Chapter II : WSTS

In the following weeks, we will discuss Well Structured Transition Systems (WSTS).

WSTS capture the following three patterns present in concurrent systems.

1. There is a notion of "more" for the configurations of a system, and "larger" configurations can make more things happen

   e.g. more threads
   more messages
   more acquired locks
   more tokens
   $\Longrightarrow$ more things happen

2. The bad behaviour that we wont to show our program avoids is preserved under "moreness"

   e.g. two threads in the critical section is bad, more threads is also bad.

3. Even if there are infinitely many configurations, eventually the "moreness" wins out.

   e.g. any sequence of infinitely many natural numbers have an unboundedly not decreasing subsequence.

   6 5 3 2 1 0 9 1 10 3 12 ...

Using these properties, we can reason about infinite state systems in finite time.
We build up to the WSTS definition by modelling these properties.
We first need to do some order theory.

Order Theory I : Definitions

We deal with ordered sets $(Q, \leq)$ of states ("$\leq$" captures the idea of moreness).
We recall some basic definitions.
We say that a relation $\preccurlyeq \subseteq Q \times Q$ on Q is

- reflexive iff $\forall q \in Q.\ q \preccurlyeq q$.
- transitive iff $\forall q,p,r \in Q.\ (q \preccurlyeq p \wedge p \preccurlyeq r) \Rightarrow (q \preccurlyeq r)$.
- symmetric iff $\forall p,q.\ q \preccurlyeq p \Leftrightarrow p \preccurlyeq q$.
- anti-symmetric iff $\forall p,q.\ (q \preccurlyeq p \wedge p \preccurlyeq q) \Rightarrow (p = q)$.
- total iff $\forall p,q.\ (p \Rightarrow q) \Rightarrow \neg(p \preccurlyeq q \Leftrightarrow q \preccurlyeq p)$ ← exactly one must be true.

We say that $\preccurlyeq \subseteq Q \times Q$ is a quasi order (qo), if it is reflexive and transitive.
is a partial order (po), if it is reflexive, transitive, and anti-symmetric.
is a total order, if it is reflexive, transitive, anti-symmetric, and total.

Examples

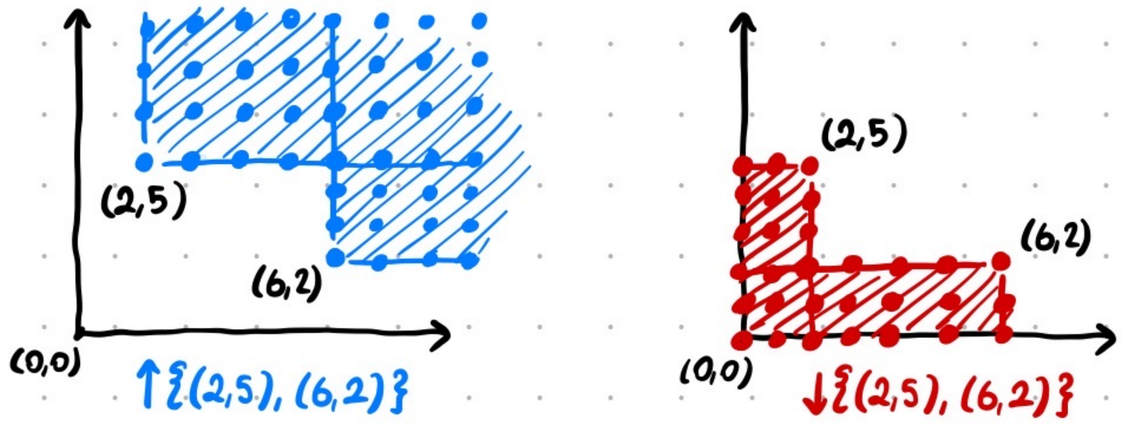
- total order : $(\mathbb{N}, \leq)$ with the usual order
- partial order : $(\mathbb{N}^2, \leq)$ with the component order (eg. $(0,1) \leq (2,3)$ but $(0,9) \not\leq (1,2)$)
- quasi order : $(\mathbb{N}^3, \leq')$ where the first component is ignored (e.g. $(9,0,1) \leq (0,2,3)$ but $(0,0,9) \not\leq (1,1,2)$)

Let $(Q, \leq)$ be a quasi order. We call $S \subseteq Q$

- upward closed iff for all $q \in S$ and $p \geq q$, $p \in S$ as well.
- downward closed iff for all $q \in S$ and $p \leq q$, $p \in S$ as well.

We write $\uparrow S = \{p \in Q \mid q \in S, q \leq p\}$ to denote the upward closure of $S \subseteq Q$ and
$\downarrow S = \{p \in Q \mid q \in S, q \geq p\}$ to denote the downward closure of $S \subseteq Q$.

