Proseminar
Turing Award Topics
Einführungsveranstaltung

Thomas Noll

Lehrstuhl für Informatik 2
(Software Modeling and Verification)

RWTH AACHEN UNIVERSITY

http://moves.rwth-aachen.de/teaching/ws-1415/turing/

17. Oktober 2014

Übersicht

Seminarthema

Turing Award

- Preis der US-amerikanischen Association for Computing Machinery (ACM)
- seit 1966 jährlich vergeben
- Kandidaten: “individual selected for contributions of a technical nature made to the computing community”
- Kriterien: Bedeutung und Nachhaltigkeit der wissenschaftlichen Beiträge
- gilt als höchste Auszeichnung in der Informatik
  ($\approx$ Nobelpreis, Fields-Medaille)

Seminarthema

- Darstellung eines ausgewählten Beitrags der Preisträger(innen)
- [Lebenslauf]
- [Weitere Forschungsergebnisse]

Zielsetzung

Ziele des Proseminars

- Selbständiges Einarbeiten in ein neues Thema
- Literaturrecherche
- Darstellen des Inhalts in einer wissenschaftlichen Ausarbeitung
- Verständliches Präsentieren

Anforderungen zur Ausarbeitung

Ausarbeitung

- Selbständiges Verfassen einer ca. 15-seitigen Ausarbeitung
- Vollständiges Literaturverzeichnis
- Korrektes Zitieren
- Plagiarismus:
  Die nicht gekennzeichnete Übernahme fremder Inhalte führt zum sofortigen Ausschluss.
- Schriftgröße 11pt, übliche Seitenränder
- Titelseite mit Thema, Titel Proseminar, Semester, Name, Datum
- Sprache Deutsch oder Englisch
- Korrekte Sprache wird vorausgesetzt:
  $\geq$ 10 Fehler pro Seite $\Longrightarrow$ Abbruch der Korrektur

Anforderungen Vortrag

Vortrag

- 30-minütiger Vortrag
- Zielgruppengerechte Präsentation der Inhalte
- Übersichtliche Folien:
  - $\leq$ 15 Textzeilen
  - sinnvoller Einsatz von Farben
- Vortrag in Deutsch oder Englisch

Übersicht

Themenauswahl

Verfahren

- Themenliste wurde/wird ausgehändigt
- Priorisierte Auswahl
- Wir bemühen uns (ohne Garantie) um ein “optimales” Matching
- Zuordnung der Themen bis 22. Oktober online
- Betreuer wurden bereits zugeordnet

Rücktritt vom Proseminar

- Bis zu drei Wochen nach Einführung: ohne Folgen
- Danach: Fehlversuch

Bibliothekseinführung

Einführung in die Literaturrecherche

- Einweisung in themenspezifische Literaturrecherche
- Dauer: ca. zwei Stunden
- Teilnahme für BSc-Studierende verpflichtend
- Termine zur Auswahl:
  - Do, 30.10., 13.30 - 15.30 Uhr
  - Di, 04.11., 12.30 - 14.30 Uhr
  - Mi, 05.11., 11.00 - 13.00 Uhr

Deadlines

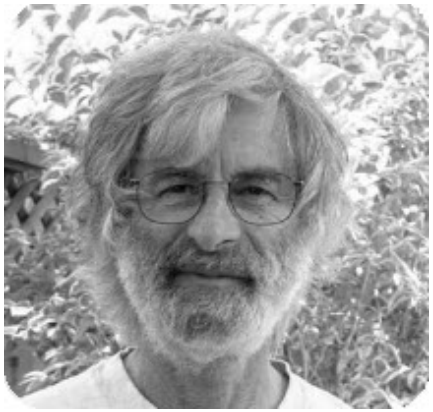
Deadlines

Folgende Termine sind einzuhalten:

- 07.11.2014: letzte Rücktrittsmöglichkeit
- 14.11.2014: Vorlage der Inhaltsübersicht
- 08.12.2014: erste vollständige Fassung der Ausarbeitung
- 05.01.2015: endgültige Fassung der Ausarbeitung
- 19.01.2015: erste vollständige Fassung der Folien
- 26.01.2015: endgültige Fassung der Folien
- 09./10.02.2015: Blockseminar

Übersicht

1: Leslie Lamport
(USA, 2013)



Auszeichnung

For fundamental contributions to artificial intelligence through the development of a calculus for probabilistic and causal reasoning.

