and $c^T x \leq \delta$ is valid for P, i.e., the halfspace defined by $c^T x \leq \delta$ contains P. The cutting plane $c^T x \leq \lfloor \delta \rfloor$ is valid for all integral points in P and thus for the convex hull of integral vectors in P, the integer hull P_I. The addition of a cutting plane to the system of inequalities defining P results in a better approximation of the integer hull.

The elementary closure P' of a polyhedron P is the intersection of P with all its Gomory-Chvátal cutting planes. P' is a rational polyhedron provided that P is rational (see [3]). The Chvátal-Gomory procedure [1] is the iterative application of the elementary closure operation to P. The Chvátal rank is the minimal number of iterations needed to obtain P_I. It is always finite, but already in R^2 one can construct polytopes of arbitrary large Chvátal rank. We show that the Chvátal rank of polytopes contained in the n-dimensional 0/1 cube is $O(n^2 \log n)$ and prove the lower bound $(1+\varepsilon)n$, for some $\varepsilon>0$.

We show that the separation problem for the elementary closure of a rational polyhedron is NP-hard. This solves a problem posed by Schrijver [4].

Last we consider the elementary closure in fixed dimension. The known bounds for the number of inequalities defining P' are exponential, even in fixed dimension. We show that the number of inequalities needed to describe the elementary closure of a rational polyhedron is polynomially bounded in fixed dimension. Finally, we present a polynomial algorithm in vary-

ing dimension, which computes cutting planes for a simplicial cone from this polynomial description in fixed dimension with a maximal degree of violation in a natural sense.

References

[1] V. Chvátal. Edmonds polytopes and a hierarchy of combinatorial problems. *Discrete Mathematics*, 4:305 — 337, 1973.

[2] R. E. Gomory. Outline of an algorithm for integer solutions to linear programs. *Bulletin of the American Mathematical Society*, 64:275 — 278, 1958.

[3] A. Schrijver. On cutting planes. *Annals of Discrete Mathematics*, 9:291 — 296, 1980.

[4] A. Schrijver. *Theory of Linear and Integer Programming.* John Wiley, 1986.

Request-Prediction and Hyperlink-Proposals - A Similar Mathematical and Methodological Approach

Ernst-Georg Haffner, Institut für Telematik, Trier

Due to the breathtaking growth of the World Wide Web (WWW), the need for high quality hypertexts is rapidly increasing, and finding appropriate links is one of the most difficult of tasks. Ultra-modern online authoring systems that provide possibilities to check link-consistencies and administrate link management should also propose links in order to improve the usefulness of the HTML-documents. Another major problem of today's Internet applications - and, at first glance, an entirely different one to finding hyperlinks - is the performance of Client/Server communication: servers often take a long time to respond to a client's request. There are several strategies to overcome this problem of high user-perceived latencies; one of them is to predict future requests. This way, time-consuming calculations on the server's side can be performed even before a special request is being made.

If the server is "sure" that certain documents will soon be requested, the associated data can be sent to the client in advance (or can be pre-fetched by the client) even while the user is unaware of this process.

These two problem categories do not seem to have much in common. In this doctoral thesis, we mean to show that there are certain, similar solution strategies to take care of both problems. Therefore, we will have a closer look at hyperlink-proposals and we will present a general prediction scenario too.

A comparison and an abstraction of both methodologies will lead to comfortable synergetic effects. For example, advanced strategies to foresee future user-requests by modeling time and document aging can be use to improve the quality of hyperlink-proposals.

Online diagnosis in intelligent computer based mathematical training

Martin Hennecke, Institut für Mathematik und Angewandte Informatik, Universität Hildesheim

The ability of human teachers to diagnose students misconceptions and to adapt their teaching methods, is a necessary prerequisite for direct support or individualising measures. Due to the high expenditure of time this is nearly impossible in practice. In computer-assisted mathematical training systems these diagnostic abilities were not available until the present day, because existing diagnostic systems were not fast or flexible enough.

