Complexity Analysis of the Backward Coverability Algorithm for VASS

Pierre Ganty
IMDEA Software Institute
Madrid, Spain

Laura Bozzelli
UPM
Madrid, Spain

▶ RP '11, Genova ◀

Safety checking for systems with infinitely many states

Coverability checking

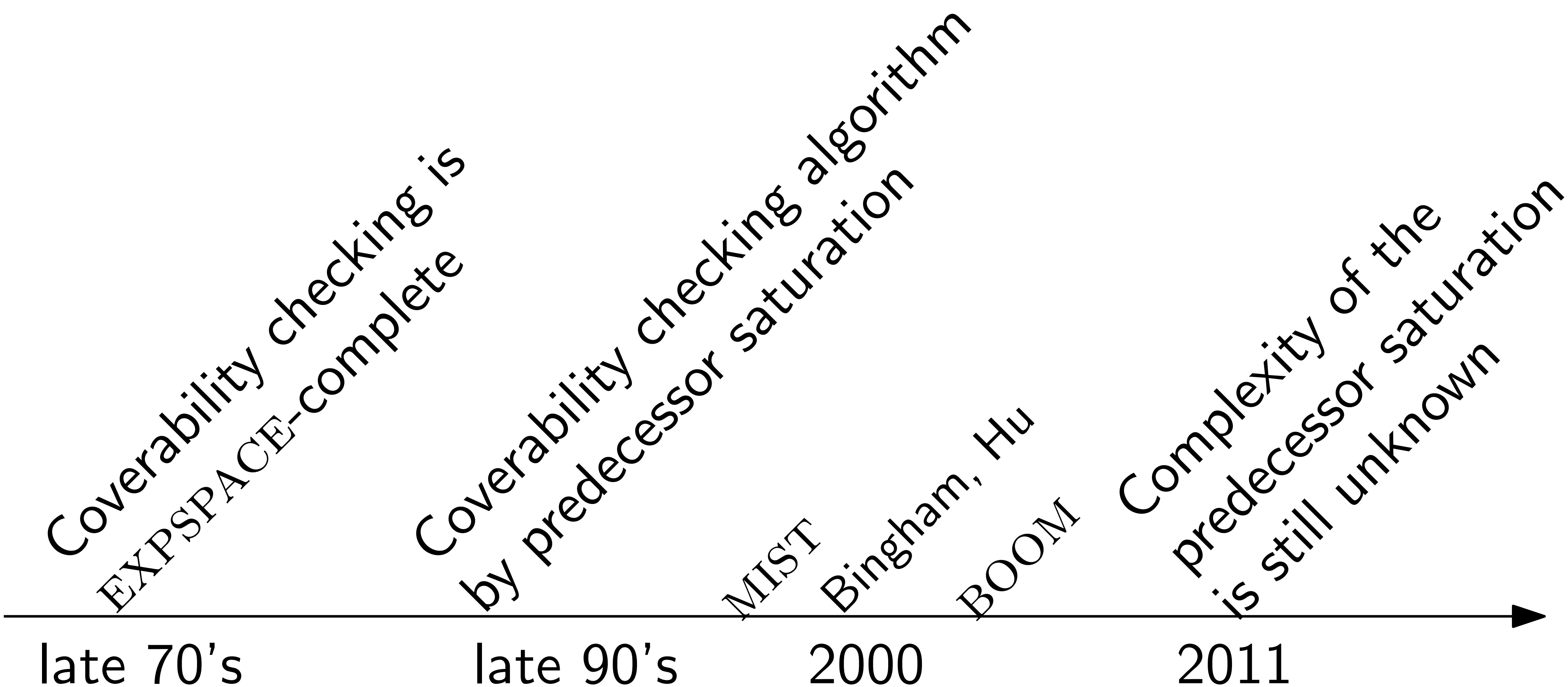
Vector Addition Systems with States

Low supply of decidable cases, e.g. coverability checking for VASS

Coverability checking for VASS is useful for verification:
- Multithreaded Software Libraries (Ball, Chaki, Rajamani in TACAS '01)
- Asynchronous programs
(Majumdar, Jhala, Sen, Viswanathan in POPL '{07,09}, CAV '06, TCS '09)
- Parameterized Concurrent Programs
(Kroening, Kaiser, Wahl in CAV '10)

VASS coverability checker have been implemented:
- Delzanno, Raskin, Van Begin, G (MIST, 2000–2007)
- Bingham, Hu (2005)
- Kaiser, Kroening, Wahl (BOOM, 2009–present)

Complexity of problem vs solution



VASS

A d-$\textsc{vass}$ consists of a pair (Q, Δ)

- Q are the control states
- $\Delta \subseteq Q \times \mathbb{Z}^d \times Q$ is the finite set of transitions

Semantics as an infinite transition system $(Q \times \mathbb{N}^d, \rightarrow)$

