On Certificates, Expected Runtimes, and Termination in Probabilistic Pushdown Automata

Tobias Winkler, Joost-Pieter Katoen

Software Modeling and Verification Chair
RWTH AACHEN UNIVERSITY

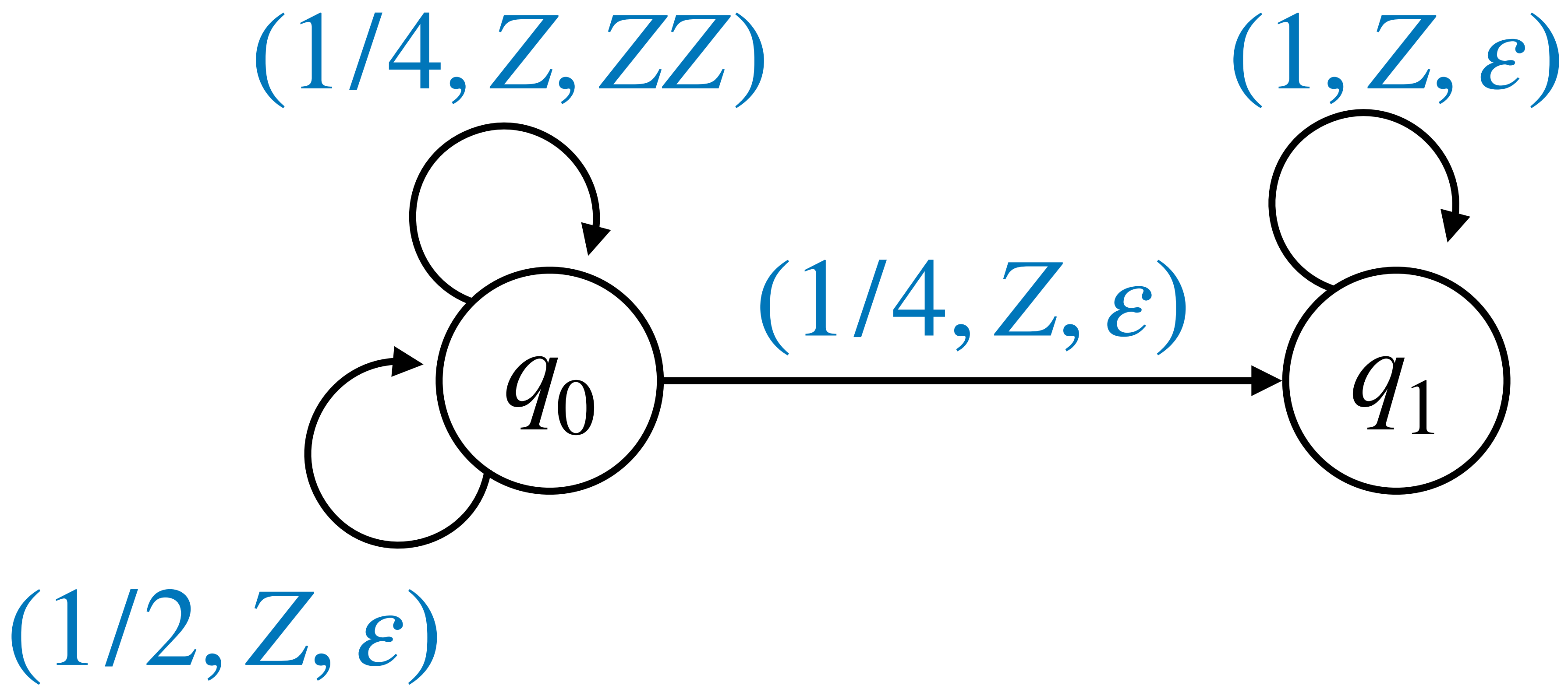
DFG Research Training Group 2236

European Research Council

LICS 2023

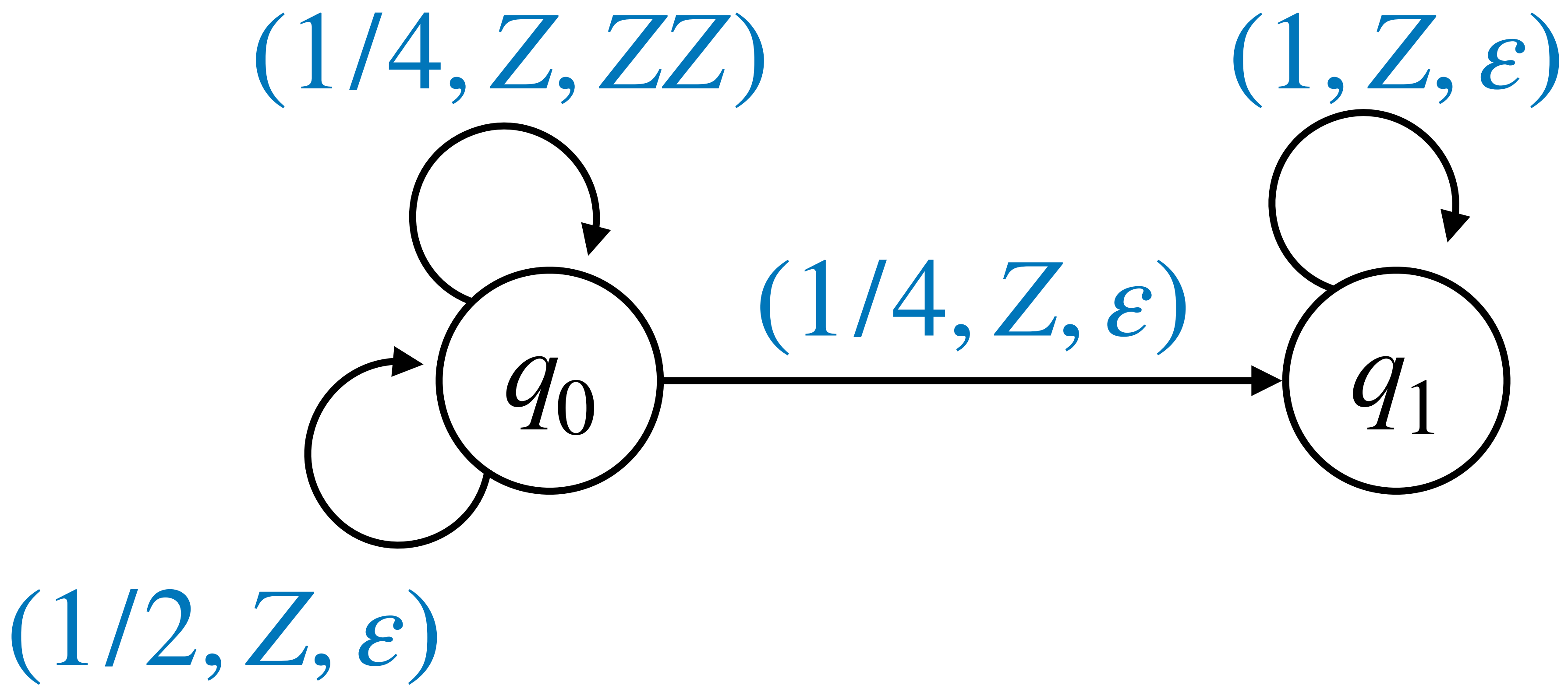
Probabilistic Pushdown Automata (pPDA)

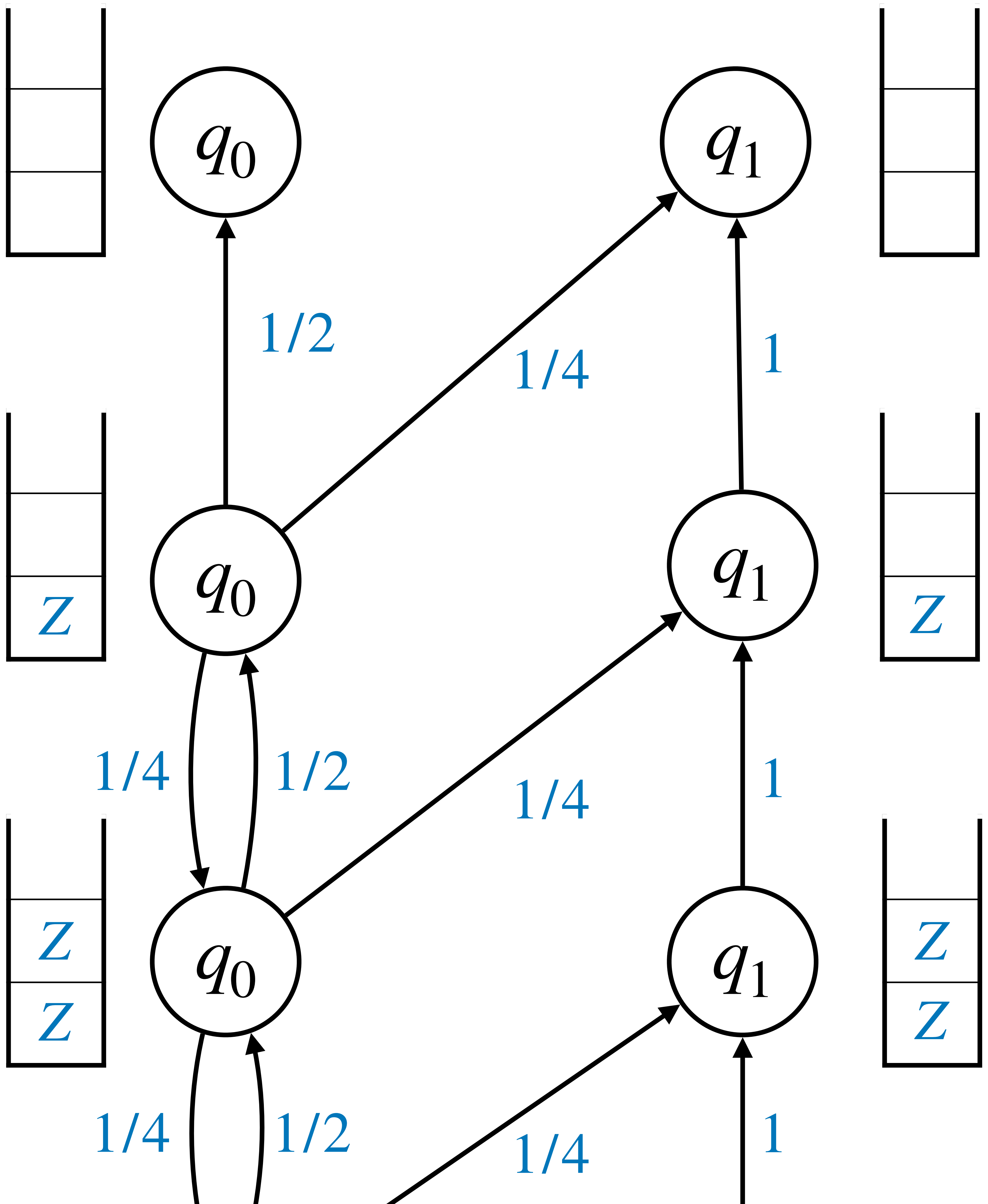
[Esparza, Kucera, Mayr LICS '04, Etessami & Yannakakis STACS '05]



Probabilistic Pushdown Automata (pPDA)

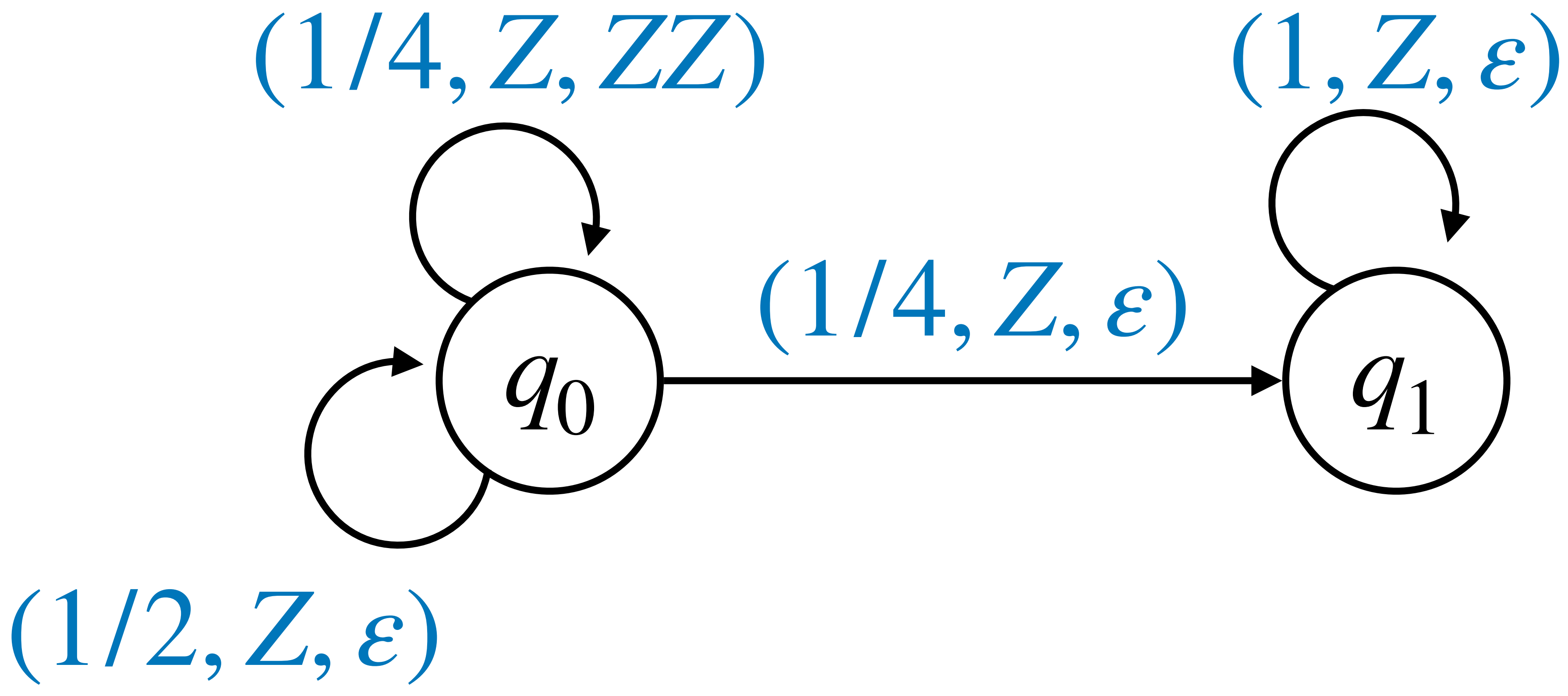
[Esparza, Kucera, Mayr LICS '04, Etessami & Yannakakis STACS '05]



