Institut für Computersprachen
Technische Universität Wien
Prof. Dr. J. Knoop

A-1040 Wien
Argentinierstr. 8
Tel.: 01-58801-18510

"Analyse und Verifikation (185.276, VU 2.0, ECTS 3.0)" SS 2011

Übungsblatt 1 15.03.2011

Aufgabe 1 : (25 Punkte)

Im Artikel *"A Few Billion Lines of Code Later: Using Static Analysis to Find Bugs in the Real World"* beschreiben die Autoren ihre Erfahrungen, einen Forschungsprototypen zur Fehlersuche in C-Programmen zu einem industriellen Ansprüchen genügenden kommerziellen Produkt zu machen.

Lesen Sie den Artikel und beantworten Sie folgende Fragen:

1. "Ein Werkzeug, das Fehler in Produktionscode findet, ist ein gutes Werkzeug. Ein Werkzeug, das mehr Fehler findet, ist ein besseres Werkzeug."

   Wie wird diese Aussage aus einer wissenschaftlichen, wie aus einer kommerziellen Perspektive im Artikel beurteilt? Welche Gründe werden dafür, welche dagegen angeführt?

2. *Sound* bedeutet korrekt. In welchem Sinn wird der Begriff *sound* im Zusammenhang mit dem Fehlerfindewerkzeug der Fa. Coverity verwendet?

3. Was bedeuten die Begriffe *false positives* und *false negatives* im Zusammenhang mit dem Fehlerfindewerkzeug der Fa. Coverity?

4. Wie können sich *false positives* und *false negatives* auf die Akzeptanz eines Fehlerfindewerkzeugs auswirken und warum?

5. Im Artikel heißt es (s.S. 70 unten): "The C language does not exist; neither does Java, C++, and C#". Was ist damit gemeint? Welche Probleme ergeben sich daraus für die Kommerzialisierung eines Forschungswerkzeugs wie im Fall der Fa. Coverity?

Hinweis: Sie können den Artikel

- 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.

aus dem TU-Netz heraus in der ACM Digital Library (`www.acm.org/dl`) aufrufen.

Abgabe: Dienstag, den 22.03.2011, vor der Vorlesung.