This Ph. D. thesis proposes a new algorithm for online diagnosis in computer-based training systems in mathematical domains. It extends the standard term rewriting by numerous new concepts to describe students behaviours and combines term rewriting techniques with dynamic programming. The proposed data types enable an efficient memory management by maximum structure sharing. The design and a possible implementation of an appropriate diagnostic module, called BugFix, is presented. To demonstrate its abilities a bug library for fraction arithmetic was developed. After analysing over 6000 in-

correct calculations of 500 learners, a set of around 200 correct and incorrect rules was put together. In this domain BugFix is able to consider several billion different student calculations for one task, without a subjectively perceptible waiting period for the learner.

BugFix represents an efficient and easily usable diagnostic component for the application in intelligent computer-based training systems. The diagnostic information obtained can be used both by the training system and by the human teacher to avoid and correct learners misconceptions.

Retargetable Postpass Optimisation by Integer Linear Programming

Daniel Kästner, Universität des Saarlandes, Saarbrücken

In the area of embedded systems stringent timing constraints in connection with severe cost restrictions have led to the development of specialised, irregular hardware architectures designed to efficiently execute typical applications of digital signal processing. The code quality achieved by traditional high-level language compilers for irregular architectures often cannot satisfy the requirements of the target applications. Thus many DSP applications are still developed in assembly language. However due to the increasing software complexity and the shrinking design-cycles of embedded processors there is an urgent demand for code generation techniques that are able to produce high-quality code for irregular architectures.

In my thesis the PROPAN system is presented as a retargetable framework for high-quality code optimisations and machine-dependent program analyses at postpass, i.e. assembly level. The postpass orientation allows PROPAN to be integrated in existing tool chains with moderate effort. All relevant information about the target architecture is concisely specified in a dedicated machine description language TDL. PROPAN has been implemented in a generic, i.e. machine-independent way; the necessary target-specific information is derived from the machine description. Generating high-quality code for irregular architectures requires taking the phase-coupling problem between

different code generation subtasks into account. The code generation process can be subdivided into several phases of high computational complexity. For complexity reasons they are usually addressed separately by heuristic methods. While the heuristic approaches perform well for regular architectures, suboptimal combinations of suboptimal partial results can lead to a poor code quality for irregular architectures. The PROPAN framework allows the phase-coupled modelling of instruction scheduling, register assignment and functional unit binding based on integer linear programming. In contrast to previous approaches the optimisation scope is not restricted to basic block level. The integer linear programs can be solved either exactly providing a provably optimal solution to the modelled problems, or by the use of ILP-based approximations. The basic idea of the approximative methods is the iterative solution of partial relaxations of the original problem. This way the computation time can be reduced significantly and still a very high solution quality can be obtained. The measured computation times are acceptable for practical use.

With PROPAN ILP-based postpass optimisers for two widely used contemporary digital signal processors, the Analog Devices ADSP-2106x and the Philips Trimedia TM1000 have been generated. Additionally PROPAN is integrated in a framework for calculating worst-case execution time guarantees for real-time systems where a TDL specification of the Infineon TriCore µC/DSP is used. Finally PROPAN has been successfully used in a commercial postpass optimiser for the Infineon C166 microprocessor.

Atomic Architectural Component Recovery for Program Understanding and Evolution

Rainer Koschke, Institut für Informatik, Universität Stuttgart

The literature is rich of fully automatic and semi-automatic techniques for component recovery and their number is still growing. The abundance of published methods calls for frameworks to unify, classify, and compare them in order to make informed decisions. This thesis introduces a classification of component

recovery techniques based on a unification of 23 techniques. Focussing on structural techniques, 16 fully automatic techniques are classified into connection-, metric-, graph-, and concept-based subcategories and the commonalities and variabilities of these techniques are discussed in depth. Beyond the qualitative comparison, 12 structural techniques are evaluated quantitatively (concept-based techniques were excluded). To that end, an evaluation scheme is introduced that allows to measure recall and precision of component recovery techniques with respect to a set of reference components ascertained by software engineers. Among the evaluated techniques is our new metric-based technique named Similarity Clustering. The evaluation scheme based on a set of expected components manually compiled by 5 software engineers for four C systems with altogether 136 KLOC shows that Similarity Clustering is among the best techniques for all systems, but it also has more false positives than other techniques. The overall result of this comparison is that none of the fully automatic techniques has a sufficient detection quality.