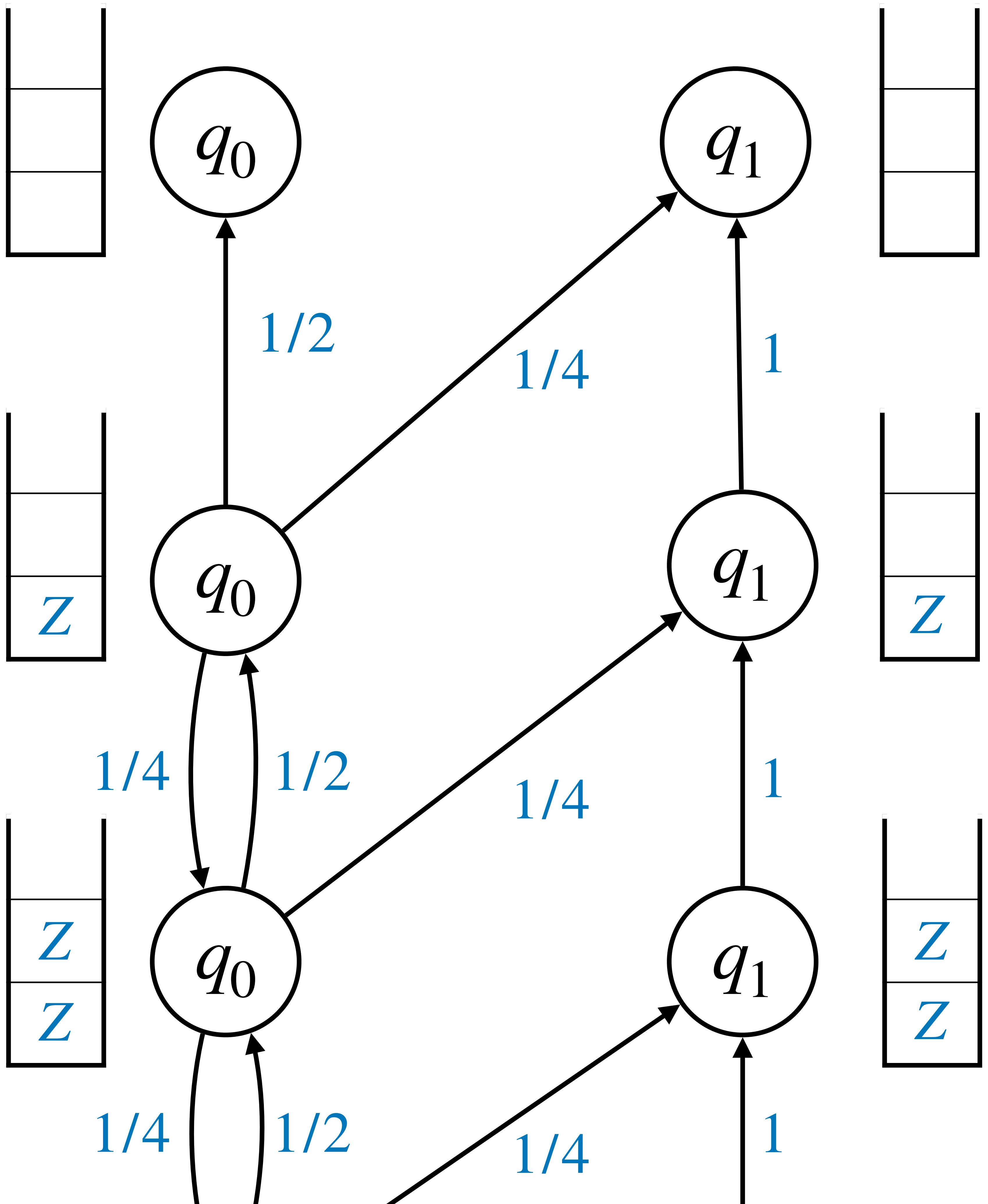


Probabilistic Pushdown Automata (pPDA)

[Esparza, Kucera, Mayr LICS ’04, Etessami & Yannakakis STACS ’05]

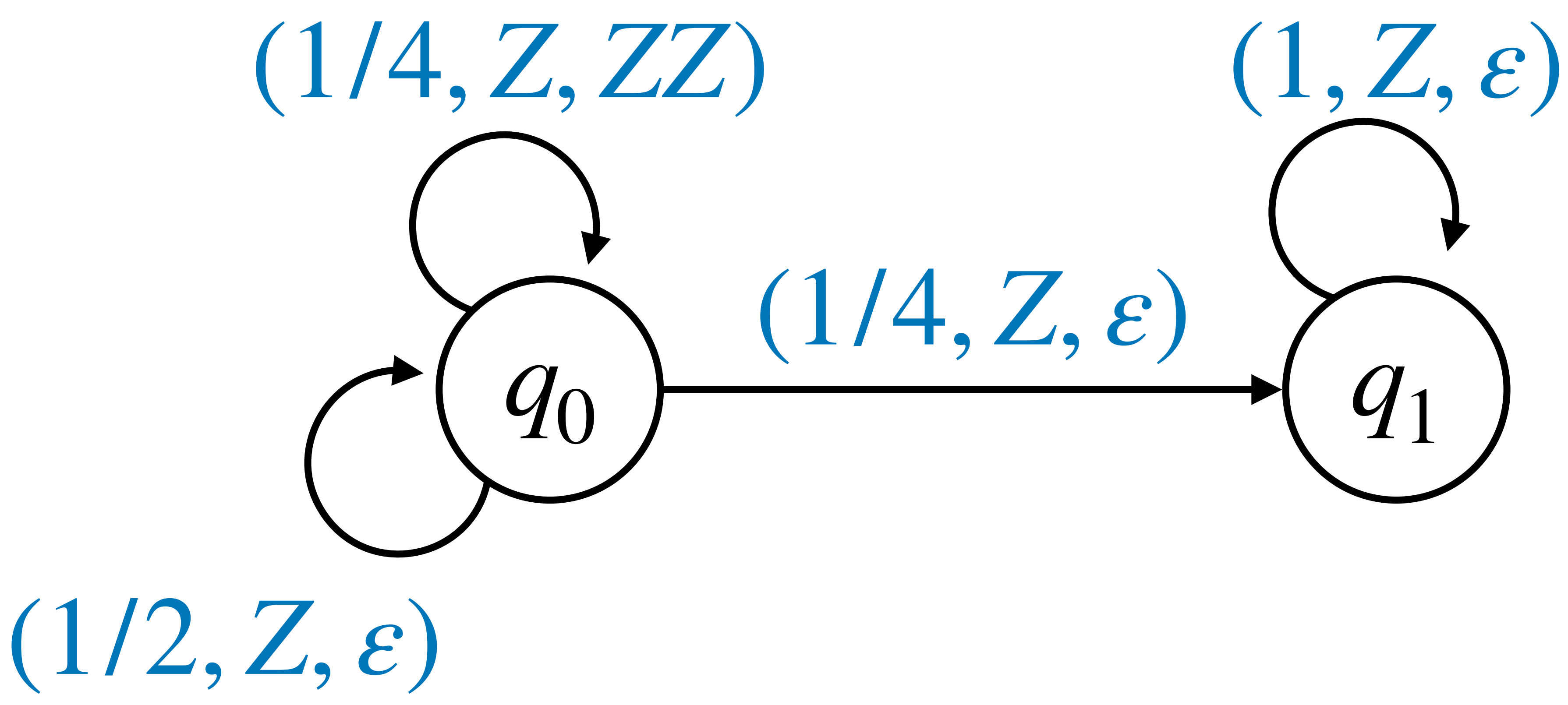



```
boolean f(boolean x) {
  if(x) {
    pchoice {
      0.5: return true;
      0.25: return false;
      0.25: return f(f(x));
    }
  } else {
    return false;
  }
}
```



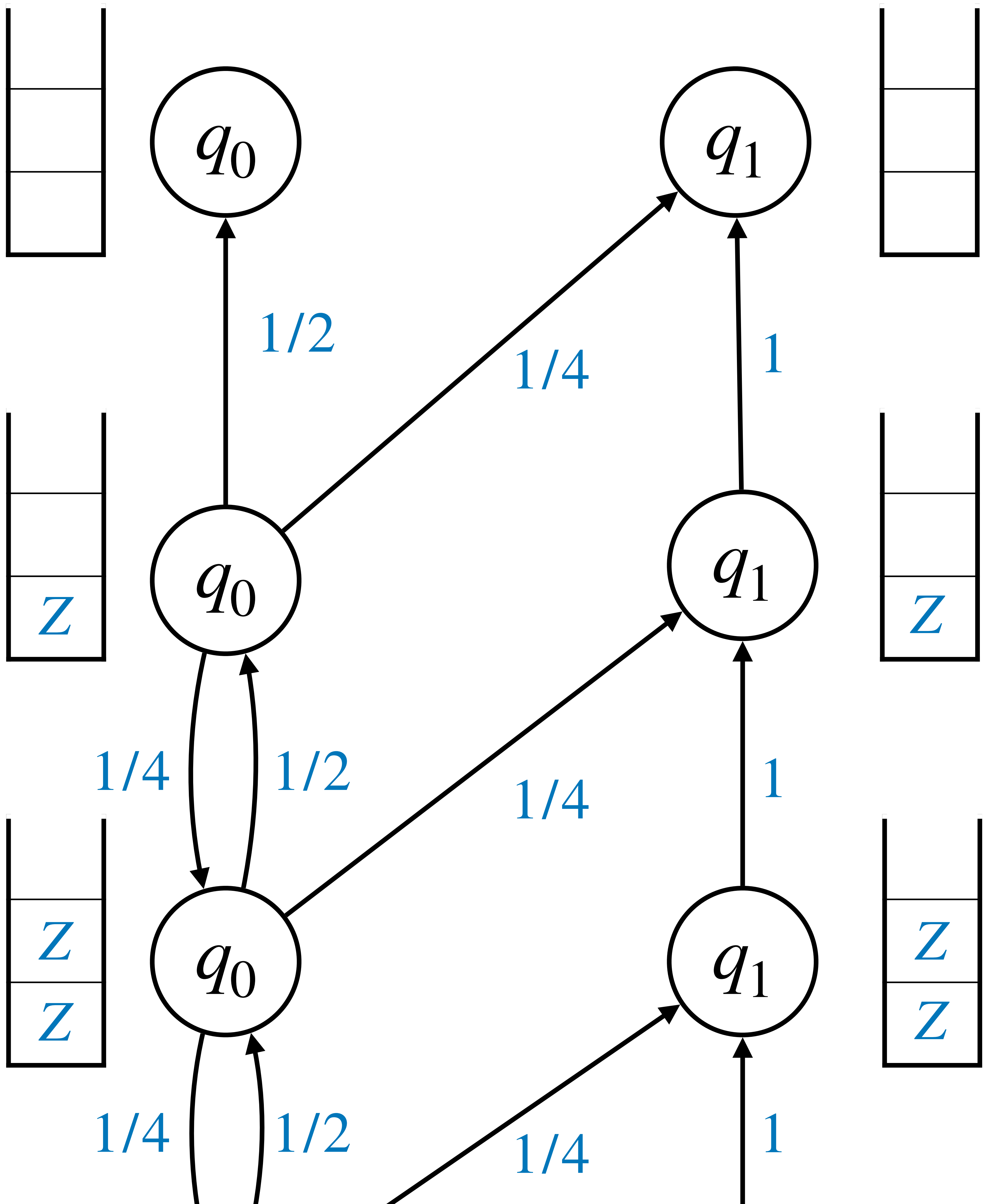
Probabilistic Pushdown Automata (pPDA)

[Esparza, Kucera, Mayr LICS ’04, Etessami & Yannakakis STACS ’05]




```
boolean f(boolean x) {
  if(x) {
    pchoice {
      0.5: return true;
      0.25: return false;
      0.25: return f(f(x));
    }
  } else {
    return false;
  }
}
```

`f(true)` returns `true` with probability $2 - \sqrt{2}$



Termination in pPDA

Termination in pPDA

- Termination = reach empty stack

Termination in pPDA

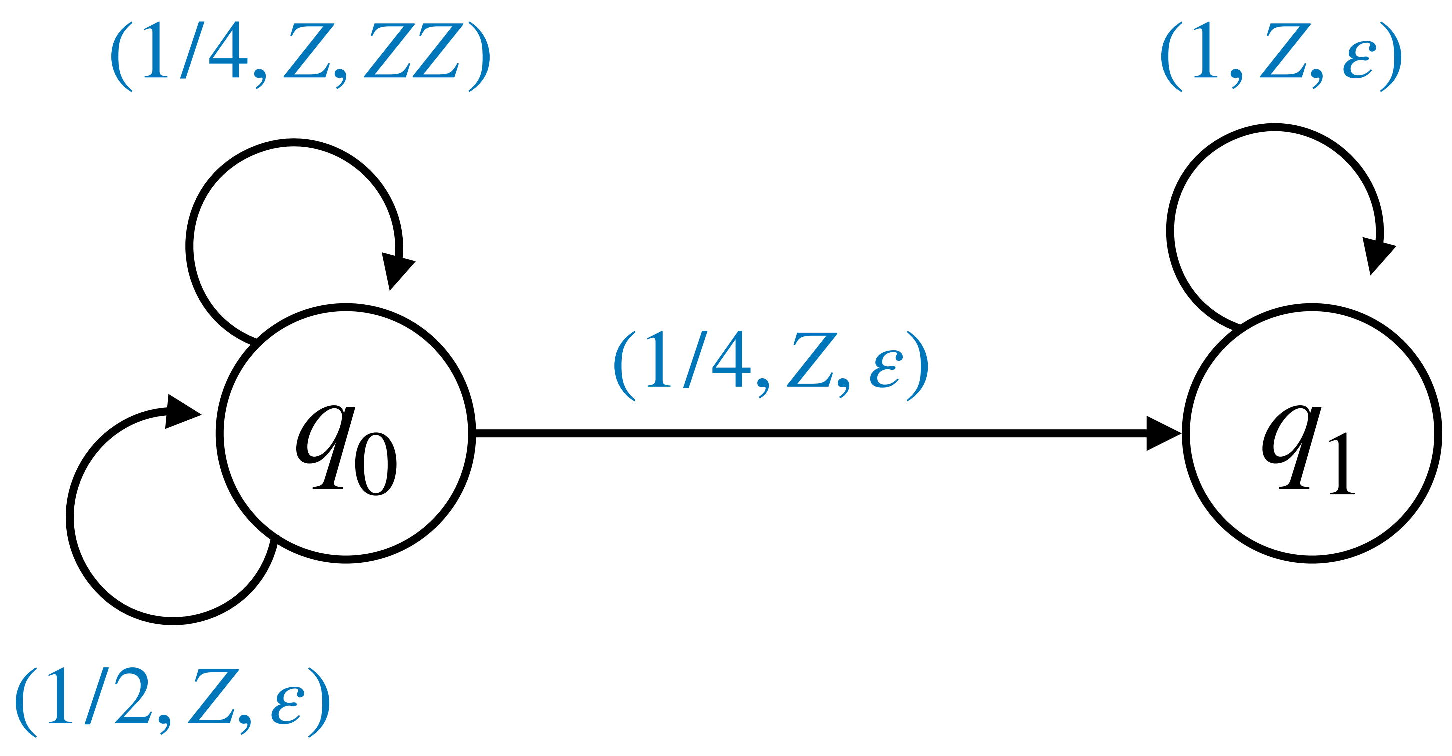
- Termination = reach empty stack
- almost-sure termination (AST) = all configurations terminate with probability 1

Termination in pPDA

- Termination = reach empty stack
- almost-sure termination (AST) = all configurations terminate with probability 1
- positive almost-sure termination (PAST) = expected runtime is finite ($\Longrightarrow$ AST)

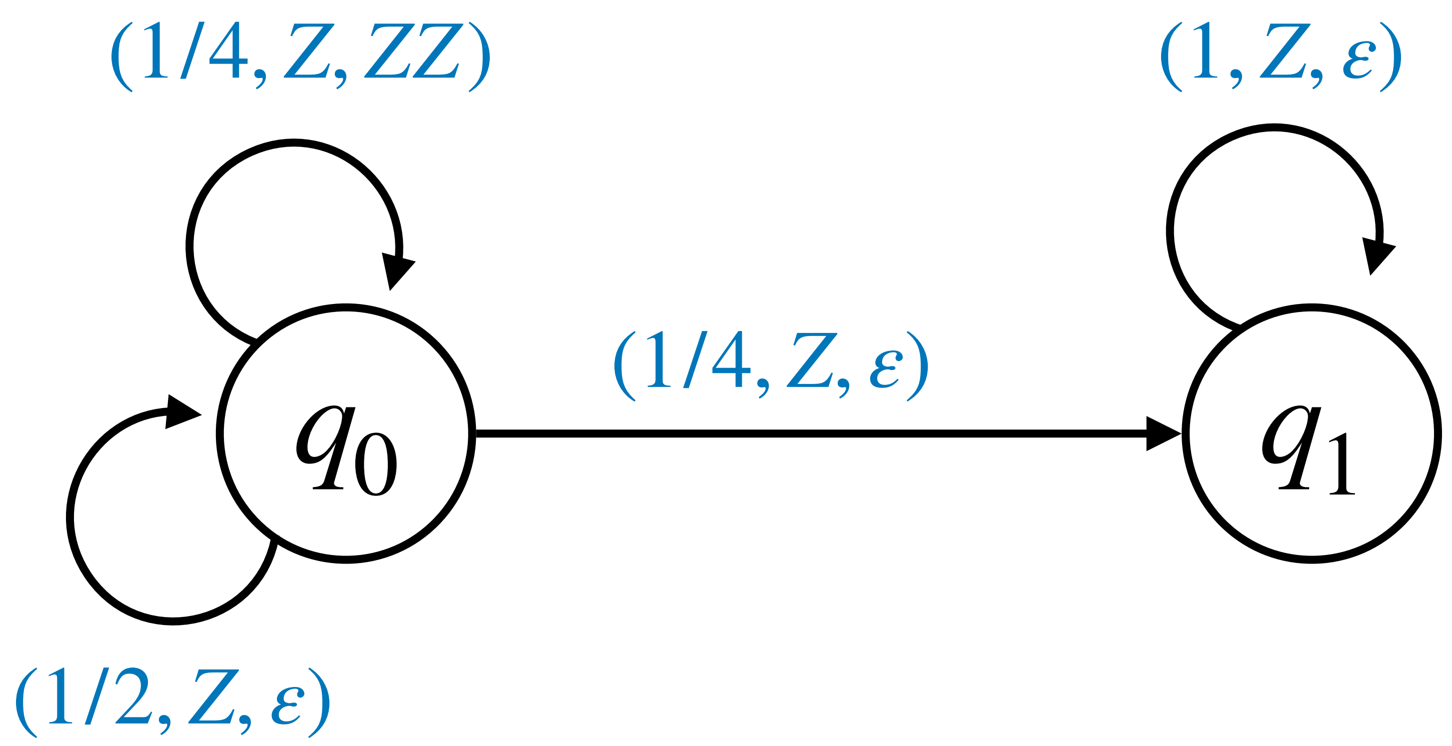
Termination in pPDA

- Termination = reach empty stack
- almost-sure termination (AST) = all configurations terminate with probability 1
- positive almost-sure termination (PAST) = expected runtime is finite ($\Longrightarrow$ AST)



