Coverability is in EXPSPACE [Rackoff '78]

Recall: A marking M_1 covers M_2 if $M_1 \geq M_2$

A marking M_2 is coverable from M_1 if there is $\sigma \in T^*$ so that $M_1 [\sigma\rangle M$ and $M \geq M_2$

Coverability problem

Given: Petri net $N = (S, T, W)$ and markings $M_S, M_f \in \mathbb{N}^S$

Question: Is M_f coverable from M_S?

The key insight is the following:

Short Sequence Property If M_f is coverable from M_S, then there is a short sequence σ so that $M_S [\sigma\rangle M \geq M_f$.

What is short?

$|\sigma| \leq 2^{2^n}$ with $n = \text{size}(N, M_S, M_f)$

With this insight there is a simple non-deterministic algorithm:

1. Guess a short sequence σ with $|\sigma| \leq 2^{2^n}$
2. Return YES if the $M_S [\sigma\rangle M \geq M_f$
3. Return NO otherwise

Why does this procedure only need exponential space?

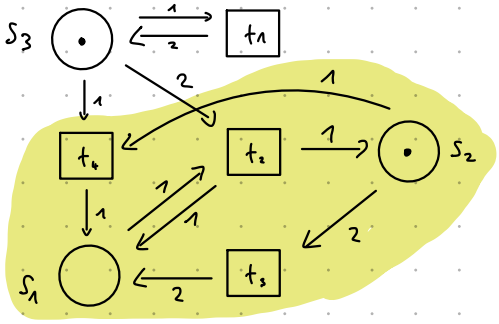
↳ We store only the latest marking and do not guess the full sequence at once. Formally we store

- the length of the already guessed sequence in binary. This needs $\log 2^{2^n} = 2^n$ bits
- the latest marking M
  a place can have more than $2^{2^n} \cdot 2^n$ tokens (# transitions · max. change)
  binary representation needs $\log 2^{2^n} \cdot 2^n = \log 2^{2^n} + \log 2^n = 2^n + n$ bits

Then Savitch theorem (NEXPSPACE = EXPSPACE) yields a deterministic algorithm in EXPSPACE.

Challenge: Establish the short sequence property.

Rackoff's idea illustrated on an example:



Is $\begin{pmatrix}2\\0\\0\end{pmatrix}$ coverable from $\begin{pmatrix}0\\1\\1\end{pmatrix}$?

→ yes:

$$\begin{pmatrix}0\\1\\1\end{pmatrix} |t_1 t_2 t_1 t_4\rangle \begin{pmatrix}0\\1\\5\end{pmatrix} |t_4\rangle \begin{pmatrix}1\\0\\4\end{pmatrix} |t_2 t_2\rangle \begin{pmatrix}1\\2\\0\end{pmatrix} |t_3\rangle \begin{pmatrix}3\\0\\0\end{pmatrix} \geq \begin{pmatrix}2\\0\\0\end{pmatrix}$$

- Assume we already have a bound for short sequences in Petri nets with 2 places (like the yellow one)
- Then we can bound short sequences in Petri nets with 3 places by bounding the number of tokens in each place by:

$$\leq \underbrace{\text{Max subtracted tokens in any transition}}_{2} \cdot \underbrace{\text{bound on short seq. with 2 places}}_{4} + \underbrace{\text{Max tokens in } M_f}_{2}$$

In the example: $2 \cdot 4 + 2 = 10$

$$\begin{pmatrix}0\\1\\\_\end{pmatrix} |t_4\rangle \begin{pmatrix}1\\0\\\_\end{pmatrix} |t_2 t_2\rangle \begin{pmatrix}1\\2\\\_\end{pmatrix} |t_3\rangle \begin{pmatrix}3\\0\\\_\end{pmatrix} \geq \begin{pmatrix}2\\0\\\_\end{pmatrix}$$

- So if place s_1 has 10 or more tokens we can ignore s_1 in the search for a short covering sequence.

Formally: Show short seq. property by induction on number of places

For induction hypothesis we use a slightly stronger statement.

