Analyse und Verifikation

AK der Praktischen Informatik 2 und

AK der Praktischen Informatik 1

(WS 2005/2006, 185.260, VU 2.0h / 185.259 VU 1.0h)

Jens Knoop
Institut für Computersprachen

`knoop@complang.tuwien.ac.at`
`http://www.complang.tuwien.ac.at/knoop/`

Montag, 16:00 Uhr bis 18:00 Uhr, EI 6 Eckert-Hörsaal
(Gußhausstraße 25 - 29, 1040 Wien)

Motivation (1)

Programme/Programmsysteme werden...

- zunehmend komplexer
- verstärkt auch in *sicherheitskritischen* Anwendungen eingesetzt mit unmittelbarer Verantwortung für
  - Leib und Leben (Kernkraftwerkssteuerung, Flugüberwachungssoftware, Airbagsteuerung,...)
  - Vermögen (Finanzdienstleistungen,...)

Speziell für sicherheitskritische Anwendungen...

- Nachweis "korrekten Funktionierens" essentiell!

Konsequenz...

- Testen allein nicht ausreichend!
- Einsatz fundierter und formaler *Analyse*-, *Verifikations*- und *Transformations*methoden erforderlich!

Motivation (2)

Tatsächlich gewinnt der...

- Einsatz fundierter und formaler Methoden zur
  - Analyse, Verifikation und Transformation

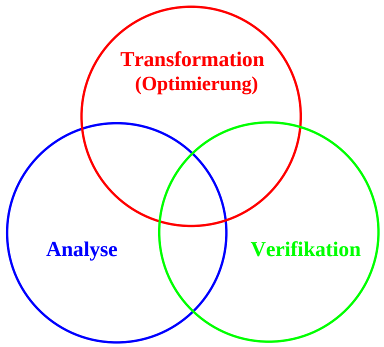
von Programmen/Programmsystemen zunehmend an Bedeutung, auch in der Industrie!

Prominente Beispiele:

- *Luftfahrtindustrie*: Airbus, Boeing
- *Automobilindustrie*: BMW Group, Infineon, T Systems, MPI Informatik, TU München und weitere Partner: Verisoft-Projekt (`www.verisoft.de`)
- ...

Thematisches Umfeld der LVA (1)

Abgesteckt durch die Themenkreise...



Thematisches Umfeld der LVA (2)

...und den für sie zentralen Eigenschaften:

- *Korrektheit* (engl. *soundness*)
- *Vollständigkeit* (engl. *completeness*)
- *Optimalität* (engl. *optimality*)

Inhalte der Lehrveranstaltung

Korrektheit, Vollständigkeit, Optimalität in...

- Programm*verifikation*
  Methode von Hoare, Korrektheit, Vollständigkeit (soundness, completeness), stärkste Nachbedingungen, schwächste Vorbedingungen,...
- Programm*analyse*
  Datenflussanalyse, erschöpfende vs. anforderungsgetriebene Analyse (exhaustive vs. demand-driven analysis), intraprozedural, interprozedural, parallel, abstrakte Interpretation, Model-checking,...
- Programm*transformation*, speziell *Optimierung*

Ziele der Lehrveranstaltung

- Überblick über fundamentale Prinzipien und Konzepte in Programmverifikation, -analyse und -transformation
- Herausarbeiten und Verstehen von Gemeinsamkeiten, Analogien und Unterschieden zwischen Programmverifikation und -analyse
- Erkennen, Einschätzen und Bewerten der Möglichkeiten und Grenzen insbesondere automatischer Programmanalyse, -verifikation und -optimierung

Was Sie mitbringen sollten...

Voraussetzungen

- Grundlagen in Theoretischer Informatik, grundlegende Programmierkenntnisse
- Kenntnisse im Übersetzerbau sind hilfreich, etwa aus der LVA Übersetzerbau (185.175 LU 3.0h bzw. 185.548 VO 2.0h), aber nicht zwingend erforderlich
- Abgeschlossenes Bakkalaureat, falls Anrechnung für Magisterstudium geplant

Eine perfekte Ergänzung in diesem Semester...

- Parallelbesuch der LVA Optimierende Übersetzer (185.187 VU 3.0h), Dr. Markus Schordan

Anrechenbarkeit

...non scholae, sed vitae discimus.

