Abstract Refinement for Emptiness Checking of Alternating Data Automata

Radu IOSIF & Xiao XU

VERIMAG – CNRS / Université de Grenoble Alpes, France

Verification Problems

Alternating Data Automata (ADA)

Interpolation

Emptiness Checking of ADA

Verification Problems
Introduction

$$\{P\} \quad C \quad \{Q\}$$

Verification Problems

Introduction

$$\{P\} \quad C \quad \{Q\}$$

- $P \;\Rightarrow\; WP\,(C, Q)$ Logical Entailment

Weakest Precondition

Verification Problems

Introduction

$$\{P\} \quad C \quad \{Q\}$$

- $P \Rightarrow WP(C, Q)$ Logical Entailment

A_P $A_{WP(C, Q)}$ MSO(words, trees)

Verification Problems
Introduction

$\{P\} \quad C \quad \{Q\}$

- $P \Rightarrow WP(C, Q)$ — Logical Entailment

$A_P \subseteq A_{WP(C, Q)}$ — Inclusion of Automata

Verification Problems

Introduction

$\{P\} \quad C \quad \{Q\}$

- $P \quad \Rightarrow \quad WP\,(C, Q)$ Logical Entailment

$\updownarrow \qquad\qquad \updownarrow \qquad\qquad \updownarrow$

$A_P \quad \subseteq \quad A_{WP\,(C,\,Q)}$ Inclusion of Automata

Infinite Alphabet?

Verification Problems

Introduction

$$\{P\} \quad C \quad \{Q\}$$

- $P \Rightarrow WP(C, Q)$ — Logical Entailment

$$A_P \subseteq A_{WP(C, Q)}$$ — Inclusion of Automata

Data Automata

Verification Problems
Introduction

$$\{P\} \quad C \quad \{Q\}$$

- $P \;\Rightarrow\; WP(C, Q)$ — Logical Entailment

$$A_P \subseteq A_{WP(C,Q)}$$ — Inclusion of Automata

(Data Automata)

$$A_P \cap \overline{A_{WP(C,Q)}} = \emptyset$$

Verification Problems

Introduction

$$\{P\} \quad C \quad \{Q\}$$

- $P \;\; \Rightarrow \;\; WP\,(C, Q)$ — Logical Entailment

$\updownarrow$

$A_P \;\subseteq\; A_{WP\,(C,\,Q)}$ — Inclusion of Automata

$\updownarrow$ (Data Automata)

$A_P \cap \overline{A_{WP\,(C,\,Q)}} = \emptyset$ — Emptiness of Alternating Automata (Alternating Data Automata)

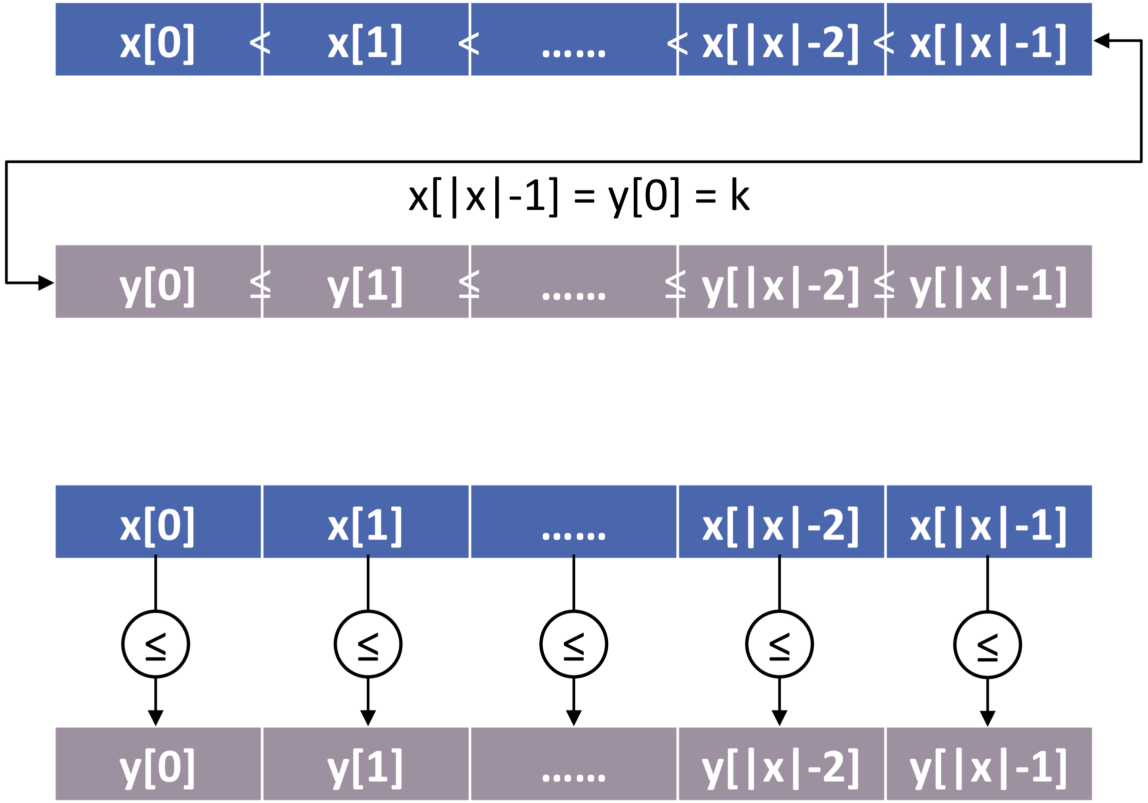
Verification Problems

Introduction

Emptiness Checking	Finite Alphabet	Infinite Alphabet
Classical (Non-Alternating)	Based on Reachability NLOGSPACE	Semi-Algorithm (PA, IMPACT)
Alternating	PSPACE	?

Verification Problems

Example



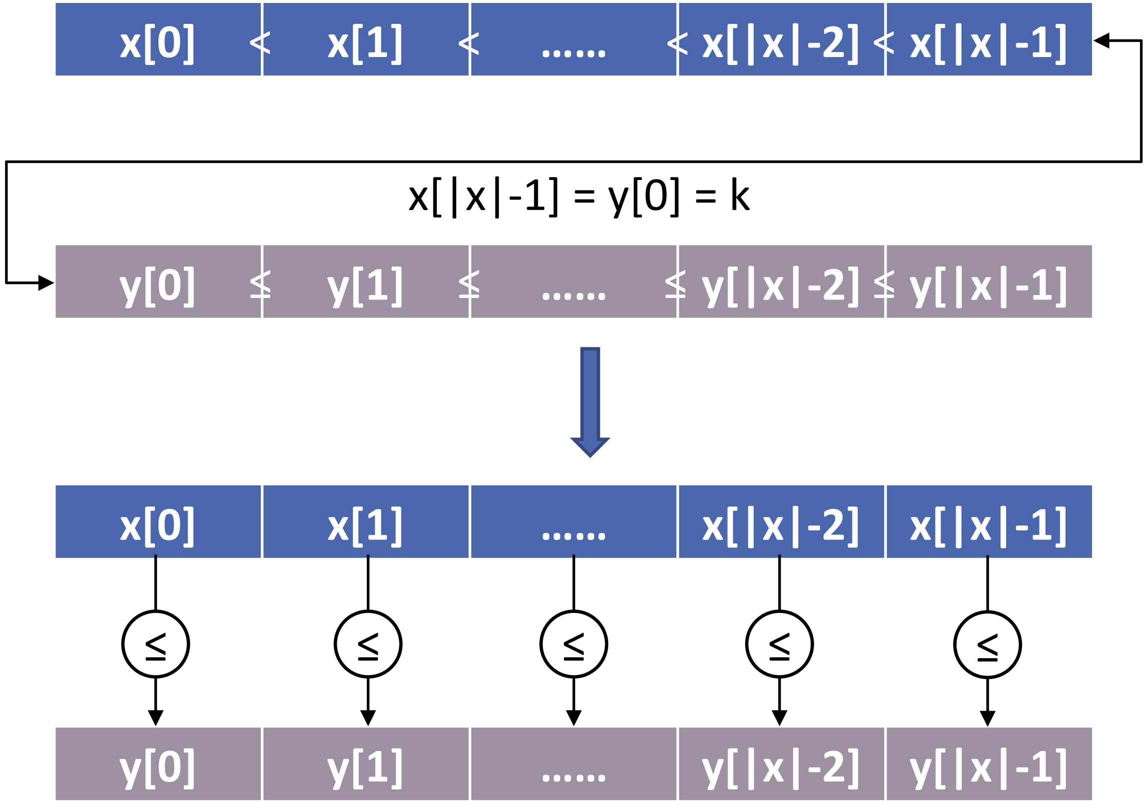

```
for(i = 0; i < n – 1; i++)
      assume(m > 0 ∧ n ≥ 0)
      x[i + 1] := x[i] + m
      y[i + 1] := y[i] + n

assume(x[i + 1] = y[0])

for(i = 0; i < n; i++)
      assert(x[i] ≤ y[i])
```

