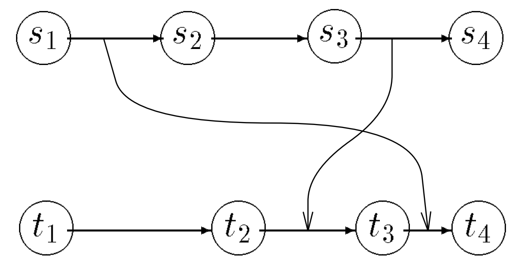
Objectives of this Lecture

- Induction on $\rightarrow$

- Induction on $\not\rightarrow$

- Formal proof of the vector clock algorithm

Causally precedes and its complement



- $\xrightarrow{k}$ relation used for induction on $\rightarrow$.
  For $k > 0$,
  $$s \xrightarrow{k} t \triangleq ml(s,t) = k$$
  Thus $s \xrightarrow{k} t$ if and only if $s \rightarrow t$ and the longest chain from s to t has length k.

Induction on $\rightarrow$

Lemma 1 $s \rightarrow t \;\Leftrightarrow\; (\exists k : k > 0 : s \xrightarrow{k} t)$

Lemma 2 $s \xrightarrow{1} t \;\Rightarrow\; s \prec_1 t \vee s \leadsto t$ Is Converse true ?

Proof:

$$
\begin{array}{lll}
 & s \xrightarrow{1} t & \\
\Rightarrow & ml(s,t) = 1 & \{ \text{ defn of } \xrightarrow{k} \} \\
\Rightarrow & \exists c : first(c) = s \wedge last(c) = t \wedge len(c) = 1 & \\
\Rightarrow & s \prec_1 t \;\wedge\; s \leadsto t & \{ \text{ defn of a chain } \}
\end{array}
$$

■

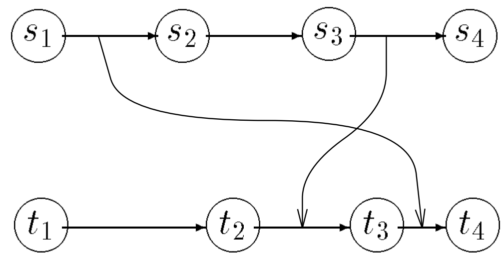
Lemma 3 $(s \xrightarrow{k} t) \;\wedge\; (k > 1) \;\Rightarrow\; (\exists u :: s \xrightarrow{k-1} u \wedge u \xrightarrow{1} t)$

Proof:

$$
\begin{array}{lll}
 & (s \xrightarrow{k} t) \;\wedge\; (k > 1) & \\
\Rightarrow & (ml(s,t) = k) \;\wedge\; (k > 1) & \{ \text{ defn of } \xrightarrow{k} \\
\Rightarrow & (\exists u \;::\; ml(s,u) = k-1 \;\wedge\; ml(u,t) = 1) & \{ \text{ chain lemma} \\
\Rightarrow & (\exists u :: s \xrightarrow{k-1} u \wedge u \xrightarrow{1} t) & \{ \text{ defn of } \xrightarrow{k}
\end{array}
$$

■

The relation $\not\to$



Define for $k \geq 0$:

$$s \overset{k}{\not\to} t \stackrel{\triangle}{=} s \not\to t \wedge ml(Init, t) = k$$

Thus $s \overset{k}{\not\to} t$ if and only if $s \not\to t$ and the longest chain from some initial state to t has length k.

Induction on $\not\rightarrow$

Lemma 4 $s \not\rightarrow t \;\Leftrightarrow\; (\exists k : k \geq 0 : s \overset{k}{\not\rightarrow} t)$

Proof:

$$
\begin{array}{cll}
 & s \not\rightarrow t & \\
\Leftrightarrow & (s \not\rightarrow t) \;\wedge\; (ml(Init,t) \geq 0) & \{ \text{ by defn of } ml(Init,t) \text{ } \} \\
\Leftrightarrow & (\exists k : k \geq 0 : s \overset{k}{\not\rightarrow} t) & \{ \text{ defn of } \overset{k}{\rightarrow} \text{ } \}
\end{array}
$$

■

Lemma 5 $s \overset{0}{\not\rightarrow} t \;\Leftrightarrow\; Init(t)$

Induction on $\not\rightarrow$ [Contd.]