Termination in pPDA

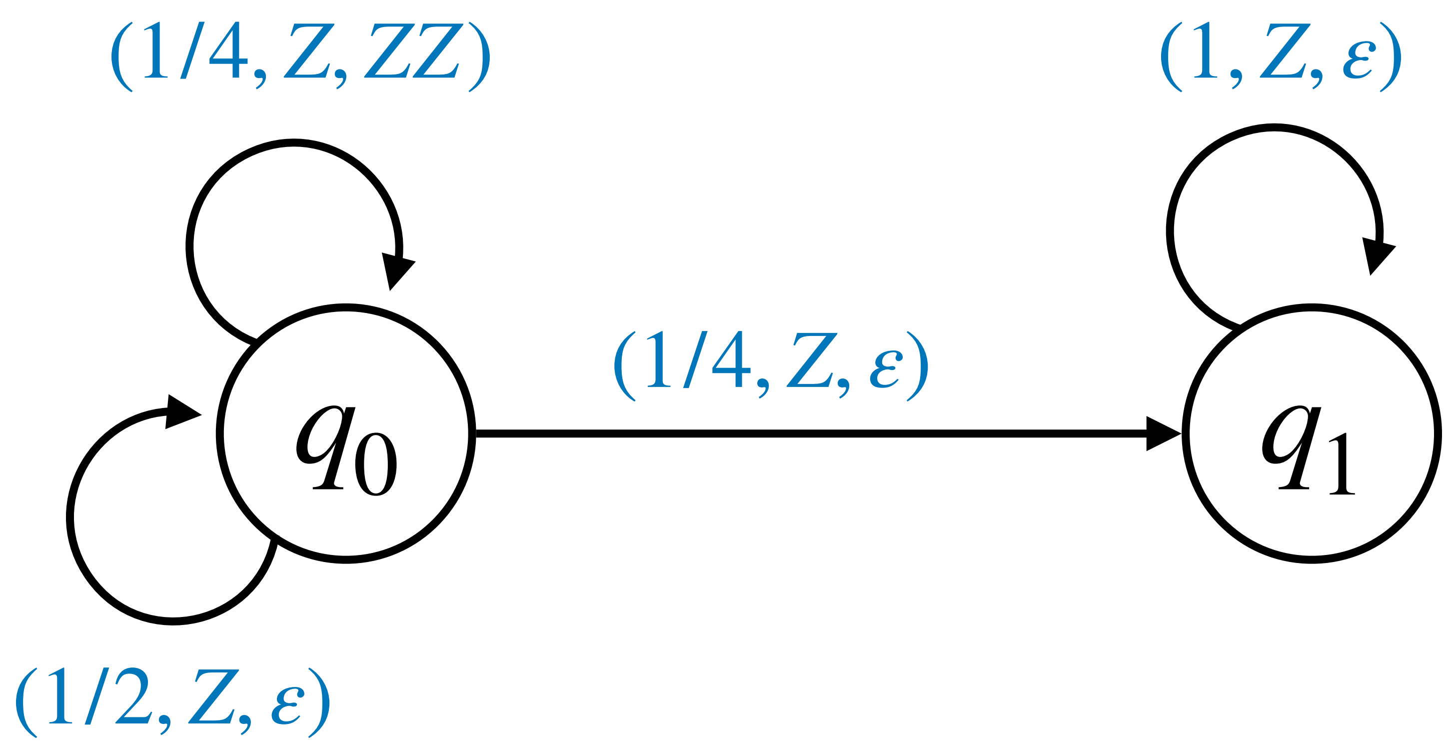
- Termination = reach empty stack
- almost-sure termination (AST) = all configurations terminate with probability 1
- positive almost-sure termination (PAST) = expected runtime is finite ($\implies$ AST)



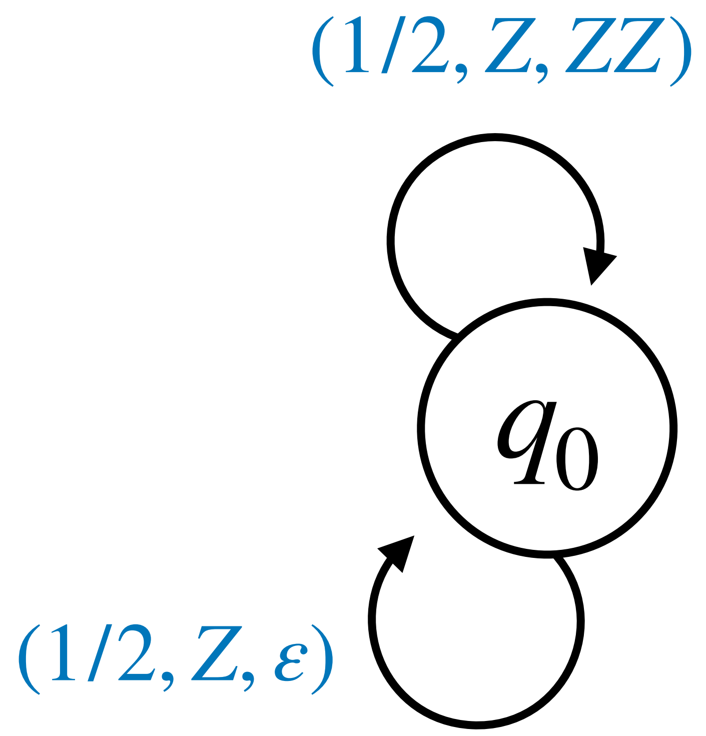
AST and PAST

Termination in pPDA

- Termination = reach empty stack
- almost-sure termination (AST) = all configurations terminate with probability 1
- positive almost-sure termination (PAST) = expected runtime is finite ($\Longrightarrow$ AST)



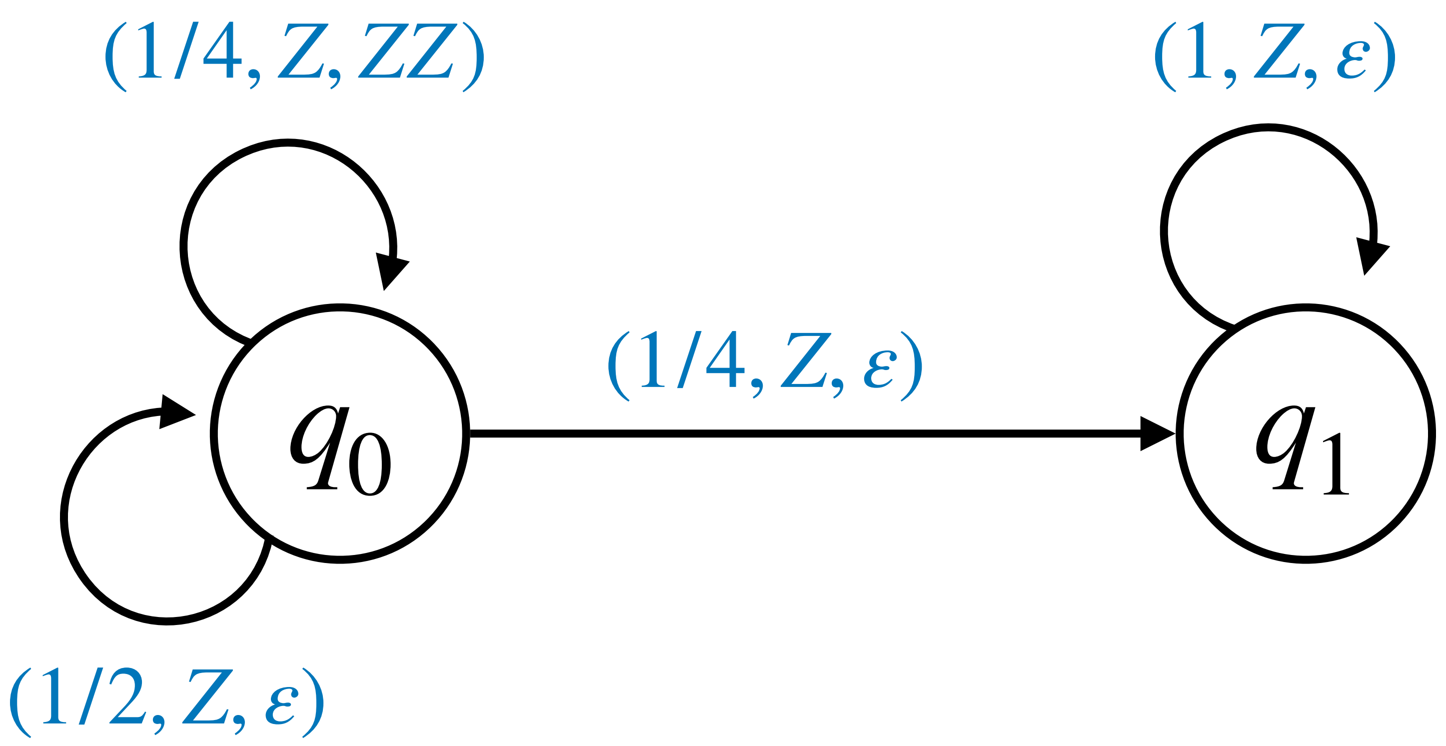
AST and PAST



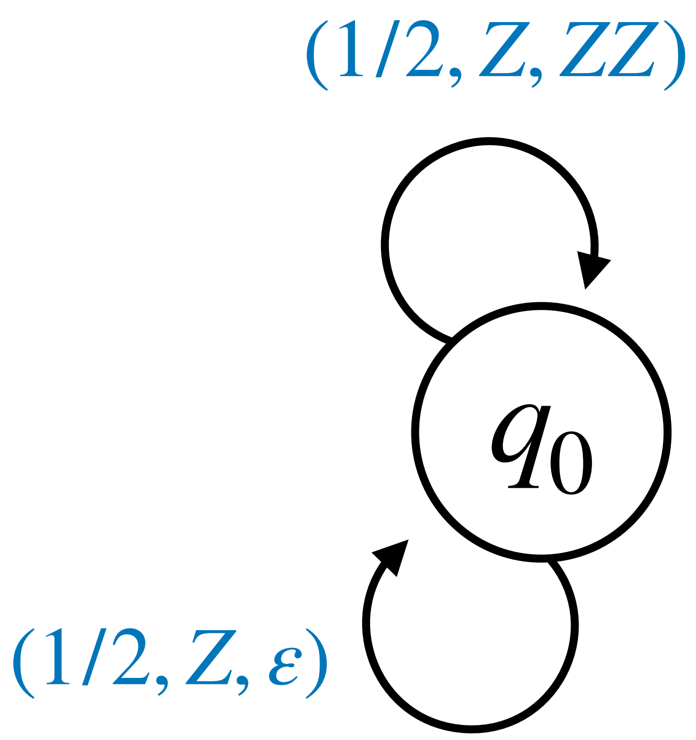
AST, but not PAST

Termination in pPDA

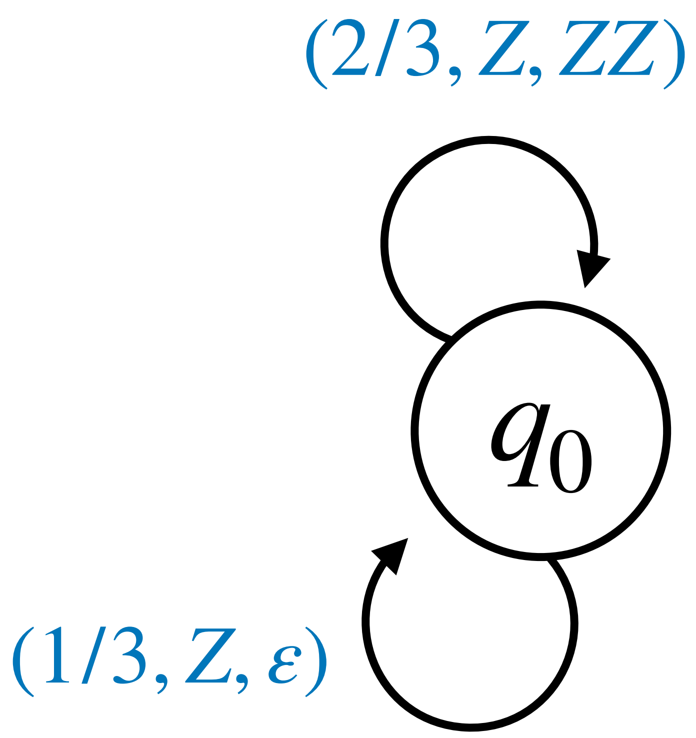
- Termination = reach empty stack
- almost-sure termination (AST) = all configurations terminate with probability 1
- positive almost-sure termination (PAST) = expected runtime is finite ($\Longrightarrow$ AST)



