2. Coverability is in EXPSPACE, Rackoff '78

Coverability:

Given: Petri net $N = (S, T, W)$ and markings $M_1, M_2 \in \mathbb{N}^S$.

Problem: $\exists M \in R(M_1) : M \geq M_2$?

Next week: Lower bound

Coverability is EXPSPACE-hard, Lipton '76.

Now: Upper bound

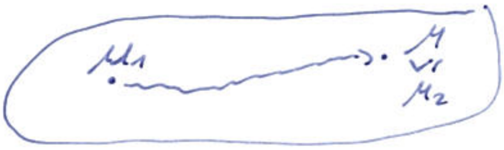
Coverability is in EXPSPACE, Rackoff '78.

This means there is an algorithm that

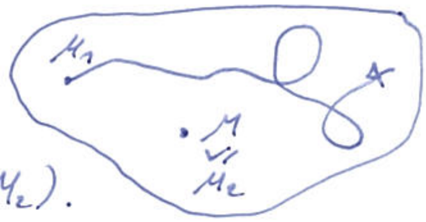
- decides coverability and
- needs only exponential space (in the size of the input)

Together: Coverability is EXPSPACE-complete.

Approach due to Rackoff:



- Guess a path from M_1 to M
- Terminate if the path becomes too long
- Too long = longer than 2^{2^n}, $n = \text{Size}(N, M_1, M_2)$.



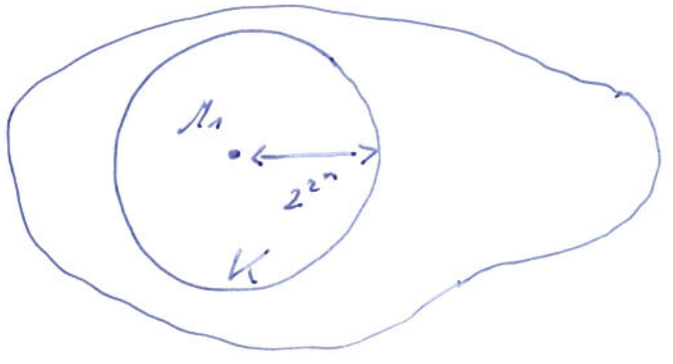
Why does the procedure only need exponential space?

↳ Length of the path (up to 2^{2^n}) can be stored in binary with $\log 2^{2^n} = 2^n$ bits.

↳ To continue the path, we only need the last marking

↳ Given that the length of the path is 2^{2^n}, no place can have more than 2^{2^n} tokens. Again use binary representation.

Statement of Rackoff's theorem:



- The markings coverable from M_1 form the ball $K\downarrow$.
- Phrased differently, every marking coverable from M_1 is covered in K.

Note:

- The algorithm is non-deterministic.
- This means we have shown that coverability is in NEXPSPACE.
- But NEXPSPACE = EXPSPACE by Savitch's theorem.
- This yields a deterministic algorithm in EXPSPACE.

Challenge:
Establish property of short paths:
If $M_2 \in R(M_1)\downarrow$, then there is $\tau \in T^*$ with $|\tau| \leq 2^{2^n}$ so that $M_1[\tau\rangle M$ with $M \geq M_2$.

Definition (i-r-bounded, i-covering):

- Let $W \in \mathbb{Z}^k$ and $i \in [0, k]$, k = dimension of PN N.
  ↳ Call W i-bounded, if for all $1 \leq j \leq i$ we have $0 \leq W(j)$

$$W = \left(\begin{array}{c} i \\ \\ \end{array}\right)\begin{array}{l} \}\ \mathbb{N} \\ \}\ \mathbb{Z} \end{array}$$

↳ Let $r \in \mathbb{N} \setminus \{0\}$.
Call W *i-r-bounded*, if for all $1 \leq j \leq i$ we have

$$0 \leq W(j) < r.$$

• Consider a sequence of (generalized) markings

$$\sigma = W_1 W_2 \dots W_m \in (\mathbb{Z}^k)^*$$

↳ The sequence is called *i-bounded* (*i-r-bounded*), if this holds for every marking.

