СЕМИНАР
„АЛГЕБРА И ЛОГИКА”

Драги колеги,
Следващите две заседания на семинара ще се проведат на
9 и 16 август 2013 г. (петък) от 11:00 часа в зала 578 на ИМИ – БАН.
Доклади на тема

A Confinement Framework for Encapsulating Objects

(9 август)

и

Deductive Verification of Hybrid Systems

(16 август)

ще изнесе Dr Wang Shuling, ISCAS, Beijing,
visiting the Carl von Ossietzky Universitaet, Oldenburg.

Поканват се всички желаещи.

От секция „Алгебра и логика” на ИМИ – БАН

http://www.math.bas.bg/algebra/seminarAiL/

==========

Abstracts

A Confinement Framework for Encapsulating Objects: Confinement is encapsulation of dynamic objects and thus is able to prohibit safety-critical objects from unintended access. The most well-known approach for achieving confinement is ownership types, which introduces into Java-like languages a set of type annotations for representing object ownership and accordingly access permission between objects. In this work, we present a different approach for specifying and verifying object confinement in object-oriented (OO) programs. Instead of expressing the confinement requirements within a class for possible future usage, as ownership templates in ownership types, we specify confinement requirements of the class in its usage class which indeed intends to confine the parts as internal representations. We extend a Java-like language as follows: on one hand, an optional “conf” clause is introduced in class declarations for declaring the confined attribute-paths; and on the other hand, a “same type and confinement” notation is introduced for expressing type and confinement dependence among attributes, parameters, and return values of methods. Following this approach, we define a type system for checking the well-confinedness of OO programs with respect to the given confinement requirements.

Deductive Verification of Hybrid Systems: To establish a deductive method for verifying hybrid systems, a modeling language with compositionality and a logic with inductive inference system for the language are prerequisites. In this work, we choose Hybrid CSP (HCSP) as the formal modeling language for hybrid systems, which, as an extension of CSP, introduces differential equations for representing continuous evolution and several forms of interruption for discrete control. The interaction between different components is realized by communication and parallel composition. To specify and verify the behavior of HCSP, we extend Hoare Logic to hybrid systems, by adding history formulas to describe continuous properties throughout the whole execution, and define Hybrid Hoare Logic (HHL). The logic is aimed to be compositional, i.e., it can reduce properties of HCSP processes to properties of their parts. Based on HHL, we have implemented in Isabelle/HOL a HCSP prover, which, given a HCSP model annotated with HHL assertions, checks whether the HCSP model conforms to the annotated property, by interactive theorem proving. We demonstrate our approach on a combined scenario originating from the Chinese High-speed Train Control System Level 3.