Verification Problems

Example



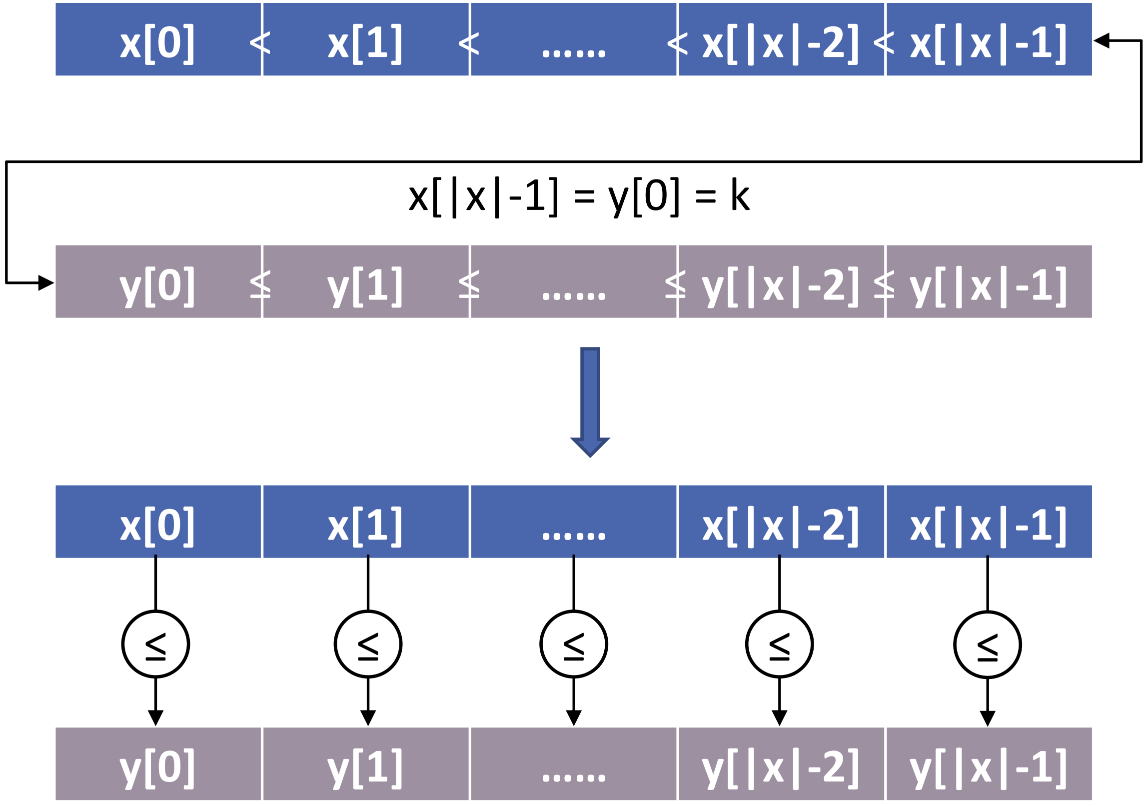
$\forall i: x[i] < x[i+1] \wedge y[i] \leq y[i+1] \wedge x[|x|-1] = y[0]$

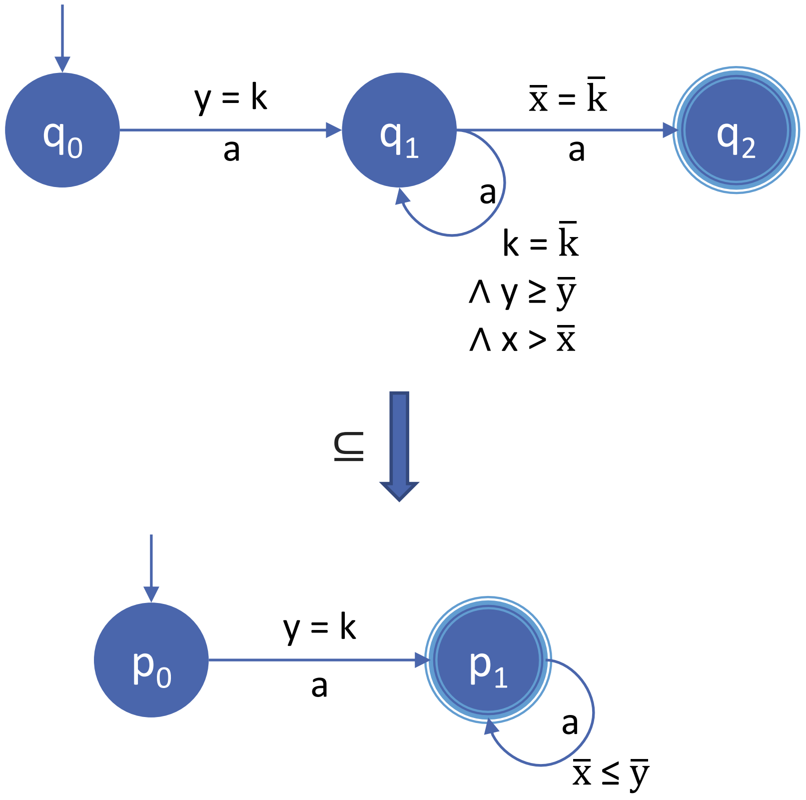
$\Downarrow$

$\forall i: x[i] \leq y[i]$

Verification Problems

Example





Verification Problems

Example

Initial State: q_0 Set of Final States: $\{q_2\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}$

$q_1 \xrightarrow{a} q_2 \wedge \overline{x} = \overline{k}$

A

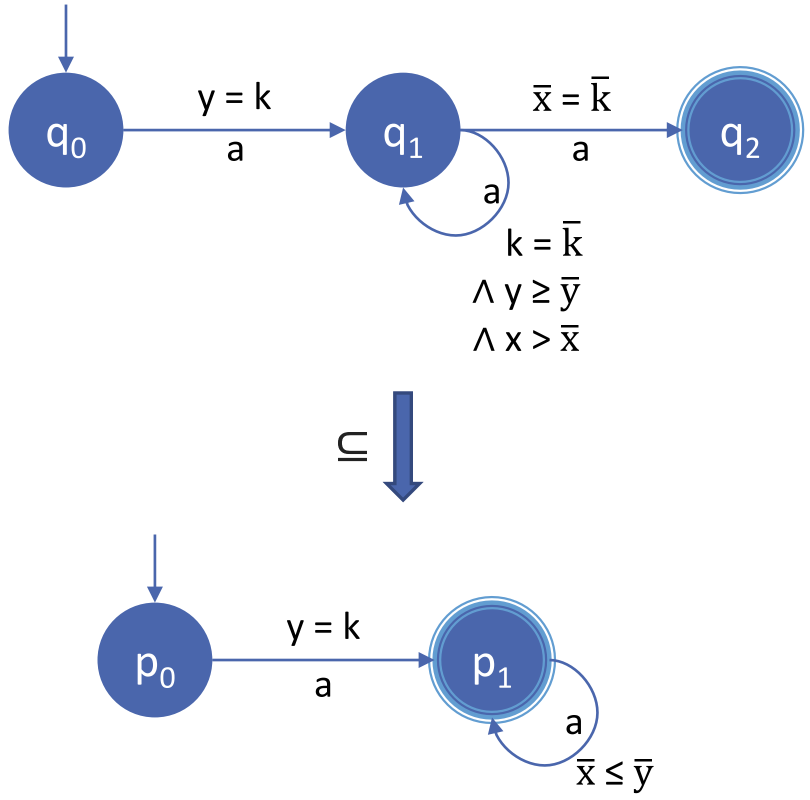
Initial State: p_0 Set of Final States: $\{p_1\}$

Transitions:

$p_0 \xrightarrow{a} p_1 \wedge y = k$

$p_1 \xrightarrow{a} p_1 \wedge \overline{x} \leq \overline{y}$

B



Verification Problems
Example

Initial State: q_0 Set of Final States: $\{q_2\}$
Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}$

$q_1 \xrightarrow{a} q_2 \wedge \overline{x} = \overline{k}$

A

Initial State: p_0 Set of Final States: $\{p_1\}$
Transitions:

$p_0 \xrightarrow{a} p_1 \wedge y = k$

$p_1 \xrightarrow{a} p_1 \wedge \overline{x} \leq \overline{y}$

B

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$
Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

$A \cap \overline{B}$

Verification Problems

Example

Initial State: q_0 Set of Final States: $\{q_2\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}$

$q_1 \xrightarrow{a} q_2 \wedge \overline{x} = \overline{k}$

A

Initial State: p_0 Set of Final States: $\{p_1\}$

Transitions:

$p_0 \xrightarrow{a} p_1 \wedge y = k$

$p_1 \xrightarrow{a} p_1 \wedge \overline{x} \leq \overline{y}$

B

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

$A \cap \overline{B}$

$$\boxed{A \subseteq B \quad \Leftrightarrow \quad A \cap \overline{B} = \emptyset}$$

Verification Problems

Alternating Data Automata (ADA)

Interpolation

Emptiness Checking of ADA

Alternating Data Automata (ADA)

Definition

$\mathbb{A} = < X, Q, i, F, \Delta >$

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Alternating Data Automata (ADA)
Definition

$\mathbb{A} = < X, Q, i, F, \Delta >$

- $X \subset Var$ Finite Set of Variables

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Alternating Data Automata (ADA)

Definition

$\mathbb{A} = < X, Q, i, F, \Delta >$

- $X \subset Var$ Finite Set of Variables
- $Q \subset Var$ Finite Set of States (Boolean)

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Alternating Data Automata (ADA)

Definition

$\mathbb{A}$ = < X, Q, i, F, Δ >

- $X \subset Var$ Finite Set of Variables
- $Q \subset Var$ Finite Set of States (Boolean)
- $i \in Form^{+}(Q, \emptyset)$ Initial Configuration

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Alternating Data Automata (ADA)

Definition

$\mathbb{A} = < X, Q, i, F, \Delta >$

- $X \subset Var$ Finite Set of Variables
- $Q \subset Var$ Finite Set of States (Boolean)
- $i \in Form^{+}(Q, \emptyset)$ Initial Configuration
- $F \subseteq Q$ Set of Final States

