CS 524
Lecture 23
J. Meseguer

1. More on Sequential Systems: Topmost Theories

Recall that a rewrite theory $\mathcal{R} = (\Sigma, \phi, E \cup B, R)$ specifies a sequential system iff it has: (i) no sideways parallelism, and (ii) no nested concurrency.

A very useful class of sequential rewrite theories is provided by so-called topmost rewrite theories where any one-step rewrite must happen at the top of the term, i.e., must be of the form:

$$[u] \xrightarrow{[l(v_1,..,v_n)]} [v]$$

with: $l: t \to t' \in R$, $t(v_1,..,v_n) \in [u]$, $t'(v_1,..,v_n) \in [v]$.

Definition Let $\mathcal{R} = (\Sigma, \phi, E \cup B, R)$ be a rewrite theory with $\Sigma = ((S, \leq), \Sigma)$ an order-sorted signature. Then $\mathcal{R}$ is called topmost iff there is a connected component of the graph/poset of sorts $[s] \in S/(\leq \cup \geq)^+$ such that:

① any $l : t \to t'$ in R has $l_s(t), l_s(t') \in [s]$

② For any term $u \in T_\Sigma(X)$, and nonempty position $p \in pos(u) \setminus \{\epsilon\}$, if $l_s(u|_p) \in [s]$, then p is a frozen position in u according to ϕ.

An easy sufficient condition for $\mathcal{R}$ to be topmost on kind $[s]$, which does not depend on ϕ, but only on Σ is:

- for any $f : s_1 \ldots s_n \to s'$ in Σ, $n \geq 1$, $s_1, \ldots, s_n \notin [s]$

Essentially this means that the kind $[s]$ acts as a "black hole": whenever you syntactically enter $[s]$, you can never leave $[s]$ by performing any operations in Σ.

The following lemma is left as an exercise:

Lemma If $\mathcal{R} = (\Sigma, \phi, E \cup B, R)$ is topmost, then $\mathcal{R}$ is sequential.

Topmost rewrite theories look very restrictive. However, it is very often quite easy to *transform* a rewrite theory $\mathcal{R}$ into a topmost one $\mathcal{R}^T$ such that $\mathcal{R}$ and $\mathcal{R}^T$ *have the same interleaving computations*. That is, in $\mathcal{R}^T$ we *lose all concurrency*, but for some reasoning purposes, e.g., LTL model checking, or reasoning about invariants, maybe the only things that matters is whether we can *reach* a given state. And from that point of view $\mathcal{R}$ and $\mathcal{R}^T$ becomes *reachability equivalent*.

Let us illustrate the $\mathcal{R} \mapsto \mathcal{R}^T$ transformation for the case of <u>concurrent object-oriented systems</u>, where, remember that all rules have the [very] general form:

$$(\star)\ l : \langle O_1 | ATTS_1 \rangle \cdots \langle O_n | ATTS_n \rangle\ m_1 \cdots m_n$$
$$\longrightarrow \langle O_{i_1} | ATTS'_{i_1} \rangle \cdots \langle O_{i_p} | ATTS'_{i_p} \rangle\ \langle Q_1 | ATTS''_1 \rangle \cdots \langle Q_k | ATTS''_k \rangle\ m'_1 \cdots m'_q$$

We can make such $\mathcal{R}$ concurrent by:

1. Adding a new sort <u>System</u> not belonging to any connected component of sorts, and
2. Adding an operator $\{-\} : \underline{Configuration} \to \underline{System}$
3. Transforming any rule of the form $(\star)$ into a rule:

$$(\ddagger)\ l : \{\langle O_1 | ATTS_1 \rangle \cdots \langle O_n | ATTS_n \rangle\ m_1 \cdots m_n\ C\}$$
$$\to \{\langle O_{i_1} | ATTS'_{i_1} \rangle \cdots \langle O_{i_r} | ATTS'_{i_r} \rangle \langle Q_1 | ATTS''_1 \rangle \cdots \langle Q_k | ATTS''_k \rangle\ m'_1 \cdots m'_q\ C\}$$