↳ The sequence is called *i-covering* if

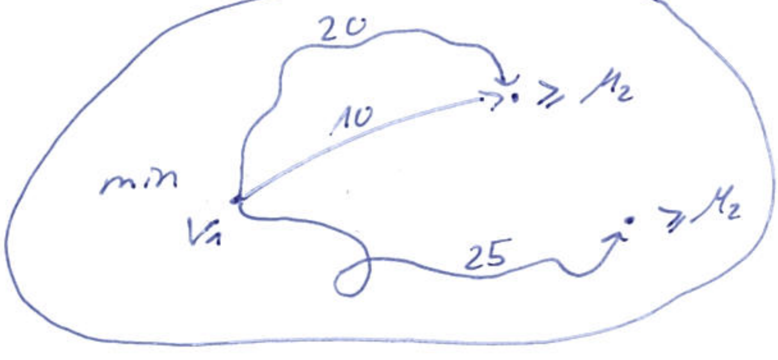
$$W_m(j) \geq M_2(j) \quad \text{for all } 1 \leq j \leq i.$$

Definition (Worst-case bounds on shortest covering sequences):
Let $V \in \mathbb{Z}^k$. Define

$$m(\underset{\substack{\uparrow \\ \text{initial marking}}}{i, V}) := \begin{cases} \min\{ |\sigma| \mid \sigma \in (\mathbb{Z}^k)^* \text{ is } i\text{-bounded and } i\text{-covering in } (N, V)\}, & \text{if exists} \\ 0 & \text{, otherwise.} \end{cases}$$

Illustration

$m(i, V_1) =$



$= 10.$

Moreover, define

$$f(i) := \max\{ m(i, V) \mid V \in \mathbb{Z}^k \}.$$

Intuition:
• $f(i)$ = maximal length of a shortest covering sequence.

To be more precise:

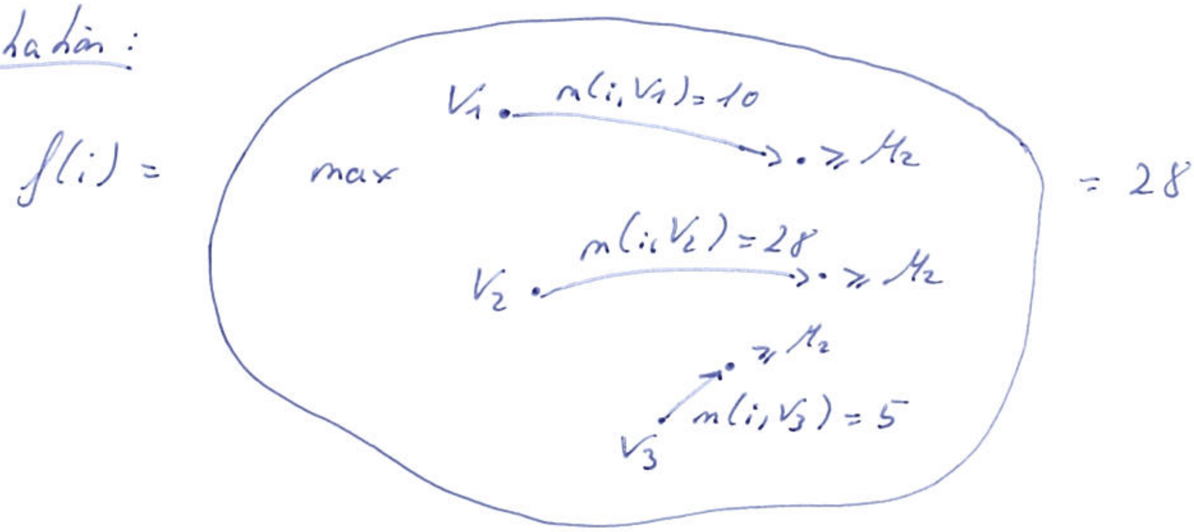
↳ Consider all initial markings

↳ How long can it take

↳ to cover $M_2(j)$ for all $1 \leq j \leq i$ and

↳ maintain the first i-dimensions positive.

Illustration:



Lemma:

Let $V \in \mathbb{Z}^k$ and $M_2 \in \mathbb{N}^k$. Let N be of dimension k.

Then $M_2 \in R(N, V)\downarrow$ iff

there is a k-bounded and k-covering path.

Proof:

"$\Rightarrow$" Since $M_2 \in R(N, V)\downarrow$, there is a sequence

$V, V_1, \ldots, V_m \geq M_2$.

↳ Since this is a PN-path,

all vectors are positive in all entries.

Hence, the sequence is k-bounded.

↳ Moreover, $V_m \geq M_2$ by assumption.

Hence, the sequence is k-covering.

"$\Leftarrow$" Consider a k-bounded and k-covering path.