AST and PAST



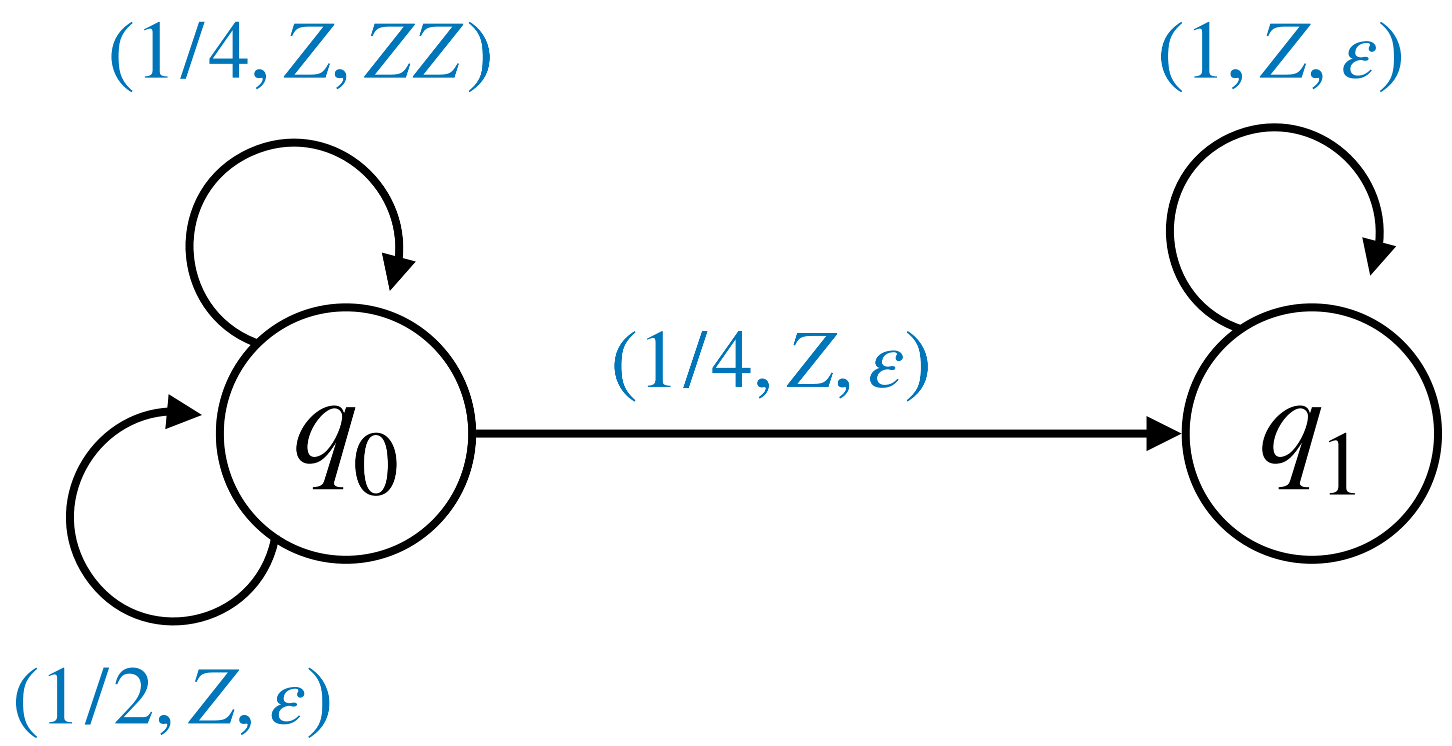
AST, but not PAST



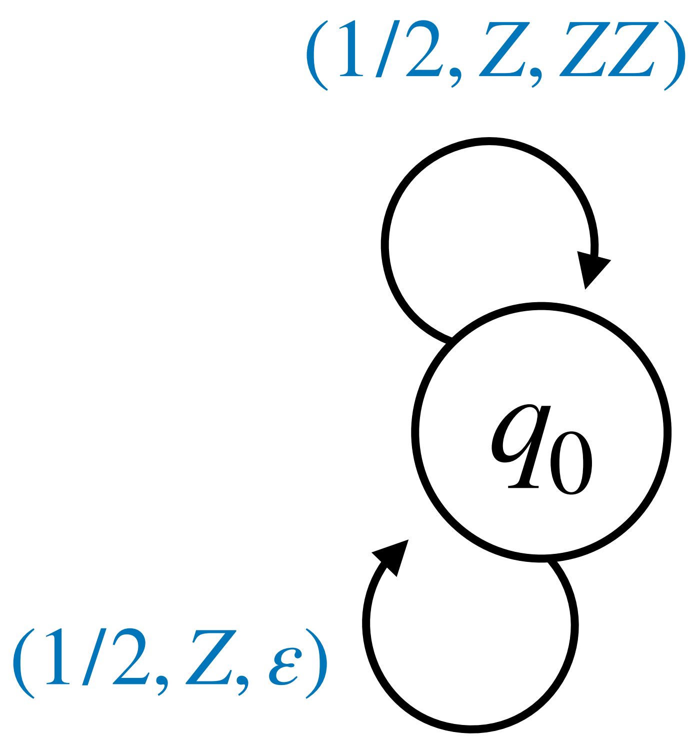
not AST

Termination in pPDA

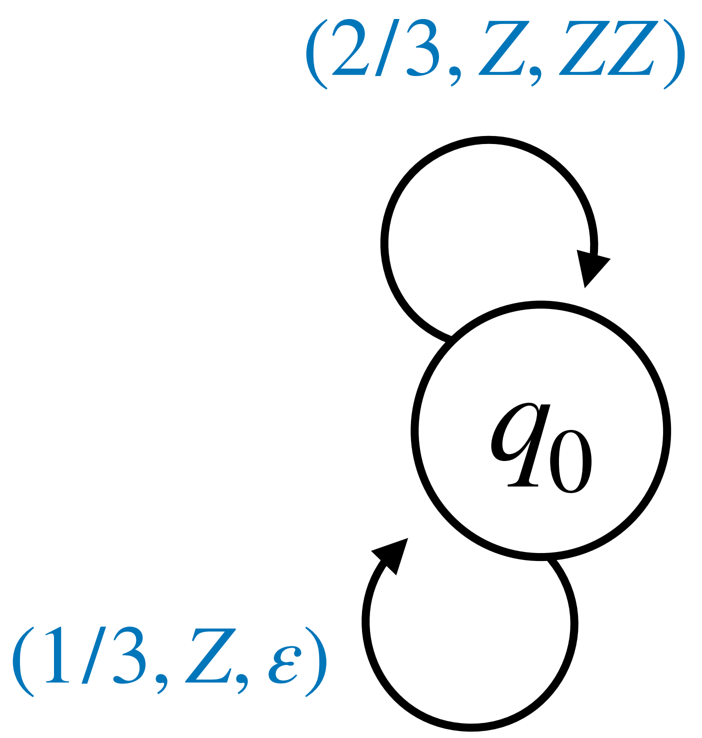
- Termination = reach empty stack
- almost-sure termination (AST) = all configurations terminate with probability 1
- positive almost-sure termination (PAST) = expected runtime is finite ($\Longrightarrow$ AST)



AST and PAST



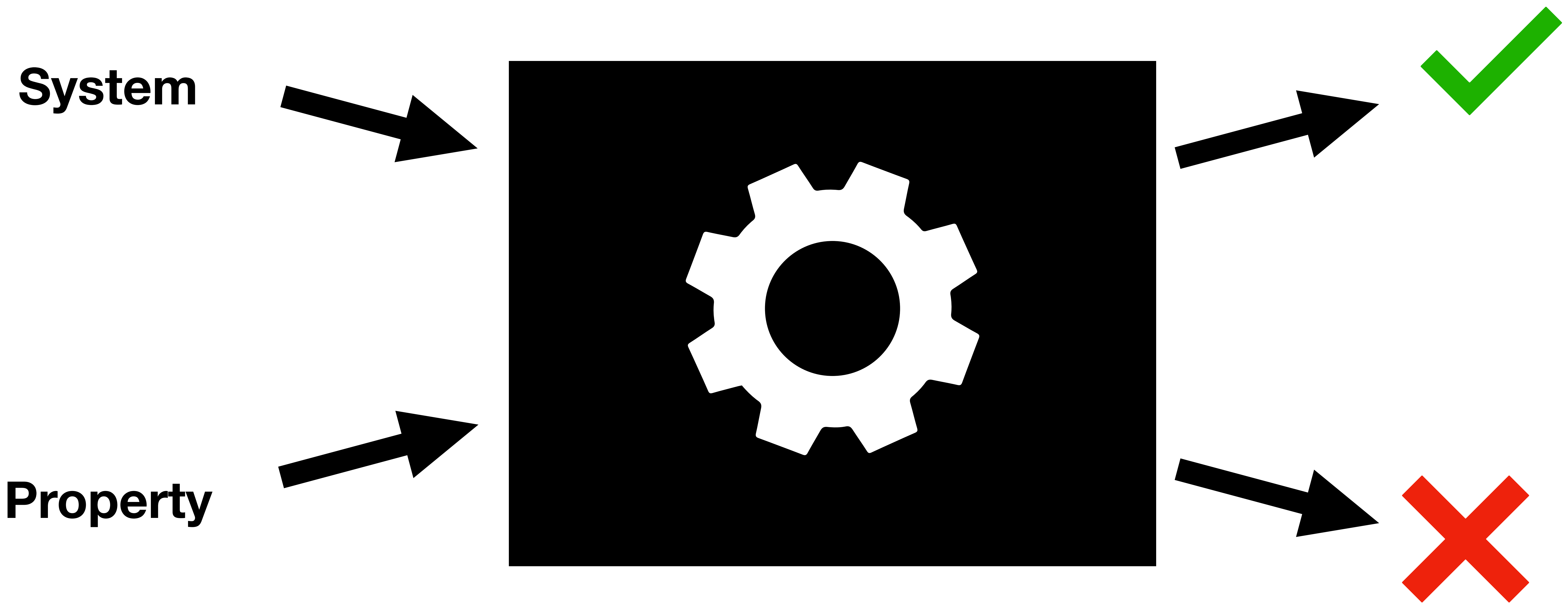
AST, but not PAST



not AST

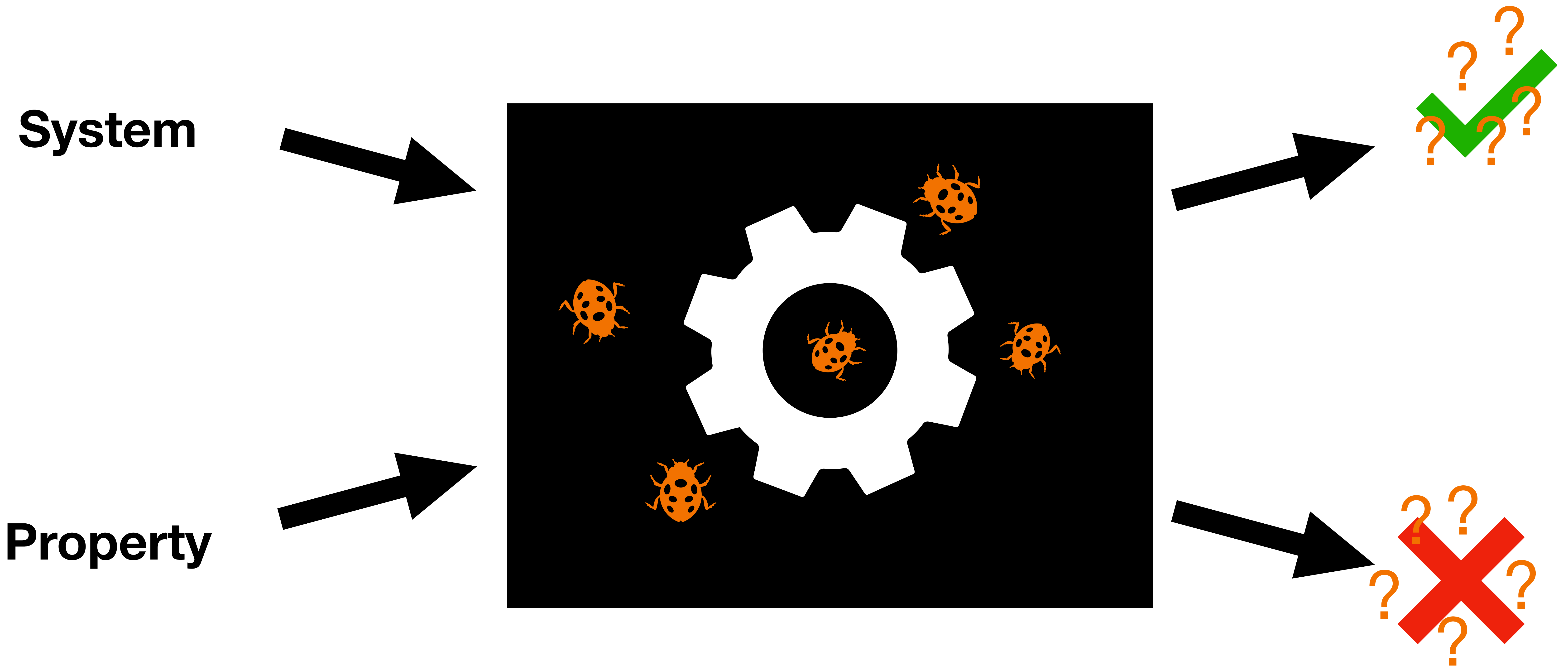
All decidable in PSPACE by reduction to $\exists\mathbb{R}$ [Esparza et al. LICS ’04 + ’05]

Do you trust your verification tool?



Do you trust your verification tool?

Do you trust your verification tool?



Main Result: Certificates for PAST

A pPDA Δ terminates with probability 1 in finite expected runtime (PAST)

$$\iff$$

Main Result: Certificates for PAST

A pPDA Δ terminates with probability 1 in finite expected runtime (PAST)

$$\Longleftrightarrow$$

there exist **rational** vectors $\overrightarrow{u} \in \mathbb{Q}^n_{\geq 0}$, $\vec{r} \in \mathbb{Q}^m_{\geq 0}$ such that

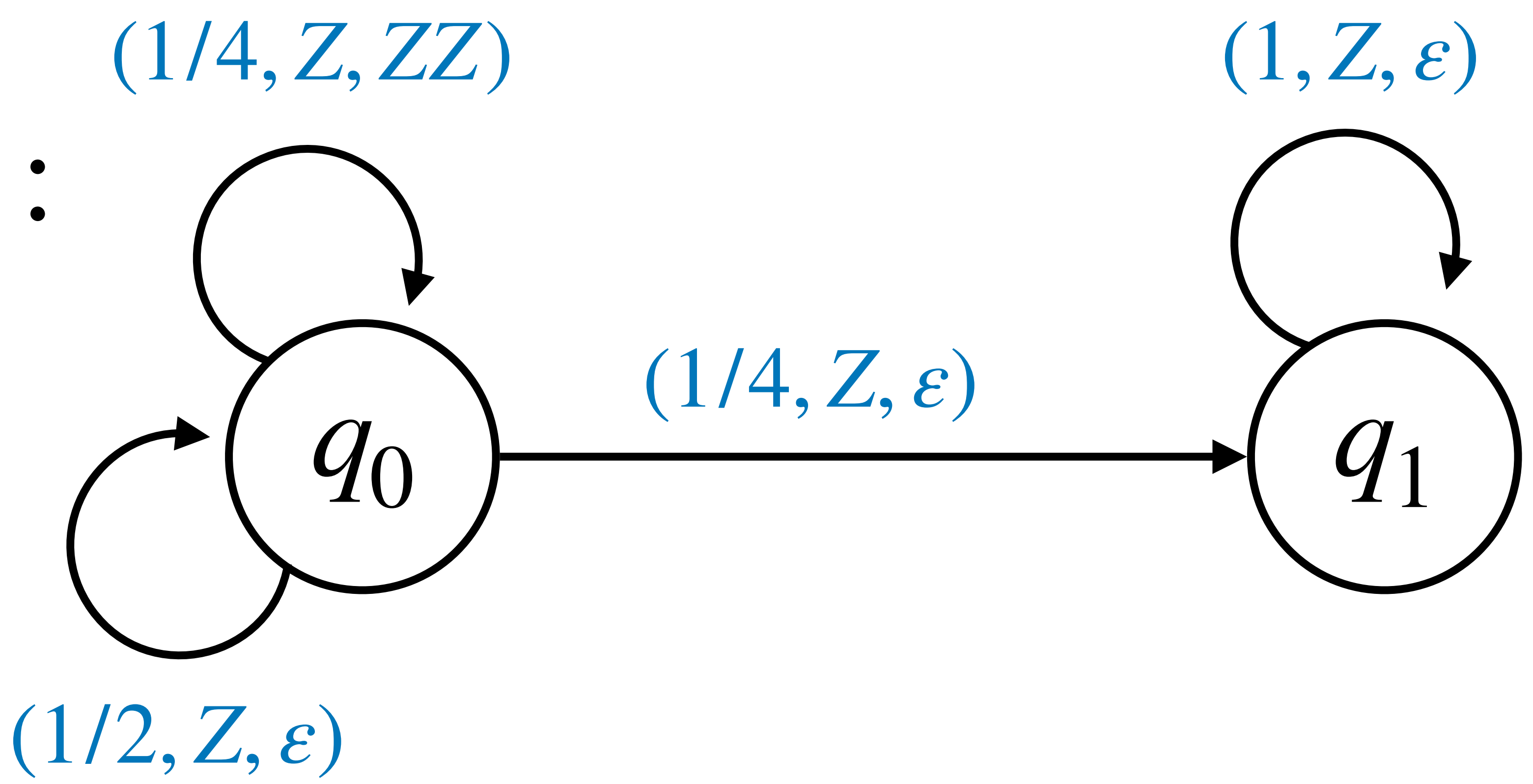
(1) $\vec{f}_\Delta(\overrightarrow{u}) \leq \overrightarrow{u}$

(2) $M_\Delta(\overrightarrow{u})\vec{r} + \overrightarrow{1} \leq \vec{r}$

where $\vec{f}_\Delta \in \mathbb{Q}_{\geq 0}[x_1, \ldots, x_n]^n$ and $M_\Delta \in \mathbb{Q}_{\geq 0}[x_1, \ldots, x_n]^{m \times m}$ can be constructed in polynomial time in the size of Δ.