Let $q \xrightarrow{\vec{u}} q'$ be a transition where $\vec{u} = \langle u_1, \ldots, u_d \rangle$ then

$$\langle q, v_1, \ldots, v_d \rangle \rightarrow \langle q', v_1 + u_1, \ldots, v_d + u_d \rangle$$

- $\rightarrow^*$ denotes the reachability relation

VASS coverability

Define the ordering $\trianglelefteq$ on VASS states as follows:

$$\langle q, v_1, \ldots, v_d \rangle \trianglelefteq \langle q', v'_1, \ldots, v'_d \rangle$$

iff

$$q = q' \text{ and } v_i \leq v'_i \text{ for every } i \in \{1, \ldots, d\}$$

Given a VASS and two VASS-states: $\boldsymbol{s}_\imath$ and $\boldsymbol{s}_f$
Checking that $\boldsymbol{s}_f$ is coverable from $\boldsymbol{s}_\imath$ asks
if there exists a VASS-state $\boldsymbol{s}$ such that:

$$\boldsymbol{s}_\imath \rightarrow^* \boldsymbol{s} \text{ and } \boldsymbol{s}_f \trianglelefteq \boldsymbol{s}$$

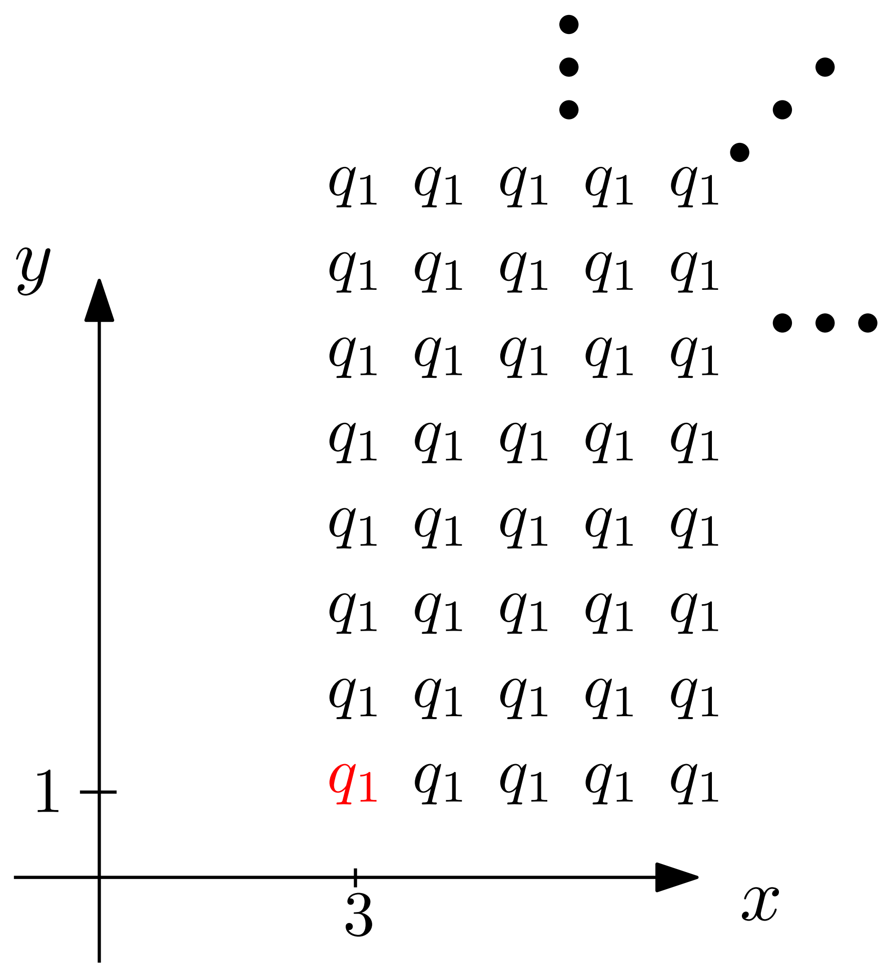
Seminal papers about the coverability problem:

- Lower bound on the coverability problem, Lipton 1976, cited 219 times
- Upper bound on the coverability problem, Rackoff 1978, cited 143 times

The coverability problem is EXPSPACE-complete

Solving VASS coverability: predecessors computation

Let a 2-VASS and call the 2 counters $\{x, y\}$ and $\boldsymbol{s}_f = \langle q, 4, 1 \rangle$



Let $t \colon q_1 \xrightarrow{\langle +1,0 \rangle} q$

$pre[t](\{\langle q, i, j \rangle \mid i \geq 4, j \geq 1\}) = \{\langle q_1, k, \ell \rangle \mid k \geq 3, \ell \geq 1\}$

Solving VASS coverability

Saturating the predecessor computation

$pre[t](X)$ predecessor of X in 1 step using t

$pre(X) = \bigcup_t pre[t](X)$ predecessor in 1 step

$pre^*(X)$ predecessors in 0 or more steps

$$pre^*(U) = \lim_{n\to\infty} X_n \qquad \text{where} \begin{cases} X_1 = U \\ X_{i+1} = U \cup pre(X_i) \end{cases}$$

$$\begin{array}{l} X_1 = U \\ \rotatebox{90}{$\subseteq$} \\ X_2 = U \cup pre(U) \\ \rotatebox{90}{$\subseteq$} \\ X_3 = U \cup pre(U) \cup pre(pre(U)) \\ \vdots \end{array}$$

