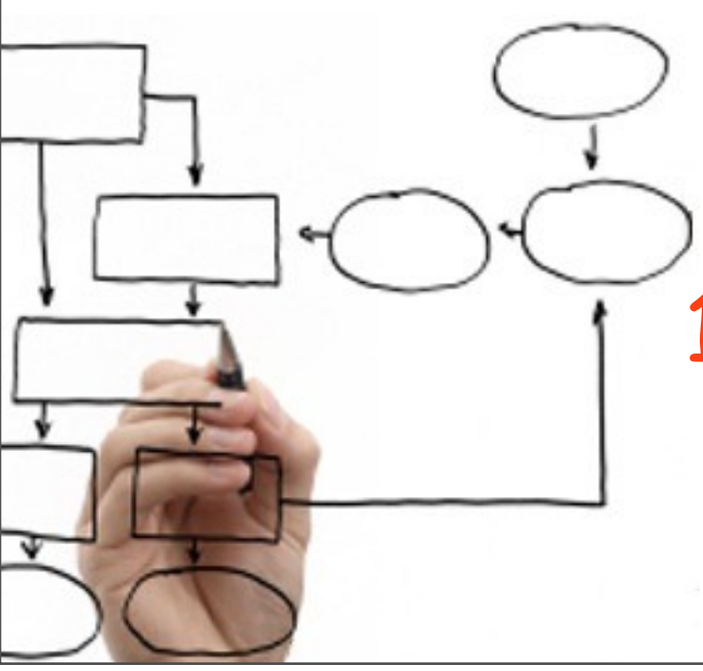
# Methods for the specification and verification of business processes

## MPB (6 cfu, 295AA)

Roberto Bruni
http://www.di.unipi.it/~bruni



## 11 - Net properties, formally

# Object

We give a formal account of some key properties of net systems

# Liveness, formally

$$(P, T, F, M_0)$$

$$\forall t \in T, \quad \forall M \in [\, M_0 \,\rangle, \quad \exists M' \in [\, M \,\rangle, \quad M' \xrightarrow{t}$$

# Liveness as invariant

**Lemma**
If $(P, T, F, M_0)$ is live and $M \in [\, M_0 \,\rangle$, then $(P, T, F, M)$ is live.

Let $t \in T$ and $M' \in [\, M \,\rangle$.

Since $M \in [\, M_0 \,\rangle$, then $M' \in [\, M_0 \,\rangle$.

Since $(P, T, F, M_0)$ is live, $\exists M'' \in [\, M' \,\rangle$ with $M'' \xrightarrow{t}$.

Therefore $(P, T, F, M)$ is live.

# Deadlock freedom, formally

$$(P, T, F, M_0)$$

$$\forall M \in [\, M_0 \,\rangle, \quad \exists t \in T, \quad M \xrightarrow{t}$$

# Deadlock freedom as invariant

**Lemma**: If $(P, T, F, M_0)$ is deadlock-free and $M \in [\, M_0 \,\rangle$, then $(P, T, F, M)$ is deadlock-free.

Let $M' \in [\, M \,\rangle$.

Since $M \in [\, M_0 \,\rangle$, then $M' \in [\, M_0 \,\rangle$.

Since $(P, T, F, M_0)$ is deadlock-free, $\exists t \in T$ with $M' \xrightarrow{t}$.

Therefore $(P, T, F, M)$ is deadlock-free.

# Boundedness, formally

$$(P, T, F, M_0)$$

$$\exists k \in \mathbb{N}, \quad \forall M \in [\, M_0 \,\rangle, \quad \forall p \in P, \quad M(p) \leq k$$

# Boundedness as invariant

**Lemma**
If $(P, T, F, M_0)$ is bounded and $M \in [\, M_0 \,\rangle$, then $(P, T, F, M)$ is bounded.

Since $(P, T, F, M_0)$ is bounded, it must be $k$-bounded for some $k \in \mathbb{N}$

Let $M' \in [\, M \,\rangle$.

Since $M \in [\, M_0 \,\rangle$, then $M' \in [\, M_0 \,\rangle$.

Since $(P, T, F, M_0)$ is $k$-bounded, $M'(p) \leq k$ for all $p \in P$.

Therefore $(P, T, F, M)$ is ($k$-)bounded.

# Boundedness lemma

**Lemma**
If $(P, T, F, M_0)$ is bounded and $M_1 \in [\, M_0 \,\rangle$ with $M_1 \geq M_0$, then $M_1 = M_0$.

Let $\sigma \in T^*$ such that $M_0 \xrightarrow{\sigma} M_1 \geq M_0$.

By the monotonicity lemma: $M_0 \xrightarrow{\sigma} M_1 \xrightarrow{\sigma} M_2 \xrightarrow{\sigma} \ldots$

Let $L = M_1 - M_0$. Clearly, $M_{i+1} = M_i + L$.
Therefore, $M_n = M_0 + nL$ for any $n \in \mathbb{N}$