In order to overcome this problem, a semi-automatic method is presented in this thesis in which computer and maintainer collaborate to detect components. The method is supported by a framework that integrates the existing fully automatic techniques. In this framework, the automatic techniques can be run successively and their results be validated by the user. For this purpose, all the techniques are enhanced to work incrementally. The unification of the automatic techniques makes it possible to implement incremental variants for whole classes of techniques. The results of the techniques can be combined by high-level operators modeled on intersection, union, and difference for fuzzy sets. An alternative way of integration is offered by a voting approach that summarizes the individual agreement of automatic techniques.

Despite of the new ways of combining the automatic techniques, the semi-automatic method inherits weaknesses of the integrated techniques. Future research should investigate whether these weaknesses may be overcome with additional, more precise information gained from dataflow analyses and more domain-oriented information. However, all methods will

always have to cope with vagueness and subjectivity of the grouping criteria for components.

Multiple Generations Audio Compression Without Loss of Perceptual Quality

Frank Kurth, Institut für Informatik, Abt. V, Universität Bonn

In this work, we develop algorithms to prevent audio signal degeneration resulting from cascaded coding, i.e., multiple compression and decompression. For this sake we combine techniques from the fields of computer science, signal processing, psychoacoustics and audio coding.

The cascaded use of low rate high quality coding in nowadays audio applications, such as digital audio broadcasting or network transmission, comes at the risk of an increasing perceptual degradation. Assuming a coder operation C and a corresponding decoder operation D we shall call, for a given signal x, DCx the first generation and, for an integer n, $DC...DCx$ (n times) the nth generation of x. Sometimes, $DC...DC$ (n times) is called n-fold tandem-coding.

We investigate the quality of nth generations of high quality signals coded with psychoacoustic audio codecs such as the MPEG or AC-2/3 family. Listening tests on extensive test material show significant degenerations, called *ageing effects*, starting from third to fifth generations. Although some codecs like MPEG-2 AAC still show good results for higher generations, those ageing effects are non-negligible in the case of many codecs.

In our work, we analyze possible causes for those ageing effects starting from a general codec model. The significant loss of information resulting from quantization gives rise for the development of a novel codec model aiming at the conservation of the first generation's signal quality. For this sake, we transfer, or *embed*, encoding parameters, implicitly containing psychoacoustic information, from each codec in a cascade to its successor.

To overcome the problem of a secondary data stream between codecs, we develop an embedding strategy to store all

encoding information in the decoded audio data. For this sake we observe that, using psychoacoustic information implicit in the quantization parameters, the decoded signal offers enough space to store the desired data without perceptual degradation.

Our work contains an implementation based on an MPEG-1 Layer II codec as well as a conceptual approach to an MPEG-1 Layer III (MP3) implementation. However, the presented method is very general and applicable to a wide range of coding applications not necessarily restricted to the audio case.

Listening tests show that in most cases, first generation audio signals could not be distinguished from the corresponding 25th generations, whereas third generations using the standard codec where generally judged to be of worse quality than first generations. For critical test material, 25th generations where generally judged to be of better quality than at least third generations using the standard codec. SNR measurements show that our coding method tends to a fixed point signal w.r.t. embedding frames, i.e., the signal is not changed any more in higher (e.g. starting from fourth or fifth) generations. Tests with very high generations, e.g. 50th, confirm a stable signal quality.

A variant of the proposed framework deals with a *region embedding* framework allowing for codecs which can be *proven*, under some mild conditions, to keep the quality of previous generations. Such region embedding codecs have also successfully been implemented in a follow-up project.

Enabling Adaptive Ubiquitous Applications

Markus Lauff, TecO, Universität Karlsruhe

Ubiquitous Computing is one of the emerging areas in computer science. Research on Ubiquitous Computing spans the development of (wireless) communication protocols (e.g. IrDA, BlueTooth), the use of proprietary technologies for evaluation of specific applications, the development of architectures supporting communication and management in heterogeneous environments (e.g. JetSend, Salutation), and research on new applications for ubiquitous environments.

However these approaches generally lack in flexible integration of already existing infrastructures, and provision of abstractions for the construction of adaptive ubiquitous computing applications.