Thema: Bakery Algorithm

- Zur Verwaltung gemeinsamer Ressourcen zwischen mehreren Prozessen
- Garantie des gegenseitigen Ausschlusses zur Vermeidung von Konflikten
- Analogie: Abarbeitung von Kundenaufträgen in Bäckerei

2: Shafi Goldwasser/Silvio Micali
(USA, 2012)

Auszeichnung

For transformative work that laid the complexity-theoretic foundations for the science of cryptography, and in the process pioneered new methods for efficient verification of mathematical proofs in complexity theory.

Thema: Goldwasser-Micali-Kryptosystem

- Kryptosystem zur Verschlüsselung einzelner Bits
- Asymmetrisch: öffentlicher und privater Schlüssel
- Erweiterung zum Benaloh-Kryptosystem für längere Nachrichten

3: Leslie Gabriel Valiant
(USA, 2010)

Auszeichnung

For transformative contributions to the theory of computation, including the theory of probably approximately correct (PAC) learning, the complexity of enumeration and of algebraic computation, and the theory of parallel and distributed computing.

Thema: "Bulk Synchronous Parallel"-Rechnermodell

- Theoretisches Rechnermodell für Entwurf und Analyse paralleler Algorithmen
- BSP-Computer:
  - Prozessoren mit lokalem Speicher
  - Netzwerk
  - Synchronisationskomponente

4: Barbara Liskov
(USA, 2008)

Auszeichnung

For contributions to practical and theoretical foundations of programming language and system design, especially related to data abstraction, fault tolerance, and distributed computing.

Thema: Programmiersprache CLU

- 1974/75 am MIT entwickelt
- Erste direkte sprachliche Unterstützung für Datenabstraktion ($\Rightarrow$ objektorientierte Programmiersprachen)
- Konzepte: Cluster (Objekte), Iteratoren, Exception Handling

5: E.M. Clarke/E.A. Emerson/J. Sifakis
(USA/USA/FR, 2007)

Auszeichnung

For their role in developing Model-Checking into a highly effective verification technology that is widely adopted in the hardware and software industries.

Thema: Model Checking

- Verfahren zur vollautomatischen Verifikation einer Systembeschreibung (Modell) gegen eine Spezifikation (Formel)
- Modell: endlicher Automat, beschriftetes Transitionssystem, ...
- Formel: LTL, CTL, ...

6: Frances Elizabeth Allen
(USA, 2006)

Auszeichnung

For pioneering contributions to the theory and practice of optimizing compiler techniques that laid the foundation for modern optimizing compilers and automatic parallel execution.

Thema: Datenflussanalyse

- Verfahren zur statischen Analyse von Computerprogrammen
- Beschreibung des Informationsflusses durch Gleichungssystem über Kontrollflussgraph
- Lösung durch Fixpunktiteration

7: Peter Naur
(DK, 2005)

Auszeichnung

For fundamental contributions to programming language design and the definition of Algol 60, to compiler design, and to the art and practice of computer programming.

Thema: Programmiersprache ALGOL 60

- ALGOrithmic Language 1960, Vorläufer von PASCAL/MODULA (siehe Wirth)
- Konzepte: Blöcke, geschachtelte Prozedurdefinitionen mit lexikalischem Scope
- Syntaxdefinition durch Backus-Naur-Form (siehe Backus)

8: Alan Kay
(USA, 2003)

Auszeichnung

For pioneering many of the ideas at the root of contemporary object-oriented programming languages, leading the team that developed Smalltalk, and for fundamental contributions to personal computing.

Thema: Programmiersprache Smalltalk

- 1980 durch Xerox PARC entwickelt
- Objektorientiert, dynamisch getypt
- Unterstützt Reflektion (Zugriff auf Programmstruktur)
- Vorläufer moderner objektorientierter Sprachen

9: L.M. Adleman/R.L. Rivest/A. Shamir
(USA/USA/IL, 2002)

Auszeichnung

For their ingenious contribution to making public-key cryptography useful in practice.

Thema: RSA-Kryptosystem

- Kryptographisches Verfahren zur Verschlüsselung und digitalen Signatur
- Asymmetrisch: öffentlicher und privater Schlüssel
- Basierend auf Faktorisierung von Primzahlprodukten

10: Andrew Chi-Chih Yao
(CN, 2000)

Auszeichnung

In recognition of his fundamental contributions to the theory of computation, including the complexity-based theory of pseudorandom number generation, cryptography, and communication complexity.