$\boldsymbol{s}_f$ is coverable from $\boldsymbol{s}_\imath$ iff $\boldsymbol{s}_\imath \in pre^*(\{\boldsymbol{s} \mid \boldsymbol{s}_f \trianglelefteq \boldsymbol{s}\})$

pr ctiveness

$\boldsymbol{s} \in U \wedge \boldsymbol{s} \trianglelefteq \boldsymbol{s'}$ implies $\boldsymbol{s'} \in U$

Convergence: If U is $\trianglelefteq$-closed then $X_1, X_2, \ldots$ is such that

- X_i is $\trianglelefteq$-closed for every i
- stabilizes after finitely many steps: $X_\dagger = X_{\dagger+1}$ for some $\dagger$

Effectiveness: Let U $\trianglelefteq$-closed, $\min(U)$ finitely represents U.

- Predicates $U_1 \subseteq U_2$ and $\boldsymbol{s}_\imath \in U$ for U, U_1, U_2 $\trianglelefteq$-closed are decidable given $\min(U), \min(U_1), \min(U_2)$.
- $\min(\mathit{pre}(U))$ is finite and computable given $\min(U)$

For $U = \{\boldsymbol{s} \mid \boldsymbol{s}_f \trianglelefteq s\}$ we have $\min(U) = \{\boldsymbol{s}_f\}$ then

$$Z_1 = \{\boldsymbol{s}_f\}$$

$$Z_{i+1} = \min\big(\{\boldsymbol{s}_f\} \cup \mathit{minpre}(Z_i)\big)$$

$$\boldsymbol{s}_f \text{ is coverable from } \boldsymbol{s}_\imath \text{ iff } \begin{cases} \boldsymbol{s}_\imath \in \mathit{pre}^*(\{s_f \mid \boldsymbol{s}_f \trianglelefteq s\}) \\ \boldsymbol{s} \trianglelefteq \boldsymbol{s}_\imath \text{ for some } \boldsymbol{s} \in Z_\dagger \end{cases}$$

Upper Bound

Complexity of the predecessor algorithm: upper bounds

Given d-VASS $G = (Q, \Delta)$ and G-state $\boldsymbol{s}_f$

Let

$$Z_1 = \{\boldsymbol{s}_f\}$$

$$Z_{i+1} = \min\big(\{\boldsymbol{s}_f\} \cup \mathit{minpre}(Z_i)\big)$$

From the EXPSPACE membership proof we derive:

- upper bound on $\dagger$ $\boxed{(|Q| \cdot b_c)^{2^{O(d \cdot \log d)}}}$
- upper bound on $|Z_i|$ for every i $\boxed{O(|Q| \cdot ((i+1) \cdot b_c)^d)}$
- upper bound b such that $Z_i \subseteq Q \times [0, b]^d$ for every $\boxed{O(i+1) \cdot b_c)}$
- hence, upper bound on the execution time $\boxed{(|Q| \cdot b_c)^{2^{O(d \cdot \log d)}}}$

Define $b_c \in \mathbb{N}_0$ be the least value such that

$$\Delta \subseteq Q \times [-b_c, +b_c]^d \times Q \text{ and } \boldsymbol{s}_f \in Q \times [0, b_c]^d$$

Rackoff's proof

A d-VASS $G = \langle Q, \Delta \rangle$ and a G-state $\boldsymbol{s}_f$

Define $\pi_{\boldsymbol{s}}$ as a shortest sequence which covers $\boldsymbol{s}_f$ from $\boldsymbol{s}$

Given G and $\boldsymbol{s}_f$, Rackoff bounds $\max_{\boldsymbol{s}} |\pi_{\boldsymbol{s}}|$

The bound is obtained by induction on the number of counters:

$$f(0) \leq f(1) \leq \cdots \leq f(d) = \max_{\boldsymbol{s}} |\pi_{\boldsymbol{s}}|$$

$i > 0$

$$\boldsymbol{s}_f = \langle q_f, v'_1, \ldots, v'_i, \underset{0}{\cancel{v'_{i+1}}}, \ldots, \underset{0}{\cancel{v'_d}} \rangle$$

