Analyse und Verifikation

(SS 2010, 185.276, VU 2.0h, ECTS 3.0, MSE/W)

Jens Knoop
Institut für Computersprachen

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

Dienstag, 16:30 Uhr bis 18:00 Uhr, EI 3a Hörsaal
(Gußhausstr. 25-29, 2. Stock, 1040 Wien)

Motivation 1(4)

Programme und Programmsysteme werden...

- zunehmend komplexer
- verstärkt eingesetzt auch in sicherheitskritischen Anwendungen mit unmittelbarer Verantwortung für
  - Leib und Leben (Flugüberwachungssoftware, fly-by-wire, drive-by-wire, (Industrie-) Anlagensteuerung (Kraftwerke, Chemieanlagen, etc.),...)
  - Vermögen (Finanzindustrie, Buchhaltungs-IT,...)

Konsequenz

- Testen allein nicht ausreichend
- Formale Methoden erforderlich

Motivation 2(4)

Tatsächlich wird der...

- Einsatz formaler Methoden zur
  - Analyse, Verifikation und Transformation

auch in der Industrie (Airbus, Boing, Microsoft,...) zunehmend üblich.

Motivation 3(4)

Zwei aktuelle Referenzen:

- Steve P. Miller, Michael W. Whalen, Darren D. Cofer. *Software Model Checking Takes Off*. Communications of the ACM, Vol. 53, No. 2, Feb. 2010, 58-64.

  "Although formal methods have been used in the development of safety- and security-critical systems for years, they have not yet achieved widespread industrial use in software or systems engineering. However, two important trends are making the industrial use of formal methods practical [...]
  The second is the growing power of formal verification tools, particularly model checkers."

Motivation 4(4)

"How Coverity built a bug-finding tool, and a business, around the unlimited supply of bugs in software systems..."

- Al Bessey, Ken Block, Ben Chelf, Andy Chou, Bryan Fulton, Seth Hallem, Charles Henri-Gros, Asya Kamsky, Scott McPeak, Dawson Engler. *A Few Billion Lines of Code Later: Using Static Analysis to Find Bugs in the Real World*. Communications of the ACM, Vol. 53, No. 2, Feb. 2010, 66-75.

  "In 2002, Coverity commercialized a research static bug finding tool. [...] We built our tool to find generic errors (such as memory corruption and data races) and system-specific or interface-specific violations (such as violations of function-ordering constraints. The tool, like all static bug finders, leveraged the fact that programming rules often map clearly to source code; thus static inspection can find many of their violations."

Inhalt der Lehrveranstaltung

Korrektheit, Vollständigkeit, Optimalität in...

- Programm*verifikation*
  Methode von Hoare, Korrektheit, Vollständigkeit stärkste Nachbedingungen, schwächste Vorbedingungen,...
- Programm*analyse*
  Datenflussanalyse, abstrakte Interpretation, Modelchecking,...
- Programm*transformation*, speziell in der 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 185.311 Übersetzerbau 185.311 VL 3.0 (oder aus einer vergleichbaren Veranstaltung wie etwa der LVA 185.175 Übersetzerbau LU 3.0h bzw. 185.548 VO 2.0h aus dem bis zum 30.09.2006 gültigen Studienplan), aber nicht zwingend erforderlich
- Abgeschlossenes Bachelor-Studium, falls Anrechnung für Master-Studium geplant

Eine perfekte Grundlage(nergänzung)

...und Vertiefung in diesem Semester durch Mitbesuch von:

- LVA 185.311 Übersetzerbau, VL 3.0, ECTS 4.5, Prof. Dr. Andreas Krall, Prof. Dr.Anton Ertl
  (Blockveranstaltung vom 04.03.2010 bis 25.03.2010):
  `www.complang.tuwien.ac.at/ubvl/index.html`
- LVA 185.274 Weiterführender Übersetzerbau, VO 2.0, ECTS 3.0, Prof. Dr. Andreas Krall (ab 25.03.2010):
  `www.complang.tuwien.ac.at/andi/185.274`
- **Gastprofessur**
  LVA 185.346 From Domains to Requirements, VU 3.0, ECTS 4.5, Prof. Dr. Dr.h.c. Dines Bjørner, ACM Fellow, IEEE Fellow, Danmarks Tekniske Universitet, Lyngby, Dänemark.
  (Blockveranstaltung vom 12.04.2010 bis 30.04.2010):
  `www.complang.tuwien.ac.at/knoop/bjorner`

Anrechenbarkeit

...non scholae, sed vitae discimus.