Anrechenbar als *Wahllehrveranstaltung* für folgende *Bakkalaureatsstudien*:

- Data Engineering & Statistics (BDS/W)
- Software & Information Engineering im Schwerpunkt "Software Engineering" (BSIa/W)
- Medizinische Informatik (BZI/W)

Anrechenbar als *Wahllehrveranstaltung* für folgendes *Magisterstudium*:

- Software Engineering & Internet Computing (MSE/W)

Aufbau der Lehrveranstaltung

- Vorlesung
- Übung in 2er-Gruppen
- Vorlesungsprüfung

  (über Vorlesungsstoff und Übungsbeispiele)

Unterlagen

- **Verifikation:**
  Krzysztof R. Apt, Ernst-Rüdiger Olderog. *Verification of Sequential and Concurrent Programs*, Springer, 1997.
- **Analyse:**
  Flemming Nielson, Hanne R. Nielson, Chris Hankin. *Principles of Program Analysis*, Springer, 1999.
- **Transformation:**
  Stephen S. Muchnick. *Advanced Compiler Design and Implementation*, Morgan Kaufmann, San Francisco, California, 1997.
- *Weitere Literatur:*
  ...insbesondere Originalarbeiten, wird nach Bedarf angegeben.

Anmeldung

In zwei Stufen...

- Stufe 1: *Anmeldung*
  ...jeder für sich über ein elektronisches Anmeldesystem bis Montag, den 24.10.2005
  ...genauere Informationen dazu in Kürze auf der Webseite der LVA:
  `http://www.complang.tuwien.ac.at/knoop/ak2_ws0506.html`
- Stufe 2: *Gruppenbildung*
  ...persönlich jeweils zusammen mit Gruppenpartner in der Vorlesung am 24. oder 31. Oktober 2005.

Vorlesung und Übung

- Montags von 16:00 Uhr c.t. - 18:00 Uhr im EI 6 Eckert-Hörsaal, Gußhausstraße (**Achtung**: Abweichend davon am **Mo, 17.10.2005: 16:00 Uhr s.t. - 16:45 Uhr**)
  - 16:15 Uhr - bis ca. 17:15 Uhr: Vorlesung
  - ab ca. 17:15 Uhr - 17:45 Uhr: Übung (Abgabe und Besprechung der Übungsaufgaben der Vorwoche, Ausgabe der neuen Übungsaufgaben (auch im Web erhältlich))
- beginnend mit dem 17.10.2005 im Regelfall jeden Montag ein neues Aufgabenblatt
- insgesamt ca. 10 Abgaben

Beurteilung

- Mündliche Prüfung zu Vorlesung und Übung.

Bei Fragen und Problemen

- Webseite:
  `http://www.complang.tuwien.ac.at/knoop/ak2_ws0506.html`
- Fragen und Antworten in Vorlesung und Übung
- E-Mail: `knoop@complang.tuwien.ac.at`
- Sprechstunde: mittwochs, 15 Uhr - 16 Uhr
  (bitte vorher kurz anmelden)

Einladung zu Antrittsvorlesungen

Die Fakultät für Informatik der TU Wien lädt ein zu den Antrittsvorlesungen von...

- Herrn **Univ.-Prof. Dr. Schahram Dustdar** über
  Service-Oriented Computing – Fundament moderner Internet-Technologien
- Herrn **Univ.-Prof. Dr. Reinhard Pichler** über
  Daten im Web – Neue Herausforderungen für die Datenbankforschung

am

Montag, den 17.10.2005, um 17:00 Uhr s.t.,
in den Hlawka-Hörsaal EI 9, Stiege 1, EG, Gußhausstr. 25-29

Alle Interessenten sind herzlich willkommen!

Ich wünsche Ihnen...

...viel Erfolg bei dieser Lehrveranstaltung und dass Sie auch über die unmittelbare Veranstaltung hinaus davon profitieren!

Zu guter Letzt:

Vorlesung und Übung leben mit Ihnen! Ihre Rückmeldungen, Anregungen, Verbesserungsvorschläge sind willkommen! Natürlich auch Hinweise, wenn Ihnen etwas gut gefallen hat!