↳ Since k-bounded, it is a PN-path.

↳ Since h-covering, we have $V_{last} \geq M_2$.

Hence, $M_2 \in R(N, V)\downarrow$ $\square$

Goal: · Determine an upper bound on $f(h)$

· Then we have

$$f(h) \geq m(h, M_1) \text{ by definition.}$$

· But $m(h, M_1)$ is precisely the length of the shortest path that M_1 needs to cover M_2.

Approach: Use induction.

Lemma:

$f(0) = 1$

nowhere positive } Satisfied by initial vector.
nowhere covering }

Lemma:

$f(i+1) \leq (2^\wedge f(i))^{i+1} + f(i)$ f.a. $0 \leq i < k$.

Proof:

Let $V \in \mathbb{Z}^k$ and $0 \leq i < k$
so that there is an $(i+1)$-bounded, $(i+1)$-covering path
starting in V.

Case 1: There is an $(i+1)$-$(2^\wedge f(i))$-bounded path that is $(i+1)$-covering.

↳ Then there is such a path
that does not repeat vectors.
To be more precise: where the vectors do not repeat
in the first $(i+1)$ places.

↳ Such a non-repeating path has a length
of at most
$(2^\wedge f(i))^{i+1}$.

Why? There are $2^\wedge f(i)$ possible values per entry/dimension
and $(i+1)$ entries.

Case 2: Otherwise

↳ Consider an $(i+1)$-bounded, $(i+1)$-covering path
that is not
$(i+1)$-$(2^\wedge f(i))$-bounded.

↳ The path can be decomposed into

$$\sigma = \sigma_1 . \sigma_2$$

so that

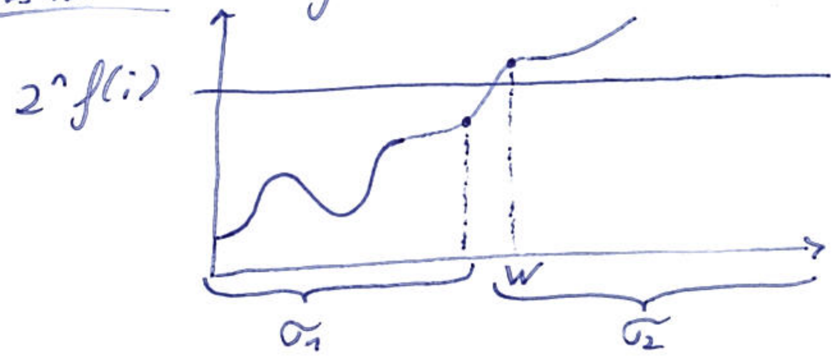
- σ_1 <u>is</u> $(i+1)$-$(2^\wedge f(i))$-bounded and
- σ_2 starts with a vector W that is <u>not</u> $(i+1)$-$(2^\wedge f(i))$-bounded.

Wlog. assume

$$W(i+1) \geq 2^\wedge f(i),$$

which means entry $(i+1)$ exceeds $2^\wedge f(i)$.

<u>Illustration:</u> Entry $(i+1)$



↳ Like in Case 1, we argue that

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

↳ Since σ_2 is an i-bounded, i-covering path in (N, W), there is an alternative path σ_2' that is also i-bounded and i-covering and moreover satisfies

$$|\sigma_2'| \leq f(i).$$

<u>Goal:</u> show that also

$$\sigma_1 . \sigma_2'$$

is an $(i+1)$-bounded and $(i+1)$-covering path in (N, V).

Clearly, $\sigma_1 \sigma_2'$ has a length of at most

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

↳ All edge weights in the PN are $\leq 2^n$
(by definition of vector size as the length of the binary encoding and the fact that $n = \mathrm{Size}(N, M_1, M_2)$).

↳ Since $|\sigma_2'| \leq f(i)$,
and since a path (of vectors) of length $f(i)$ has at most $f(i)-1$ transitions,
σ_2' can remove at most

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

tokens from $W(i+1)$.

↳ Since $W(i+1) \geq 2^n f(i)$,
this leaves us with

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

tokens.

↳ Again by the definition of vector sizes, M_2 has at most 2^n tokens per place.

↳ This means

$$\sigma_1 . \sigma_2'$$

is $(i+1)$-bounded and $(i+1)$-covering. □

Goal: Give an upper bound on $f(k)$
that does not need recursion.