Initial State: $q_0 \wedge p_0$

Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Alternating Data Automata (ADA)

Definition

$\mathbb{A} = < X, Q, i, F, \Delta >$

- $X \subset Var$ Finite Set of Variables
- $Q \subset Var$ Finite Set of States (Boolean)
- $i \in Form^+(Q, \emptyset)$ Initial Configuration
- $F \subseteq Q$ Set of Final States
- $\Delta : Q \times \Sigma \to Form^+(Q, x \cup \overline{x})$

$\overline{x}$: previous value

x : current value

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Alternating Data Automata (ADA)
Data Word

(a, 3)   (b, 2)   (a, 3)   …

Alternating Data Automata (ADA)

Data Word

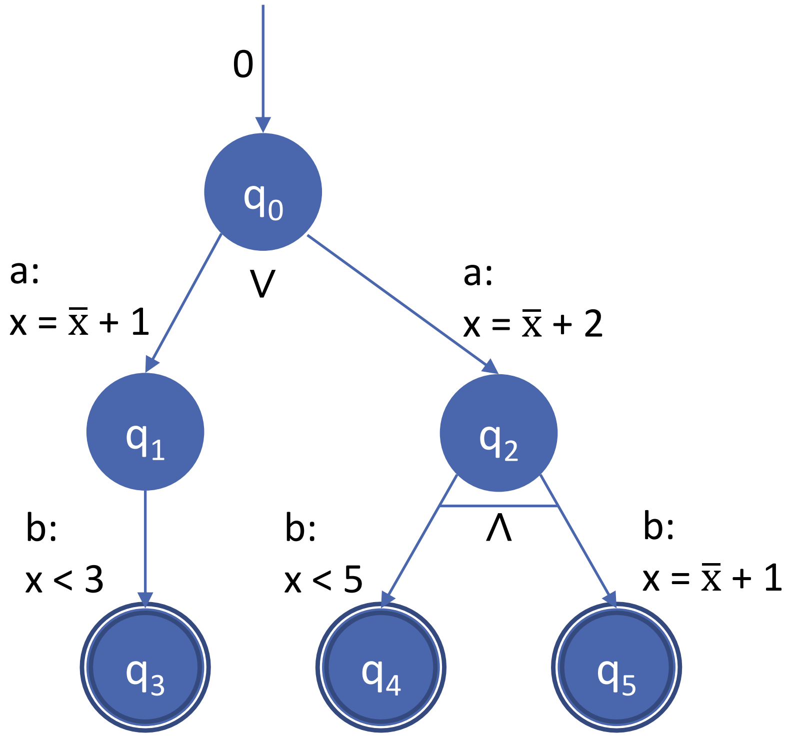
$\mathbb{N}$ (Infinite)

(a, 3) (b, 2) (a, 3) …

Σ (Finite)

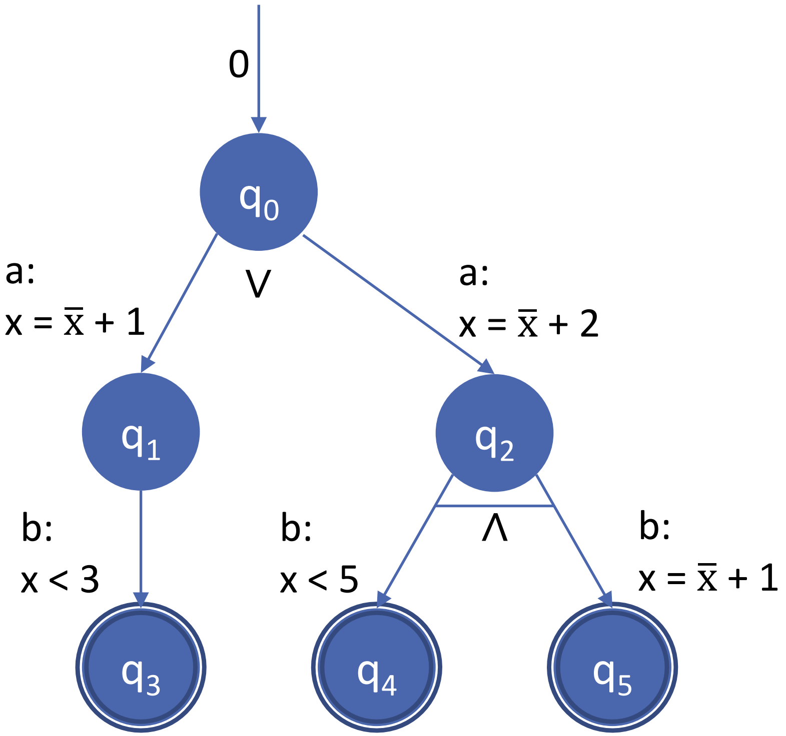
Alternating Data Automata (ADA)

Accepting Word



Alternating Data Automata (ADA)

Accepting Word

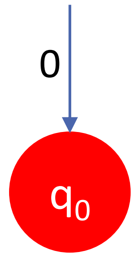


For example, the left alternating data automaton accepts the data word:

(a, 2) (b, 3)

Alternating Data Automata (ADA)

Accepting Word



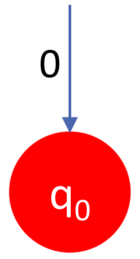
$x_0 = 0$

For example, the left alternating data automaton accepts the data word:
(a, 2) (b, 3)

Previous Data	Current Data
/	$x_0 = 0$

Alternating Data Automata (ADA)

Accepting Word



$x_0 = 0$

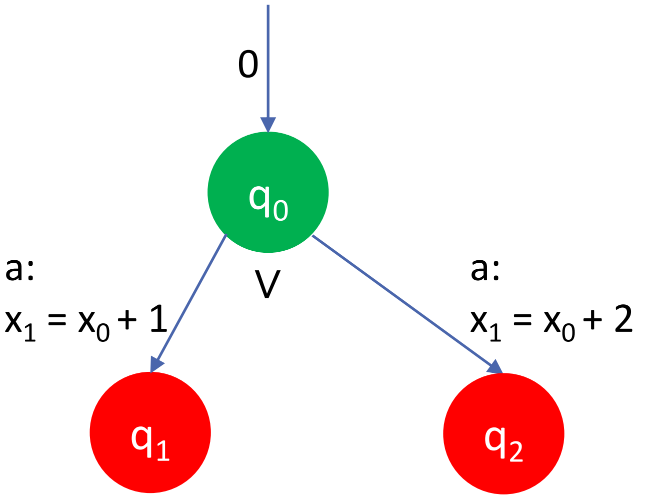
Time Stamp

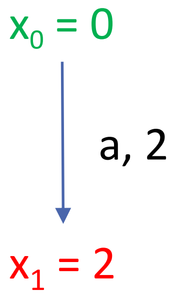
For example, the left alternating data automaton accepts the data word:
(a, 2) (b, 3)

Previous Data	Current Data
/	$x_0 = 0$

Alternating Data Automata (ADA)

Accepting Word



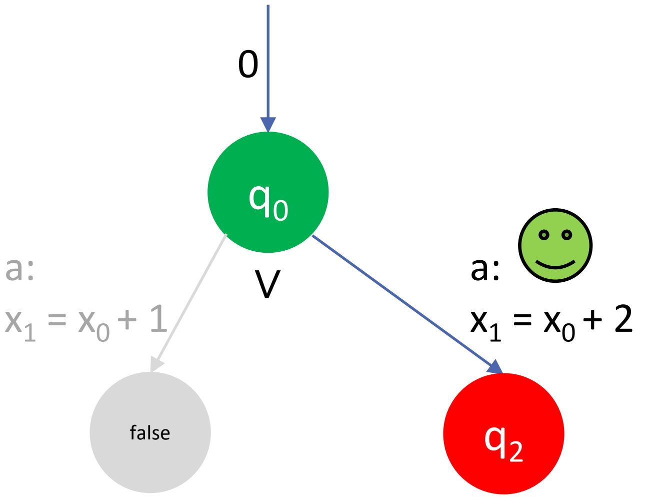


For example, the left alternating data automaton accepts the data word:
(a, 2) (b, 3)

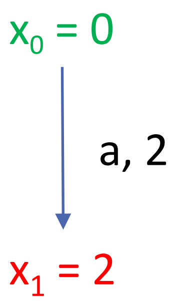
Previous Data	**Current Data**
$x_0 = 0$	$x_1 = 2$

Alternating Data Automata (ADA)

