Goals of the lecture

- Decentralized Consensus Protocols
- Verification of Synchronous Protocols
- Algorithms for computing functions of global state.

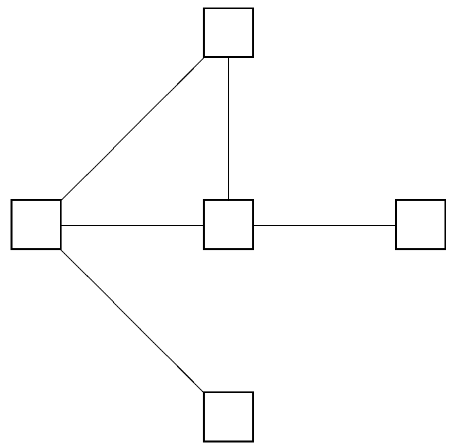
Bermond, Konig, and Raynal

Consensus Protocols

- Systems $<$ Transformation / Reactive

  - n nodes
  - connected topology
  - bi-directional channels
  - m channels
  - D diameter
  - no shared memory/clock
  - message-based communication
  - reliable delivery
  - each node knows its identity and channels adjacent to it

Consensus Protocols



- initial data distributed on the nodes
- required symmetric algorithm
- aim is to compute a global function/predicate

such protocols are called Consensus protocols.

Ideas in the algorithm

- Computation in phases:

  Init, phase_1, phase_2, $\cdots$, phase_k, term.

- Logical synchronization induced

  - wakeup on receivinga message

- Termination : node iterates phase so long as it receives new information

  $\Rightarrow$ different nodes may terminate at different times

  If D is known, the algorithm stops after D phases.

Filtering Notions

1. In phase p send only the new information that is received in phase $p-1$.

2. if $sent(c) = received(c)$ then processes connected thru that channel can never learn any new information along that channel.

3. At phase p:
   - P learns $received(c) - sent(c)$.
   - Send "end" message if this is already known.

Algorithm to compute the routing table

Process P:

- D known
- p : number of the current phase
- c : any channel incident on P

Inf : global information known by P
{ identities of the nodes for which P knows a shortest route }

New : new information obtained since the beginning of this phase.

sent(c) : message sent on channel c at the current phase.

receive(c) : message received through channel c.

Algorithm [Contd.]

Init
$p \leftarrow 0$
Inf $\leftarrow$ { identity of the node }
sent(c) $\leftarrow$ Inf for all c

Phases
while $p < D$ do
    $p \leftarrow p + 1$
    send$\langle$sent$(c)\rangle$ on all channels c
    New $\leftarrow \phi$
    For every channel c do
        receive $\langle$ received$(c)\rangle$ on c
        $\forall y \in$ received(c) $-$ Inf $-$ New : Rout (c) $\leftarrow$ Rout (c) $\cup\{y\}$
        New $\leftarrow$ New $\cup$ (received(c) $-$ Inf)
    Inf $\leftarrow$ Inf $\cup$ New
    sent(c) $\leftarrow$ New $-$ received(c)

Term
Rout : minimum routing table
Inf : identities of all nodes

General Algorithm

- D not known
- OPEN : set of channels still open

<u>Init</u>: $p \leftarrow 0$; Inf $\leftarrow$ {initial data }
New $\leftarrow$ Inf ; OPEN $\leftarrow$ set of all channels
$\forall c$: received(c) $\leftarrow \phi$

<u>Phases</u> : while OPEN $\neq \phi$ do
$p \leftarrow p + 1$
$\forall c \in$ OPEN do
sent(c0 $\leftarrow$ New $-$ received(c)
send $\langle$send(c)$\rangle$ on c
New $\leftarrow \phi$
$\forall c \in$ OPEN do
received $\langle$received(c)$\rangle$ on c
if (received(c) = send(c)) then OPEN $\leftarrow$ OPEN $-\{c\}$
New $\leftarrow$ New $\cup$ (received(c) $-$ Inf)
call compute
Inf $\leftarrow$ Inf $\cup$ New

Proof Idea

- During phase p a node P receives the information contained in the nodes at distance exactly p from itself.