Let $(q \xrightarrow{\vec{u}} q') \in \Delta$ where $\vec{u} = \langle u_1, \ldots, u_i, \overset{0}{\cancel{u_{i+1}}}, \ldots, \overset{0}{\cancel{u_d}} \rangle$ then

$$\langle q, v_1, \ldots, v_i, v_{i+1}, \ldots, v_d \rangle$$

$$\rightarrow$$

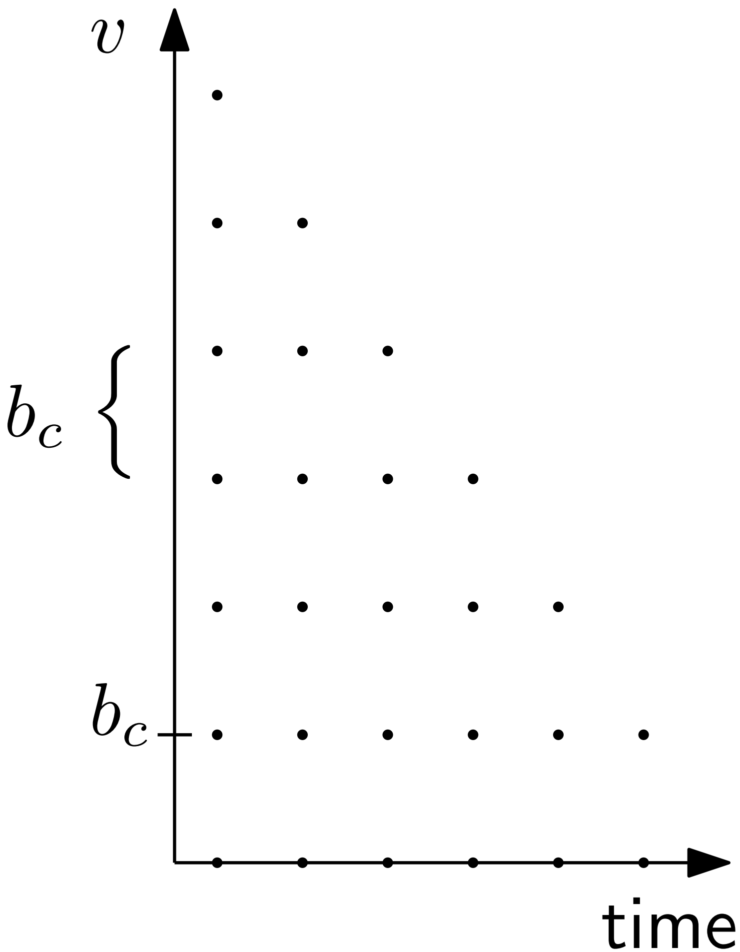
$$\langle q', v_1 + u_1, \ldots, v_i + u_i, v_{i+1} + \underset{0}{\cancel{u_{i+1}}}, \ldots, v_d + \underset{0}{\cancel{u_d}} \rangle$$

We will now characterize $f(i)$ using $f(i-1)$

Characterizing $f(i)$ using $f(i-1)$

Recall $b_c \in \mathbb{N}_0$ is the least value such that

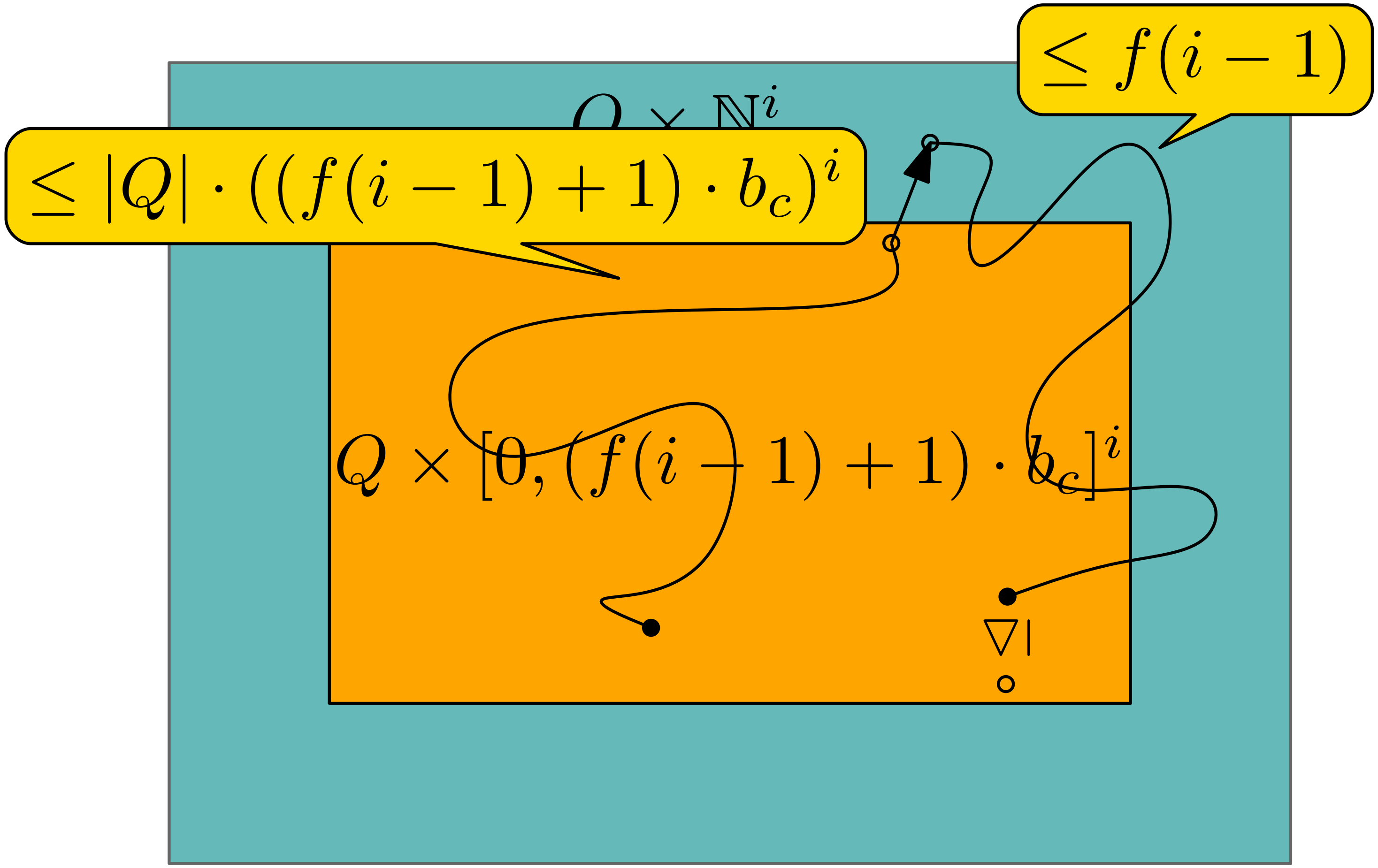
$$\Delta \subseteq Q \times [-b_c, +b_c]^d \times Q \text{ and } \boldsymbol{s}_f \in Q \times [0, b_c]^d$$