Accepting Word



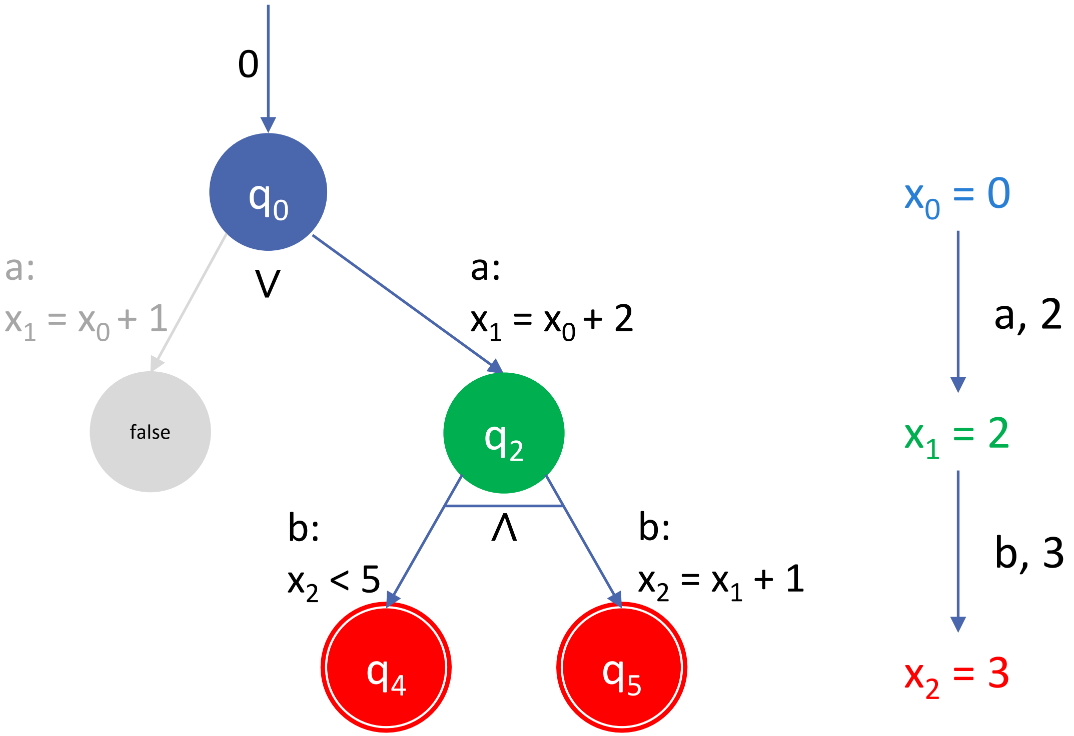
For example, the left alternating data automaton accepts the data word:
(a, 2) (b, 3)



Previous Data	**Current Data**
$x_0 = 0$	$x_1 = 2$

Alternating Data Automata (ADA)

Accepting Word

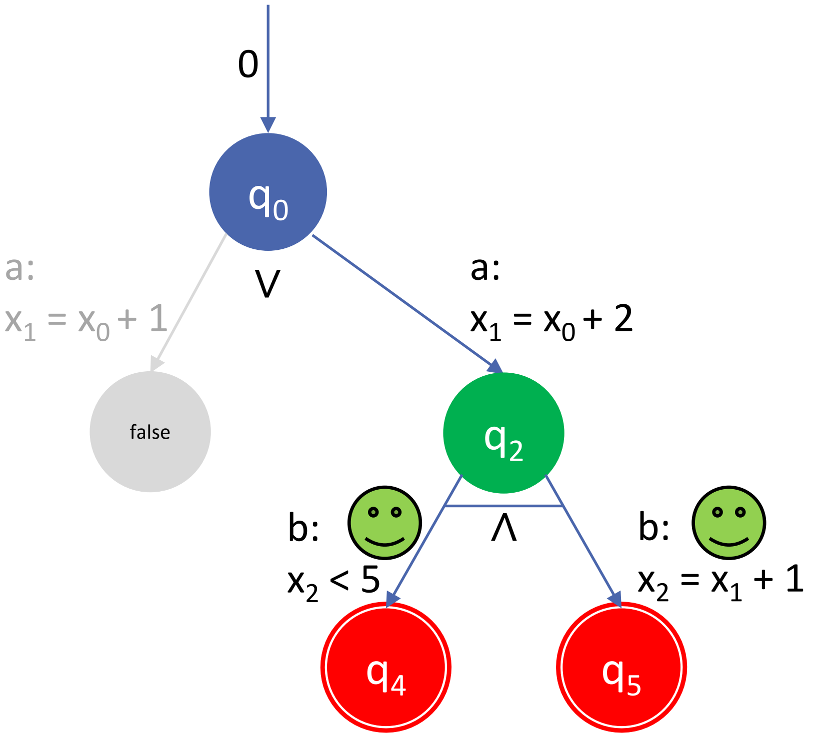


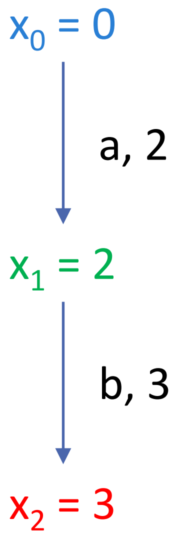
For example, the left alternating data automaton accepts the data word:
(a, 2) (b, 3)

Previous Data	Current Data
$x_1 = 2$	$x_2 = 3$

Alternating Data Automata (ADA)

Accepting Word



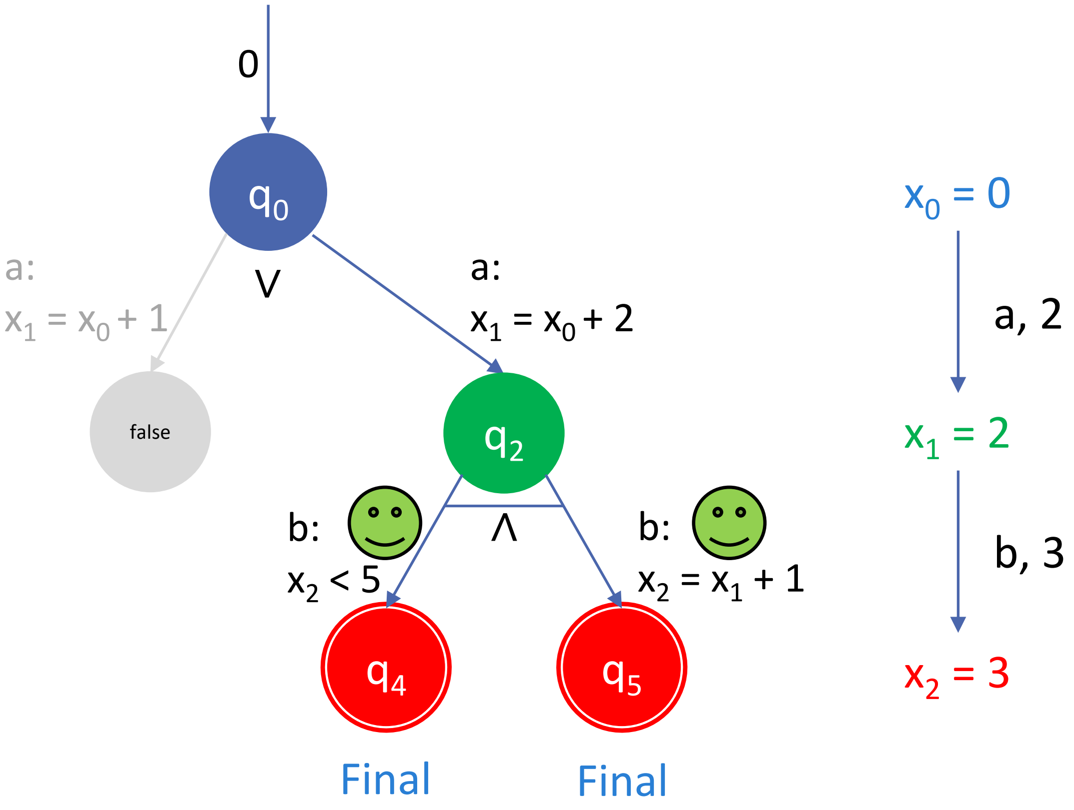


For example, the left alternating data automaton accepts the data word:
(a, 2) (b, 3)

Previous Data	**Current Data**
$x_1 = 2$	$x_2 = 3$

Alternating Data Automata (ADA)

Accepting Word

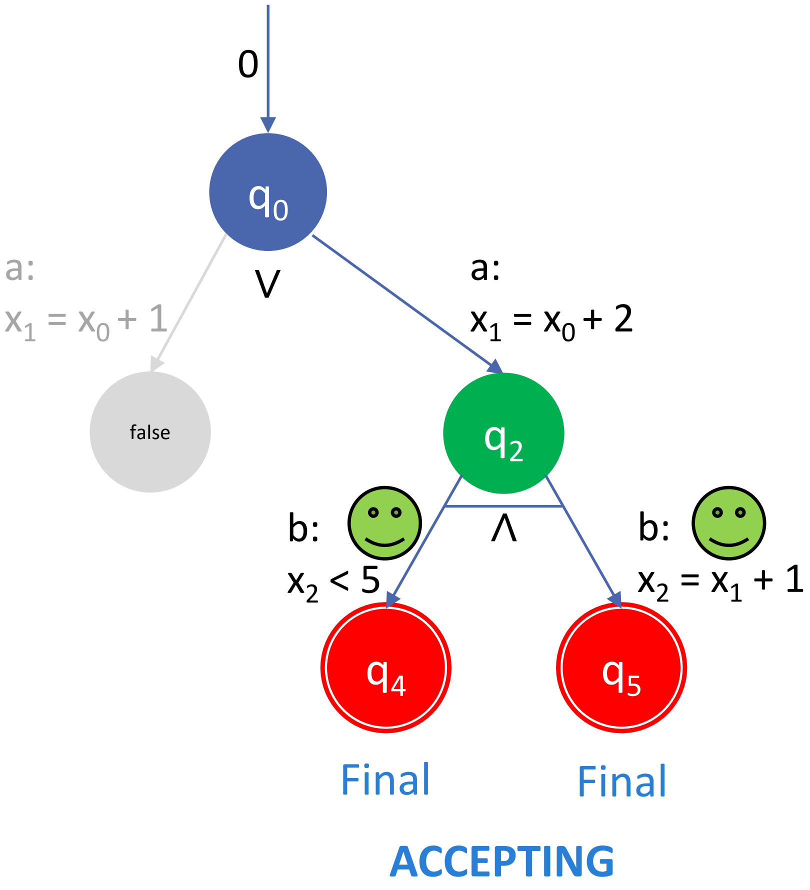


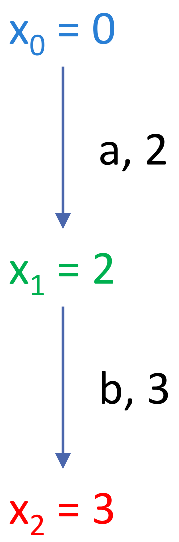
For example, the left alternating data automaton accepts the data word:
(a, 2) (b, 3)