Anrechenbar als *Wahllehrveranstaltung* für den *Master*-Studiengang:

- Software Engineering & Internet Computing (MSE/W)

Aufbau der Lehrveranstaltung

- Vorlesung
- Übung in 2er-Gruppen
- Vorlesungsprüfung
  (über Vorlesungsstoff und Übungsbeispiele)

Literatur

1. Janusz Laski, William Stanley. *Software Verification and Analysis. An Integrated, Hands-On Approach*. Springer, 2009.
2. Hanne R. Nielson, Flemming Nielson. *Semantics with Applications: An Appetizer*, Springer, 2007.
3. Krzysztof R. Apt, Ernst-Rüdiger Olderog. *Verification of Sequential and Concurrent Programs*, Springer, 1997.
4. Flemming Nielson, Hanne R. Nielson, Chris Hankin. *Principles of Program Analysis*, Springer, 1999.
5. Stephen S. Muchnick. *Advanced Compiler Design and Implementation*, Morgan Kaufmann, San Francisco, California, 1997.
6. Weitere Literatur, insbesondere Originalarbeiten, wird im Verlauf der Veranstaltung angegeben.

Anmeldung

In zwei Stufen...

- Stufe 1: *Anmeldung*
  ...jeder für sich über ein arbeitsbereichsinternes elektronisches Anmeldesystem bis Montag, den 19.03.2010:
  `http://www.complang.tuwien.ac.at/anmeldung`
- Stufe 2: *Gruppenbildung*
  ...mithilfe desselben Anmeldesystems: eines der Gruppenmitglieder kreiert die Gruppe

Siehe auch Angaben zur Anmeldung auf der Webseite der LVA:

`http://www.complang.tuwien.ac.at/knoop/auv185276_ss2010.html`

Vorlesung und Übung

- Dienstags von 13:30 Uhr s.t. - 15:00 Uhr in der Bibliothek E185.1, Argentinierstr. 8, 4. Stock (Mitte), 1040 Wien (**ab Di, 16.03.2010!**).
  - 13:30 Uhr - bis ca. 14:30 Uhr: Vorlesung
  - ab ca. 14:30 Uhr - 15:00 Uhr: Übung (Abgabe und Besprechung der Übungsaufgaben der Vorwoche, Ausgabe der neuen Übungsaufgaben (im Web erhältlich))
- beginnend mit dem 09.03.2010 im Regelfall jeden Dienstag 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/auv185272_ss2010.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)

Interesse an einem geförderten Auslandsstudium?

Die Erasmus/LLP-Programmlinie der EU bietet eine Vielzahl lohnender Möglichkeiten, z.B.

- Universidade do Minho, Braga, Portugal
- Technical University of Lissabon, Portugal
- The University of Copenhagen, Dänemark
- Universität Halle-Wittenberg, Deutschland
- Universität Paderborn, Deutschland
- Universidad Politècnica de València, Spanien
- ...

Mehr dazu auf:

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

Einladung zur Mitgliedschaft im...

[IN:N] Informatik-Netzwerk!

...eine Initiative der Fakultät für Informatik an der TU Wien zum Informationsaustausch und zur Kontaktpflege zwischen Universität(sangehörigen), ehemaligen Studierenden, Wirtschaft und Öffentlichkeit.

http://inn.tuwien.ac.at/

Werden Sie Mitglied! Ihre Mitgliedschaft ist kostenlos, aber sicher nicht umsonst!

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!