Thema: Millionärsproblem

- Musterproblem für sichere Kommunikation zwischen mehreren Parteien
- Ziel: bestimme reicheren von zwei Millionären (Alice und Bob), ohne das Vermögen offenzulegen
- Anwendung in E-Commerce und Data Mining

11: James Nicholas Gray
(USA, 1998)

Auszeichnung

For seminal contributions to database and transaction processing research and technical leadership in system implementation.

Thema: Transaktionskonzept

- ACID-Eigenschaften für zuverlässige Transaktionen in Datenbanken
  - Atomicity: "alles oder nichts"
  - Consistency: Transaktion überführt in zulässigen Zustand
  - Isolation: nebenläufige Ausführung mehrerer Transaktionen entspricht sequentiellem Ergebnis
  - Durability: Ergebnis einer vollständigen Transaktion bleibt erhalten

12: Amir Pnueli
(USA, 1996)

Auszeichnung

For seminal work introducing temporal logic into computing science and for outstanding contributions to program and system verification.

Thema: Temporallogik

- Linear Temporal Logic (LTL)
- Spezifiziert Eigenschaften von Aktionsfolgen (Traces)
- Anwendung: Model Checking

13: Manuel Blum
(USA, 1995)

Auszeichnung

In recognition of his contributions to the foundations of computational complexity theory and its application to cryptography and program checking.

Thema: Berechnung des Medians in Linearzeit

- Allgemein: Bestimmung der i.-größten von n Zahlen (meist $i = \frac{n}{2}$)
- Algorithmus veröffentlicht in 1972
- Bis dato nur quadratische Algorithmen (Sortierung)

14: Robin Milner
(UK, 1991)

Auszeichnung

For three distinct and complete achievements:

1. LCF, the mechanization of Scott's Logic of Computable Functions, probably the first theoretically based yet practical tool for machine assisted proof construction;
2. ML, the first language to include polymorphic type inference together with a type-safe exception-handling mechanism;
3. CCS, a general theory of concurrency.

In addition, he formulated and strongly advanced full abstraction, the study of the relationship between operational and denotational semantics.

Thema: Calculus of Communicating Systems

- Kalkül zur Beschreibung nebenläufiger Prozesse
- Operationen: Aktion, Prefixing, Auswahl, Produkt, ...
- Anwendungen: Kommunikationsprotokolle etc.

15: William M. Kahan
(USA, 1989)

Auszeichnung

For his fundamental contributions to numerical analysis. One of the foremost experts on floating-point computations. Kahan has dedicated himself to "making the world safe for numerical computations"!

Thema: Genaue Addition von Gleitpunktzahlen

- Summationsalgorithmus von Kahan
- Minimiert Rundungsfehler durch parallele Berechnung eines Kompensationswerts
- Beiträge zu IEEE-Standards für binäre Gleitkommazahlen

16: John E. Hopcroft/Robert E. Tarjan
(USA, 1986)

Auszeichnung

For fundamental achievements in the design and analysis of algorithms and data structures.

Thema: Starke Zusammenhangskomponenten in Graphen

- Eingabe: zusammenhängender ungerichteter Graph (ohne Brücken)
- Ausgabe: Kantenorientierung, so dass entstehender gerichteter Graph stark zusammenhängend

17: Richard M. Karp
(USA, 1985)

Auszeichnung

For his continuing contributions to the theory of algorithms including the development of efficient algorithms for network flow and other combinatorial optimization problems, the identification of polynomial-time computability with the intuitive notion of algorithmic efficiency, and, most notably, contributions to the theory of NP-completeness. Karp introduced the now standard methodology for proving problems to be NP-complete which has led to the identification of many theoretical and practical problems as being computationally difficult.

Thema: Rabin-Karp-Algorithmus zur Stringsuche

- Suche von Mustern p in Text w
- Naives Verfahren: Aufwand $|p| \cdot |w|$
- Beschleunigung durch Hashwerte (siehe Knuth)

18: Niklaus E. Wirth
(CH, 1984)

Auszeichnung

For developing a sequence of innovative computer languages, EULER, ALGOL-W, MODULA and PASCAL. PASCAL has become pedagogically significant and has provided a foundation for future computer language, systems, and architectural research.