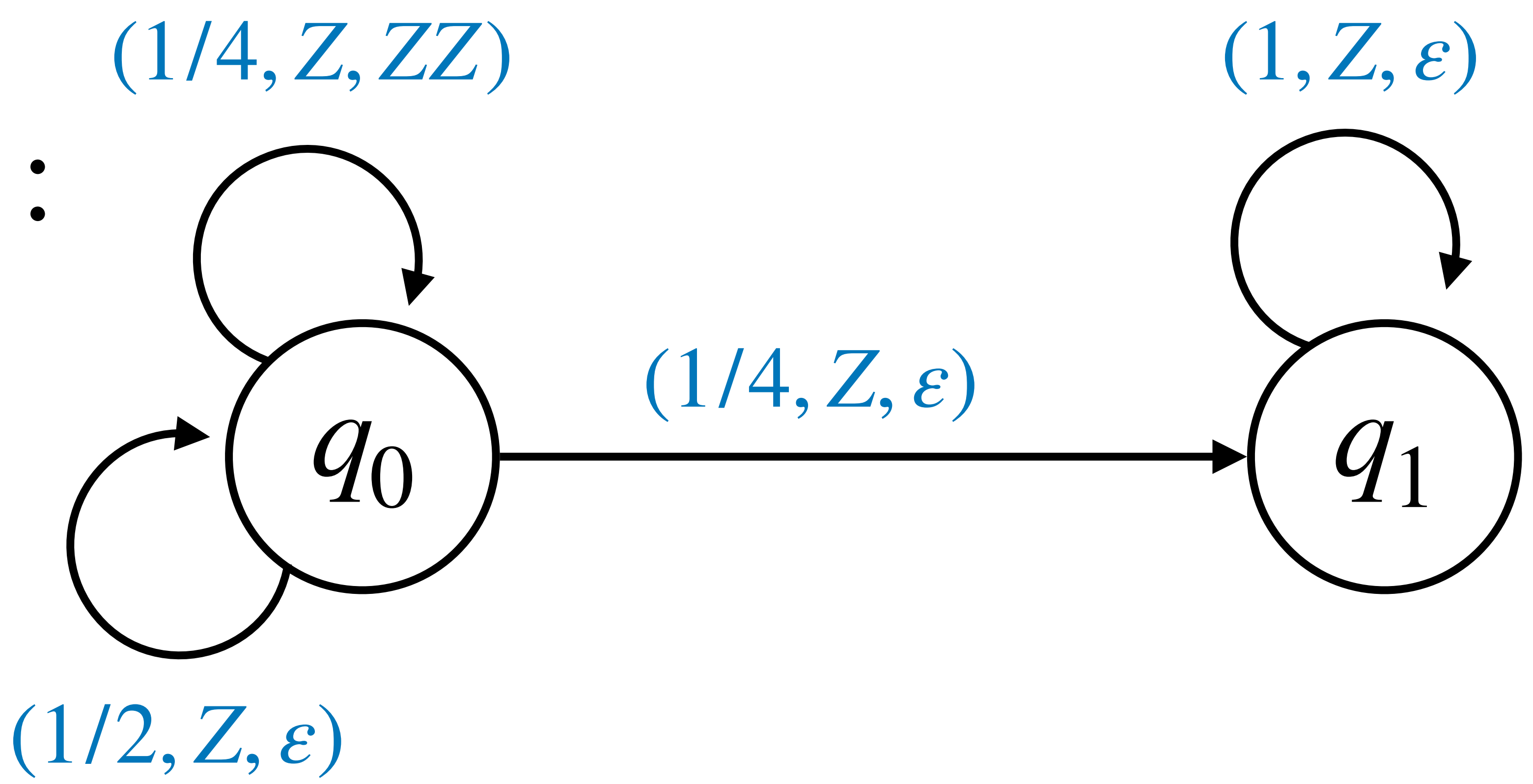
Certifying PAST — Concrete Example

$\Delta :$



Certifying PAST — Concrete Example

Δ :



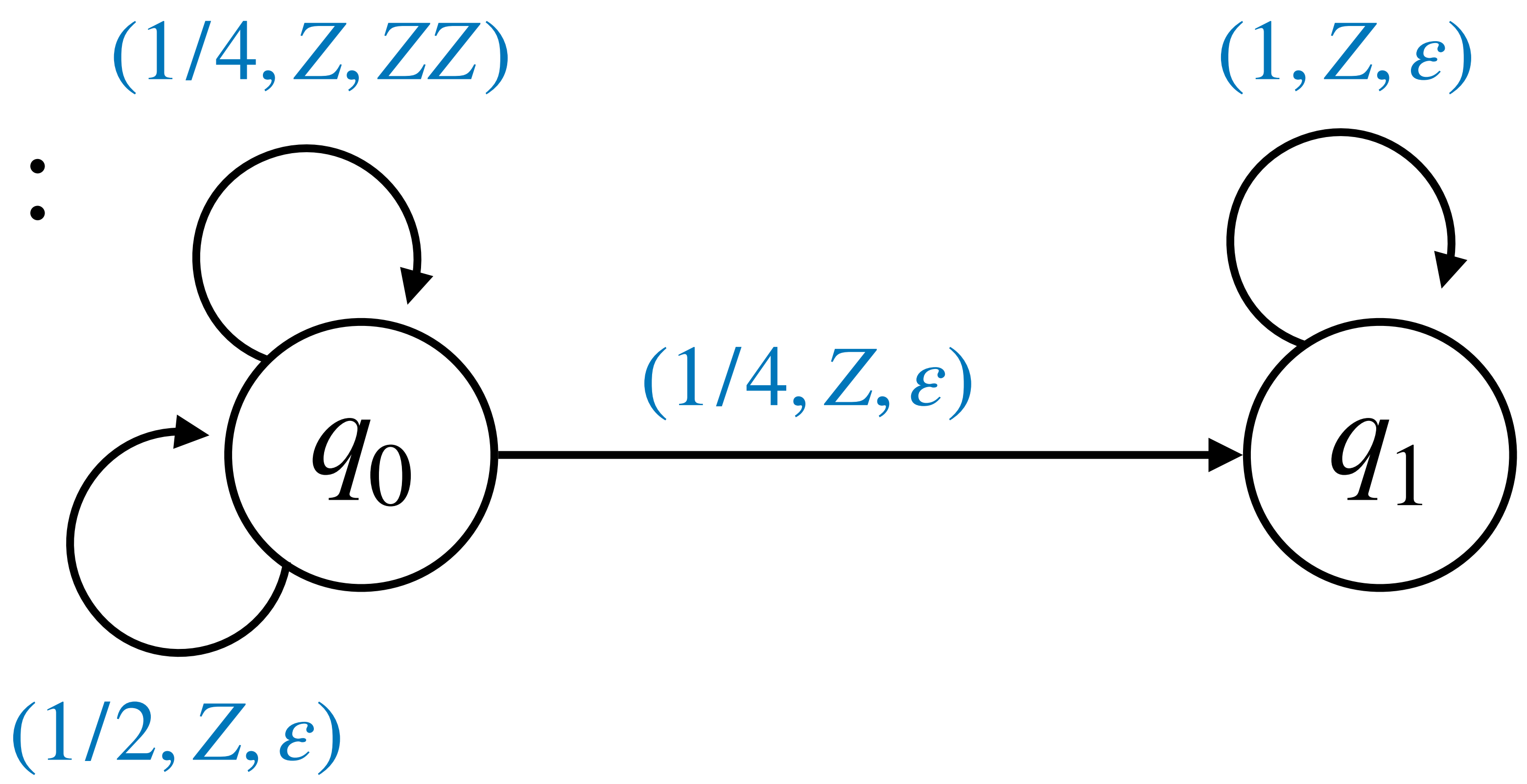
Read off from Δ:

$$\vec{f}_\Delta = \begin{pmatrix} \frac{1}{4}x_0^2 + \frac{1}{2} \\ \frac{1}{4}x_0x_1 + \frac{1}{4}x_1 + \frac{1}{4} \end{pmatrix}$$

$$M_\Delta = \begin{pmatrix} \frac{1}{4} + x_0 & \frac{1}{4} + x_1 \\ 0 & 0 \end{pmatrix}$$

Certifying PAST — Concrete Example

Δ :



Certificate: $\vec{u} = \begin{pmatrix} \frac{3}{5} \\ \frac{1}{2} \end{pmatrix}, \vec{r} = \begin{pmatrix} \frac{45}{14} \\ 1 \end{pmatrix}$

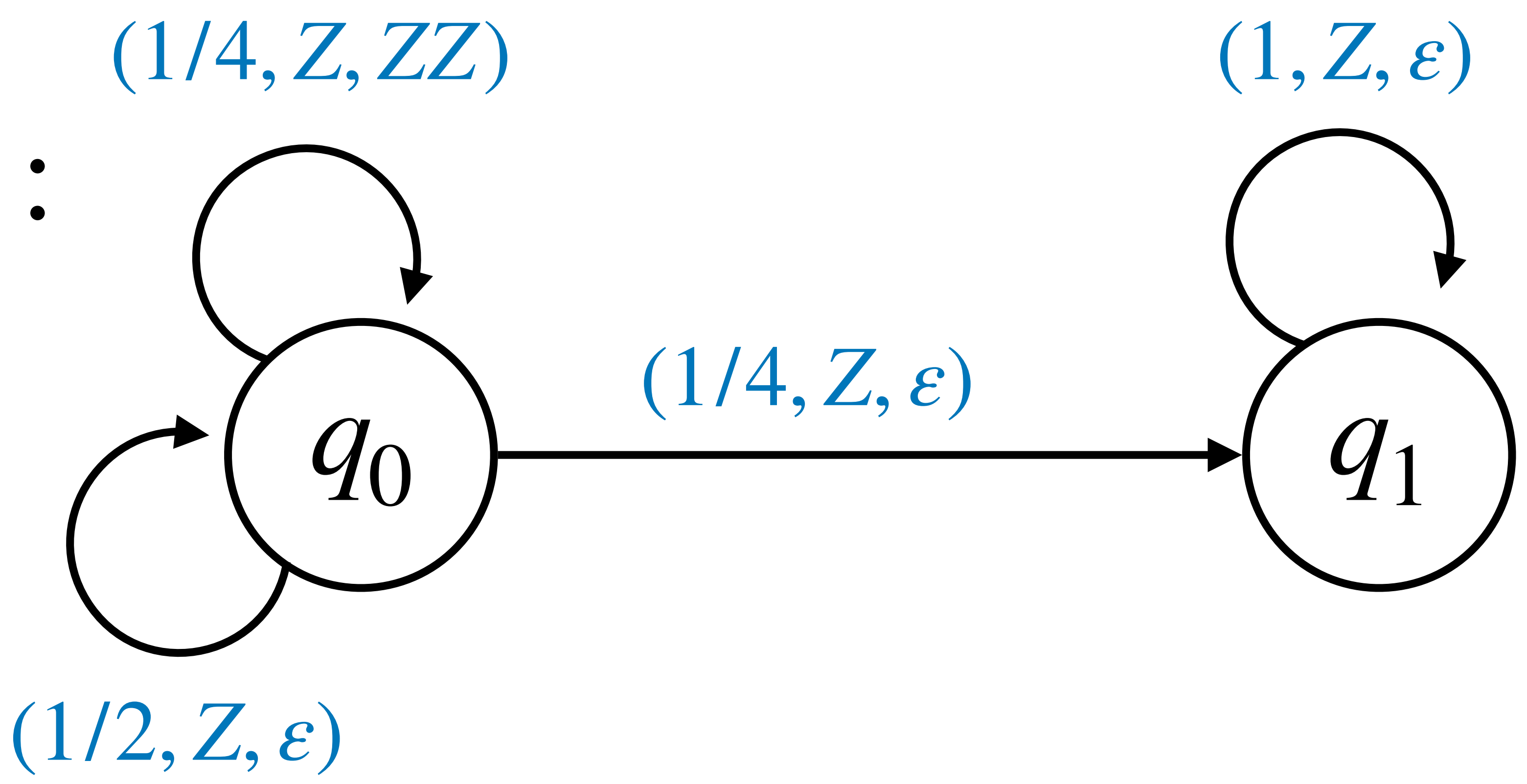
Read off from Δ:

$$\vec{f}_\Delta = \begin{pmatrix} \frac{1}{4}x_0^2 + \frac{1}{2} \\ \frac{1}{4}x_0x_1 + \frac{1}{4}x_1 + \frac{1}{4} \end{pmatrix}$$

$$M_\Delta = \begin{pmatrix} \frac{1}{4} + x_0 & \frac{1}{4} + x_1 \\ 0 & 0 \end{pmatrix}$$

Certifying PAST — Concrete Example

Δ :



Certificate: $\vec{u} = \begin{pmatrix} \frac{3}{5} \\ \frac{1}{2} \end{pmatrix}, \vec{r} = \begin{pmatrix} \frac{45}{14} \\ 1 \end{pmatrix}$

Check:

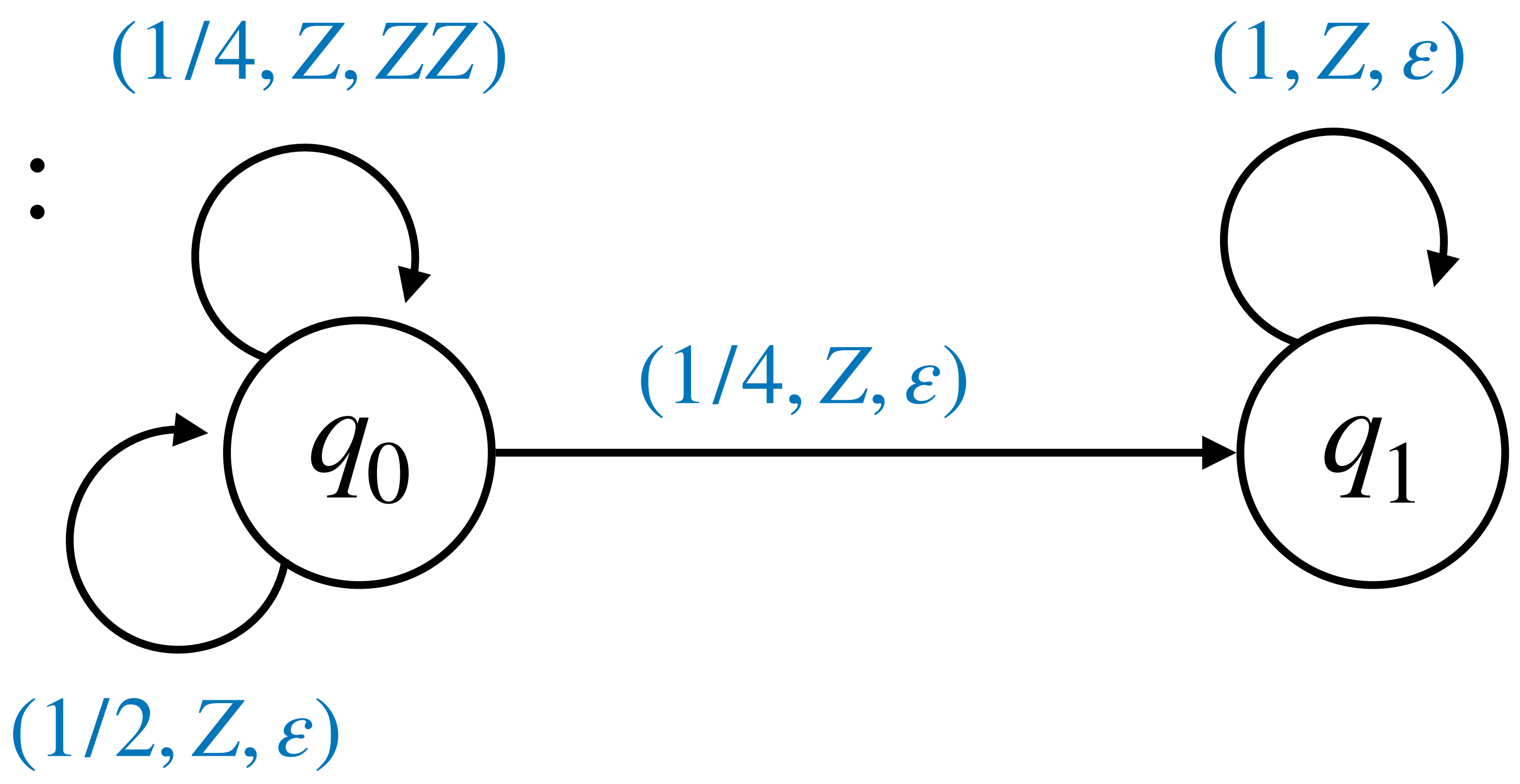
Read off from Δ:

$$\vec{f}_\Delta = \begin{pmatrix} \frac{1}{4}x_0^2 + \frac{1}{2} \\ \frac{1}{4}x_0x_1 + \frac{1}{4}x_1 + \frac{1}{4} \end{pmatrix}$$

$$M_\Delta = \begin{pmatrix} \frac{1}{4} + x_0 & \frac{1}{4} + x_1 \\ 0 & 0 \end{pmatrix}$$

