# Overview

Goal: verification of concurrent systems

Approach – introduce Petri nets and WSTS to model concurrent systems
– study fundamental verification problems for Petri nets / WSTS (e.g. reachability, coverability)

## 1. Petri Nets

A <u>Petri net</u> is a triple $(S, T, W)$ with

- finite set of <u>places</u> $S$
- finite set of <u>transitions</u> $T$
- <u>weight function</u> $W : (S \times T) \cup (T \times S) \to \mathbb{N}$

A <u>marking</u> $M \in \mathbb{N}^S$ assigns <u>tokens</u> to places

A transition <u>$t$ is enabled in $M$</u>, $M\,|t\rangle$, if

$$M \geq W(-, t)$$

This induces the <u>firing relation</u> $|\cdot\rangle \subseteq \mathbb{N}^S \times T \times \mathbb{N}^S$ with

$$M_1\,|t\rangle\,M_2 \quad \text{if} \quad M_1\,|t\rangle \quad (t \text{ is enabled in } M_1)$$
$$\text{and} \quad M_2 = M_1 - W(-, t) + W(t, -)$$

We extend the firing relation to sequences of transitions $t_1 \dots t_k \in T^*$

$$|t_1 \dots t_k\rangle = |t_1\rangle \circ \dots \circ |t_k\rangle$$

($\circ$: relational composition)

A marking <u>$M_2$ is reachable from $M_1$</u> if there is a transition sequence $\sigma \in T^*$ s.t. that

$$M_1\,|\sigma\rangle\,M_2$$

<u>Reachability</u>: The reachability problem will be our main verification problem of interest.

> <u>REACH</u> Given: Petri net $(S, T, W)$ and two markings $M_1, M_2 \in \mathbb{N}^S$
> Question: Is there $\sigma \in T^*$ with $M_1\,|\sigma\rangle\,M_2$?

- one of the biggest problems in theoretical computer science
- has been open for 50 years and solved these days
- reachability is $\mathbb{F}_\omega$-complete
  - ↳ Upper bound: Leroux & Schmitz [LICS '19] (following known results)
  - ↳ Lower bound: Leroux [FOCS '21] and Czerwinski & Orlikowski [FOCS '21]

↳ $F_\omega$ is a complexity class with Ackermannian growth defined by Schmitz [13]

What is Ackermann?

$f_0(n) = n+1$ — Addition

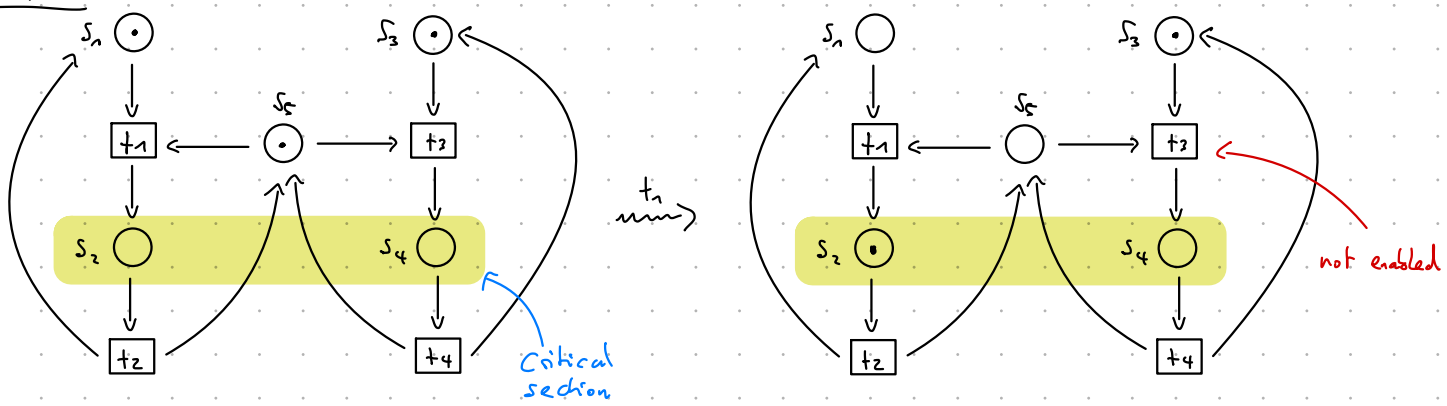
$f_1(n) = f_0^n(n) = \underbrace{n+1+\dots+1}_{n \text{ times}} = 2n$ — Multiplication