From TecO's experience with prototyping of ubiquitous computing applications, the following requirements for an infrastructure to support ubiquitous computing have arrived:

1. management of resources and environments, supporting dynamics such as device and resource mobility;
2. integration of arbitrary communication protocols and ubiquitous computing management systems, to support heterogeneous resources, to reuse existing infrastructure; and
3. provision of abstractions for application development, and of mechanisms for adaptations to particular environments and resources.

The presented work "Enabling adaptive ubiquitous applications" is based on a catalog of requirements built from an explorative analysis of several different ubiquitous scenarios. The catalog is structured to the requirements on

1. administration of ubiquitous systems,
2. abstraction to technical realization of resources,
3. integration of existing infrastructure, and
4. adaptation of applications.

With respect to this catalog of requirements the following specification of the UCMA (Ubiquitous Computing Management Architecture) models allow the formal description of an ubiquitous system. Therefore the different models are build to describe and structure the physical environment, to describe the resources of ubiquitous system, and to describe the existing communication and execution infrastructure.

The main goal of the UCMA architecture is to operate heterogenous ubiquitous computing environments and to support adaptation of applications according to resources available in

the selected environment. The focus is therefore on the integration of existing infrastructure and on the adaption of applications according to the available resources.

The UCMA architecture is based on three layers:

1. Adaptation Layer to enable the adaptation and integration of communication protocols and other management systems,
2. Service Layer consisting of service modules to maintain device, location, communication, and user dependent services, and
3. API Layer to provide uniform access to the managed resources.

Finally the work evaluates the models and architecture using a prototypical UCMA implementation compared to other similar approaches as Jini, Salutation, and UPnP. Further work is identified in the areas of conflict management while accessing resources, and flexible distributed security mechanisms.

Processing Relational Queries using a Multidimensional Access Technique

Volker Markl, Fakultät für Informatik der Technischen Universität München

Our thesis investigates the UB-Tree, a multidimensional access method, and its applicability for relational database management systems (RDBMS). In the thesis, we introduce a formal model for multidimensional partitioned relations and discuss several typical query patterns. The model identifies the significance of multidimensional range queries and sort operations. After describing the UB-Tree and its standard algorithms for insertion, deletion, point queries, and range queries, we introduce the spiral algorithm for nearest neighbour queries with UB-Trees and the Tetris algorithm for efficient access to a table in arbitrary sort order. We then describe the complexity of the involved algorithms and give solutions to selected algorithmic

problems for a prototype implementation of UB-Trees on top of several RDBMSs. A cost model for sort operations with and without range restrictions is used both for analyzing our algorithms and for comparing UB-Trees with state-of-the-art query processing. Performance comparisons with traditional access methods practically confirm the theoretically expected superiority of UB-Trees and our algorithms over traditional access methods: Query processing in RDBMS is accelerated by several orders of magnitude, while the resource requirements in main memory space and disk space are substantially reduced. Benchmarks on some queries of the TPC-D benchmark as well as the data warehousing scenario of a fruit juice company illustrate the potential impact of our work on relational algebra, SQL, and commercial applications. The results of this thesis were developed by the author managing the MISTRAL project, a joint research and development project with SAP AG (Germany), Teijin Systems Technology Ltd. (Japan), NEC (Japan), Hitachi (Japan), Gesellschaft für Konsumforschung (Germany), and TransAction Software GmbH (Germany). In this paper we merely sketch a major application area of our thesis, data warehousing, and give analytical performance comparisons for our method compared to classical RDBMS indexes.

Generating Program Analyzers

Florian Martin, Universität des Saarlandes, Saarbrücken

In this work the automatic generation of program analyzers from concise specifications is presented. It focuses on provably correct and complex interprocedural analyses for real world sized imperative programs. Thus, a powerful and flexible specification mechanism is required, enabling both correctness proofs and efficient implementations. The generation process relies on the theory of data flow analysis and on abstract interpretation. The theory of data flow analysis provides methods to efficiently implement analyses. Abstract interpretation provides the relation to the semantics of the programming language. This allows the systematic derivation of efficient provably correct, and terminating analyses. The approach has been implemented

in the program analyzer generator PAG. It addresses analyses ranging from "simple" intraprocedural bit vector frameworks to complex interprocedural alias analyses.