Previous Data	Current Data
$x_1 = 2$	$x_2 = 3$

Alternating Data Automata (ADA)

Accepting Word





For example, the left alternating data automaton accepts the data word:
(a, 2) (b, 3)

Previous Data	Current Data
$x_1 = 2$	$x_2 = 3$

Alternating Data Automata (ADA)
Symbolic Execution

$a(q_0 \wedge p_0)$

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Alternating Data Automata (ADA)

Symbolic Execution

$a(q_0 \wedge p_0)$

$\Rightarrow\ a(q_0) \wedge a(p_0)$

$\Rightarrow\ q_1 \wedge y_1 = k_1 \wedge (p_1 \vee y_1 \neq k_1)$

$\Rightarrow\ q_1 \wedge p_1 \wedge y_1 = k_1$

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Alternating Data Automata (ADA)

Symbolic Execution

$$a(q_0 \wedge p_0)$$
$$\Rightarrow a(q_0) \wedge a(p_0)$$
$$\Rightarrow q_1 \wedge y_1 = k_1 \wedge (p_1 \vee y_1 \neq k_1)$$
$$\Rightarrow q_1 \wedge p_1 \wedge y_1 = k_1$$

$$a(q_1 \wedge p_1 \wedge y_1 = k_1)$$
$$\Rightarrow a(q_1) \wedge a(p_1) \wedge y_1 = k_1$$
$$\Rightarrow ((q_1 \wedge k_2 = k_1 \wedge y_2 \geq y_1 \wedge x_2 > x_1) \vee (q_2 \wedge x_1 = k_1))$$
$$\wedge (p_1 \vee x_1 > y_1)$$
$$\wedge y_1 = k_1$$

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$$q_0 \xrightarrow{a} q_1 \wedge y = k$$
$$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$$
$$p_0 \xrightarrow{a} p_1 \vee y \neq k$$
$$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$$

Alternating Data Automata (ADA)
Symbolic Execution

$a(q_0 \wedge p_0)$
$\Rightarrow a(q_0) \wedge a(p_0)$
$\Rightarrow q_1 \wedge y_1 = k_1 \wedge (p_1 \vee y_1 \neq k_1)$
$\Rightarrow q_1 \wedge p_1 \wedge y_1 = k_1$

$a(q_1 \wedge p_1 \wedge y_1 = k_1)$
$\Rightarrow a(q_1) \wedge a(p_1) \wedge y_1 = k_1$
$\Rightarrow ((q_1 \wedge k_2 = k_1 \wedge y_2 \geq y_1 \wedge x_2 > x_1) \vee (q_2 \wedge x_1 = k_1))$
$\wedge (p_1 \vee x_1 > y_1)$
$\wedge y_1 = k_1$
……

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$
Transitions:
$q_0 \xrightarrow{a} q_1 \wedge y = k$
$q_1 \xrightarrow{a} (q_1 \wedge k = \bar{k} \wedge y \geq \bar{y} \wedge x > \bar{x}) \vee (q_2 \wedge \bar{x} = \bar{k})$
$p_0 \xrightarrow{a} p_1 \vee y \neq k$
$p_1 \xrightarrow{a} p_1 \vee \bar{x} > \bar{y}$

Alternating Data Automata (ADA)

Acceptance

$a(q_0 \wedge p_0)$ $\color{red}{Acc(q_0 \wedge p_0, a)}$

$\Rightarrow$ $a(q_0) \wedge a(p_0)$

$\Rightarrow$ $q_1 \wedge y_1 = k_1 \wedge (p_1 \vee y_1 \neq k_1)$

$\Rightarrow$ $q_1 \wedge p_1 \wedge y_1 = k_1$

$a(q_1 \wedge p_1 \wedge y_1 = k_1)$ $\color{red}{Acc(q_0 \wedge p_0, aa)}$

$\Rightarrow$ $a(q_1) \wedge a(p_1) \wedge y_1 = k_1$

$\Rightarrow$ $((q_1 \wedge k_2 = k_1 \wedge y_2 \geq y_1 \wedge x_2 > x_1) \vee (q_2 \wedge x_1 = k_1))$

$\wedge (p_1 \vee x_1 > y_1)$

$\wedge y_1 = k_1$

……

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Alternating Data Automata (ADA)

Acceptance

$a(q_0 \wedge p_0)$
$\Rightarrow a(q_0) \wedge a(p_0)$
$\Rightarrow q_1 \wedge y_1 = k_1 \wedge (p_1 \vee y_1 \neq k_1)$
$\Rightarrow q_1 \wedge p_1 \wedge y_1 = k_1$

$a(q_1 \wedge p_1 \wedge y_1 = k_1)$ Acc($q_0 \wedge p_0$, aa)
$\Rightarrow a(q_1) \wedge a(p_1) \wedge y_1 = k_1$
$\Rightarrow ((q_1 \wedge k_2 = k_1 \wedge y_2 \geq y_1 \wedge x_2 > x_1) \vee (q_2 \wedge x_1 = k_1))$
$\wedge (p_1 \vee x_1 > y_1)$
$\wedge y_1 = k_1$
…… Accepting by the automaton?

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Alternating Data Automata (ADA)

Acceptance

$Acc(q_0 \wedge p_0, aa)$

$((q_1 \wedge k_2 = k_1 \wedge y_2 \geq y_1 \wedge x_2 > x_1) \vee (q_2 \wedge x_1 = k_1))$
$\wedge (p_1 \vee x_1 > y_1)$
$\wedge y_1 = k_1$

Initial State: $q_0 \wedge p_0$

Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Alternating Data Automata (ADA)

Acceptance

$Acc(q_0 \wedge p_0, aa)$

$((\text{false} \wedge k_2 = k_1 \wedge y_2 \geq y_1 \wedge x_2 > x_1) \vee (\text{true} \wedge x_1 = k_1))$
$\wedge (\text{false} \vee x_1 > y_1)$
$\wedge y_1 = k_1$

Initial State: $q_0 \wedge p_0$

Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Alternating Data Automata (ADA)
Acceptance

$\text{Acc}(q_0 \wedge p_0, aa)$

$((\text{false} \wedge k_2 = k_1 \wedge y_2 \geq y_1 \wedge x_2 > x_1) \vee (\text{true} \wedge x_1 = k_1))$
$\wedge\ (\text{false} \vee x_1 > y_1)$
$\wedge\ y_1 = k_1$
$\Rightarrow$ false

Not Satisfiable

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Alternating Data Automata (ADA)

Emptiness

$Acc(q_0 \wedge p_0, aa)$

$((\text{false} \wedge k_2 = k_1 \wedge y_2 \geq y_1 \wedge x_2 > x_1) \vee (\text{true} \wedge x_1 = k_1))$
$\wedge\ (\text{false} \vee x_1 > y_1)$
$\wedge\ y_1 = k_1$
$\Rightarrow$ false

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$
Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Accepting Formula ⇔ Counter Example (of Emptiness)

Verification Problems

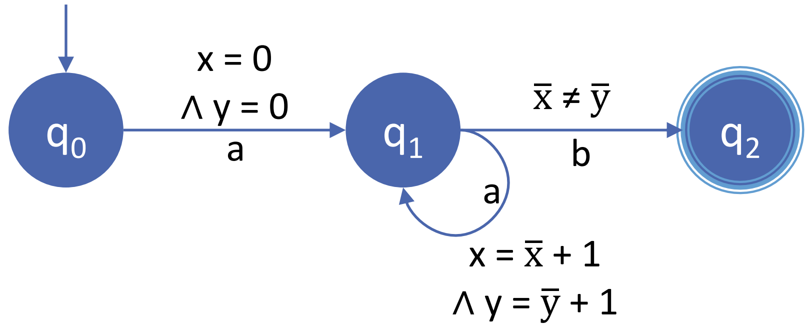
Alternating Data Automata (ADA)