- If $v \geq 6 \cdot b_c$ then after firing any sequence π of transitions such that $|\pi| \leq 5$, then $v \geq b_c$
- If $v \geq (f(i-1)+1) \cdot b_c$ then any sequence π of transitions such that $|\pi| \leq f(i-1)$ yields $v \geq b_c$
- If some counter ever goes above $(f(i-1)+1) \cdot b_c$ then we are in the $i-1$ case

The induction hypothesis appears

Characterizing $f(i)$ using $f(i-1)$ (cont'd)



- $f(i) \leq |Q| \cdot ((f(i-1)+1) \cdot b_c)^i + f(i-1)$
- Hence we can show that: $f(d) \leq \left(|Q| \cdot b_c\right)^{2^{O(d \cdot \log d)}}$

Back to the predecessor algorithm

Given d-VASS $G = (Q, \Delta)$ and G-state $\boldsymbol{s}_f$

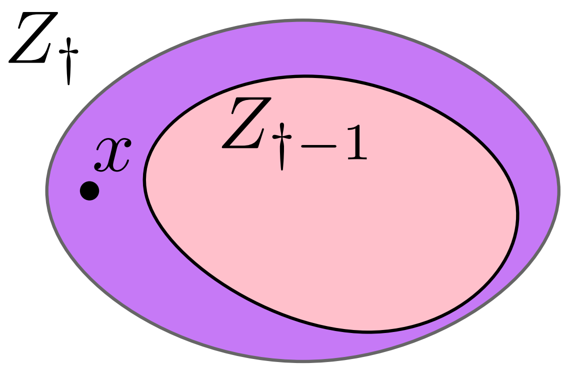
Let

$$Z_1 = \{\boldsymbol{s}_f\}$$
$$Z_{i+1} = \min\big(\{\boldsymbol{s}_f\} \cup \mathit{minpre}(Z_i)\big)$$

Recall:

$\pi_{\boldsymbol{s}}$ is a shortest run to cover $\boldsymbol{s}_f$ from $\boldsymbol{s}$ and $f(d) \geq \max_{\boldsymbol{s}} |\pi_{\boldsymbol{s}}|$

Suppose $\dagger > f(d)$. From there we conclude $\dagger > \max_{\boldsymbol{s}} |\pi_{\boldsymbol{s}}|$



Z_i = the states covering $\boldsymbol{s}_f$ in at most i steps

x covers $\boldsymbol{s}_f$ in no less than $\dagger$ steps, hence $|\pi_{\boldsymbol{x}}| > \max_{\boldsymbol{s}} |\pi_{\boldsymbol{s}}|$

Therefore $\dagger \leq f(d)$ and $\dagger = \big(|Q| \cdot b_c\big)^{2^{O(d \cdot \log d)}}$

Lower Bound

Complexity of the predecessor algorithm: lower bounds

Lipton's EXPSPACE-hardness result for reachability in VASS ...
defines a family $\{(G_i, \langle q_i, 0, \ldots, 0\rangle)\}_{i\in\mathbb{N}_0}$ of VASS+G_i-state for which the sequence $Z_1, Z_2, \ldots$ given by

$$Z_1 = \{\langle q_i, 0, \ldots, 0\rangle\}$$
$$Z_{j+1} = \min\Big(\{\langle q_i, 0, \ldots, 0\rangle\} \cup \mathit{minpre}(Z_j)\Big)$$

is such that:

- $\dagger_i \geq 2^{2^i}$
- $|Z_{\dagger_i}| \geq 2^{2^i}$
- the highest number in $Z_{\dagger_i}$ is at least $2^{2^{\Omega(i)}}$

Each d-VASS $G_i = \langle Q_i, \Delta_i\rangle$ is such that:

- $d = O(i)$
- $|Q_i| = O(i)$
- $|\Delta_i| = O(i)$
- $\Delta_i \subseteq Q_i \times [-1, 1]^d \times Q_i$

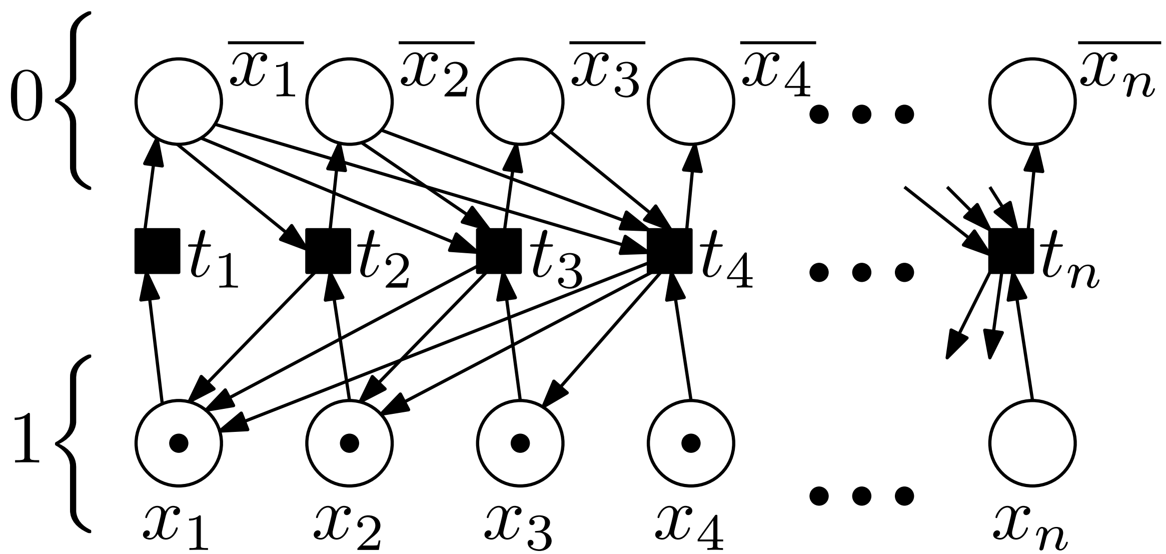
Proof ideas

We want 2^n
- a "large" value for $\dagger$
- "many" (incomparable) elements in $Z_\dagger$.