A high level specialized functional language is used as specification mechanism enabling elegant and concise specifications even for complex analyses. Additionally, it allows the automatic selection of efficient implementations for the underlying abstract datatypes, such as balanced binary trees, binary decision diagrams, bit vectors, and arrays. For the interprocedural analysis the functional approach, the call string approach, and a novel approach especially targeting on the precise analysis of loops can be chosen. In this work the implementation of PAG as well as a large number of applications of PAG are presented.

Using Public-Key Cryptography in CORBA-Systems

Zoltán Nochta, Institut für Telematik, Universität Karlsruhe

Applications running in distributed environments are getting more and more important to customers these days, due to the fact that they use them in daily business. One of the most popular object-oriented middleware platforms is the Common Object Request Broker Architecture (CORBA) standardized by the Object Management Group (OMG).

In the past, many CORBA-systems have been designed for the use in secure networks such as intranets protected by firewalls. Since using public networks, CORBA-applications are exposed to more security attacks then ever. A central component of CORBA is the Object Request Broker (ORB). The ORB-Core only provides basic communication mechanisms between objects implemented in different programming languages. OMG recognized security requirements and specified the CORBA Security Services (CSS). This specification defines object protection mechanisms, policies and interfaces specific for CORBA. One shortcoming of this specification is that the integration of security systems based on public-key cryptography is not provided.

In Saarbrücken, I would like to present concepts to provide and manage end-to-end security on CORBA-applications. In

order to provide security in *legacy* CORBA-systems security unaware objects using an unsecured ORB should run securely without any active involvement. The implementation of the CSS based on public-key certificates is a difficult task for developers. Last but not least *new* applications should be developed to use the facilities of implemented CSS. All of the concepts focus on technical and organizational aspects of integration of Public-Key Infrastructure and Privilege Management Infrastructure (X.509) services in CORBA.

Fast Signal Transforms for Quantum Computers

Martin Rötteler, Graduiertenkolleg "Beherrschbarkeit Komplexer Systeme", Universität Karlsruhe

The fascination of the emerging field of quantum information processing is in part due to the quantum algorithms which have been found recently. Defining BQP to be the class of languages which can be accepted by a Quantum Turing Machine with bounded error probability, Peter Shor managed to show in 1994 that the problems Factoring and Discrete Logarithm belong to BQP. It is not known whether there exist classical polynomial algorithms for these problems.

In both cases the use of the discrete Fourier transform, considered as a unitary transform the quantum computer is able to carry out, makes it possible to solve the problem of determining the period length of certain functions, allowing in turn for the solution of the mentioned problems. Applying recursion formulas it is possible to compute the discrete Fourier transform with an exponential speedup compared to the classical case. We present the resulting quantum circuits for the discrete Fourier transform and some variations thereof. We also give circuits for generalised Fourier transforms, as well as for transforms which are well-known from classical signal processing and may play a role in quantum information processing.

The algorithms of Shor are instances of a more general concept, namely the so called hidden subgroup problem. This class of problems has obtained much interest recently, partly because the graph isomorphism problem, for which like in the

case of Factoring no polynomial time algorithm is known, has an easy reduction to it. We present a short introduction into hidden subgroup problems and give the first example of a family of nonabelian groups for which the hidden subgroup problem can be efficiently solved.

Increasing the Power of OBDDs by Functional Extensions

Harald Sack, FB IV - Informatik, Universität Trier

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

Besides relaxing the ordering restriction, easing the read-once property of the input variables, or the usage of different decomposition types for Boolean functions, we are focusing on the extension of OBDDs with functional operator nodes, esp. Parity-OBDDs ($\oplus$-OBDDs), i.e. OBDDs with additional operator nodes computing the Boolean parity of their successors. By introducing $\oplus$-nodes the representation has the potential of being more compact while on the other hand giving up canonicity. Therefore, the identification of two $\oplus$-OBDDs representing the same Boolean function becomes an essential operation. We present an efficient probabilistic equivalence test for

⊕-OBDDs that admits working with ⊕-OBDDs in an professional environment. Due to the fact that the size of Decision Diagrams crucially depends on the order of the input variables we show how to apply heuristics for ⊕-OBDD minimization based on dynamic changes in the variable order and the relocation of ⊕-nodes inside the data structure.