Interpolation

Emptiness Checking of ADA

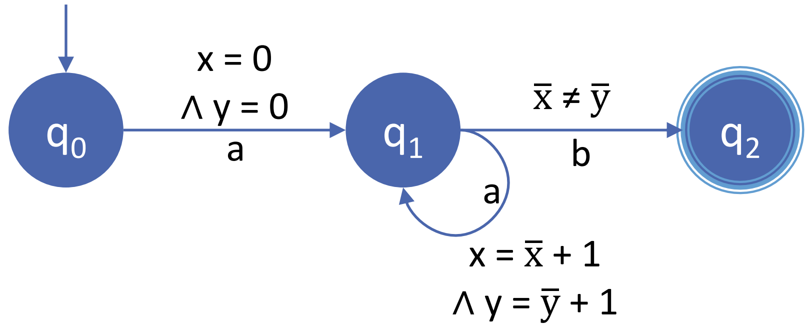
Interpolation

Introduction



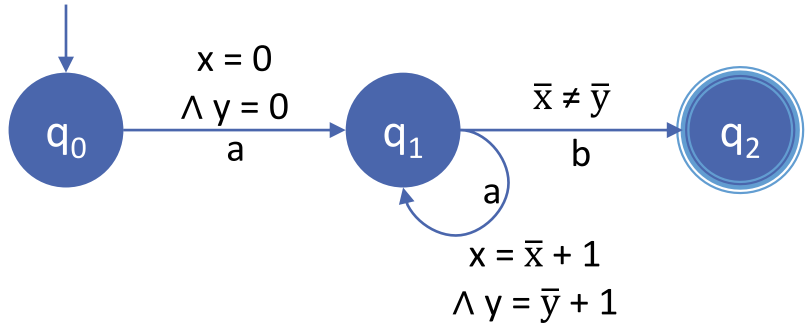
Interpolation
Introduction

q_0



Interpolation
Introduction

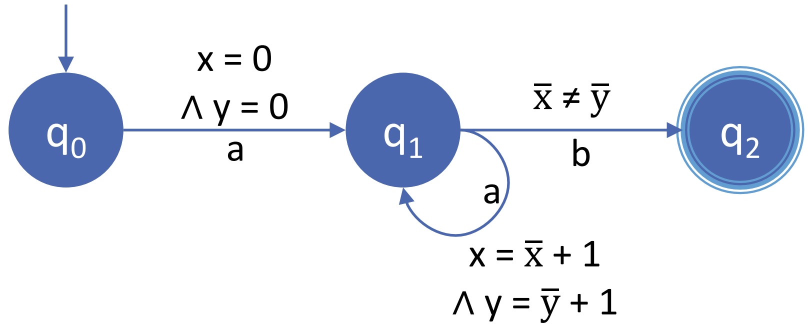
$$q_0 \xrightarrow{a} q_1 \wedge x = 0 \wedge y = 0 \xrightarrow{b} \perp$$



Interpolation

Introduction

$$\begin{tikzcd}
q_0 \arrow[d, "a"'] & \\
q_1 \wedge x = 0 \wedge y = 0 \arrow[d, "a"'] \arrow[r, "b"] & \bot \\
q_1 \wedge x = 1 \wedge y = 1 \arrow[r, "b"] & \bot
\end{tikzcd}$$



Interpolation

Introduction

q_0

$\downarrow a$

$q_1 \wedge x = 0 \wedge y = 0 \xrightarrow{b} \perp$

$\downarrow a$

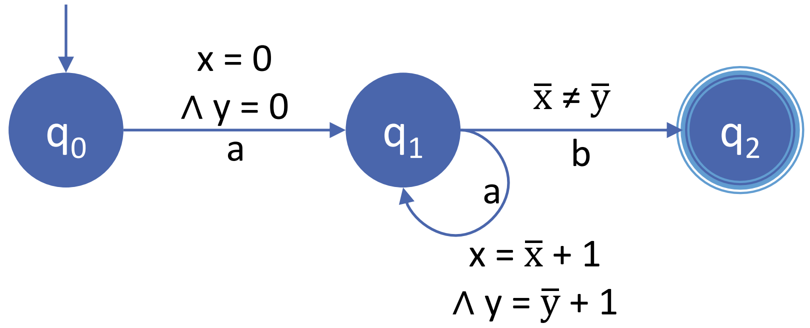
$q_1 \wedge x = 1 \wedge y = 1 \xrightarrow{b} \perp$

$\downarrow a$

$q_1 \wedge x = 2 \wedge y = 2 \xrightarrow{b} \perp$

$\downarrow a$

…



Interpolation
Introduction

q_0

$\downarrow a$

$q_1 \wedge x = 0 \wedge y = 0 \xrightarrow{b} \perp$

$\downarrow a$

$q_1 \wedge x = 1 \wedge y = 1 \xrightarrow{b} \perp$

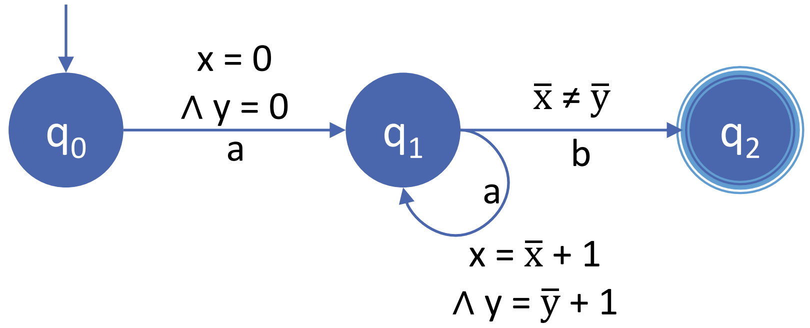
$\downarrow a$

$q_1 \wedge x = 2 \wedge y = 2 \xrightarrow{b} \perp$

$\downarrow a$

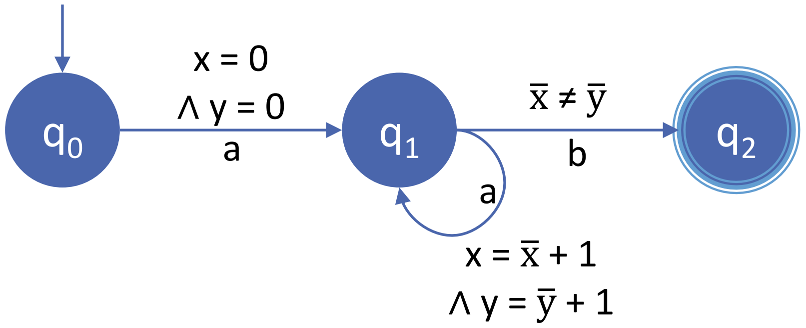
…

Will never terminate…



Interpolation
Introduction

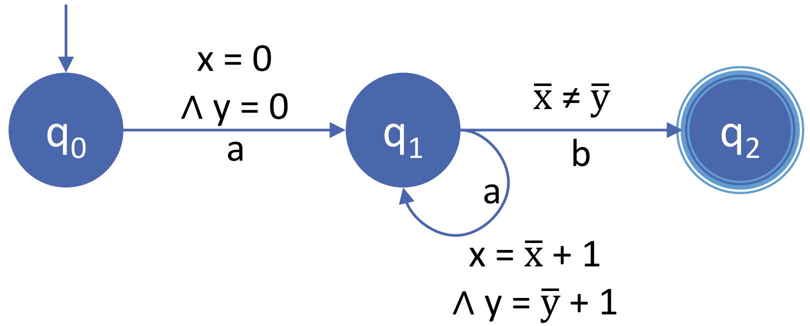
q_0



Interpolation

Introduction

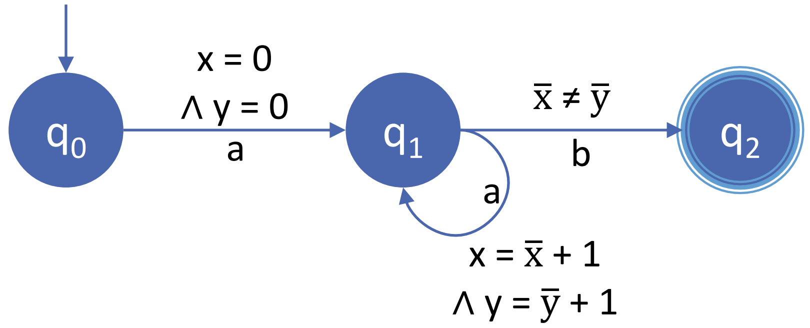
$$q_0 \xrightarrow{a} q_1 \wedge x = 0 \wedge y = 0 \xrightarrow{b} \bot$$



Interpolation

Introduction

$$
\begin{tikzcd}
q_0 \arrow[d, "a"'] & \\
q_1 \wedge x = 0 \wedge y = 0 \arrow[r, "b"] & \bot
\end{tikzcd}
$$



$(x = 0 \wedge y = 0) \wedge (x \neq y) \rightarrow \bot$

get an interpolant: $x = y$ (an over-approximation of $x = 0 \wedge y = 0$)

we have:

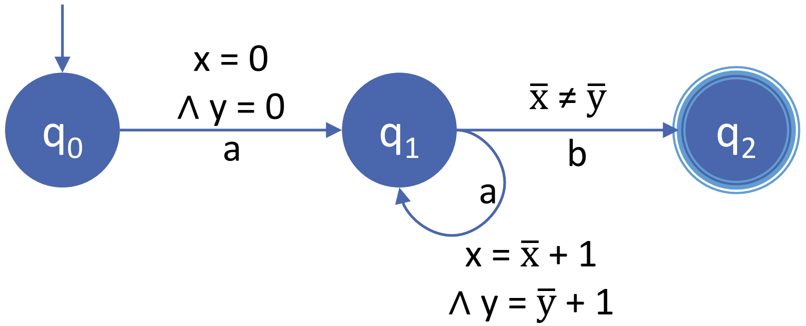
$(x = 0 \wedge y = 0) \rightarrow (x = y)$

$(x = y) \wedge (x \neq y) \rightarrow \bot$

Interpolation

Introduction

$$q_0$$
$$\downarrow a$$
$$\cancel{q_1 \land x = 0 \land y = 0} \xrightarrow{b} \bot$$
$$q_1 \land x = y$$



$(x = 0 \land y = 0) \land (x \neq y) \rightarrow \bot$

get an interpolant: $x = y$ (an over-approximation of $x = 0 \land y = 0$)

we have:

$(x = 0 \land y = 0) \rightarrow (x = y)$

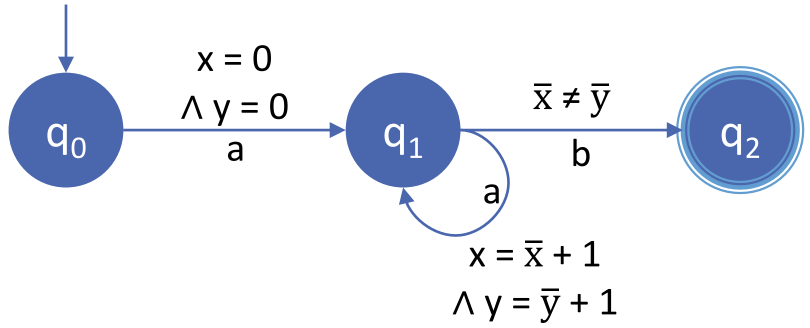
$(x = y) \land (x \neq y) \rightarrow \bot$

Interpolation
Introduction

$$q_0$$

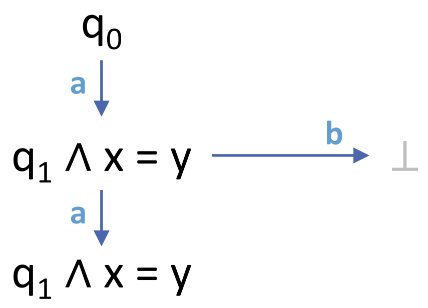
$$\downarrow a$$

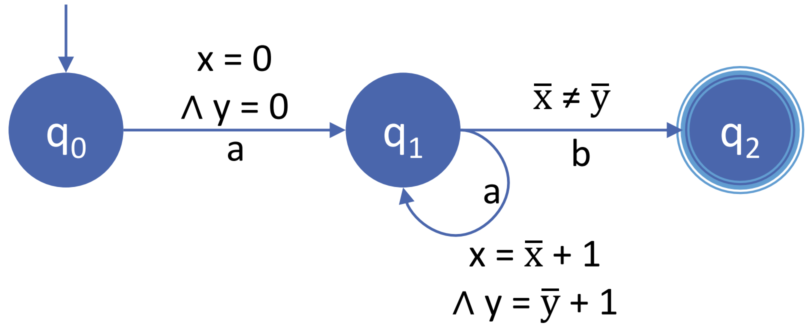
$$q_1 \land x = y \xrightarrow{b} \bot$$



Interpolation

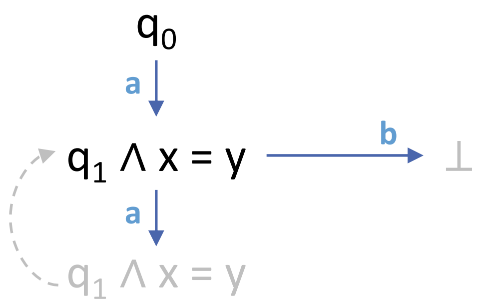
Introduction

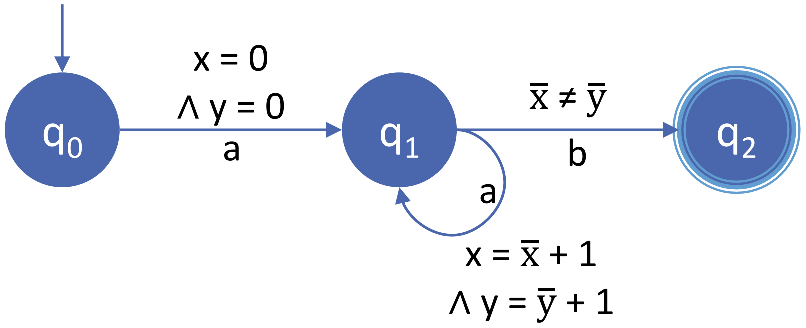




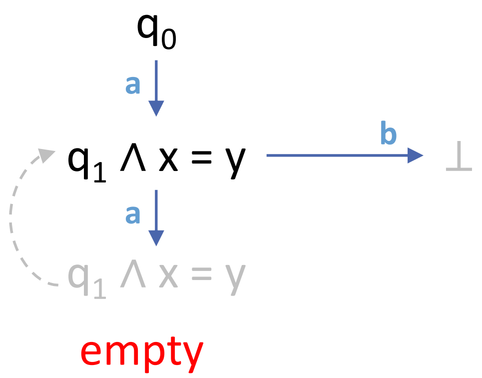
Interpolation

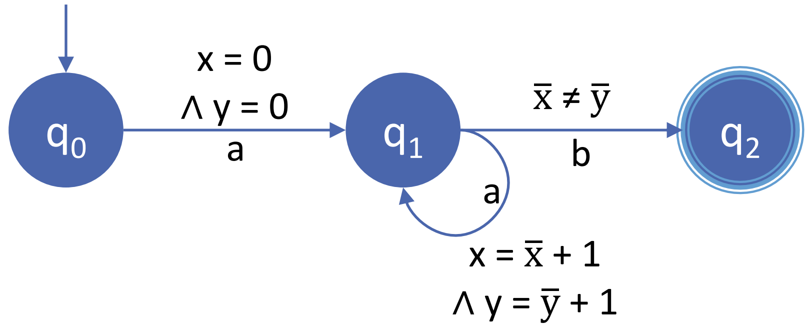
Introduction





Interpolation
Introduction





Interpolation

Computation of Alternating Interpolants

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Interpolation

Computation of Alternating Interpolants

$a(q_0 \wedge p_0)$
$\Rightarrow \quad a(q_0) \wedge a(p_0)$
$\Rightarrow \quad q_1 \wedge y_1 = k_1 \wedge (p_1 \vee y_1 \neq k_1)$
$\Rightarrow \quad q_1 \wedge p_1 \wedge y_1 = k_1$

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \bar{k} \wedge y \geq \bar{y} \wedge x > \bar{x}) \vee (q_2 \wedge \bar{x} = \bar{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \bar{x} > \bar{y}$

Interpolation

Computation of Alternating Interpolants

$a(q_0 \wedge p_0)$ $\quad$ $Acc(q_0 \wedge p_0, a)$

$\Rightarrow \; a(q_0) \wedge a(p_0)$

$\Rightarrow \; q_1 \wedge y_1 = k_1 \wedge (p_1 \vee y_1 \neq k_1)$

$\Rightarrow \; q_1 \wedge p_1 \wedge y_1 = k_1$

F_1 : $q_0 \wedge p_0$

F_2 : $(q_0 \rightarrow q_1 \wedge y_1 = k_1) \wedge (p_0 \rightarrow p_1 \vee y_1 \neq k_1)$

F_3 : $(q_1 \rightarrow \text{false}) \wedge (p_1 \rightarrow \text{false})$

Initial State: $q_0 \wedge p_0$ $\quad$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Interpolation
Computation of Alternating Interpolants

$a(q_0 \wedge p_0)$ $\quad$ $Acc(q_0 \wedge p_0, a)$

$\Rightarrow$ $a(q_0) \wedge a(p_0)$

$\Rightarrow$ $q_1 \wedge y_1 = k_1 \wedge (p_1 \vee y_1 \neq k_1)$

$\Rightarrow$ $q_1 \wedge p_1 \wedge y_1 = k_1$

F_1 : $q_0 \wedge p_0$

F_2 : $(q_0 \rightarrow q_1 \wedge y_1 = k_1) \wedge (p_0 \rightarrow p_1 \vee y_1 \neq k_1)$

F_3 : $(q_1 \rightarrow \text{false}) \wedge (p_1 \rightarrow \text{false})$

Initial State: $q_0 \wedge p_0$ $\quad$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \bar{k} \wedge y \geq \bar{y} \wedge x > \bar{x}) \vee (q_2 \wedge \bar{x} = \bar{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \bar{x} > \bar{y}$

Interpolation

Computation of Alternating Interpolants

$a(q_0 \wedge p_0)$ $\qquad$ $Acc(q_0 \wedge p_0, a)$

$\Rightarrow \; a(q_0) \wedge a(p_0)$

$\Rightarrow \; q_1 \wedge y_1 = k_1 \wedge (p_1 \vee y_1 \neq k_1)$

$\Rightarrow \; q_1 \wedge p_1 \wedge y_1 = k_1$

$F_1 : \; q_0 \wedge p_0$

$F_2 : \; (q_0 \rightarrow q_1 \wedge y_1 = k_1) \wedge (p_0 \rightarrow p_1 \vee y_1 \neq k_1)$

$F_3 : \; (q_1 \rightarrow \text{false}) \wedge (p_1 \rightarrow \text{false})$

Initial State: $q_0 \wedge p_0$ $\qquad$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \bar{k} \wedge y \geq \bar{y} \wedge x > \bar{x}) \vee (q_2 \wedge \bar{x} = \bar{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \bar{x} > \bar{y}$

Interpolation

Computation of Alternating Interpolants

$a(q_0 \wedge p_0)$ $\quad$ $Acc(q_0 \wedge p_0, a)$

$\Rightarrow\ a(q_0) \wedge a(p_0)$

$\Rightarrow\ q_1 \wedge y_1 = k_1 \wedge (p_1 \vee y_1 \neq k_1)$

$\Rightarrow\ q_1 \wedge p_1 \wedge y_1 = k_1$

F_1 : $q_0 \wedge p_0$

F_2 : $(q_0 \rightarrow q_1 \wedge y_1 = k_1) \wedge (p_0 \rightarrow p_1 \vee y_1 \neq k_1)$

F_3 : $(q_1 \rightarrow \text{false}) \wedge (p_1 \rightarrow \text{false})$

$F_1 \wedge F_2 \wedge F_3 \rightarrow \text{false}$

Initial State: $q_0 \wedge p_0$ $\quad$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Interpolation