Lemma 6

$$(k > 0) \wedge (s \overset{k}{\not\rightarrow} t) \wedge (u \rightarrow t) \Rightarrow (\exists j : 0 \leq j < k : s \overset{j}{\not\rightarrow} u)$$

Proof :

$$k > 0 \wedge s \overset{k}{\not\rightarrow} t \wedge u \rightarrow t$$

$$\Rightarrow k > 0 \wedge s \not\rightarrow u \wedge s \overset{k}{\not\rightarrow} t \qquad \{\text{otherwise } s \rightarrow t\}$$

$$\Rightarrow k > 0 \wedge s \not\rightarrow u \wedge ml(Init, t) = k \qquad \{\text{defn of } \overset{k}{\not\rightarrow}\}$$

$$\Rightarrow k > 0 \wedge s \not\rightarrow u \wedge ml(Init, u) < k$$

$$\{\text{otherwise } ml(Init, t) > k\}$$

$$\Rightarrow (\exists j : 0 \leq j < k : s \overset{j}{\not\rightarrow} u) \qquad \{\text{defn of } \overset{j}{\not\rightarrow}\} \quad \blacksquare$$

A variant of the vector clock algorithm

- vector components incremented less frequently; it maintains:

$$(\forall s,t : s.p \neq t.p : s.v < t.v \quad \Leftrightarrow \quad s \rightarrow t)$$

For any initial state s:

$$(\forall i : i \neq s.p : s.v[i] = 0) \wedge (s.v[s.p] = 1)$$

Rule for a send event (s, snd, t):

$$t.v := s.v;$$
$$t.v[t.p] + +;$$

Rule for a receive event $(s, rcv(u), t)$:

$$t.v := \max(s.v, u.v);$$

Rule for an internal event (s, int, t):

$$t.v := s.v;$$

Proof

- $(\forall s,t : s.p \neq t.p : s.v < t.v \quad \Leftrightarrow \quad s \rightarrow t)$. accomplished by

$$s.p \neq t.p \wedge s \rightarrow t \quad \Rightarrow \quad s.v < t.v \tag{1}$$
$$s.p \neq t.p \wedge s.v < t.v \quad \Rightarrow \quad s \rightarrow t \tag{2}$$

Lemma 7 $s \rightarrow t \quad \Rightarrow \quad s.v \leq t.v$

Proof [Contd.]

Proof : Sufficient to show that $\forall\, k > 0 : s \xrightarrow{k} t \Rightarrow s.v \leq t.v$

Base $(k = 1)$:

$$
\begin{array}{lll}
 & s \xrightarrow{1} t & \\
\Rightarrow & s \prec_1 t \vee s \leadsto t & \{\text{lemma 2 }\} \\
\Rightarrow & (s, int, t) \vee (s, snd, t) \vee (\exists u :: (s, rcv(u), t)) & \\
 & \quad \vee (\exists u :: (u, rcv(s), t)) & \{\text{expand } s \prec t \text{ and } s \leadsto t\} \\
\Rightarrow & (s.v = t.v) \vee (s.v < t.v) \vee (s.v \leq t.v) \vee (s.v \leq t.v) & \\
 & & \{\text{Snd, Rcv, and Int rules}\} \\
\Rightarrow & s.v \leq t.v & \{\text{ simplify }\}
\end{array}
$$

Induction: $(k > 1)$

$$
\begin{array}{lll}
 & s \xrightarrow{k} t \wedge (k > 1) & \\
\Rightarrow & (\exists u :: s \xrightarrow{k-1} u \wedge u \xrightarrow{1} t) & \{\text{lemma 3}\} \\
\Rightarrow & (\exists u :: s.v \leq u.v \wedge u.v \leq t.v) & \{\text{induction hypothesis}\} \\
\Rightarrow & s.v \leq t.v & \{\text{simplify}\} \quad \blacksquare
\end{array}
$$

Use of induction on $\overset{k}{\not\to}$ [Base Case]

Contrapositive of 2:

$$\forall s, t : s.p \neq t.p : s \not\to t \;\Rightarrow\; \neg(s.v < t.v).$$

Lemma 8 $(\forall s, t : s.p \neq t.p : s \not\to t \;\Rightarrow\; t.v[s.p] < s.v[s.p])$