- closed(c) at the end of phase $p \equiv \left(T^{p-1}(P) = T^{p-1}(Q)\right)$
  - $T^i(P)$ = set of nodes at distance at most i from P.

Proof [Contd.]

Notation :

$N^i(P) =$ set of nodes at distance i from P.

$T^i(P) = \cup_{j \leq i} N^i(P)$

$c =$ channel(P, Q)

$$
\begin{aligned}
\forall c \in \mathsf{open}_{p-1} \;:\; \qquad \mathsf{sent}_p(c) &\leftarrow \mathsf{new}_{p-1} - recd_{p-1}(c) \\
\forall c \in \mathsf{open}_{p-1} \;:\; \mathsf{received}_p(c) &\leftarrow \mathsf{sent}_p(\overline{c})
\end{aligned}
$$

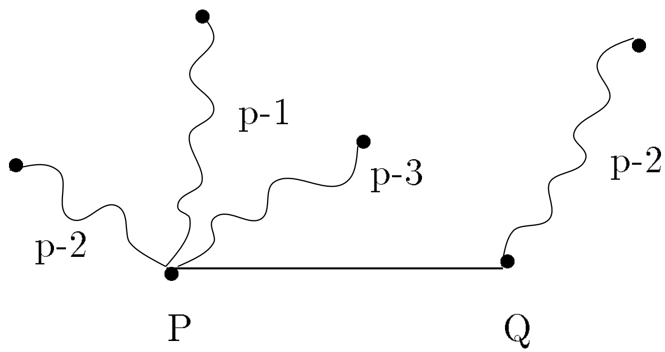
$$
\begin{aligned}
\mathsf{open}_p &\leftarrow \mathsf{open}_{p-1} - \{\, c \mid \mathsf{sent}_p(c) = \mathsf{received}_p(c)\} \\
\mathsf{new}_p &\leftarrow \cup\, \mathsf{received}_p(c) - \mathsf{inf}_{p-1} \\
\mathsf{inf}_p &\leftarrow \mathsf{inf}_{p-1} \cup \mathsf{new}_p
\end{aligned}
$$

Theorem :

$$
\begin{aligned}
\mathsf{new}_p &= N^p(P) \\
\mathsf{sent}_p(c) &= N^{p-1}(P) - N^{p-2}(Q) \\
\mathsf{received}_p(c) &= N^{p-1}(Q) - N^{p-2}(P) \\
\mathsf{open}_p &= \{\, (P, Q) \mid T^{p-1}(P) \neq T^{p-1}(Q)\} \\
\mathsf{inf}_p &= T^p(P)
\end{aligned}
$$

Lemma closed$_p = \{\, (P, Q) \mid T^{p-1}(P) = T^{p-1}(Q)\}$ (B)

$\Rightarrow$ Given $N^{p-1}(P) - N^{p-2}(Q) = N^{p-1}(Q) - N^{p-2}(P)$.



$$
\begin{aligned}
T^{p-1}(P) &= T^{p-2}(Q) \cup N^{p-1}(P) \cup N^{p-2}(P) \\
&= T^{p-2}(Q) \cup \big(N^{p-1}(P) - N^{p-2}(Q)\big) \cup N^{p-2}(P) \\
&= T^{p-2}(Q) \cup \big(N^{p-1}(Q) - N^{p-2}(P)\big) \cup N^{p-2}(P) \\
&= T^{p-2}(Q) \cup N^{p-1}(Q) \\
&= T^{p-1}(Q)
\end{aligned}
$$

$\Leftarrow$

Given $\left(T^{p-1}(P) \neq T^{p-1}(Q)\right)$

To show that $N^{p-1}(P) - N^{p-2}(Q) = N^{p-1}(Q) - N^{p-2}(P)$