Certifying PAST — Concrete Example

Δ :



Read off from Δ:

$$\vec{f}_\Delta = \begin{pmatrix} \frac{1}{4}x_0^2 + \frac{1}{2} \\ \frac{1}{4}x_0 x_1 + \frac{1}{4}x_1 + \frac{1}{4} \end{pmatrix}$$

$$M_\Delta = \begin{pmatrix} \frac{1}{4} + x_0 & \frac{1}{4} + x_1 \\ 0 & 0 \end{pmatrix}$$

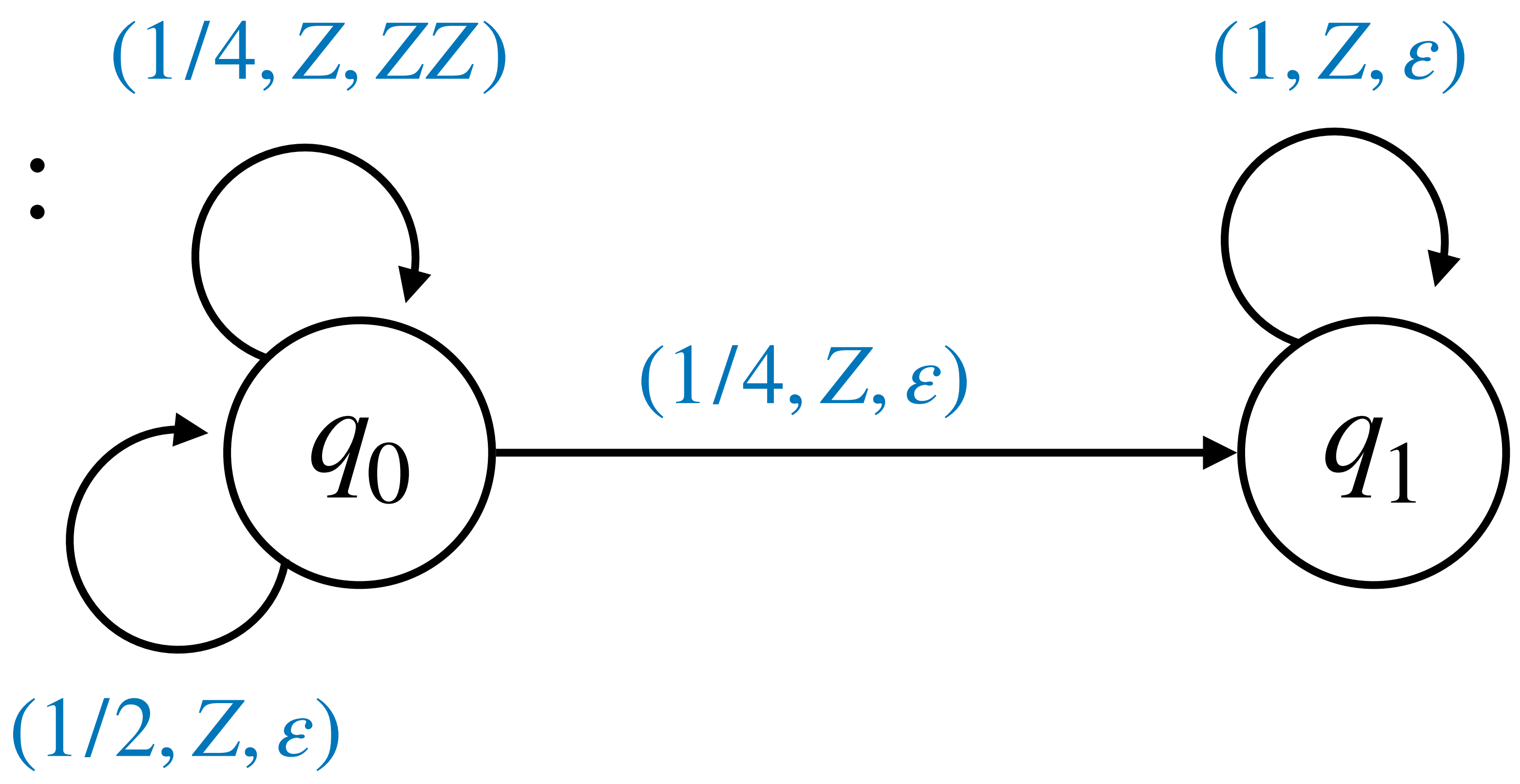
Certificate: $\vec{u} = \begin{pmatrix} \frac{3}{5} \\ \frac{1}{2} \end{pmatrix}, \vec{r} = \begin{pmatrix} \frac{45}{14} \\ 1 \end{pmatrix}$

Check:

(1) $\vec{f}_\Delta(\vec{u}) = \begin{pmatrix} \frac{1}{4} \cdot (\frac{3}{5})^2 + \frac{1}{2} \\ \frac{1}{4} \cdot \frac{3}{5} \cdot \frac{1}{2} + \frac{1}{4} \cdot \frac{1}{2} + \frac{1}{4} \end{pmatrix} = \begin{pmatrix} \frac{59}{100} \\ \frac{9}{20} \end{pmatrix} \leq \begin{pmatrix} \frac{3}{5} \\ \frac{1}{2} \end{pmatrix} = \vec{u}$

Certifying PAST — Concrete Example

Δ :



Read off from Δ:

$$\vec{f}_\Delta = \begin{pmatrix} \frac{1}{4}x_0^2 + \frac{1}{2} \\ \frac{1}{4}x_0x_1 + \frac{1}{4}x_1 + \frac{1}{4} \end{pmatrix}$$

$$M_\Delta = \begin{pmatrix} \frac{1}{4} + x_0 & \frac{1}{4} + x_1 \\ 0 & 0 \end{pmatrix}$$

Certificate: $\vec{u} = \begin{pmatrix} \frac{3}{5} \\ \frac{1}{2} \end{pmatrix}, \vec{r} = \begin{pmatrix} \frac{45}{14} \\ 1 \end{pmatrix}$

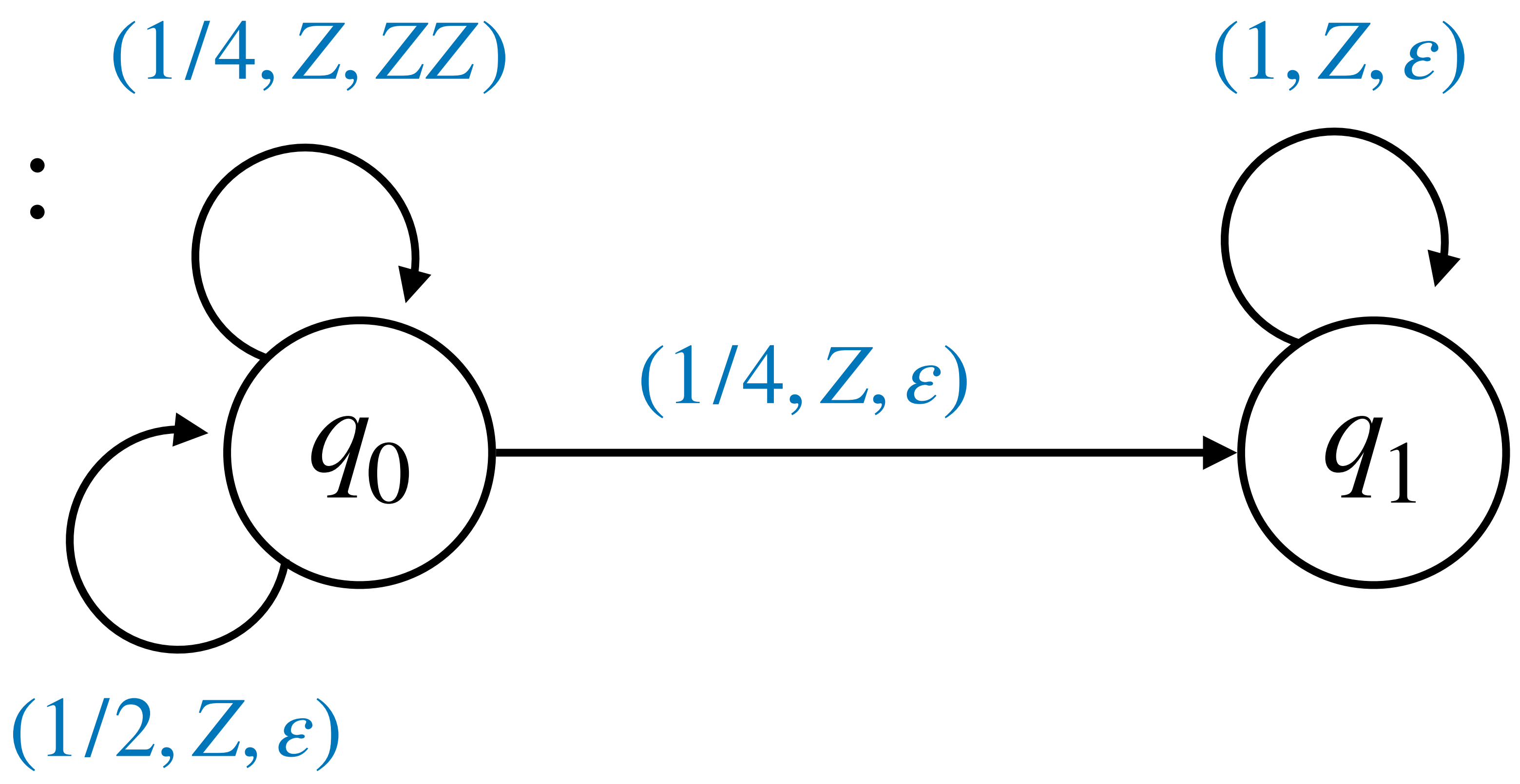
Check:

(1) $\vec{f}_\Delta(\vec{u}) = \begin{pmatrix} \frac{1}{4} \cdot (\frac{3}{5})^2 + \frac{1}{2} \\ \frac{1}{4} \cdot \frac{3}{5} \cdot \frac{1}{2} + \frac{1}{4} \cdot \frac{1}{2} + \frac{1}{4} \end{pmatrix} = \begin{pmatrix} \frac{59}{100} \\ \frac{9}{20} \end{pmatrix} \leq \begin{pmatrix} \frac{3}{5} \\ \frac{1}{2} \end{pmatrix} = \vec{u}$

(2) $M_\Delta(\vec{u})\vec{r} + \vec{1} = \begin{pmatrix} \frac{1}{4} + \frac{3}{5} & \frac{1}{4} + \frac{1}{2} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{45}{14} \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{251}{56} \\ 1 \end{pmatrix} \leq \vec{r}$

Certifying PAST — Concrete Example

Δ :



Read off from Δ:

$$\vec{f}_\Delta = \begin{pmatrix} \frac{1}{4}x_0^2 + \frac{1}{2} \\ \frac{1}{4}x_0x_1 + \frac{1}{4}x_1 + \frac{1}{4} \end{pmatrix}$$

$$M_\Delta = \begin{pmatrix} \frac{1}{4} + x_0 & \frac{1}{4} + x_1 \\ 0 & 0 \end{pmatrix}$$

Certificate: $\vec{u} = \begin{pmatrix} \frac{3}{5} \\ \frac{1}{2} \end{pmatrix}, \vec{r} = \begin{pmatrix} \frac{45}{14} \\ 1 \end{pmatrix}$

Check:

(1) $\vec{f}_\Delta(\vec{u}) = \begin{pmatrix} \frac{1}{4} \cdot (\frac{3}{5})^2 + \frac{1}{2} \\ \frac{1}{4} \cdot \frac{3}{5} \cdot \frac{1}{2} + \frac{1}{4} \cdot \frac{1}{2} + \frac{1}{4} \end{pmatrix} = \begin{pmatrix} \frac{59}{100} \\ \frac{9}{20} \end{pmatrix} \leq \begin{pmatrix} \frac{3}{5} \\ \frac{1}{2} \end{pmatrix} = \vec{u}$

(2) $M_\Delta(\vec{u})\vec{r} + \vec{1} = \begin{pmatrix} \frac{1}{4} + \frac{3}{5} & \frac{1}{4} + \frac{1}{2} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{45}{14} \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{251}{56} \\ 1 \end{pmatrix} \leq \vec{r}$

This proves PAST (soundness).

For every PAST pPDA we can find such a certificate (completeness).

Main Result: Certificates for PAST

A pPDA Δ terminates with probability 1 in finite expected runtime (PAST)

$\Longleftarrow$ (soundness)

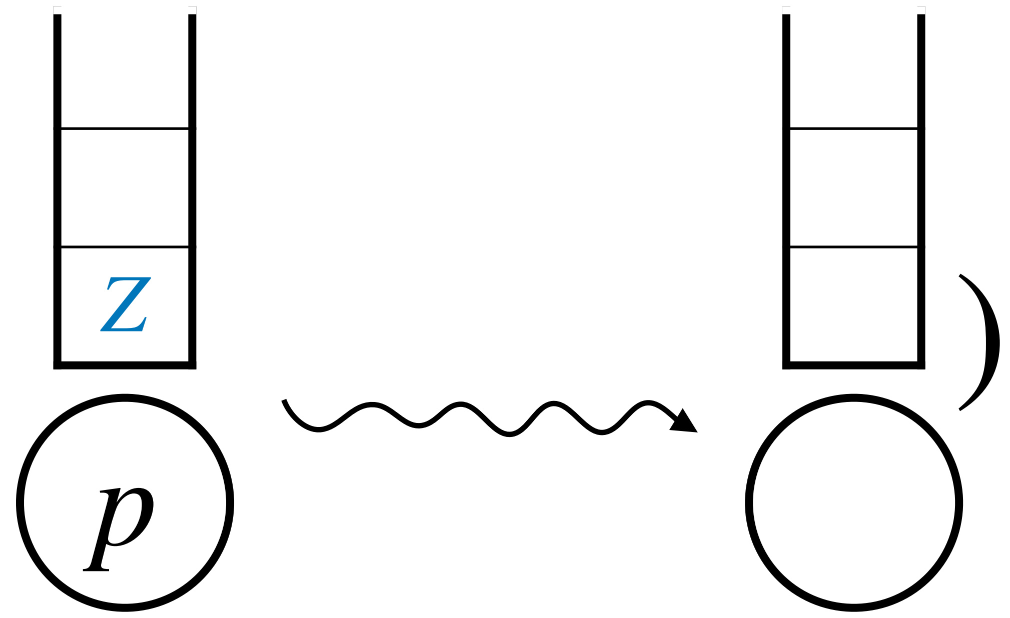
there exist **rational** vectors $\vec{u} \in \mathbb{Q}^n_{\geq 0}$, $\vec{r} \in \mathbb{Q}^m_{\geq 0}$ such that

(1) $\vec{f}_\Delta(\vec{u}) \leq \vec{u}$

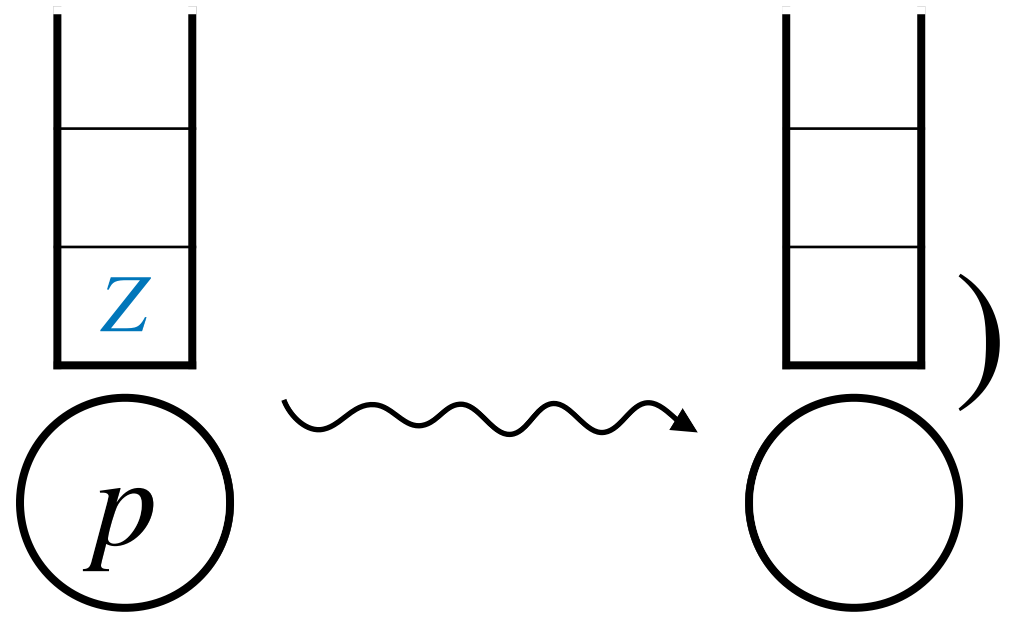
(2) $M_\Delta(\vec{u})\vec{r} + \vec{1} \leq \vec{r}$

where $\vec{f}_\Delta \in \mathbb{Q}_{\geq 0}[x_1, \ldots, x_n]^n$ and $M_\Delta \in \mathbb{Q}_{\geq 0}[x_1, \ldots, x_n]^{m \times m}$ can be constructed in polynomial time in the size of Δ.