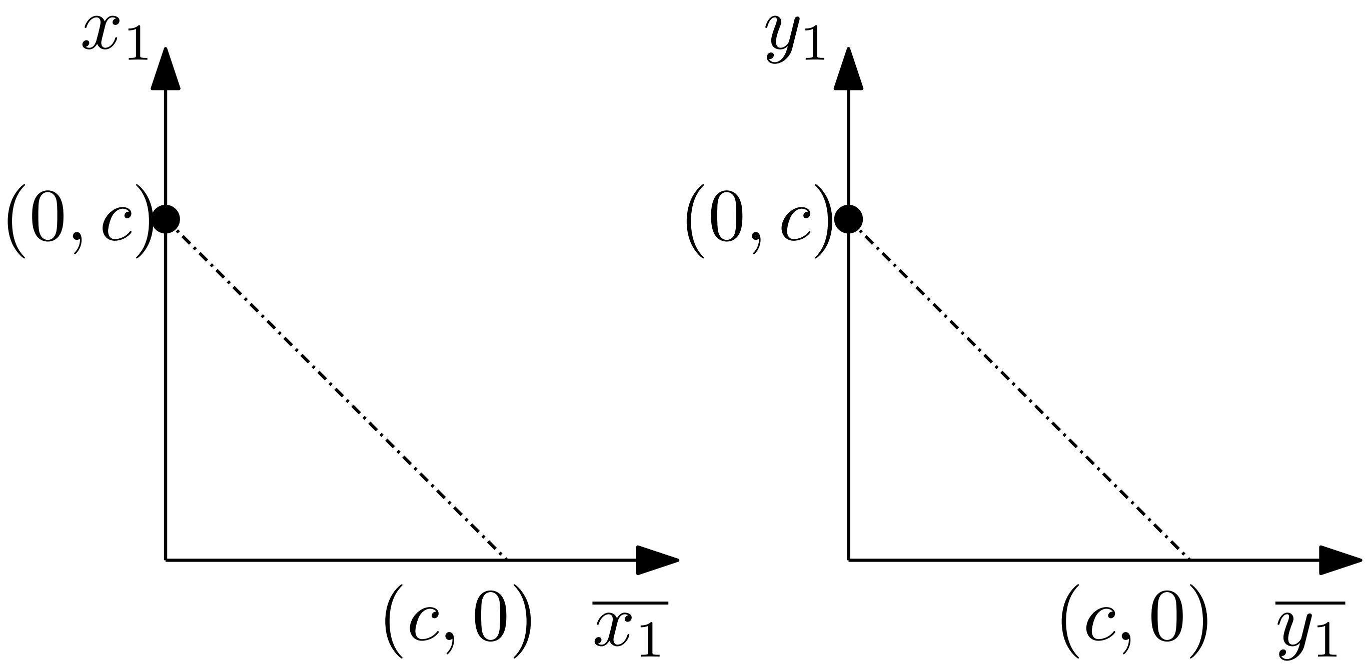
2^n

First idea, a

$x_i + \overline{x_i}$ constant for every i yields 2^n incomparable



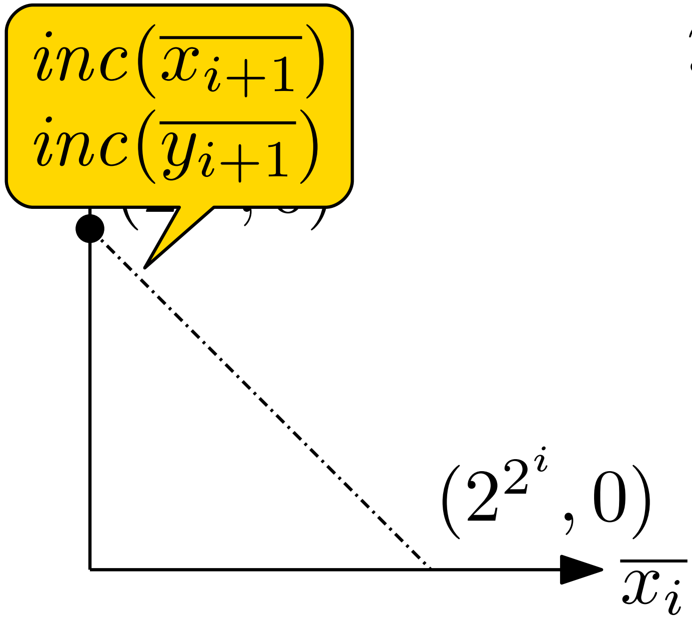
Towards double exponential

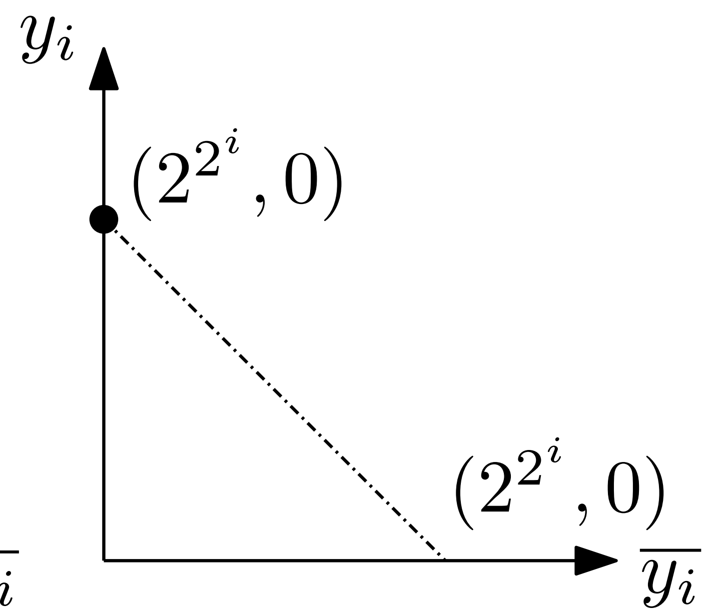


Let $c = 2^{2^i}$, then $\{(x_1, \overline{x_1}, y_1, \overline{y_1}) \mid x_1 + \overline{x_1} = c,\ y_1 + \overline{y_1} = c\}$ has $c \cdot c = 2^{2^{i+1}}$ incomparable states