Many problems in practice require the transformation of symbolic variables to a binary encoding for getting accessible with OBDDs or ⊕-OBDDs. Extending the OBDD data structure from the binary domain to a finite domain results in so called Multivalued Decision Diagrams (MDDs) and the binary encoding of symbolic variables is not necessary anymore. The already introduced ⊕-OBDDs can now be extended towards Mod-p-Decision Diagrams (Mod-p-DDs), i.e. MDDs with additional operator nodes representing an integer addition modulo p, p - prime. Such decision diagrams have a potential of being more space-efficient than MDDs. However, they are not a canonical representation and thus, the equivalence test of two Mod-p-DDs is more difficult than the test of two MDDs. To overcome this problem, we design a fast probabilistic equivalence test for Mod-p-DDs based on the transformation of integer functions represented by Mod-p-OBDDs to polynomials over a finite domain and show how to apply heuristics for their minimization.

Programming Constraint Inference Services

Christian Schulte, Forschungsbereich Programmiersysteme, Universität des Saarlandes, Saarbrücken

Constraint programming has become the method of choice for modeling and solving many types of problems in a wide range of areas: artificial intelligence, databases, combinatorial optimization, and user interfaces, just to name a few. Even though search is a salient feature for constraint programming, todays constraint programming systems offer a fixed and small set of search strategies. Search cannot be programmed which prevents the construction of new search strategies and the deployment of existing strategies.

The thesis addresses this severe limitation by developing abstractions that allow high-level programming of constraint inference services including search strategies.

The thesis presents the design, application, implementation, and evaluation of simple abstractions that allow for high-level programming of constraint inference services that excel today's constraint programming systems. The abstractions proposed are computation spaces which are shown to be:

Widely Applicable

They cover standard (single, all, best-first, best-solution) search. Their application to parallel search is effortless yet makes excellent use of networked computers. They serve as a simple foundation for deep-guard combinators. They support the construction of services new to constraint programming such as interactive visual search.

Concurrency Enabled

They encapsulate constraint-based computations which are typically speculative. Encapsulation is a must for integration with concurrent and reactive computations. Encapsulation enables the deployment of constraint based application in todays concurrent and distributed computing infrastructure.

Efficient

An implementation of computation spaces that builds on copying and recomputation rather than on trailing is demonstrated to provide competitive performance. The implementation is shown to outperform existing constraint programming systems on several large examples.

Seen from the point of view of industrial research we believe Virtual Reality to be one of the 'leading-edge' technologies of the next decade that will have a significant impact on animation and simulation. VR will be of utmost importance in defining the development processes of the future. The physical modeling of virtual objects, and the simulation of rigid body dynamics in virtual environments will play a very important role throughout the whole manufacturing- and engineering-industry.

The Panel Discussion is sponsored by

Schöne virtuelle Welt - wie Abbilder die Wirklichkeit verändern

Öffentliche Podiumsdiskussion

Mittwoch, 30. August 2000, 19 Uhr
Universität des Saarlandes, Gebäude 45 (Informatik), Hörsaal 001

Die Podiumsdiskussion wird anläßlich des 10-jährigen Bestehens des Informatikzentrums Schloß Dagstuhl vom Saarländischen Rundfunk in Zusammenarbeit mit dem Informatikzentrum veranstaltet.

Teilnehmer

- Priv. Doz. Dr. Hans-Peter Lehnhof, Max-Planck-Institut für Informatik, Saarbrücken
- Prof. Dr. Dr. h.c. Hermann Maurer, TU Graz
- Prof. Dr. Rudi Schmiede, Soziologie, TU Darmstadt
- Prof. Dr.-Ing. Jörg Siekmann, Deutsches Forschungszentrum für Künstliche Intelligenz, Saarbrücken

- Moderation:
  Dr. Helmut Scheidgen, Saarländischer Rundfunk

Die Diskussion wird aufgezeichnet und später über SR2 Kulturradio gesendet.

Die Saar Bank lädt die Teilnehmer und Gäste der Veranstaltung zu einem Imbiß vor der Diskussion und zu einem Umtrunk zum Ausklang in das Foyer des Gebäudes 45 ein.

