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 $\lessdot$ 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:
  - $\text{Init, phase}_1, \text{phase}_2, \ldots, \text{phase}_k, \text{term.}$

- Logical synchronization induced
  - \text{wakeup on receiving a 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 \( \text{sent}(c) = \text{received}(c) \) then processes connected thru that channel can never learn any new information along that channel.

3. At phase \( p \):
   - \( P \) learns \( \text{received}(c) - \text{sent}(c) \).
   - 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 $P$

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

$\textbf{New}$: new information obtained since the beginning of this phase.

$\text{sent}(c)$: message sent on channel $c$ at the current phase.

$\text{receive}(c)$: message received through channel $c$. 
Algorithm [Contd.]

**Init**
\[
\begin{align*}
    p & \leftarrow 0 \\
    \text{Inf} & \leftarrow \{ \text{identity of the node} \} \\
    \text{sent}(c) & \leftarrow \text{Inf} \text{ for all } c
\end{align*}
\]

**Phases**
\[
\text{while } p < D \text{ do} \\
\begin{align*}
    p & \leftarrow p + 1 \\
    \text{send}(\text{sent}(c)) \text{ on all channels } c \\
    \text{New} & \leftarrow \emptyset \\
    \text{For every channel } c \text{ do} \\
    \begin{align*}
        \text{receive } (\text{received}(c)) \text{ on } c \\
        \forall y \in \text{received}(c) - \text{Inf} - \text{New} : \text{Rout}(c) & \leftarrow \text{Rout}(c) \cup \{y\} \\
        \text{New} & \leftarrow \text{New} \cup (\text{received}(c) - \text{Inf}) \\
        \text{Inf} & \leftarrow \text{Inf} \cup \text{New} \\
        \text{sent}(c) & \leftarrow \text{New} - \text{received}(c)
    \end{align*}
\end{align*}
\]

**Term**
\[
\text{Rout} : \text{minimum routing table} \\
\text{Inf} : \text{identities of all nodes}
\]
General Algorithm

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

**Init:**

- $p \leftarrow 0$; \( \text{Inf} \leftarrow \{\text{initial data}\} \)
- New \( \leftarrow \text{Inf} \); OPEN \( \leftarrow \) set of all channels
- \( \forall c : \text{received}(c) \leftarrow \phi \)

**Phases:** while OPEN \( \neq \phi \) do

- $p \leftarrow p + 1$
- \( \forall c \in \text{OPEN} \) do
  - sent(\( c0 \) \( \leftarrow \) New \( - \) received(\( c \))
  - send \( \langle \text{send}(c) \rangle \) on \( c \)
- New \( \leftarrow \phi \)
- \( \forall c \in \text{OPEN} \) do
  - received \( \langle \text{received}(c) \rangle \) 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.

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

Notation:

\[ N^i(P) = \text{set of nodes at distance } i \text{ from } P. \]
\[ T^i(P) = \bigcup_{j \leq i} N^j(P) \]
\[ c = \text{channel}(P, Q) \]
Decentralized Consensus Protocols

∀c ∈ open_{p-1} : \quad \text{sent}_p(c) \leftarrow \text{new}_{p-1} - \text{recd}_{p-1}(c)

∀c ∈ open_{p-1} : \quad \text{received}_p(c) \leftarrow \text{sent}_p(\bar{c})

\text{open}_p \leftarrow \text{open}_{p-1} - \{ \ c \mid \text{sent}_p(c) = \text{received}_p(c) \} \\
\text{new}_p \leftarrow \cup \text{received}_p(c) - \text{inf}_{p-1}

\text{inf}_p \leftarrow \text{inf}_{p-1} \cup \text{new}_p

Theorem :

\text{new}_p = N^p(P)

\text{sent}_p(c) = N^{p-1}(P) - N^{p-2}(Q)

\text{received}_p(c) = N^{p-1}(Q) - N^{p-2}(P)

\text{open}_p = \{ \ (P, Q) \mid T^{p-1}(P) \neq T^{p-1}(Q) \} \\
\text{inf}_p = T^p(P)
\[ \text{Lea}\, p = \{ (P, Q) \mid T^{p-1}(P) = T^{p-1}(Q) \} \]  

(B)  

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

\[ T^{p-1}(P) = T^{p-2}(Q) \cup N^{p-1}(P) \cup N^{p-2}(P) \]
\[ = T^{p-2}(Q) \cup (N^{p-1}(P) - N^{p-2}(Q)) \cup N^{p-2}(P) \]
\[ = T^{p-2}(Q) \cup (N^{p-1}(Q) - N^{p-2}(P)) \cup N^{p-2}(P) \]
\[ = T^{p-2}(Q) \cup N^{p-1}(Q) \]
\[ = T^{p-1}(Q) \]
\[ \iff \]

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

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