

Sillabo di “Modelli Formali e Analisi di Sistemi”

Contesto

L'ampia disponibilità di potenze di calcolo e la crescente richiesta di servizi software hanno portato negli ultimi anni gli specialisti informatici ad affrontare l'analisi delle *proprietà computazionalmente interessanti* dei sistemi critici (per uno specifico dominio applicativo) e complessi (dal punto di vista computazionale, strutturale, di comunicazione, etc.). Tipici esempi sono rappresentati dai sistemi di sicurezza, dal calcolo distribuito, dalle reti, e in particolare dalle reti mobili, dal Grid computing e sistemi Cloud e MobileCloud, e così via. Tra le varie proposte sorte nel corso degli anni, numerosi ricercatori ritengono che l'approccio formale sia lo strumento concettuale più adeguato. In particolare, un'ampia letteratura affronta il tema facendo riferimento alle tecniche di model checking, che sono però influenzate da limitazioni di natura computazionale e di natura di applicabilità pratica. Il corso intende quindi presentare alcuni modelli formali alternativi alle tecniche di model checking per discuterne la capacità specifica, facendo riferimento a esempi reali.

Scopo

Il corso si focalizza su alcuni modelli formali particolarmente adatti a descrivere sistemi critici ad elevata complessità, quali reti di Petri, Abstract State Machine, alcuni process calculi. Tali modelli favoriscono l'analisi di un insieme di proprietà particolarmente interessanti dal punto di vista computazionale, sia di natura generale, come ad esempio deadlock e livelock, starvation e liveness, reachability, reversibility. Nell'a.a. 2017-18 il corso presterà particolare attenzione alla modellazione dei protocolli e dei sistemi di sicurezza.

Organizzazione

Il corso è organizzato ponendo in stretta relazione lo studio dei modelli formali introdotti con i problemi ricorrenti in alcuni esempi (protocolli e sistemi di sicurezza, reti mobili ad-hoc - MANET, gestione dei job nei sistemi Grid, e così via). L'obiettivo di tale organizzazione è quello di mostrare come un'opportuna modellazione favorisca l'analisi delle proprietà specifiche del sistema modellato.

Argomenti trattati

- **Proprietà computazionalmente interessanti:** il corso è orientato all'analisi di particolari proprietà dei sistemi, in genere di difficile valutazione, quali: correttezza del comportamento di protocolli di sicurezza e di routing, raggiungibilità degli stati del sistema, limitatezza/illimitatezza delle risorse, vitalità del sistema, reversibilità, completezza, multimodalità e complessità.
- **Reti di Petri:** concetti di base per la modellazione di sistemi dinamici discreti. Sarà inoltre approfondito il loro uso nell'analisi delle proprietà computazionalmente interessanti della dinamica di sistemi discreti asincroni e concorrenti. Saranno sviluppati esempi di applicazione delle Reti di Petri nell'ambito del routing e della sicurezza per Mobile Ad-hoc NETWORKS (MANET).
- **Abstract State Machine (ASM) e Distributed ASM (DASM):** Con ASM si intende sia un modello di rappresentazione di sistemi complessi, che un metodo per lo sviluppo di tali sistemi basato sul modello stesso. Il sistema da sviluppare è modellizzato da automi a stati generalizzati (le ASM, appunto). Il metodo prevede di modellizzare il sistema con incrementi successivi sia verticali, per dettagliare le varie componenti, che orizzontali, per l'integrazione di nuove componenti. Le DASM rappresentano l'evoluzione delle ASM in contesti in cui l'attività computazionale è fornita da più sistemi che operano sia

sincronamente che asincronamente. Anche nell'ambito delle ASM e DASM sarà trattato il problema dell'analisi delle proprietà computazionalmente interessanti. Saranno sviluppati esempi di applicazione delle ASM nell'ambito delle MANET e della gestione dei job in sistemi Grid.

- **Comunicazione tra processi sequenziali**, mediante Hoare's CSP: Saranno forniti i concetti basilari del formalismo CSP e discusso il loro uso per la comunicazione tra processi, anche in riferimento a linguaggi di programmazione quali il linguaggio Go e Erlang. Saranno infine sviluppati esempi di applicazione del CSP nell'ambito dei protocolli di sicurezza
- **Altre applicazioni dei modelli presentati**: casi di studio svolti da studenti negli anni precedenti, tesi di laurea, esempi tratti dalla letteratura.

Il corso prevede 6 CFU, di cui 4 di lezioni frontali, 2 di esercitazioni guidate.

Valutazione

Sono previste due modalità per la valutazione: quella *tradizionale*, che consiste in una prova orale sull'intero programma trattato e quella di *approfondimento*, in cui dovrà essere discusso un particolare aspetto, eventualmente svolgendo un caso di studio proposto dagli studenti.

Bibliografia

E. Börger, R. Stärk, *Abstract State Machine – A Method for High-Level System Design and Analysis*, Springer 2003.

C.A.R. Hoare *Communicating Sequential Processes*, Prentice Hall International, 1985 (disponibile all'indirizzo <http://www.usingcsp.com./cspbook.pdf>)

R. David, H. Alia, *Discrete, Continuous, and Hybrid Petri Nets*, Springer 2003.

AA.VV. *The Go Programming Language*, <http://golang.org/>

AA.VV. *Erlang Programming Language*, <http://www.erlang.org>

Articoli, dispense e risorse on line distribuiti o segnalati durante il corso.