Since the system is bounded, it must be $L = \mathbf{0}$ and $M_n = M_0$

# Exercise

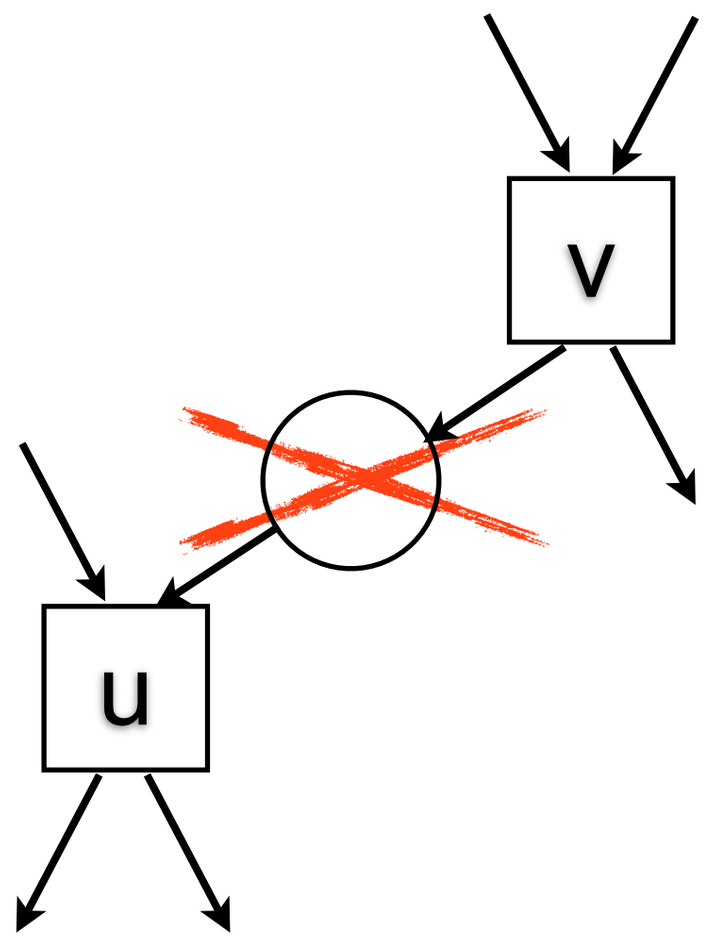
Prove that Cyclicity is an invariant

Or give a counter-example

# Exchange Lemmas (whose proofs are optional reading)

# Exchange lemma (1)

**Lemma**: Let $u, v \in T$ with $\bullet u \cap v \bullet = \emptyset$.
If $M \xrightarrow{vu} M'$, then $M \xrightarrow{uv} M'$



# Exchange lemma (1)

**Lemma**: Let $u, v \in T$ with $\bullet u \cap v\bullet = \emptyset$.
If $M \xrightarrow{vu} M'$, then $M \xrightarrow{uv} M'$

Let $M \xrightarrow{v} K \xrightarrow{u} M'$ and $K' = K - \bullet u$.
Clearly $M' = K' + u\bullet$.

Since $\bullet u \cap v\bullet = \emptyset$, then: $M'' \xrightarrow{v} K'$ with $M'' = M - \bullet u$

Therefore:
$M = M'' + \bullet u \xrightarrow{u} M'' + u\bullet \xrightarrow{v} K' + u\bullet = M'$

# Exchange lemma (2)

**Lemma**: Let $V \subset T$ and $u \in T \setminus V$, with $\bullet u \cap V \bullet = \emptyset$ .
If $M \xrightarrow{\sigma u} M'$ with $\sigma \in V^*$, then $M \xrightarrow{u\sigma} M'$

The proof is by induction on the length of $\sigma$

**base ($\sigma = \epsilon$):** trivially $M \xrightarrow{u} M'$

**induction ($\sigma = \sigma' v$ for some $\sigma' \in V^*$ and $v \in V$):**

Let $M \xrightarrow{\sigma'} M'' \xrightarrow{vu} M'$. Note that $\bullet u \cap v \bullet = \emptyset$

By exchange lemma 1: $M \xrightarrow{\sigma'} M'' \xrightarrow{uv} M'$.

Let $M \xrightarrow{\sigma' u} M''' \xrightarrow{v} M'$.

By inductive hypothesis: $M \xrightarrow{u\sigma'} M''' \xrightarrow{v} M'$

Thus, $M \xrightarrow{u\sigma} M'$

# Exchange lemma (3)

**Lemma**: Let $U, V \subset T$ and $U \cap V = \emptyset$, with $\bullet U \cap V \bullet = \emptyset$.
If $M \xrightarrow{\sigma} M'$ with $\sigma \in (U \cup V)^*$, then $M \xrightarrow{\sigma_{|U}\sigma_{|V}} M'$

The proof is by induction on the length of $\sigma_{|U}$

**base ($\sigma_{|U} = \epsilon$):** trivially $\sigma_{|V} = \sigma$

**induction ($\sigma_{|U} = u\sigma'$ for some $u \in U$ and $\sigma' \in U^*$):**

Let $M \xrightarrow{\sigma_0}\xrightarrow{u}\xrightarrow{\sigma_1} M'$, with $\sigma = \sigma_0 u \sigma_1$ and $\sigma_0 \in V^*$.

Note that $\sigma' = (\sigma_1)_{|U}$ and $\bullet u \cap V \bullet = \emptyset$

By exchange lemma 2: $M \xrightarrow{u}\xrightarrow{\sigma_0}\xrightarrow{\sigma_1} M'$.

Note that $(\sigma_0\sigma_1)_{|U} = (\sigma_1)_{|U} = \sigma'$ and $(\sigma_0\sigma_1)_{|V} = \sigma_{|V}$.

By inductive hypothesis: $M \xrightarrow{u}\xrightarrow{\sigma'}\xrightarrow{\sigma_{|V}} M'$

Since $\sigma_{|U} = u\sigma'$, we conclude that $M \xrightarrow{\sigma_{|U}}\xrightarrow{\sigma_{|V}} M'$

# Two theorems on strong connectedness whose proofs we omit

# Strong connectedness theorem

**Theorem**: If a weakly connected system is live and bounded then it is strongly connected

(the proof exploits many of the previous results, but it also requires a few technical lemmas that we prefer to omit)

# Strong connectedness via invariants

**Theorem**: If a weakly connected net has a positive S-invariant and a positive T-invariant then it is strongly connected

(the proof exploits requires a few technical lemmas that we prefer to omit)