

Obligatorisk oppgave 1 – IN5100

Peter C. Ölveczky

31. august 2023

1 Formaliteter

- Man jobber enten én og én, eller i grupper om *to* personer. Hvis man jobber i gruppe på to, leverer man *samme* besvarelse og markerer at man har levert felles besvarelse med NN.
- Besvarelsen skal leveres innen 22/9 2023 kl 23.59 GMT +2.
- Besvarelsen skal leveres på dertil egnet måte i Devilry.
- Besvarelsen skal være fint formatert (L^AT_EX/Word eller lignende), og skal også inkludere Maude kode, inklusive eksekveringskommandoene som er blitt brukt (disse kan kommenteres bort), slik at kursledelsen kan eksekvere Maude-spesifikasjonen.
- Instituttets standard “jeg-har-ikke-juksset” skjema skal, i utfylt stand, muligens vedlegges besvarelsen. Jeg kommer tilbake med informasjon hvis dette er nødvendig.

Kursledelsen forbeholder seg retten til å endre på ovenstående parametre.

2 Oppgaven

Oppgaven dreier seg om å spesifisere og analysere *reliable broadcast protocol* (RBP) – slik som denne er beskrevet i artikkelen “J.J. Garcia-Luna-Aceves and Y. Zhang, *Reliable Broadcasting in Dynamic Networks*, Proc. IEEE ICC '96, Dallas, Texas, June 23-27, 1996” – i Maude 3.3. Artikkelen er også tilgjengelig på <http://olveczky.se/IN5100-23/garcia-luna.pdf>.

Man skal begrense seg til å spesifisere protokollen for *statiske* nettverk. I tillegg bør man spesifisere protokollen for én broadcast-runde. Protokollen slik som den er beskrevet i artikkelen har mulighet for at flere “source nodes” kan starte runder av protokollen samtidig, men slik at hver source node maksimalt ønsker å kringkaste én melding. Jeg kan ikke forstå noe annet enn at slike runder er uavhengige av hverandre, slik at korrektheten til protokollen ikke skulle berøres av en slik forenkling. (Man slipper bare en masse indekser her og der.)

Se forøvrig lysarkene til forelesning 2 for utfyllende fakta om denne innleveringsoppgaven.

2.1 Oppgave 1: Spesifikasjon av RBP i Maude

1. Modellér/spesifiser RBP protokollen (med de begrensningene som er gitt ovenfor) i Maude 3.3. Kommentér og forklar godt, og gjør rede for eventuelle antagelser du har gjort. Du bør bruke objekt-basert modellering i Maude.
2. Redegjør for hvorvidt artikkelens beskrivelse av protokollen inneholder *viktige* “implisitte antagelser” (dvs. ting de sannsynligvis antar, men som ikke nødvendigvis er opplagt for andre som leser protokollen) og/eller tvetydigheter.

2.2 Oppgave 2: Analyse av protokollen i Maude

1. Definér noen passende initialtilstander og analysér protokollen ved eksekvering i Maude av din Maude spesifikasjon. Målet er prøve å finne ut hvorvidt protokollen er korrekt. Du skal kjøre noen simuleringer vha kommandoene `rew` og/eller `frew`, og (om nødvendig) gjøre dypere analyse ved bruk av Maude’s søkekommando. Kommentér resultatene av kjøringene.
2. Vurdér analysen. Hva kan vi slutte av analysen?
 - Har vi *bevist* at protokollen er korrekt?
 - Har vår *tillit* til at protokollen er korrekt blitt styrket som følge av analysen?
 - Er protokollen gal? I så fall, forklar hvorfor protokollen er gal.

Begrunn svaret.

2.3 Oppgave 3: Sammenligning av spesifikasjonsstiler og analysemetoder

Vi har nå sett to måter å spesifisere en slik kommunikasjonsprotokoll på: Maude og artikkelens uformelle beskrivelse. Vi har også sett to måter å analysere en protokoll på: Maude omskrivning og søk på den ene siden og artikkelens metode, nemlig håndbevis med teoremer og lemma som bevises “for hånd” samt simuleringer ved simuleringsverktøy (i dette tilfellet Drama).

Sammenlign de to metodene (Maude spesifikasjon og analyse vs. uformell beskrivelse med håndbeviser og simulering i Drama) og nevnt fordeler og ulemper ved begge metodene.

Lykke til!