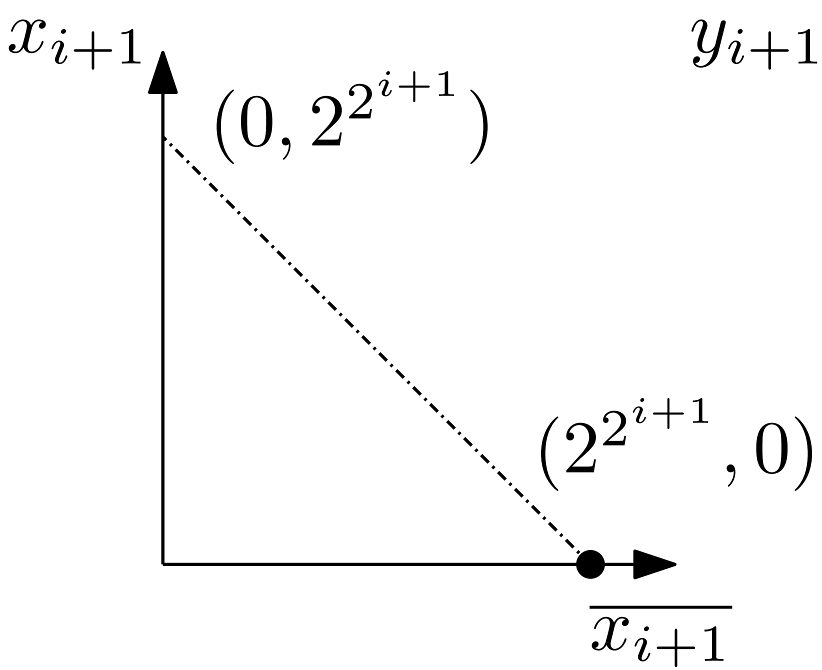
Recall that $\Delta_i \subseteq Q_i \times [-1, 1]^d \times Q_i$, so direct increment / decrement / test of 2^{2^i} is not allowed.
Moreover, setting initial value to 2^{2^i} is not allowed.

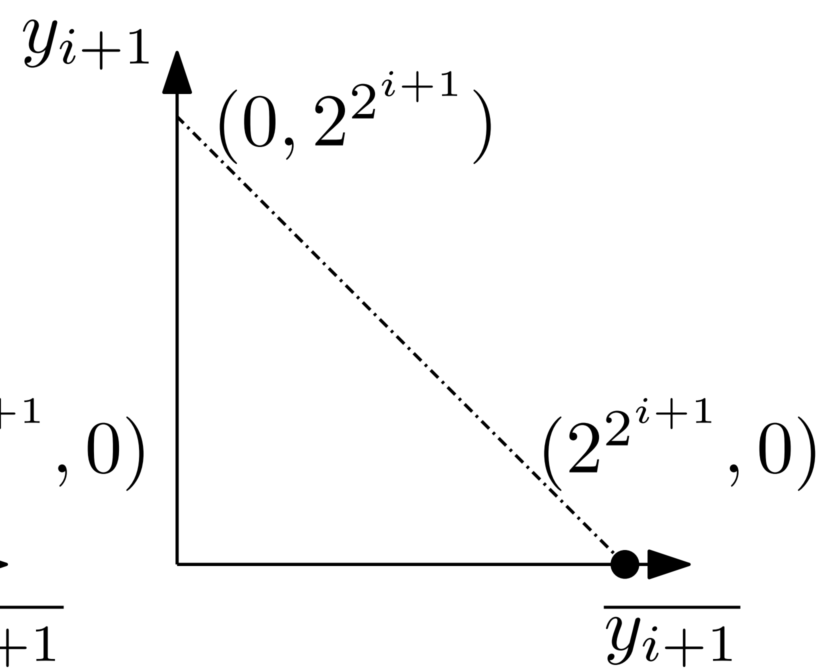
Towards double exponential (cont'd)





We have $2^{2^i} \cdot 2^{2i} = 2^{2^{i+1}}$ calls to inc, so $\overline{x_{i+1}} = \overline{y_{i+1}} = 2^{2^{i+1}}$



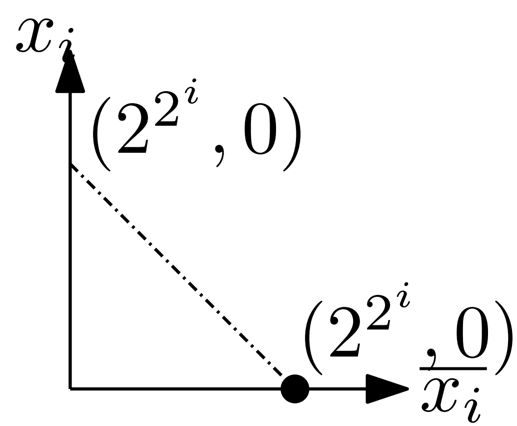


Back to the predecessor algorithm

We define a family $\{(G_i, \langle q_i, 0, \ldots, 0\rangle)\}_{i\in\mathbb{N}_0}$ of $\mathrm{VASS}+G_i$-state for which the sequence $Z_1, Z_2, \ldots$ given by

$$Z_1 = \{\langle q_i, 0, \ldots, 0\rangle\}$$
$$Z_{j+1} = \min\big(\{\langle q_i, 0, \ldots, 0\rangle\} \cup \mathit{minpre}(Z_j)\big)$$

is such that:



- $\dagger_i \geq 2^{2^i}$
- $|Z_{\dagger_i}| \geq 2^{2^i}$
- the highest number in $Z_{\dagger_i}$ is at least $2^{2^{\Omega(i)}}$

Conclusions

- The predecessor computation has been showed to be optimal w.r.t. the complexity of the coverability problem
  - Easily derived from the complexity proof

Thank You!

- Rather surprising contrast with the forward algorithm (Karp and Miller) that is non-recursive primitive