Dnr: 2018/2846-3.1.2.2

Kursplan

Fakulteten för teknik

Institutionen för datavetenskap och medieteknik

4DV701 Formella metoder, 5 högskolepoäng
Formal methods, 5 credits

Huvudområde
Datavetenskap

Ämnesgrupp
Informatik/Data- och systemvetenskap

Nivå
Avancerad nivå

Fördjupning
A1F

Fastställande
Fastställd av Fakulteten för teknik 2018-10-08
Kursplanen gäller från och med höstterminen 2019

Förkunskaper
4DV650 Modellering och simulering av system, 5 hp

Mål

Efter genomförd kurs skall studenten kunna:

- resonera kring vad säkerhet (security och safety) betyder för ett mjukvaruprogram eller system och vilka egenskaper som krävs
- beskriva metoder för och svårigheter med att formellt verifiera egenskaper relaterade till säkerhet och korrekthet hos mjukvarusystem samt vilka begränsningar olika metoder har
- redogöra för de senaste rönen inom formella metoder och verifikation
- redogöra för hur runtime-övervakning kan användas för att genomdriva säkerhetskrav
- uttrycka säkerhetsegenskaper hos (jämnlöpande) system och mjukvaruprogram formellt med hjälp av olika typer av logik
- använda olika metoder för att verifiera korrekthet och säkerhet hos system under modellering och mjukvaruprogram
- använda de vanligaste verktygen och programmen för att beskriva och verifiera system och mjukvaruprogram
- resonera kring vilka samhällskostnader (och konsekvenser) felaktig och osäker mjukvara medför samt hur formella metoder kan spela in för att t.ex. reglera mjukvara inom vissa domäner.

Innehåll

Kursen ger en introduktion till formell verifikation. Den bygger vidare på sats och predikatlogik och introducerar t.ex. logiker som tar hänsyn till tid.

Följande moment behandlas:

- Introduktion till formell verifikation
- Klassifikation av olika verifikationstekniker
- Processalgebra (CCS), samt hur dessa kan utökas med tidsfördröjningar
- Tidstillståndsmaskin (timed automata)
- Fördjupning av sats- och predikatlogik, samt temporallogik (LTL och CTL)
- Programspråkssemantik
- Programverifikation med hjälp av Hoare-logik och separationslogik
- Modellkontroll med hjälp av LTL och CTL
- Runtime-övervakning

Undervisningsformer

Undervisningen består av föreläsningar och lärarledda laborationer. Kursen innehåller även en serie gästföreläsningar där industrirepresentanter och forskare presenterar hur och varför de använder formell verifikation samt vilka metoder och verktyg de använder.

Examination

Kursen bedöms med betygen A, B, C, D, E, Fx eller F.
Betyget A utgör det högsta betygssteget, resterande betyg följer i fallande ordning där betyget E utgör det lägsta betygssteget för att vara godkänd. Betyget F innebär att studentens prestationer bedömts som underkända.

Bedömning av de studerandes prestationer sker genom formell verifikation av ett mjukvaruprogram (inlämningsuppgifter), formell verifikation av en systemmodell (inlämningsuppgifter) och en skriftlig tentamen. För studerande som inte blivit godkänd vid ordinarie provtillfälle anordnas förnyad prövning i nära anslutning till ordinarie prov.

För godkänt betyg på kursen krävs minst betyg E på samtliga moment. Slutbetyget bestäms från: formell verifikation av ett mjukvaruprogram (inlämningsuppgifter) (20%), formell verifikation av en systemmodell (inlämningsuppgifter) (20%) och skriftlig tentamen (60%).

Kursvärdering

Under kursens genomförande eller i nära anslutning till kursen genomförs en kursvärdering. Resultat och analys av kursvärderingen ska återkopplas till de studenter som genomfört kursen och de studenter som deltar vid nästa kurstillfälle. Kursvärderingen genomförs anonymt. Den sammanställda rapporten arkiveras.

Övrigt

Betygskriterier för A-F-skalan kommuniceras till studenten via särskilt dokument. Studenten informeras om kursens betygskriterier senast i samband med kursstart.

Kursen genomförs på ett sådant sätt att kursdeltagarnas erfarenheter och kunskap görs synlig och utvecklas. Det innebär till exempel att vi har ett inkluderande förhållningssätt och strävar efter att ingen ska känna sig exkluderad. Detta kan yttra sig på olika sätt i en kurs, till exempel genom att som läraren använder sig utav könsneutrala exempel.

Kurslitteratur och övriga läromedel

Luca Aceto, Anna Ingólfsdóttir, Kim Guldstrand Larsen och Jiri Srba, *Reactive Systems: Modelling, Specification and Verification*, Cambridge University Press, senaste upplagan. Antal sidor: 150 av 281.

Michael Huth, och Mark Ryan, *Logic in Computer Science: Modelling and Reasoning about Systems*, Cambridge University Press, senaste upplagan. Antal sidor: 300 av 412.

- Kompendium med vetenskapliga artiklar