Approach: (1) Give a simpler recursive function $g(k)$
that upper-bounds $f(k)$.
(2) Give a non-recursive (closed-form) upper bound for $g(k)$.

Definition:
Define function $g: \mathbb{N} \to \mathbb{N}$ as follows:
$g(0) := 2^{3n}$ and $g(i+1) := (g(i))^{3n}$ f.a. $0 \leq i < k < n$.

Lemma:
For all $0 \leq i \leq k$ we have
$f(i) \leq g(i)$.

Proof:
By induction along i.
Base case: $i=0$ $f(0) = 1 < 8 \leq 2^{3n} = g(0)$.
Induction step: Assume the claim holds for $0 \leq i < k$.
Consider

$$
\begin{aligned}
& f(i+1) \\
\text{(Lemma above)} \leq\ & (2^n f(i))^{i+1} + f(i) \\
=\ & 2^{n(i+1)} \cdot f(i)^{i+1} + f(i) \\
\text{(Induction hypothesis)} \leq\ & 2^{n(i+1)} \cdot g(i)^{i+1} + g(i) \\
\text{(Lemma below)} \leq\ & g(i) \cdot g(i)^{i+1} + g(i) \\
\leq\ & 2 g(i)\, g(i)^{i+1} \\
\leq\ & 2 g(i)\, g(i)^{n} \\
=\ & 2 g(i)^{n+1} \\
\leq\ & g(i)^{n+2} \leq g(i)^{3n} = g(i+1).
\end{aligned}
$$

$\square$

Lemma:

$2^{n(i+1)} \leq g(i)$ f.a. $0 \leq i \leq k$.

Proof:

Base case: ($i=0$) $2^n \leq 2^{3n}$.

Induction step: Assume the inequality holds for $0 \leq i \leq k$.

Then

$$
\begin{aligned}
& 2^{n((i+1)+1)} \\
&= 2^{n(i+1)} \cdot 2^n \\
\text{(Induction hypothesis)} &\leq g(i) \cdot 2^n \\
&\leq g(i) \cdot g(0) \\
&\leq g(i)^2 \\
&\leq g(i+1).
\end{aligned}
$$

$\square$

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

Lemma:

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

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

Proof:

(a)

$$
\begin{aligned}
& g(k) \\
\text{(Definition)} &= \underbrace{\left(\ldots\left(\left(2^{(3n)}\right)^{(3n)}\right)^{(3n)} \ldots\right)^{(3n)}}_{(k+1) \text{ powers of } (3n).} \\
&= \left(\ldots\left(\left(2^{(3n)}\right)^{(3n)}\right)^{(3n)} \ldots\right)^{(3n)(3n)} \\
&= 2^{(3n)^{k+1}} \\
&\leq 2^{(3n)^n}.
\end{aligned}
$$

(b) $(3n)^n$

$$= (3 \cdot 2^{ld n})^n$$
$$\leq (2^2 \cdot 2^{ld n})^n$$
$$= (2^{2+ld n})^n$$
$$\leq (2^{4 ld n})^n$$
$$= 2^{4 n ld n}$$
$$= 2^{(4l) n \log n} \quad . \qquad \square$$

<u>Altogether</u>:

There is a k-bounded, k-covering path in (N, V) of length $\leq 2^{2^{cn\log n}}$.

<u>Lemma</u>:

In all markings on this path, the token count is $\leq 2^{2^{dn \log n}}$.

<u>Proof</u>:

Note that every transition changes at most 2^n tokens:

$$\underbrace{2^n}_{\text{Initial marking}} + 2^n \underbrace{\left(2^{2^{cn\log n}} - 1\right)}_{\text{Transitions}}$$

$$= 2^n \cdot 2^{2^{cn \log n}}$$
$$= 2^{2^{cn\log n} + n}$$
$$= 2^{2^{cn\log n} + 2^{l \cdot \log n}}$$

(*) $\leq 2^{2^{s \cdot c \cdot n \log n} + 2^{t \cdot l \cdot \log n}}$

$$\leq 2^{2^{s \cdot c \cdot n\log n} \cdot 2^{t \cdot l \cdot \log n}}$$
$$\leq 2^{2^{s \cdot c \cdot n \log n} \cdot 2^{t \cdot l \cdot n \log n}}$$
$$= 2^{2^{(sc + tl) n \log n}} \quad . \qquad \square$$

(*) s is chosen such that $2^{s \cdot c \cdot n \log n} \geq 2$ and similar for t.