$f_2(n) = f_1^n(n) = \underbrace{n \cdot \underbrace{2 \cdot \dots \cdot 2}_{n \text{ times}}}_{?} \approx 2^n$ — Exponentiation

$f_3(n) = f_2^n(n) \approx 2^{\cdot^{\cdot^{\cdot^{2}}}}\}n$ times — Tower

→ Ackerman of $n$ is $f_n(n)$ — Diagonalization

Example:




Formally: $\begin{pmatrix}1\\0\\1\\0\\1\end{pmatrix} |t_1\rangle \begin{pmatrix}0\\1\\1\\0\\0\end{pmatrix}$ $t_3$ not enabled: $\begin{pmatrix}0\\0\\1\\0\\1\end{pmatrix} \not| \begin{pmatrix}0\\1\\1\\0\\0\end{pmatrix}$

The Petri net represents a simple concurrent system with
- two threads
- one lock (token in $s_5$)
- initially both threads are enabled (tokens in $s_1$ and $s_3$) and the lock is not held
- the places $s_2$ and $s_4$ are critical sections

→ Does mutual exclusion hold?
Formally, is a marking $M$ reachable with $M(s_2) > 0$ and $M(s_4) > 0$ ?

Coverability This question corresponds to another verification problem known as the Coverability problem.

> COVER Given: Petri net $(S, T, W)$ and two markings $M_1, M_2 \in \mathbb{N}^S$
> Question: Is there $\sigma \in T^*$ with $M_1 |\sigma\rangle M_3$ and $M_3 \geq M_2$ ?

- Coverability overapproximates reachability: every marking $M_2$ that is reachable from $M_1$ is also coverable from $M_1$.

- coverability is used as a subprocedure to decide reachability.
- coverability is EXPSPACE-complete
  - ↳ lower bound: Lipton ['76]
  - ↳ upper bound: Rackoff ['78]

## 2. WSTS

- There are other concurrent models like lossy channel systems (which are used to model network protocols)
- well-structured transition systems (WSTS) generalize Petri nets and lossy channel systems
- some techniques for Petri nets can be extended to WSTS

**Idea:** WSTS are (possibly infinite state) transition systems where
- states are ordered (by a well-quasi-order)
- larger states simulate smaller states as follows:
  For a transition $s_1 \xrightarrow{t} s_2$ and a larger state $s_3 \geq s_1$ there is a state $s_4$ so that $s_3 \xrightarrow{t} s_4$ and $s_4 \geq s_2$.

$$\begin{array}{ccc} s_1 & \xrightarrow{t} & s_2 \\ \rotatebox{90}{$\geq$} & & \rotatebox{90}{$\geq$} \\ s_3 & \xrightarrow{t} & s_4 \end{array} \quad \leftarrow \text{order on states}$$

- Reachability for WSTS is undecidable in general
- Coverability is decidable [Abdulla '96]

**Example: Petri nets** Markings are ordered by componentwise comparison

↳ $M_1 \,|t\rangle\, M_2$ implies $M_1 + M \,|t\rangle\, M_2 + M$ for $M_1, M_2, M \in \mathbb{N}^S$

By induction on the length of $\sigma^* \in T$ we also get:

**Lemma (Monotonicity of firing)**

$M_1 \,|\sigma\rangle\, M_2$ implies $M_1 + M \,|\sigma\rangle\, M_2 + M$