Let

$$\text{ball}(M_f) = \{ M \in \mathbb{N}^S \mid \exists \sigma \in T^* \; M \,|\sigma\rangle\, M' \geq M_f \}$$

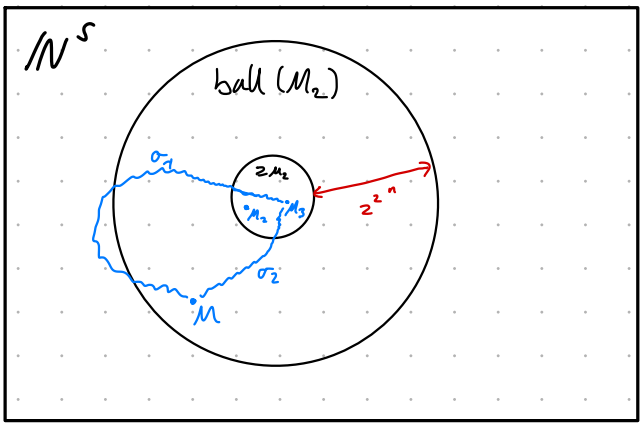
be all markings from which M_f is coverable.

We show:

Lemma For all $M \in \text{ball}(M_f)$ there is a short sequence σ so that $M \,|\sigma\rangle\, M' \geq M_f$

Why is this stronger? – the statement considers all markings from which M_f is coverable not only for M_s!

Illustration:



inner circle: markings that covers M_f

. outer circle: markings from ball (M_f)

Definition (i-marking, i-covering)

Let (S, T, W) Petri net with $S = \{s_1, \dots s_k\}$.

A generalized marking $M \in \mathbb{Z}^S$ allows also negative number of tokens.

It is called an i-marking if $M(s_j) \in \mathbb{N}$ for $1 \le j \le i$

$$M = \begin{pmatrix} s_1 \\ \vdots \\ s_i \\ \vdots \\ s_k \end{pmatrix} \begin{matrix} \} \mathbb{N} \\ \\ \} \mathbb{Z} \end{matrix}$$

An transition t is i-enabled in M if $M(s_j) \ge W(-, t)$ for $1 \le j \le i$

A marking M_1 is i-covering if $M(s_i) \ge M_2(s_j)$ for $1 \le j \le i$

An sequence $t_1 \dots t_k \in T^*$ is i-covering from M_1 if

$$M_1 \,|t_1\rangle\, M_2 \,|t_2\rangle \dots \dots |t_k\rangle\, M_m$$

and all M_i are i-marking and M_m is i-covering.

Note: M_1 covers M_2 iff M_1 k-covers M_2

Example (continued): The sequence $t_4 t_2 t_2 t_3$ is i-covering from $\begin{pmatrix} 0 \\ \underline{1} \end{pmatrix}$ for any value of s_3:

$$\begin{pmatrix} 0 \\ \underline{1} \end{pmatrix} |t_4\rangle \begin{pmatrix} 1 \\ \underline{0} \end{pmatrix} |t_2 t_2\rangle \begin{pmatrix} 1 \\ \underline{2} \end{pmatrix} |t_3\rangle \begin{pmatrix} 3 \\ \underline{0} \end{pmatrix} \ge \begin{pmatrix} 2 \\ \underline{0} \end{pmatrix}$$

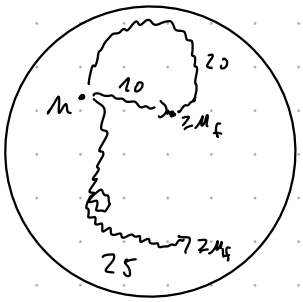
Shortest i-covering sequences

For $M \in \text{ball}(M_f)$ we define

$$\text{minSeq}(i, M) = \min \{ |\sigma| + 1 \mid \sigma \in T^* \text{ and } \sigma \text{ is } i\text{-covering from } M \}$$

(count # markings)

Illustration:

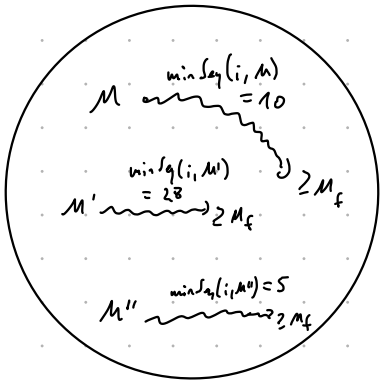


$\text{minSeq}(i, M) = 10$

We now consider the length needed to cover M_f from any marking in $\text{ball}(M_f)$

$$f(i) = \max \{ \text{minSeq}(i, M) \mid M \in \text{ball}(M_f) \}$$

Illustration:



$f(i) = 28$

Goal: Determine bound on $f(k)$

If M_f is coverable from M_s, we then have

$$f(k) \geq \text{minSeq}(k, M_s)$$

Thus, $f(k)$ is an upper bound on the length of the shortest sequence from M_s that covers M_f.

Lemma $f(0) = 1$ ← no places need to be covered

$$f(i+1) \leq \left(2^n \, f(i)\right)^{i+1} + f(i) \quad \text{for } 0 \leq i \leq k$$

Proof: Let $M_1 \in \mathbb{N}^S$ with i-covering sequence $\sigma = t_1 \dots t_m$ from M_1:

$$M_1 \,|t_1\rangle\, M_2 \,|t_2\rangle \dots |t_m\rangle\, M_m \geq M_f$$

Easy Case: markings $M_1, \dots, M_m$ have less than $2^n f(i)$ tokens in places $s_1, \dots, s_{i+1}$.

→ Then there are

$$\underbrace{\left(2^n \, f(i)\right)}_{\text{\# token values } \{0, \dots, 2^n f(i) - 1\}}^{i+1} \quad \text{↑ \# places}$$

distinct markings in $M_1, \dots M_m$ (if we only consider places $s_1, \dots, s_{i+1}$)

→ Since there is a sequence that does not repeat markings (wrt. to $s_1 \dots s_{i+1}$) we can assume

$$|\sigma| \leq \left(2^n \, f(i)\right)^{i+1} \leq \left(2^n \, f(i)\right)^{i+1} + f(i)$$

Hard Case: markings $M_1, \dots M_m$ $2^n f(i)$ tokens in some place $s_1, \dots, s_{i+1}$.

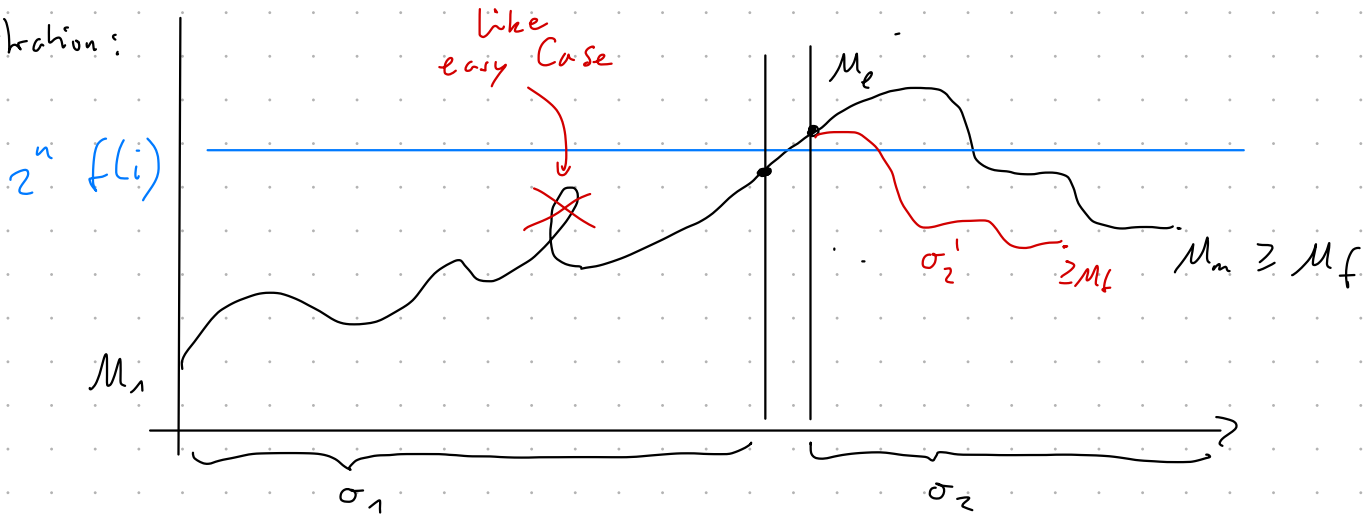
Consider first marking M_ℓ that has a place with at least $2^n f(i)$ tokens. Wlog. let

$$M_\ell(s_{i+1}) \geq 2^n f(i)$$ (Otherwise we could rename places)