Characterizing the Expected Runtime (*ert*)

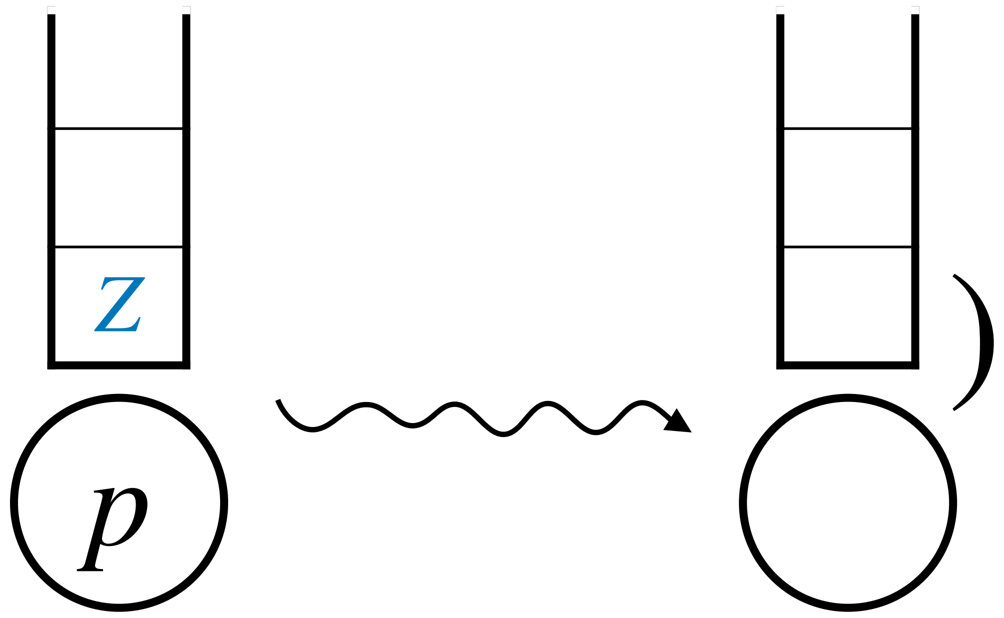
$ert[pZ] = E[len($  $)]$

Characterizing the Expected Runtime (*ert*)

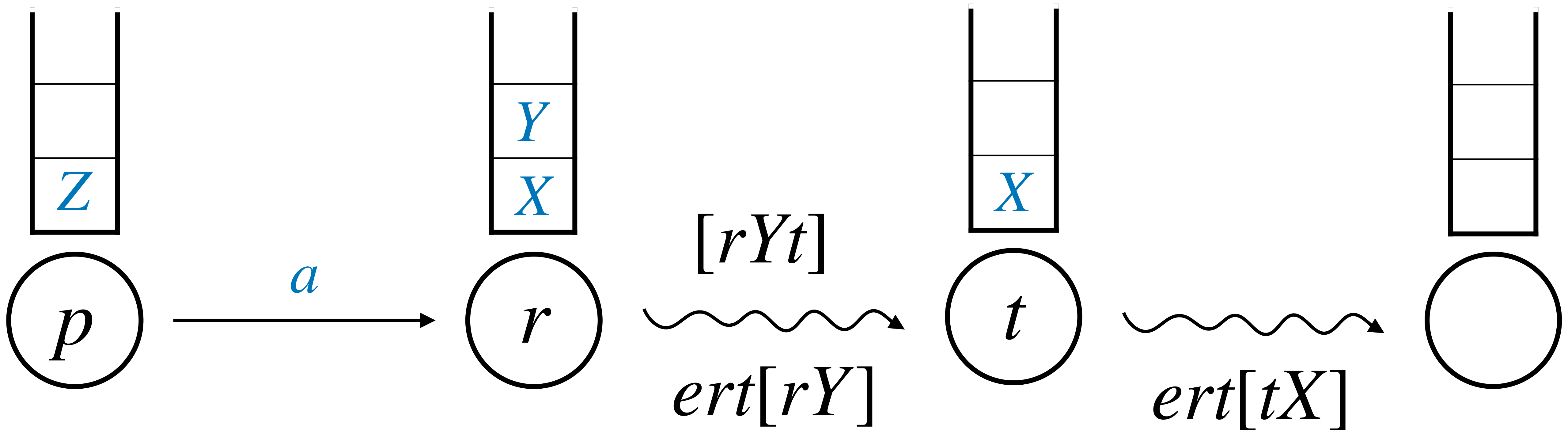
$ert[pZ] = E[len($  $)]$

$$ert[pZ] = 1 + \sum_{pZ \xrightarrow{a} rY} a \cdot ert[rY] + \sum_{pZ \xrightarrow{a} rYX} a \cdot \left(ert[rY] + \sum_{t} [rYt] \cdot ert[tX]\right)$$

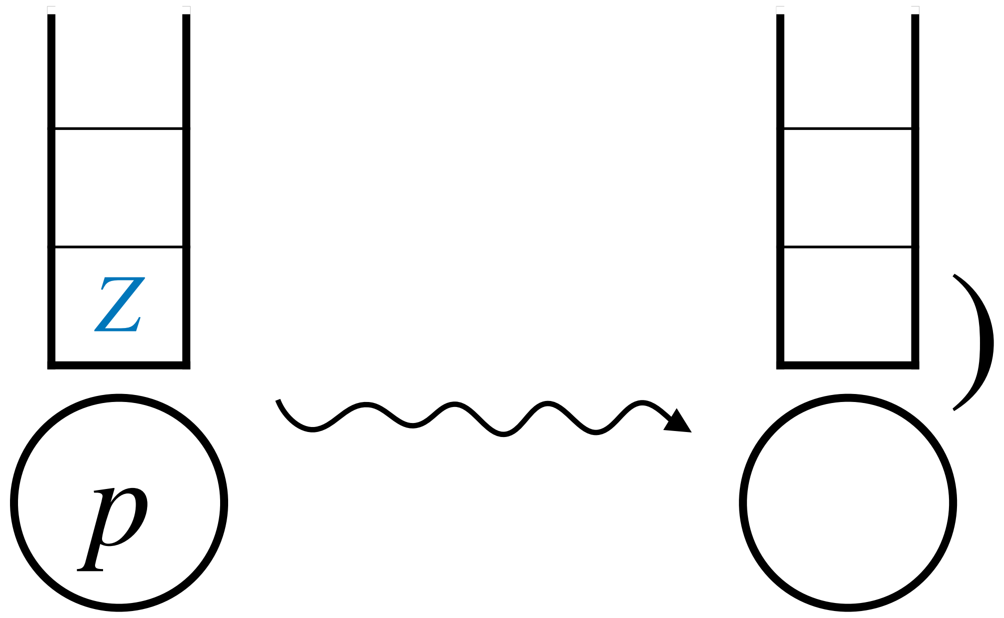
Characterizing the Expected Runtime (ert)

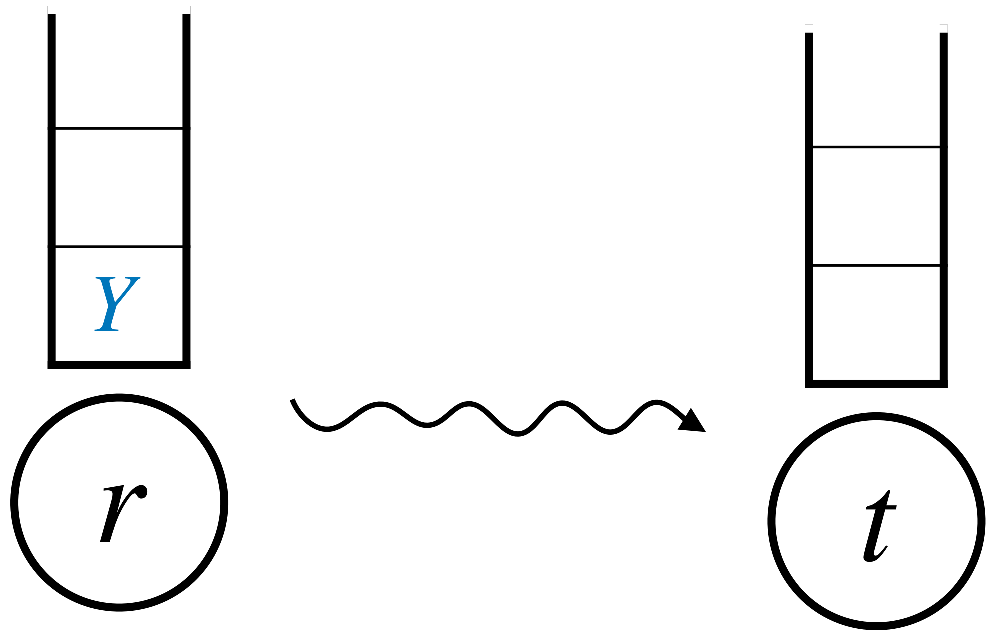
$ert[pZ] = E[len($  $)]$

$$ert[pZ] = 1 + \sum_{pZ \xrightarrow{a} rY} a \cdot ert[rY] + \sum_{pZ \xrightarrow{a} rYX} a \cdot (ert[rY] + \sum_{t} [rYt] \cdot ert[tX])$$

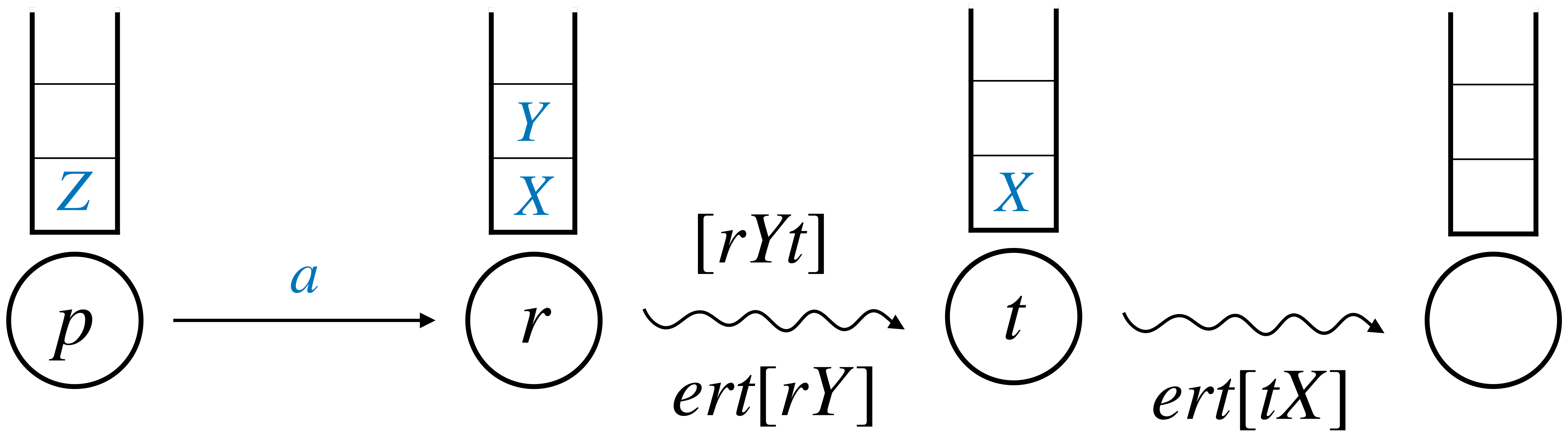


Characterizing the Expected Runtime (*ert*)

$ert[pZ] = E[len($  $)]$

$[rYt] = Pr[$  $]$

$$ert[pZ] = 1 + \sum_{pZ \xrightarrow{a} rY} a \cdot ert[rY] + \sum_{pZ \xrightarrow{a} rYX} a \cdot \left(ert[rY] + \sum_{t} [rYt] \cdot ert[tX]\right)$$



Characterizing the Expected Runtime

Theorem
The linear equation system

$$\forall p, Z \qquad ert[pZ] = 1 + \sum_{pZ \xrightarrow{a} rY} a \cdot ert[rY] + \sum_{pZ \xrightarrow{a} rYX} a \cdot \left(ert[rY] + \sum_{t} [rYt] \cdot ert[tX]\right)$$

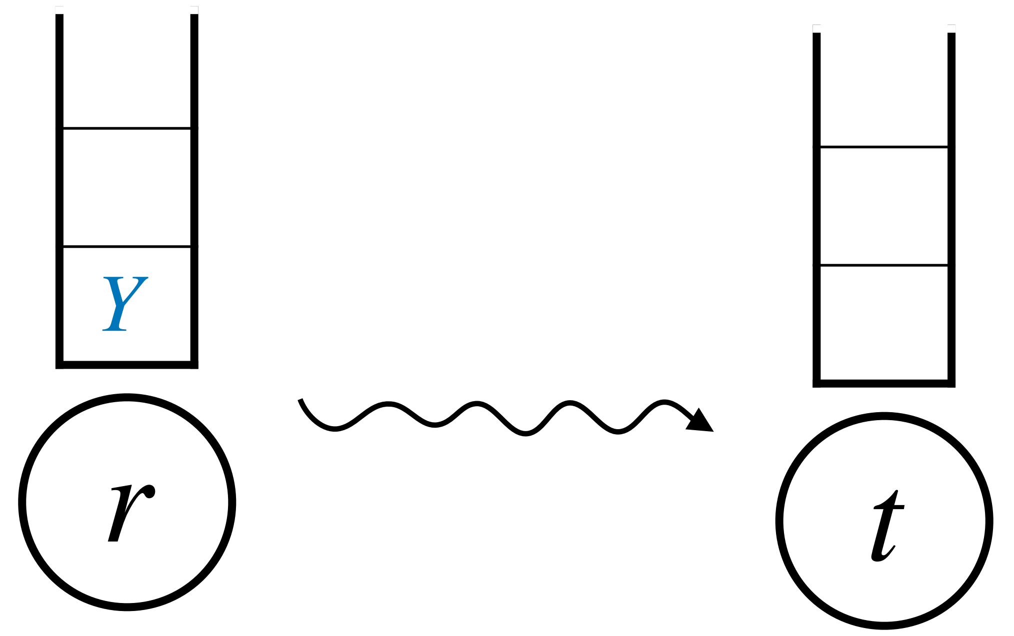
has a solution in $\mathbb{R}_{\geq 0}$ iff the pPDA is PAST.