Festveranstaltung „10 Jahre Dagstuhl"

Donnerstag, 31. August 2000, 15 Uhr
Schloss Dagstuhl, Wadern-Dagstuhl

Programm

- Begrüßung
  durch den Wiss. Dir. Prof. Dr. Reinhard Wilhelm
- Grußwort
  Jürgen Schreier, Minister für Bildung, Kultur und Wissenschaft des Saarlandes
- Grußwort
  Prof. Dr. Heinz Schwärtzel, Vorsitzender des IBFI Aufsichtsrates
- Festvortrag
  "Search for the Important Problems in Informatics"
  Prof. Dr. Juris Hartmanis, Cornell University
- Musikalische Begleitung
  Dr. Dietrich W. Paul, München
- 16.30 Uhr
  Führung durch den historischen Teil von Schloss Dagstuhl
- 17 Uhr
  Konzert im Weissen Saal
  Christine Eisenbrand und Thomas Layes
- 17 Uhr
  Führung durch die Ausstellung von Gabriele Eickhoff
- 18 Uhr
  Grillparty

Bustransfer vom Campus nach Dagstuhl und zurück:
Abfahrt 13.30 Uhr Mensa Eingang, Rückfahrt ab 21 Uhr

Tag der offenen Tür

Samstag, 2. September 2000, 14 - 18 Uhr
Schloss Dagstuhl, Wadern-Dagstuhl

Programm

14 Uhr

- Eröffnung durch den wissenschaftlichen Direktor Prof. Dr. Reinhard Wilhelm

14.30 bis 18 Uhr

- Führungen durch den historischen Teil des Schlosses
  Willi Weinen, Leiter des Heimatmuseums Wadern
- Das Dagstuhl Konzept
  Dipl. Inform. Angelika Mueller-v. Brochowski, Leiterin Geschäftsstelle Schloss Dagstuhl
- „Dagstuhl braucht Kunst"
  Video von Sven Rech, Saarländischer Rundfunk
- „Die Geister von Schloss Dagstuhl"
  Hörstück von Sven Rech, Saarländischer Rundfunk
- Führungen durch die Dagstuhl Bibliothek
  Dipl. Bibliothekarin Petra Meyer

16 Uhr

- Vernissage der Ausstellung von Gabriele Eickhoff

Außerdem

Bücherflohmarkt, Kaffee und Kuchen, kleine Speisen und Getränke

Conference Organisation

Scientific Organisation:
Reinhard Wilhelm

Local Organisation Saarbrücken:
Angelika Mueller (IBFI), Uta Merkle (KWT)

Local Organisation Wadern-Dagstuhl:
Dietmar Kunzler

Conference Office:
Annette Beyer, Stefanie Lauer, Marion Metzen (KWT), Nicole Paulus, Melanie Spang

Systems Administrators:
Jörn Schneider, Axel Beckert, Thomas Schillo

Layout Conference Program:
Holger Dewes

Layout Conference Web Pages:
Axel Beckert

Printing:
COD, Bleichstrasse 22, Saarbrücken

Technical Information

Busses

Bus lines and tram in Saarbrücken can be used without payment by all participants with the Saartal logo on their name badge.

Lunch

Participants will receive lunch tokens to be used in the University Cafeteria (Mensa). There is a choice between two menus.