Then $\sigma = \sigma_1 . \sigma_2$ with

- markings in σ_1 have less than $2^n f(i)$ tokens
- σ_2 starts with M_ℓ

Illustration:



σ_1: Like in the easy case we argue that

$$|\sigma_1| \leq (2^n f(i))^{i+1}$$

σ_2: Since σ_2 is $i+1$-covering from M_ℓ it is also i-covering from M_ℓ

By induction hypothesis there is σ_2' with

- σ_2' is i-covering from M_ℓ
- $|\sigma_2'| + 1 \leq f(i)$

Claim: $\sigma_1 . \sigma_2'$ is $i+1$-covering from M_1.

Then the Lemma follows by:

$$|\sigma_1 . \sigma_2'| \leq (2^n f(i))^{i+1} + f(i)$$

We show the claim:

- a transition subtracts at most 2^n tokens (weights are encoded in binary)
- Then σ_2' can subtract at most

$$2^n (f(i) - 1)$$

from place s_{i+1}

- Since $M_\ell(s_{i+1}) \geq 2^n f(i)$, this leaves us with

$$\geq 2^n f(i) - 2^n (f(i) - 1) = 2^n$$

tokens

- Since $\text{size}(M_2) \leq n$ we get $2^n \geq M_f(s_{i+1})$

$\Rightarrow$ σ_2' is $i+1$ covering from M_ℓ

Goal: Obtain upper bound on $f(k)$ that does not need recursion

Approach:
1. Give simple recursive bound $g(k)$
2. Give non-recursive form for $g(k)$

Lemma Let
$$g(0) = 2^{3n}$$
$$g(i+1) = (g(i))^{3n}$$
Then for $0 \le i \le k$
(a) $2^{n(i+1)} \le g(i)$
(b) $f(i) \le g(i)$

Proof: Induction on i.

(a) - Base case: $2^n \le 2^{3n}$
- Induction step:
$$2^{n((i+1)+1)} = 2^{n(i+1)} \cdot 2^n$$
$$\{IH\} \le g(i) \cdot g(0)$$
$$\le g(i)^2 \le g(i+1)$$

(b) - Base case: $f(0) = 1 < 8 \le 2^{3n} = g(i)$
- Induction step: $f(i+1)$
$$\{\text{Lemma above}\} \le (2^n f(i))^{i+1} + f(i)$$
$$= 2^{n(i+1)} f(i)^{i+1} + f(i)$$
$$\{(a) + IH\} \le g(i)\ g(i)^{i+1} + g(i)$$
$$\{i+1 \le n\} \le g(i)\ g(i)^n + g(i)$$
$$\le g(i)^{n+2} \le g(i+1)$$

The closed-form for $g(k)$ is as follows

Lemma (a) $g(k) \leq 2^{(3n)^n}$

(b) $(3n)^n \leq 2^{c \cdot n \log n}$ where c is independent of n

Proof:

(a) $g(k) = \underbrace{\left(\left(2^{3n}\right)^{3n} \cdots\right)^{3n}}_{k+1 \text{ powers of } 3n} = 2^{(3n)^{k+1}} \leq 2^{(3n)^n}$

(b) $(3n)^n = \left(3 \cdot 2^{\log n}\right)^n \leq \left(2^2 \cdot 2^{\log n}\right)^n$

$= \left(2^{2+\log n}\right)^n \leq \left(2^{4 \log n}\right)^n = 2^{4 n \log n}$

Altogether: There is a sequence σ so that

$$\mu_S |\sigma\rangle \mu \geq \mu_S$$

with

$$|\sigma| \leq 2^{2^{c \cdot n \log n}}$$