Proof Base $(k = 0)$:

$$
\begin{array}{lll}
 & s \overset{0}{\not\to} t \wedge s.p \neq t.p & \\
\Rightarrow & Init(t) \wedge s.p \neq t.p & \{\text{lemma 7}\} \\
\Rightarrow & Init(t) \wedge s.p \neq t.p \wedge & \{\text{let } u \text{ be initial state in } s.p\} \\
 & (\exists u : Init(u) \wedge u.p = s.p : u = s \vee u \to s) & \\
\Rightarrow & Init(t) \wedge s.p \neq t.p \wedge & \{\text{lemma 7}\} \\
 & (\exists u : Init(u) \wedge u.p = s.p : u.v = s.v \vee u.v \leq s.v) & \\
\Rightarrow & t.v[s.p] = 0 \wedge & \{\text{Init rule}\} \\
 & (\exists u : u.v[s.p] = 1 : u.v = s.v \vee u.v \leq s.v) & \\
\Rightarrow & t.v[s.p] < s.v[s.p] & \{\text{simplify}\}
\end{array}
$$

Proof [Induction Case]

Induction: $(k > 0)$

$$s \overset{k}{\not\rightarrow} t \wedge s.p \neq t.p \wedge k > 0$$

$\Rightarrow$ { let u satisfy $u \prec_1 t$, u exists since $\neg Init(t)$ }

$$s \overset{k}{\not\rightarrow} t \wedge s.p \neq t.p \wedge u.p = t.p \wedge u \prec_1 t$$

$\Rightarrow$ { lemma 6 }

$$s \overset{j}{\not\rightarrow} u \wedge 0 \leq j < k \wedge u.p \neq s.p \wedge u \prec_1 t$$

$\Rightarrow$ { inductive hypothesis }

$$u.v[s.p] < s.v[s.p] \wedge u \prec_1 t$$

$\Rightarrow$ { expand $u \prec_1 t$ }

$$u.v[s.p] < s.v[s.p]$$
$$\wedge ((u, int, t) \vee (u, snd, t) \vee (u, rcv(w), t))$$

Consider each disjunct separately.

Proof of Inductive Case [Contd.]

Case 1: (u, int, t)

$$u.v[s.p] < s.v[s.p] \wedge (u, int, t)$$
$$\Rightarrow \quad u.v[s.p] < s.v[s.p] \wedge t.v = u.v \quad \text{\{Int rule\}}$$
$$\Rightarrow \quad t.v[s.p] < s.v[s.p] \quad \text{\{simplify\}}$$

Case 2: (u, snd, t)

$$u.v[s.p] < s.v[s.p] \wedge (u, snd, t)$$
$$\Rightarrow \quad u.v[s.p] < s.v[s.p] \wedge t.v[s.p] = u.v[s.p] \quad \text{\{Snd rule, } s.p \neq t.$$
$$\Rightarrow \quad t.v[s.p] < s.v[s.p] \quad \text{\{simplif}$$

Case 3: $(u, rcv(w), t)$

$$u.v[s.p] < s.v[s.p] \wedge (u, rcv(w), t)$$
$$\Rightarrow \quad u.v[s.p] < s.v[s.p] \wedge (u, rcv(w), t) \wedge \quad \text{\{Rcv rule\}}$$
$$(t.v[s.p] = u.v[s.p] \vee t.v[s.p] = w.v[s.p])$$
$$\Rightarrow \quad (t.v[s.p] < s.v[s.p]) \vee \quad \text{\{simplify\}}$$
$$((u, rcv(w), t) \wedge t.v[s.p] = w.v[s.p])$$

It suffices to prove the two cases: $w.p = s.p$ and $w.p \neq s.p$.

Proof of Inductive Case [Contd.]

Case 3A: $w.p = s.p$

$$
\begin{array}{lll}
 & t.v[s.p] = w.v[s.p] \wedge (u, rcv(w), t) & \\
\Rightarrow & t.v[s.p] = w.v[s.p] \wedge (w, snd, x) & \left\{\begin{array}{l}\text{let } x \text{ satisfy } w \prec x, \\ x \text{ exists since } w \leadsto t \\ \text{implies } \neg Final(w)\end{array}\right\} \\
\Rightarrow & t.v[s.p] = w.v[s.p] \wedge (w, snd, x) & \{\text{otherwise } s \rightarrow t\} \\
 & \wedge\, w \rightarrow s & \\
\Rightarrow & t.v[s.p] = w.v[s.p] \wedge (w, snd, x) & \{\text{since } w \prec x\} \\
 & \wedge\, (x = s \vee x \rightarrow s) & \\
\Rightarrow & t.v[s.p] = w.v[s.p] \wedge w.v[s.p] < x.v[s.p] & \\
 & \wedge\, (x = s \vee x \rightarrow s) & \{\text{Snd rule}\} \\
\Rightarrow & t.v[s.p] = w.v[s.p] \wedge w.v[s.p] < x.v[s.p] & \\
 & \wedge\, (x.v \leq s.v) & \{\text{lemma 7}\} \\
\Rightarrow & t.v[s.p] < s.v[s.p] & \{\text{simplify}\}
\end{array}
$$

Proof of Inductive Case [Contd.]