Thema: Programmiersprache PASCAL

- Weiterentwicklung von Algol 60
- Eingeführt als Lehrsprache für strukturierte Programmierung ("no goto")
- Wichtigstes Konzept: starke Typisierung ($\Rightarrow$ keine Typfehler zur Laufzeit)

19: Stephen A. Cook
(CDN, 1982)

Auszeichnung

For his advancement of our understanding of the complexity of computation in a significant and profound way. His seminal paper, "The Complexity of Theorem Proving Procedures," presented at the 1971 ACM SIGACT Symposium on the Theory of Computing, laid the foundations for the theory of NP-Completeness. The ensuing exploration of the boundaries and nature of NP-complete class of problems has been one of the most active and important research activities in computer science for the last decade.

Thema: Toom-Cook-Algorithmus

- Effizienter Algorithmus zur Multiplikation zweier ganzer Zahlen
- Basiert auf "divide and conquer"-Prinzip

20: C. Antony R. Hoare
(UK, 1980)

Auszeichnung

For his fundamental contributions to the definition and design of programming languages.

Thema: Hoare-Logik

- Formales System zum Nachweis von Korrektheitseigenschaften von Programmen
- Zentrales Konzept: Hoare-Tripel $\{P\}S\{Q\}$
- Regelsystem für partielle/totale Korrektheit

21: Robert W. Floyd
(USA, 1978)

Auszeichnung

For having a clear influence on methodologies for the creation of efficient and reliable software, and for helping to found the following important subfields of computer science: the theory of parsing, the semantics of programming languages, automatic program verification, automatic program synthesis, and analysis of algorithms.

Thema: Floyd: Floyd-Warshall-Algorithmus

- Graphentheoretischer Algorithmus zur Bestimmung von
  - kürzesten Pfade zwischen allen Paaren von Knoten (Floyd)
  - transitive Hülle des Graphen (Warshall)
- Basiert auf dynamischer Programmierung

22: Backus
(USA, 1977)

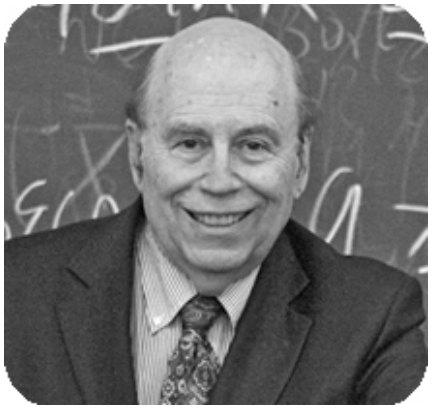
Auszeichnung

For profound, influential, and lasting contributions to the design of practical high-level programming systems, notably through his work on FORTRAN, and for seminal publication of formal procedures for the specification of programming languages.

Thema: Backus-Naur-Form

- Kompakte formale Metasprache zur Darstellung kontextfreier Grammatiken
- Erweiterte Formen (EBNF, ABNF) mit (endlicher) Wiederholung, Alternativen

23: Michael O. Rabin/Dana S. Scott
(USA, 1976)



Auszeichnung

For their joint paper "Finite Automata and Their Decision Problem," which introduced the idea of nondeterministic machines, which has proved to be an enormously valuable concept. Their classic paper has been a continuous source of inspiration for subsequent work in this field.

Thema: Endliche Automaten

- Konzept vorgestellt in 1959
- Entscheidungs- und Abschlusseigenschaften: Leerheit, Inklusion, Äquivalenz, Schnitt, Vereinigung, Komplement, ...
- Zahlreiche Anwendungen: Compiler, Verifikation, ...

24: Donald E. Knuth
(USA, 1974)

Auszeichnung

For his major contributions to the analysis of algorithms and the design of programming languages, and in particular for his contributions to the ärt of computer programmingtthrough his well-known books in a continuous series by this title.

Thema: Knuth-Morris-Pratt-Algorithmus

- Weiterer String-Matching-Algorithmus
- Ansatz: Weiterrücken des Vergleichsfensters um möglichst viele Positionen
- Aufwand $|p| + |w|$

25: Edsger W. Dijkstra
(NL, 1972)

Auszeichnung

For fundamental contributions to programming as a high, intellectual challenge; for eloquent insistence and practical demonstration that programs should be composed correctly, not just debugged into correctness; for illuminating perception of problems at the foundations of program design.

Thema: Berechnung kürzester Pfade

- Problem der kürzesten Pfade für gegebenen Startknoten eines kantengewichteten Graphen (Gewichte ≥ 0)
- Greedy-Algorithmus: bestimme in jedem Schritt die momentan aussichtsreichste Teillösung
- Liefert hier optimale Lösung