Computer and Internet Access

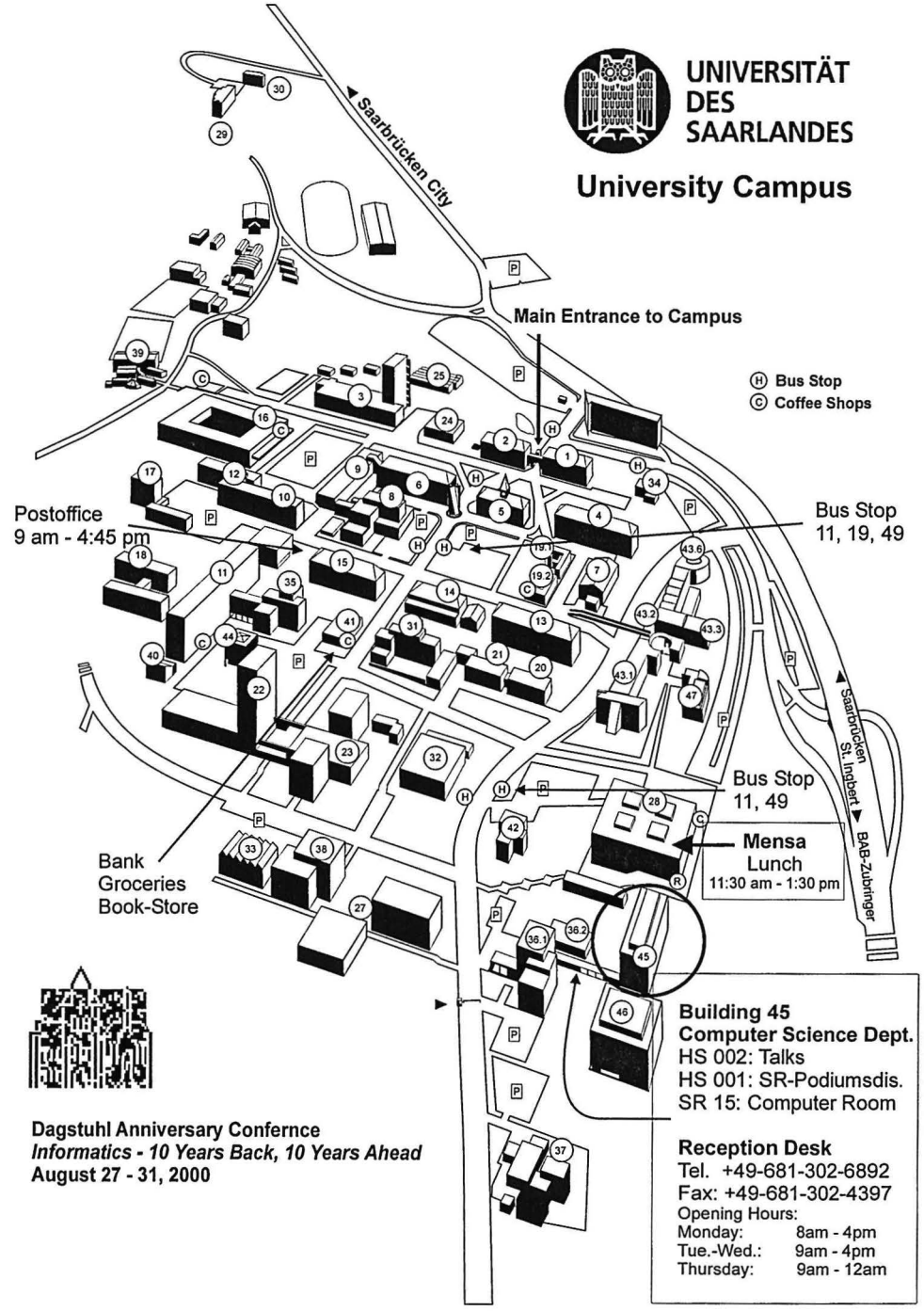
Is provided in room SR 015 opposite to the lecture hall 002.

Poster Session

The active time of the poster session is on Monday. However, most of the doctors will be present during the whole conference.

Birthday party

The busses to the Birthday party in Dagstuhl start Thursday after lunch at the main entrance of the University Cafeteria. Those who want to use it should check if they have a reservation.


UNIVERSITÄT
DES
SAARLANDES
University Campus
Saarbrücken City
Main Entrance to Campus
Bus Stop
Coffee Shops
Postoffice
9 am - 4:45 pm
Bus Stop
11, 19, 49
Bus Stop
11, 49
Saarbrücken
St. Ingbert
BAB-Zubringer
Mensa
Lunch
11:30 am - 1:30 pm
Bank
Groceries
Book-Store
Building 45
Computer Science Dept.
HS 002: Talks
HS 001: SR-Podiumsdis.
SR 15: Computer Room
Reception Desk
Tel. +49-681-302-6892
Fax: +49-681-302-4397
Opening Hours:
Monday: 8am - 4pm
Tue.-Wed.: 9am - 4pm
Thursday: 9am - 12am
Dagstuhl Anniversary Confernce
Informatics - 10 Years Back, 10 Years Ahead
August 27 - 31, 2000