Case 3B: $w.p \neq s.p$

$$
\begin{array}{ll}
 & t.v[s.p] = w.v[s.p] \wedge (u, rcv(w), t) \wedge w.p \neq s.p \\
\Rightarrow & \{ \text{ use } s \overset{k}{\not\rightarrow} t, \; k > 0, \text{ and lemma 6 } \} \\
 & t.v[s.p] = w.v[s.p] \wedge w.p \neq s.p \wedge s \overset{j}{\not\rightarrow} w \\
 & \wedge\ 0 \leq j < k \\
\Rightarrow & \{ \text{ inductive hypothesis } \} \\
 & t.v[s.p] = w.v[s.p] \wedge w.v[s.p] < s.v[s.p] \\
\Rightarrow & \{ \text{ simplify } \} \\
 & t.v[s.p] < s.v[s.p]
\end{array}
$$

■

Converse

Eqn 2 : $s.p \neq t.p \wedge s.v < t.v \quad \Rightarrow \quad s \rightarrow t$

Lemma 9 $(\forall s, t : s.p \neq t.p : s \rightarrow t \quad \Rightarrow \quad s.v < t.v)$

Proof $Base\ (k = 1)$:

$$
\begin{array}{ll}
 & s \xrightarrow{1} t \wedge s.p \neq t.p \\
\Rightarrow & s \leadsto t \wedge s.p \neq t.p \qquad \{\text{defn of } \xrightarrow{1} \text{ and lemma 2}\} \\
\Rightarrow & s.p \neq u.p \wedge (u, rcv(s), t) \qquad \{\text{let } u \text{ satisfy } u \prec t\} \\
\Rightarrow & \left\{ \begin{array}{l} \text{otherwise } t \rightarrow s \text{ (since there is only one} \\ \text{event between } u \text{ and } t) \end{array} \right\} \\
 & u \not\rightarrow s \wedge s.p \neq u.p \wedge (u, rcv(s), t) \\
\Rightarrow & s.v[u.p] < u.v[u.p] \qquad \{\text{lemma 8 and rcv rule}\} \\
 & \wedge\ (\forall i :: t.v[i] = \max(u.v[i], s.v[i])) \\
\Rightarrow & s.v < t.v
\end{array}
$$

Converse [Contd.]

$Induction\ (k > 0)$:

$$
\begin{array}{lll}
 & s \stackrel{k}{\rightarrow} t \wedge k > 0 \wedge s.p \neq t.p & \\
\Rightarrow & (\exists u :: s \stackrel{k-1}{\rightarrow} u \wedge u \stackrel{1}{\rightarrow} t \wedge s.p \neq t.p) & \{\text{lemma 3}\} \\
\Rightarrow & (\exists u :: s \stackrel{k-1}{\rightarrow} u \wedge u \stackrel{1}{\rightarrow} t \wedge & \{u.p \text{ can not have two values}\} \\
 & \quad (u.p \neq t.p \vee u.p \neq s.p)) & \\
\Rightarrow & (\exists u :: (s \stackrel{k-1}{\rightarrow} u \wedge u \stackrel{1}{\rightarrow} t \wedge u.p \neq t.p) \vee & \\
 & \quad (s \stackrel{k-1}{\rightarrow} u \wedge u \stackrel{1}{\rightarrow} t \wedge u.p \neq s.p)) & \\
\Rightarrow & (\exists u :: (s \stackrel{k-1}{\rightarrow} u \wedge u.v < t.v) \vee & \{\text{inductive hypothesis}\} \\
 & \quad (s.v < u.v \wedge u \stackrel{1}{\rightarrow} t)) & \\
\Rightarrow & (\exists u :: (s.v \leq u.v \wedge u.v < t.v) \vee & \{\text{lemma 7}\} \\
 & \quad (s.v < u.v \wedge u.v \leq t.v)) & \\
\Rightarrow & s.v < t.v &
\end{array}
$$

■

Theorem 1 $(\forall s, t : s.p \neq t.p : s \rightarrow t \quad \Leftrightarrow \quad s.v < t.v)$