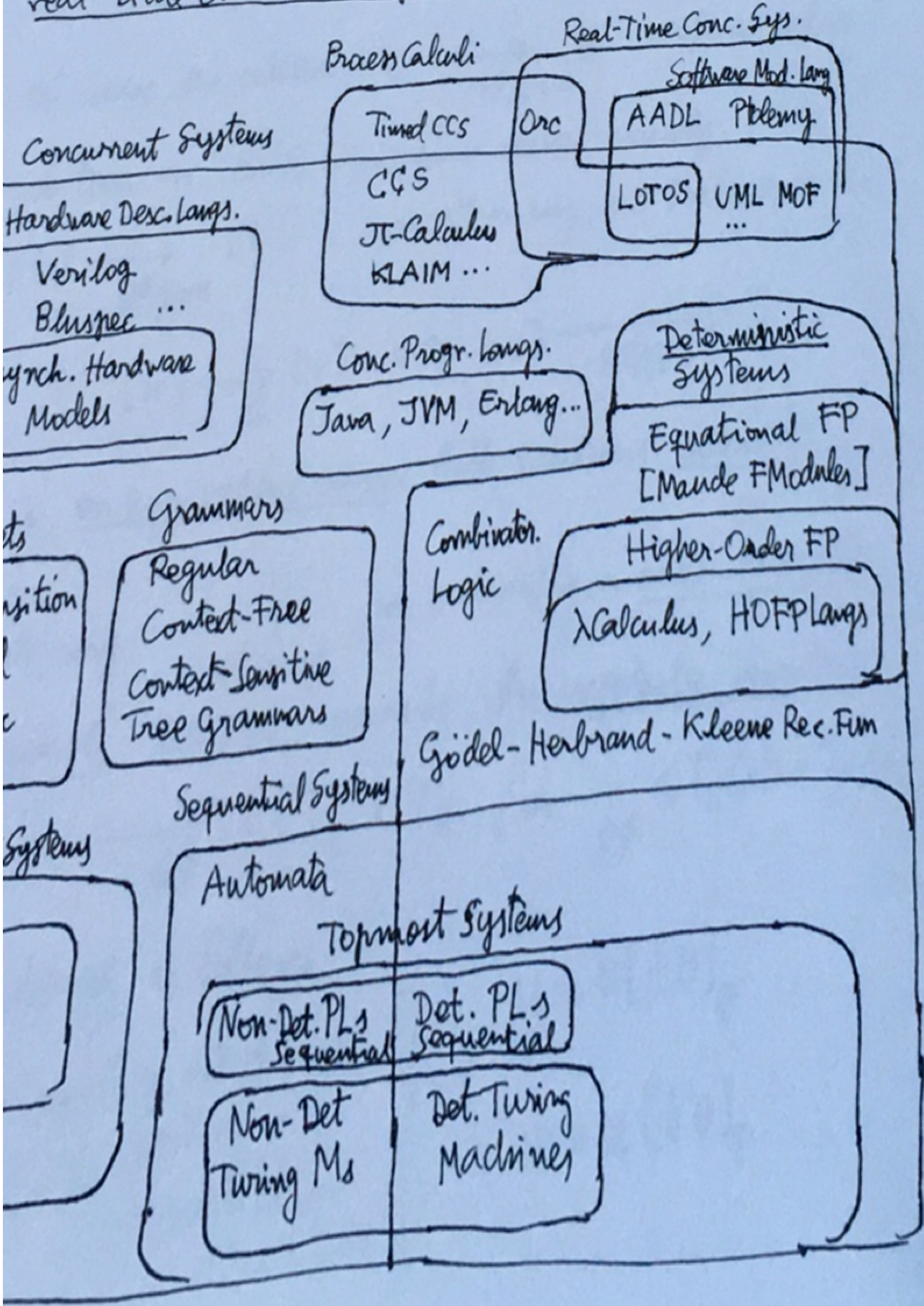
where C is a fresh new variable of sort <u>Configuration</u>.