Characterizing the Expected Runtime

Theorem
The linear equation system

$$\forall p, Z \qquad ert[pZ] = 1 + \sum_{pZ \xrightarrow{a} rY} a \cdot ert[rY] + \sum_{pZ \xrightarrow{a} rYX} a \cdot \left(ert[rY] + \sum_{t} [rYt] \cdot ert[tX]\right)$$

has a solution in $\mathbb{R}_{\geq 0}$ iff the pPDA is PAST.

$[rYt] = Pr[$  $]$

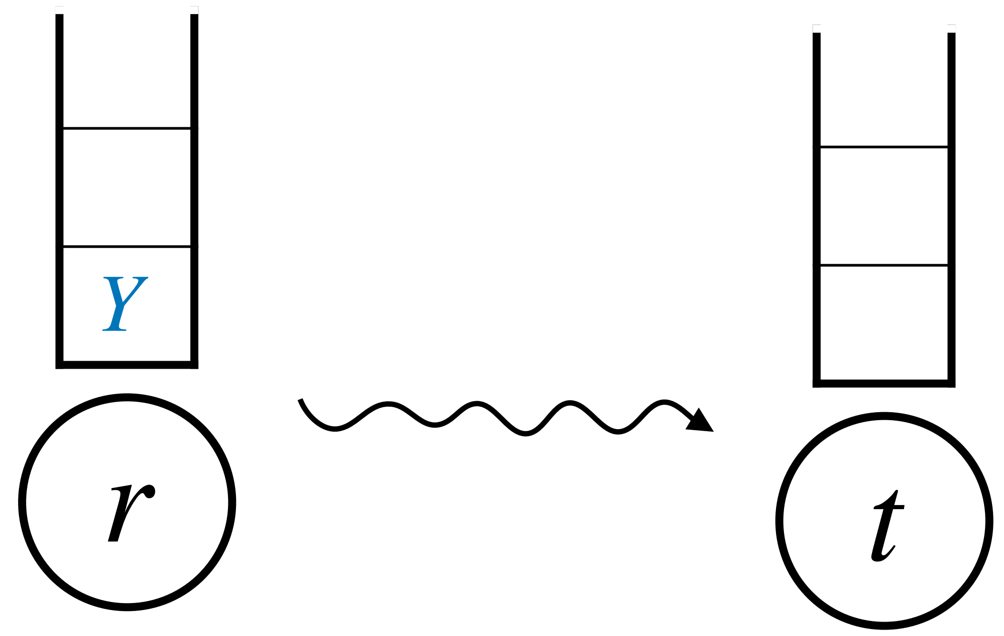
Characterizing the Expected Runtime

Matrix $M_\Delta(\overrightarrow{x})$ from certificate condition

Theorem
The linear equation system

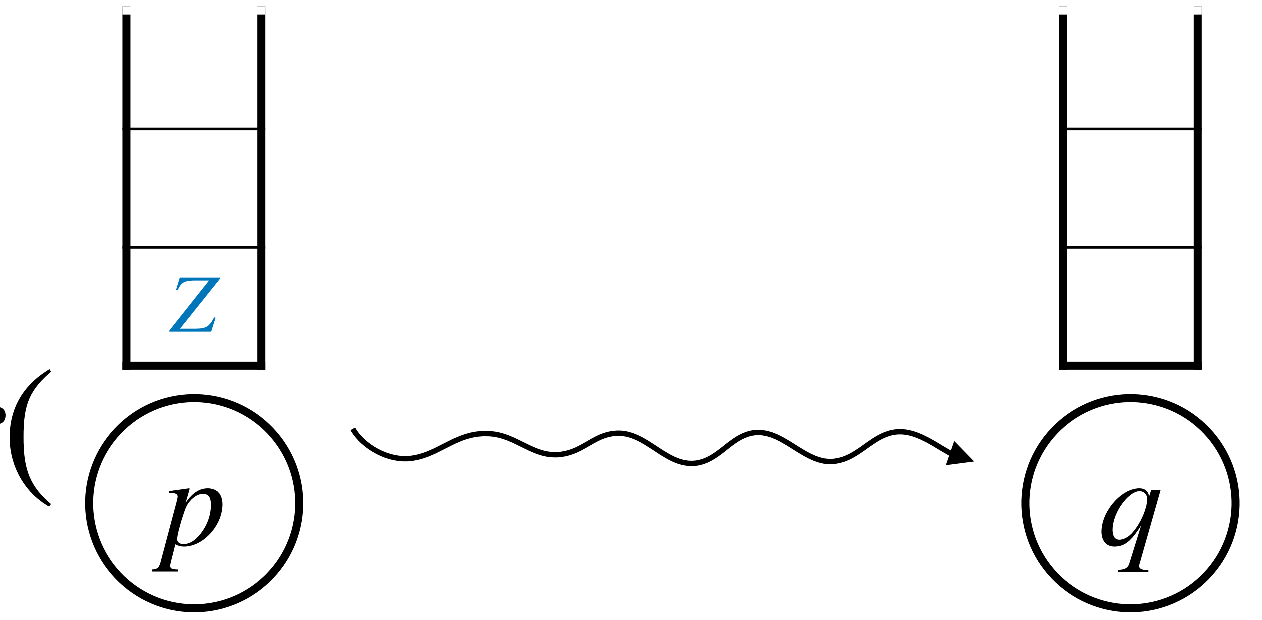
$$\forall p, Z \qquad ert[pZ] = 1 + \sum_{pZ \xrightarrow{a} rY} a \cdot ert[rY] + \sum_{pZ \xrightarrow{a} rYX} a \cdot \left(ert[rY] + \sum_{t} [rYt] \cdot ert[tX]\right)$$

has a solution in $\mathbb{R}_{\geq 0}$ iff the pPDA is PAST.

$[rYt] = Pr[$  $]$

pPDA ➡ Polynomial Equations

[Esparza et al. ’04]

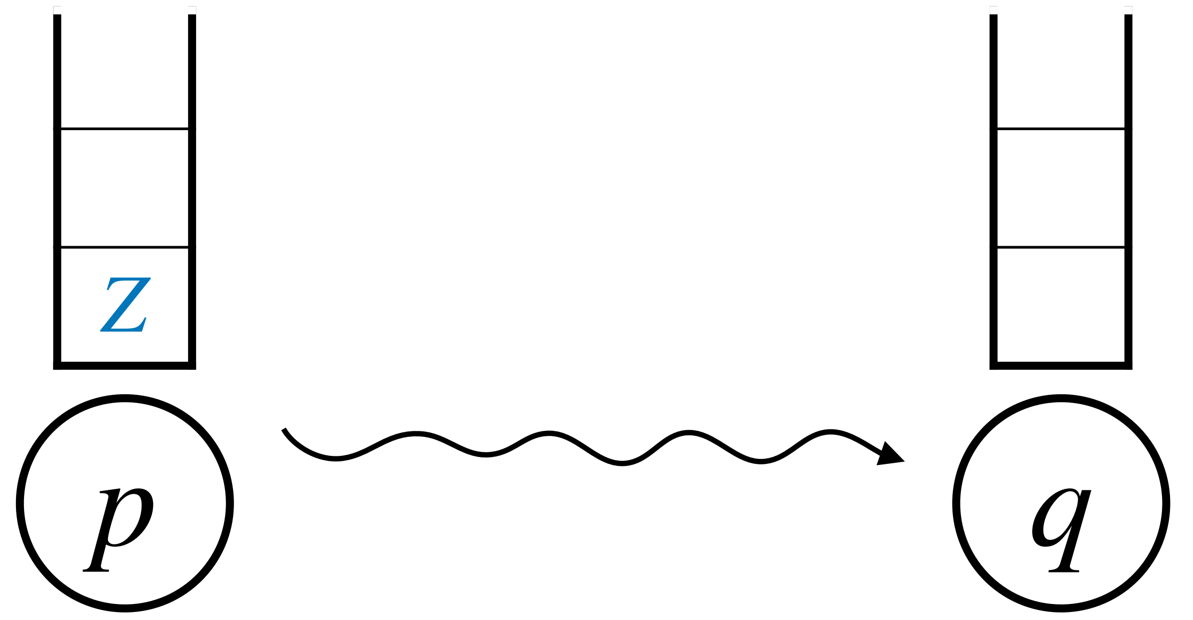
$[pZq] = Pr($  $)$

Probabilities $[pZq]$ are least solution ≥ 0 of

$$[pZq] \;=\; \sum_{pZ \xrightarrow{a} qY} a \cdot [rYq] + \sum_{pZ \xrightarrow{a} rXY} \sum_{t \in Q} a \cdot [rYt] \cdot [tXq] + \sum_{pZ \xrightarrow{a} q\epsilon} a$$

pPDA ➞ Polynomial Equations

[Esparza et al. ’04]

$[pZq] = Pr($  $)$

Probabilities $[pZq]$ are least solution ≥ 0 of

$$[pZq] \;=\; \sum_{pZ\xrightarrow{a}qY} a\cdot[rYq] + \sum_{pZ\xrightarrow{a}rXY}\;\sum_{t\in Q} a\cdot[rYt]\cdot[tXq] + \sum_{pZ\xrightarrow{a}q\epsilon} a$$

Polynomials $\vec{f}_\Delta$ from certificate condition

Certificates for Upper Bounds on [pZq]

$\vec{f} \in \mathbb{R}_{\geq 0}[x_1, \ldots, x_n]^n$ is a monotonic function $\vec{f} \colon \mathbb{R}^n_{\geq 0} \to \mathbb{R}^n_{\geq 0}$

Certificates for Upper Bounds on [pZq]

$\vec{f} \in \mathbb{R}_{\geq 0}[x_1, \ldots, x_n]^n$ is a monotonic function $\vec{f} \colon \mathbb{R}^n_{\geq 0} \to \mathbb{R}^n_{\geq 0}$

Lemma
For all $\overrightarrow{u} \in \mathbb{R}^n_{\geq 0}$: $\vec{f}(\overrightarrow{u}) \leq \overrightarrow{u} \implies \text{lfp}\, \vec{f} \leq \overrightarrow{u}$

Proof:
Knaster-Tarski fixed point theorem

Certificates for Upper Bounds on [pZq]

$\vec{f} \in \mathbb{R}_{\geq 0}[x_1, \dots, x_n]^n$ is a monotonic function $\vec{f}\colon \mathbb{R}^n_{\geq 0} \to \mathbb{R}^n_{\geq 0}$

least solution ≥ 0 of $\vec{x} = \vec{f}(\vec{x})$

Lemma

For all $\vec{u} \in \mathbb{R}^n_{\geq 0}$: $\quad \vec{f}(\vec{u}) \leq \vec{u} \implies \text{lfp}\, \vec{f} \leq \vec{u}$

Proof:

Knaster-Tarski fixed point theorem

Certificates for Upper Bounds on [pZq]

$\vec{f} \in \mathbb{R}_{\geq 0}[x_1, \ldots, x_n]^n$ is a monotonic function $\vec{f}\colon \mathbb{R}^n_{\geq 0} \to \mathbb{R}^n_{\geq 0}$

"inductive upper bound"

least solution ≥ 0 of $\vec{x} = \vec{f}(\vec{x})$

Lemma

For all $\vec{u} \in \mathbb{R}^n_{\geq 0}$: $\quad \vec{f}(\vec{u}) \leq \vec{u} \Longrightarrow \operatorname{lfp} \vec{f} \leq \vec{u}$

Proof:

Knaster-Tarski fixed point theorem

Main Result: Certificates for PAST

A pPDA Δ terminates with probability 1 in finite expected runtime (PAST)

$\Longleftarrow$ ✓

there exist **rational** vectors $\overrightarrow{u} \in \mathbb{Q}^n_{\geq 0}$, $\vec{r} \in \mathbb{Q}^m_{\geq 0}$ such that

(1) $\vec{f}_\Delta(\overrightarrow{u}) \leq \overrightarrow{u}$

(2) $M_\Delta(\overrightarrow{u})\vec{r} + \overrightarrow{1} \leq \vec{r}$

where $\vec{f}_\Delta \in \mathbb{Q}_{\geq 0}[x_1, \ldots, x_n]^n$ and $M_\Delta \in \mathbb{Q}_{\geq 0}[x_1, \ldots, x_n]^{m \times m}$ can be constructed in polynomial time in the size of Δ.

Main Result: Certificates for PAST

A pPDA Δ terminates with probability 1 in finite expected runtime (PAST)

$\Longrightarrow$ (completeness)

there exist **rational** vectors $\overrightarrow{u} \in \mathbb{Q}^n_{\geq 0}$, $\vec{r} \in \mathbb{Q}^m_{\geq 0}$ such that

(1) $\vec{f}_\Delta(\overrightarrow{u}) \leq \overrightarrow{u}$

(2) $M_\Delta(\overrightarrow{u})\vec{r} + \overrightarrow{1} \leq \vec{r}$

where $\vec{f}_\Delta \in \mathbb{Q}_{\geq 0}[x_1, \ldots, x_n]^n$ and $M_\Delta \in \mathbb{Q}_{\geq 0}[x_1, \ldots, x_n]^{m \times m}$ can be constructed in polynomial time in the size of Δ.

Main Result: Certificates for PAST

A pPDA Δ terminates with probability 1 in finite expected runtime (PAST)

$\Longrightarrow$ (completeness)

there exist **rational** vectors $\boxed{\vec{u} \in \mathbb{Q}^n_{\geq 0}}$, $\vec{r} \in \mathbb{Q}^m_{\geq 0}$ such that

$\boxed{\text{(1)}\ \ \vec{f}_\Delta(\vec{u}) \leq \vec{u}}$

(2) $M_\Delta(\vec{u})\vec{r} + \vec{1} \leq \vec{r}$

where $\vec{f}_\Delta \in \mathbb{Q}_{\geq 0}[x_1, \ldots, x_n]^n$ and $M_\Delta \in \mathbb{Q}_{\geq 0}[x_1, \ldots, x_n]^{m \times m}$ can be constructed in polynomial time in the size of Δ.

Summary

Summary

- Sound + complete certificates (“proof rule”) for PAST based on inductive upper bounds on lfp of polynomial system $\vec{f} \in \mathbb{R}_{\geq 0}[x_1, \ldots, x_n]^n$

Summary

- Sound + complete certificates ("proof rule") for PAST based on inductive upper bounds on lfp of polynomial system $\vec{f} \in \mathbb{R}_{\geq 0}[x_1, \ldots, x_n]^n$
  - Algorithm to compute such bounds in [W. & Katoen, TACAS '23]

Summary

- Sound + complete certificates ("proof rule") for PAST based on inductive upper bounds on lfp of polynomial system $\vec{f} \in \mathbb{R}_{\geq 0}[x_1, \ldots, x_n]^n$
  - Algorithm to compute such bounds in [W. & Katoen, TACAS '23]
- In paper: Certificates for lower bounds on $[pZq]$, bounds on certificate size

Summary

- Sound + complete certificates ("proof rule") for PAST based on inductive upper bounds on lfp of polynomial system $\vec{f} \in \mathbb{R}_{\geq 0}[x_1, \ldots, x_n]^n$
  - Algorithm to compute such bounds in [W. & Katoen, TACAS '23]
- In paper: Certificates for lower bounds on $[pZq]$, bounds on certificate size
- Future work: Prove NP membership for restricted versions of pPDA

Summary

- Sound + complete certificates ("proof rule") for PAST based on inductive upper bounds on lfp of polynomial system $\vec{f} \in \mathbb{R}_{\geq 0}[x_1, \ldots, x_n]^n$
  - Algorithm to compute such bounds in [W. & Katoen, TACAS '23]
- In paper: Certificates for lower bounds on $[pZq]$, bounds on certificate size
- Future work: Prove NP membership for restricted versions of pPDA

Thank you! Questions?