Example: $(\mathbb{N}^2, \leq)$



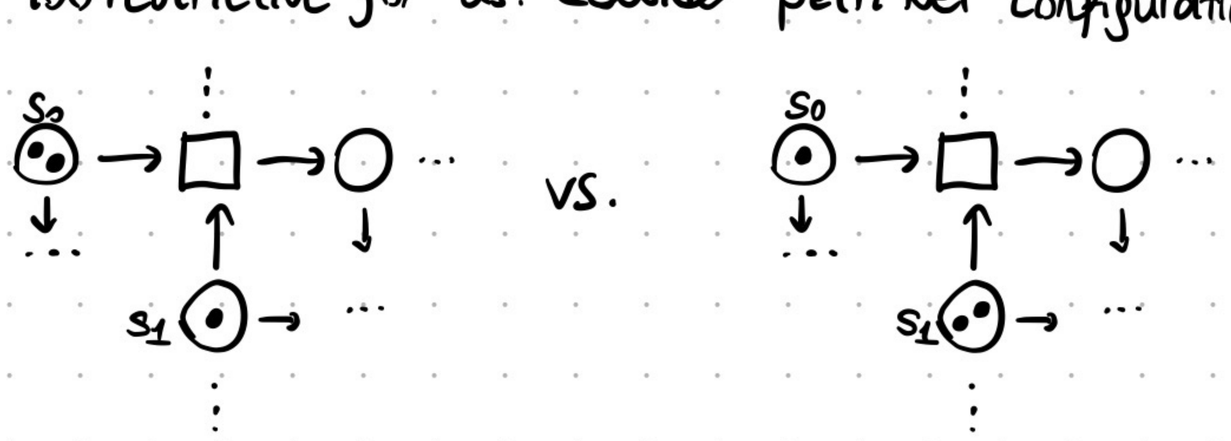
In mathematics, a very useful definition is that of a well-order.
This definition is too strict for us, but it is a good starting point, and generally cool.
A well-order $(Q, \leq)$ is a total order, such that any set $S \subseteq Q$ has a minimum element $u \in S$.
That is, for all $S \subseteq Q$, there is an $s_0 \in S$ with $\uparrow\{s_0\} = \uparrow S$.

Examples:

$(\{\bot, \top\}, \leq)$ with $\bot \leq \top$
$(\mathbb{N}, \leq)$ with the usual order
$(\mathbb{N} \cup \{\omega\}, \leq)$ with the usual order ($i \leq \omega$ for all $i \in \mathbb{N}$)

Nerd Fact: For each well order, there is an ordinal isomorphic to it and vice versa.

This is too restrictive for us. Consider petri net configurations.



The configurations above are intuitively incomparable, tokens in s_0 can enable some transitions that s_1 cannot and vice versa.

So, we need a definition that can deal with non-total orders.
The well quasi order definition does exactly this.
We call a quasi-order $(Q, \leq)$ a well quasi order (wqo), if any infinite sequence $q_0, q_1, q_2, \ldots \in Q$ has two indices $i < j$ such that $q_i \leq q_j$.

This is a very broad definition. We will discuss which orders are wqo's later.
For the moment consider the examples

$(\mathbb{N}, \leq)$: easy to see, starting from $q_0 \in \mathbb{N}$, we can only have q_0 many elements that do not dominate q_0.

$(\{a_0, \ldots, a_k\}, =)$: A finite set of incomparable elements. Clearly, after $k+1$ elements in the sequence, an element repeats.

We will study the properties of wqo's the next lecture.
Now, we use orders to model systems.

Upward Compatible Transition System (UTS) and Well-Structured Transition Systems.

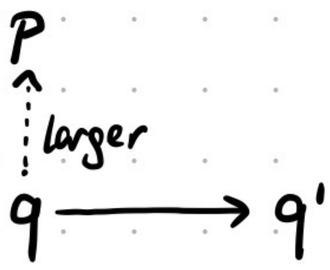
The upward compatible transition systems (UTS) capture the "moreness" phenomenon in concurrent systems.

Formally, an UTS is a labeled transition system $\mathcal{U}=(Q,\leq,I,\to)$ with

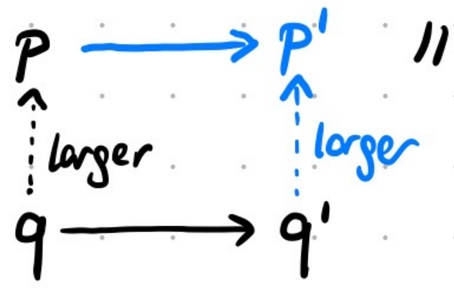
- an ordered set of states $(Q,\leq)$ (possibly infinite)
- a set of initial states $I\subseteq Q$
- a transition relation $\to\subseteq Q\times Q$ monotonous wrt. $\leq$.

The relation $\to\subseteq Q\times Q$ is monotonous wrt. $\leq\subseteq Q\times Q$ if
for all $q\to q'$ and $p\geq q$, there is a $p'\in Q$ with $p\to p'$ and $p'\geq p$.

As a picture: " for all



, there is



"

A run ρ in a UTS $\mathcal{U}=(Q,\leq,I,\to)$ is a finite sequence $\rho=q_0,q_1,\dots,q_k\in Q^*$ connected by "$\to$", i.e. for all $i<k$, $q_i\to q_{i+1}$.

A well-structured transition system (WSTS) is an UTS $W=(Q,\leq,I,\to)$ where $(Q,\leq)$ is a wqo.

We study the following questions for WSTS.

Upward Closed Reachability (Coverability)

Given: WSTS $W=(Q,\leq,I,\to)$ and upword closed $F\subseteq Q$
Decide: Is there a run $q_0,q_1,\dots,q_k$ with $q_0\in I$ and $q_k\in F$?

(Precise) Reachability

Given: WSTS $W=(Q,\leq,I,\to)$ and $p\in Q$
Decide: Is there a run $q_0,q_1,\dots,q_k$ with $q_0\in I$ and $q_k=p$?

We observe that precise reachability is undecidable in general, but upword-closed reachability is decidable (under very mild assumptions).

Next lecture

Before we can learn about the solutions to these problems, we need to understand wqo's really well.
We will also learn about some useful kinds of WSTS.