<u>Lemma</u>. Prove that for $\mathcal{R}$ the rewrite theory of a concurrent object system, the above transformation $\mathcal{R} \mapsto \mathcal{R}^T$ is such that:

1. $\mathcal{R}^T$ is topmost
2. $\mathcal{R}$ and $\mathcal{R}^T$ enjoy the property that their interleaving computations are in a <u>bijective correspondence</u>.

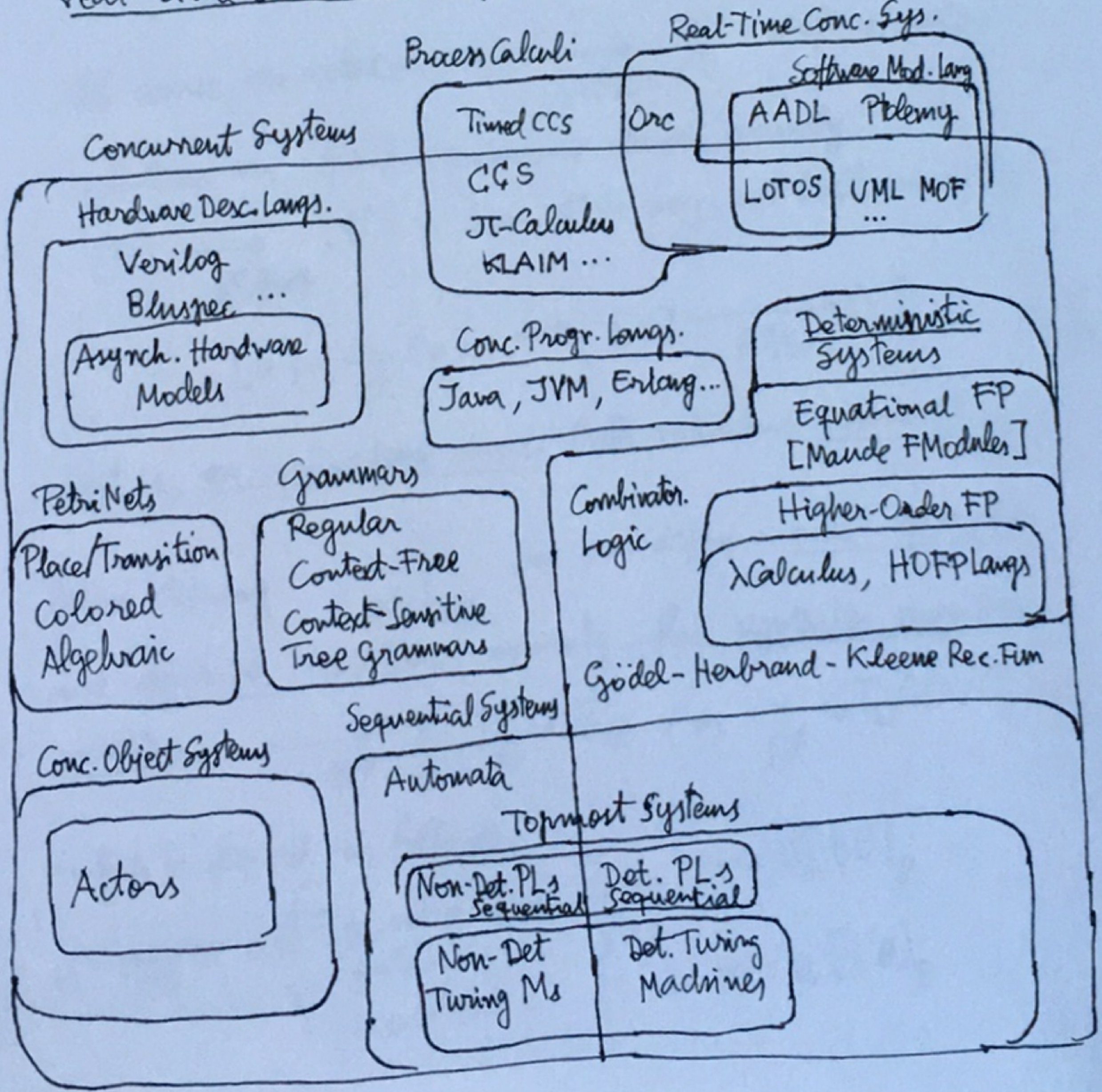
2. The Big Picture

At this point in the course we can take a bird's eye view of the entire field of concurrency. This view needs not be exhaustive, but can help us get the lay of the land; furthermore, we can take a peek at an area we did not have a chance to visit, yet quite important, namely, real-time concurrent systems. Here is the big picture:



2. The Big Picture

At this point in the course we can take a <u>bird's eye view</u> of the entire field of concurrency. This view needs not be exhaustive, but can help us get the lay of the land; furthermore, we can <u>take a peek</u> at an area we did not have a chance to visit, yet quite important, namely, <u>real-time concurrent systems</u>. Here is the big picture:



3. The $\rightarrow_{R}$ and $\xrightarrow[R/E\cup B]{\phi}$ Rewrite Relations

Thanks to lecture 22's <u>Sequentialization Lemma</u>, we know that any concurrent computation $[u] \xrightarrow{[\alpha]} [v]$ in a rewrite theory $\mathcal{R}$ has [possibly many] equivalent interleaving descriptions so that $[\alpha] = [\beta_1; \cdots; \beta_n]$, with the β_i <u>one-step rewrites</u>.

