

9. ASYNCHONOUS AGREEMENT

Magnus Jensen

Note: den her er ikke så lang, men den er svær og meget der skal skrives på tavlen. Så der burde være nok fyld. Tager den for lang tid, så tag de sidste punkter fra.

ASYNCHONOUS AGREEMENT

1. Motivation

I den Asynkorne Agreement model; har vi ikke en betegnelse for tid - faktisk bruger vi det slet ikke.

| *Ingen tid*

Det har sine fordele og ulemper

| *(+) Ingen synkron ure*

hvilket er et helt problem i sig selv

| *(-) Ikke skelne langsom, fra: ikke sendt*

Så vi kan beskyjde en part for at være ond fordi den aldrig sendte en besked. Hvorfor vi har **Eventuel Delivery** af beskeder.

| *(-) ingen runder*

En anden konsekvens af, at vi ikke kan bruge tid - er at vi ikke har nogen betegnelse om at arbejde i runder. Så hvad gør vi så?

2. Unscheduled Broadcast

Så når vi ikke har tid, og **ikke kan arbejde i runder**; så har vi at parter **ikke kan vide noget om** - hvornår at **en anden** part har planlagt at **sende en besked**.

Dette kalder vi for et Unscheduled Broadcast, eller så fint på dansk - et uplanlagt broadcast.

2.1 Betingelser for asynkron protokol

Men hvordan kan vi så udføre en handling?

For enhver asynkron protokol gælder følgende:

- *Der er aktiveringsregler*
- *Et tidspunkt venter for $n - t$ beskeder*
- *Et tidspunkt venter for $t + 1$ beskeder*
- *$n > 3t$ for stort flertal af ærlige parter.*

2.1.1 Kommandoer

- *Broadcaster B kan få: (BROADCAST, $P1$, id , m)*
- *P_j kan outputte (DELIVER, $P1$, ID , m).*

2.1.2 Egenskaber

- **Validity 1:** *Hvis en korrekt P outputter, og D er korrekt, har D sendt outputtet*
- **Agreement:** *Alle korrekte outputted det samme*
- **Validity 2:** *Hvis D er korrekt og får input m , vil alle outputte m*
- **Propagation (flooding):** *Hvis en korrekt P outputter m , vil alle korrekte*

2.2 Bracha Broadcast

2.2.1 Ideen

Når en broadcaster B flooder med en besked M , er ideen at:

- *Ærlige parter sender beskeden rundt*
- *Når det ses fra et flertal, erklæres beskeden er klar til offentliggørelse*
- *Når det ses fra et flertal, offentliggøres beskeden*

2.2.2 Protokollen

- *B skal broadcaste m , så send den til alle*
- *Besked fra D , ekko den til alle andre, medmindre man har set id'et før*
- *Ekko fra $n - t$ parter, send klarmelding*
- *Klarmelding fra $t + 1$ parter, send klarmelding*
- *Klarmelding fra $n - t$ parter, så udskriv.*

2.2.3 Analyse

Validity 2:

- m broadcasts
- Alle ærlige parter sender EKKO til alle
- Alle ærlige parter får $n > 3t$ EKKO og sender et KLAR
- Alle ærlige parter får KLAR og udskriver

Validity 1:

- Hvis B aldrig fik besked på at broadcaste, så sendte maksimalt t et ekko.
- Siden t EKKO eller KLAR ikke er nok til at udskrive, vil ingen ærlig P udskrive.

Propagation:

Vi starter med at kigge på, hvordan det kan ske, at en korrekt P har outputtet. Det vil ske fordi:

- P har modtaget KLAR fra $n - t$ parter, hvilket er minimum $2t + 1$
- t kan være korrupte; så de $t + 1$ har også sendt en klarmelding til alle andre
- Så alle ærlige parter modtager minimum $t + 1$ KLAR; hvorfor alle outputter m .

Agreement:

Vi bruger lidt af samme logik som før, og kigger på hvad der skal til for at en P_i vil outputte en m .

- t onde
- $3t + 1$ ærlige

- P_i har modtaget KLAR fra $2t + 1$ parter
- t kan være korrupte; så $t + 1$ ærlige sendte KLAR til P_i
- En P_j der outputter, vil også have modtaget klarmelding fra $t + 1$ parter
- Vi ved ikke hvilke parter der er onde; så minimum 1 ærlig part har sendt samme m til begge, hvorfor de outputter det samme.

3. Asynchronous Byzantine Agreement¹

Hurtig gennemgang.

Async Byzantine Agreement, er en afstemning der kan foregå i et distribueret system asynkront - og parterne skal nu tælle stemmer og blive enige om en beslutning.

- Hver afstemning har et id.
- Hver part kan få en stemme i input ($VOTE, id, V_i$), hvor $V_i \in \{0, 1\}$
- Hvert part kan outputte en beslutning ($DECISION, id, D_i$) hvor $D_i \in \{0, 1\}$

3.1 Weak Agreement

En protokol der opretholder async byzantine agreement, er Weak Agreement.

Den siges at være svag, og grundet at vi tillader en ærlig part at være i tvivl om hvad for en beslutning den skal tage og at der heller ej behøver at være enighed om man er i tvivl; altså kan en korrekt part outputte "?".

Protokollen virker ved:

Weak Agreement: $n > 5t$

3.1.1 Protokollen

- Alle sender v til alle andre
- Alle venter på v fra $n - t$ parter
 - Hvis $n - 2t$ af $v = 0$, output $d = 0$
 - Hvis $n - 2t$ af $v = 1$, output $d = 1$
 - Ellers $d = ?$

3.2 Fra Weak Agreement til Non-Terminating

Det kan være et problem, at det rent faktisk er en svag-enighed der gives i den forestående protokol.

- Kør Weak Agreement med input V_i og lad outputtet være D_i
- Hvis $D_i \neq ?$ så sæt $V_i = D_i$
- Hvis $D_i = ?$ så sæt V_i lig et uniformligt tilfældigt bit
- Start forfra

1. Egenskaber udenladt, se /noter/readme.md