Let us adopt the <u>notational convention</u>:

$$[u] \xrightarrow[\mathcal{R}]{} [v] \quad \text{iff} \quad [u] \xrightarrow{[t[\ell(v_1,..,v_n)]_p]} [v] \quad \text{for some}$$

$\ell : w(x_1,..,x_n) \rightarrow w'(x_1,..,x_n)$ in R, so that $t[w(v_1,..,v_n)]_p \in [u]$ and $t[w'(v_1,..,v_n)] \in [v]$. That is, iff $[u] \xrightarrow[\mathcal{R}]{} [v]$ describes the existence of a one-step rewrite in $\mathcal{R}$.

Of course, the <u>states</u> of the system described by $\mathcal{R}$ are $E\cup B$-<u>equivalence classes</u> $[u]_{E\cup B}$. But this is a quite <u>abstract</u> description, since: (1) such classes are in general infinite, and (2) the equivalence relation $=_{E\cup B}$ [provable $E\cup B$-equality] defining such classes is in general <u>undecidable</u>.

Therefore, it is useful to define a relation $\xrightarrow[R/E\cup B]{\phi}$ at the level of <u>terms</u>, that is, a binary relation

$\xrightarrow[R^\phi/E\cup B]{} \subseteq T_\Sigma \times T_\Sigma$ or, more generally,

$\xrightarrow[R^\phi/E\cup B]{} \subseteq T_\Sigma(X) \times T_\Sigma(X)$ such that given

$\mathcal{R} = (\Sigma, \phi, E\cup B, R)$ we have:

$[u] \xrightarrow[\mathcal{R}]{} [v]$ iff $\exists v' \in [v]$ s.t. $u \xrightarrow[R^\phi/E\cup B]{} v' \wedge v' \in [v]$

Of course, the relation $t \xrightarrow[R^\phi/E\cup B]{} t'$ defines also a relation on $E\cup B$-equivalence classes, namely: $[t] \xrightarrow[R^\phi/E\cup B]{} [t']$. Seen this way, all boils down to:

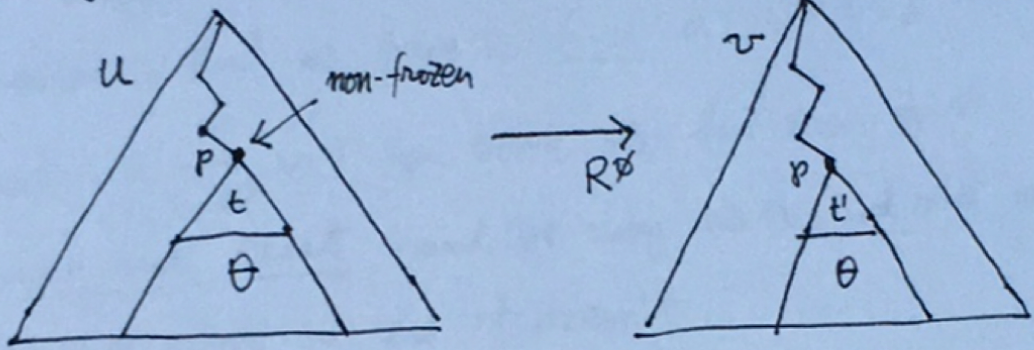
$$[u] \xrightarrow[\mathcal{R}]{} [v] \iff [u] \xrightarrow[R^\phi/E\cup B]{} [v]$$

That is, <u>on equivalence classes</u> both relations <u>coincide</u>.

Before defining $\xrightarrow[R^\phi/E\cup B]{}$ we can define a <u>much simpler</u> and <u>decidable</u> relation, namely, the <u>syntactic rewriting relation</u> $\xrightarrow[R^\phi]{} \subseteq T_\Sigma \times T_\Sigma$ (or $\xrightarrow[R^\phi]{} \subseteq T_\Sigma(X) \times T_\Sigma(X)$), which is defined as follows:

$$u \xrightarrow[R^\phi]{} v \iff \left\{ \begin{array}{l} \exists\, p, \text{ not } \phi\text{-frozen position in } u \\ \exists\, \theta \text{ substitution} \\ \exists\, l : t \to t' \text{ in } R \end{array} \right\} \text{ s.t. } \begin{array}{l} u = u[t\theta]_p \\ v = u[t'\theta]_p \end{array}$$

Pictorially:



We can now easily define $\xrightarrow[R\emptyset/E\cup B]{}$ as a composition of relations:

$$\xrightarrow[R\emptyset/E\cup B]{} \;=_{def}\; (=_{E\cup B});\ \xrightarrow[R\emptyset]{}$$

In other words: $u \xrightarrow[R\emptyset/E\cup B]{} v \Leftrightarrow \exists u' \in [u] \text{ s.t. } u' \xrightarrow[R\emptyset]{} v$

Prove as an exercise:

Lemma. For any rewrite theory $\mathcal{R} = (\Sigma, \phi, E\cup B, R)$ we have the equivalence:

$$\boxed{[u] \xrightarrow[\mathcal{R}]{} [v] \iff [u] \xrightarrow[R\emptyset/E\cup B]{} [v]}$$

3. A Serious Executability Problem

In general the relation $=_{E\cup B}$ is undecidable, i.e., semi-decidable. This actually means that given a term $u \in T_\Sigma$ we may not able to decide whether a one-step rewrite

$u \xrightarrow[R^{\emptyset}/E \cup B]{} v$ is even possible for some v. The problem is that we have to find a $u' \in [u]$ such that $u' \xrightarrow[R^{\emptyset}]{} v$ for some v; but such a u' may not exist, and we may never find out whether it does exist in case it doesn't.

A much better situation arises for axioms B such as any combination of associativity and/or commutativity and/or identity axioms for which the problem:

$$\boxed{\left.\begin{array}{l} \exists u' \in [u] \\ \exists v. \end{array}\right\} \text{ s.t. } u' \xrightarrow[R^{\emptyset}]{} v} \quad \text{is } \underline{\text{decidable}}.$$

Since, in particular, such decidability property exists for B any combination of assoc, comm and id: attributes, our next order of business will be to reduce the problem $u \xrightarrow[R^{\emptyset}/E \cup B]{} v$ to the much simpler problem $u \xrightarrow[R^{\emptyset}/B]{} v'$ under suitable conditions such that $[v]_{E \cup B} = [v']_{E \cup B}$