Computation of Alternating Interpolants

$a(q_0 \wedge p_0)$ $\quad$ $Acc(q_0 \wedge p_0, a)$

$\Rightarrow\ a(q_0) \wedge a(p_0)$

$\Rightarrow\ q_1 \wedge y_1 = k_1 \wedge (p_1 \vee y_1 \neq k_1)$

$\Rightarrow\ q_1 \wedge p_1 \wedge y_1 = k_1$

$F_1 :\ q_0 \wedge p_0$

$F_2 :\ (q_0 \rightarrow q_1 \wedge y_1 = k_1) \wedge (p_0 \rightarrow p_1 \vee y_1 \neq k_1)$

$F_3 :\ (q_1 \rightarrow \text{false}) \wedge (p_1 \rightarrow \text{false})$

$F_1 \wedge F_2 \wedge F_3 \rightarrow \text{false}$

$\downarrow I_1 \quad \downarrow I_2$

Compute Interpolants:

$\text{true} \wedge F_1 \rightarrow I_1$

$I_1 \wedge F_2 \rightarrow I_2$

$I_2 \wedge F_3 \rightarrow \text{false}$

Initial State: $q_0 \wedge p_0$ $\quad$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \bar{k} \wedge y \geq \bar{y} \wedge x > \bar{x}) \vee (q_2 \wedge \bar{x} = \bar{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \bar{x} > \bar{y}$

Interpolation

Computation of Alternating Interpolants

$a(q_0 \wedge p_0)$ $\quad\quad$ $\mathrm{Acc}(q_0 \wedge p_0, a)$

$\Rightarrow \; a(q_0) \wedge a(p_0)$

$\Rightarrow \; q_1 \wedge y_1 = k_1 \wedge (p_1 \vee y_1 \neq k_1)$

$\Rightarrow \; q_1 \wedge p_1 \wedge y_1 = k_1$

$F_1 : \; q_0 \wedge p_0$

$F_2 : \; (q_0 \rightarrow q_1 \wedge y_1 = k_1) \wedge (p_0 \rightarrow p_1 \vee y_1 \neq k_1)$

$F_3 : \; (q_1 \rightarrow \mathit{false}) \wedge (p_1 \rightarrow \mathit{false})$

$F_1 \wedge F_2 \wedge F_3 \rightarrow \mathit{false}$

$\downarrow \quad \downarrow$

$q_0 \quad q_1$

Compute Interpolants:

$\mathit{true} \wedge F_1 \rightarrow q_0$

$q_0 \wedge F_2 \rightarrow q_1$

$q_1 \wedge F_3 \rightarrow \mathit{false}$

Initial State: $q_0 \wedge p_0$ $\quad$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Verification Problems

Alternating Data Automata (ADA)

Interpolation

Emptiness Checking of ADA

Emptiness Checking of ADA

Algorithm

Semi-Algorithm (with Anti-Chains) Based on Abstraction(Over-Approximation) and Refinement

- Lazy Predicate Abstraction
- Impact

Emptiness Checking of ADA
Algorithm

Semi-Algorithm (with Anti-Chains) Based on Abstraction(Over-Approximation) and Refinement
- Lazy Predicate Abstraction
- Impact

Emptiness is proved with abstraction
- The automaton is surely empty

Counter-example (that proves the non-emptiness) is found with abstraction
- The counter-example can be spurious
- Need to refine (compute the interpolants)

Emptiness Checking of ADA

Lazy Predicate Abstraction

Π : Set of Predicates

- Exclude spurious counter examples
- Get updated once we get new interpolants (refinement)

Main Procedures

- Compute the abstract post (using elements from Π)
- Check the satisfiability of abstract post
  1. Satisfiable (can be spurious)
     - Compute the concrete symbolic execution (without abstraction)
     - Re-check the satisfiability (of the concrete post image)
       1. Still Satisfiable: NOT EMPTY
       2. Not Satisfiable: refine Π (computing interpolants), back to the PIVOT and remove the subtrees
  2. Not Satisfiable: expand the node and check the coverage (entailments)

EMPTY if not able to continue

Emptiness Checking of ADA
Impact

Core: local (in-place) refinement by strengthening the node labels

Expand
- Create a new node and label it with “true”

Refine
- Compute the concrete symbolic execution
- Re-check the satisfiability
  1. Satisfiable: NOT EMPTY
  2. Not Satisfiable: compute the interpolants and refine the nodes by strengthening the labels with interpolants

Close
- Check the coverage (entailments)

EMPTY if not able to continue

Emptiness Checking of ADA

Impact Example

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Emptiness Checking of ADA

Impact Example

$q_0 \wedge p_0$

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Emptiness Checking of ADA

Impact Example

$$
\begin{array}{c}
q_0 \wedge p_0 \\
\Big\downarrow {\scriptstyle a} \\
\top
\end{array}
$$

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Emptiness Checking of ADA

Impact Example

$$q_0 \wedge p_0 \xrightarrow{a} \cancel{\top}\ \boxed{q_1}$$

$Acc(q_0 \wedge p_0, a) = \bot$
refine

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Emptiness Checking of ADA

Impact Example

$$q_0 \wedge p_0 \xrightarrow{a} q_1$$

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \bar{k} \wedge y \geq \bar{y} \wedge x > \bar{x}) \vee (q_2 \wedge \bar{x} = \bar{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \bar{x} > \bar{y}$

Emptiness Checking of ADA

Impact Example

$$
\begin{array}{c}
q_0 \wedge p_0 \\
\downarrow a \\
q_1 \\
\downarrow a \\
\top
\end{array}
$$

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Emptiness Checking of ADA

Impact Example

$q_0 \wedge p_0$

$\downarrow a$

$\cancel{q_1}$ $\boxed{q_1 \wedge p_1 \wedge k \leq y}$

$\downarrow a$

$\cancel{\top}$ $\boxed{q_1 \vee p_1}$

$Acc(q_0 \wedge p_0, aa) = \bot$

refine

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Emptiness Checking of ADA

Impact Example

$$q_0 \wedge p_0$$

$$\big\downarrow a$$

$$q_1 \wedge p_1 \wedge k \leq y$$

$$\big\downarrow a$$

$$q_1 \vee p_1$$

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Emptiness Checking of ADA

Impact Example

$$q_0 \wedge p_0$$
$$\downarrow a$$
$$q_1 \wedge p_1 \wedge k \le y$$
$$\downarrow a$$
$$q_1 \vee p_1$$
$$\downarrow a$$
$$\top$$

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Emptiness Checking of ADA

Impact Example

$q_0 \wedge p_0$

$\downarrow a$

$q_1 \wedge p_1 \wedge k \leq y$

$\downarrow a$ $\boxed{(q_1 \vee p_1) \wedge (q_2 \vee (((p_1 \wedge k \leq y) \vee 2 \leq x - k) \wedge q_1))}$

$\cancel{q_1 \vee p_1}$

$\downarrow a$

$\cancel{\top}$ $\boxed{q_1 \vee p_1}$

Acc($q_0 \wedge p_0$, aaa) = $\perp$

refine

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Emptiness Checking of ADA

Impact Example

$$q_0 \wedge p_0$$

$$\Big\downarrow a$$

$$q_1 \wedge p_1 \wedge k \leq y$$

$$\Big\downarrow a$$

$$(q_1 \vee p_1) \wedge (q_2 \vee (((p_1 \wedge k \leq y) \vee 2 \leq x - k) \wedge q_1))$$

$$\Big\downarrow a$$

$$q_1 \vee p_1$$

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Emptiness Checking of ADA

Impact Example

$$q_0 \wedge p_0$$
$$\downarrow a$$
$$q_1 \wedge p_1 \wedge k \leq y$$
$$\downarrow a$$
$$(q_1 \vee p_1) \wedge (q_2 \vee (((p_1 \wedge k \leq y) \vee 2 \leq x - k) \wedge q_1))$$
$$\downarrow a$$
$$q_1 \vee p_1$$
$$\downarrow a$$
$$\top$$

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Emptiness Checking of ADA

Impact Example

$$q_0 \wedge p_0$$

$$\downarrow a$$

$$q_1 \wedge p_1 \wedge k \leq y$$

$$\downarrow a$$

$$(q_1 \vee p_1) \wedge (q_2 \vee (((p_1 \wedge k \leq y) \vee 2 \leq x - k) \wedge q_1))$$

$$\downarrow a$$

$$\cancel{q_1 \vee p_1} \quad \boxed{(q_1 \vee p_1) \wedge (q_2 \vee (((p_1 \wedge k \leq y) \vee 2 \leq x - k \vee 3 \leq x - k) \wedge q_1))}$$

$$\downarrow a$$

$$\cancel{\top} \quad \boxed{q_1 \vee p_1}$$

$Acc(q_0 \wedge p_0, aaaa) = \bot$

refine

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Emptiness Checking of ADA

Impact Example

$$q_0 \land p_0$$

$$\downarrow a$$

$$q_1 \land p_1 \land k \leq y$$

$$\downarrow a$$

$$(q_1 \lor p_1) \land (q_2 \lor (((p_1 \land k \leq y) \lor 2 \leq x - k) \land q_1))$$

$$\downarrow a$$

$$(q_1 \lor p_1) \land (q_2 \lor (((p_1 \land k \leq y) \lor 2 \leq x - k \lor 3 \leq x - k) \land q_1))$$

$$\downarrow a$$

$$q_1 \lor p_1$$

Initial State: $q_0 \land p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \land y = k$

$q_1 \xrightarrow{a} (q_1 \land k = \bar{k} \land y \geq \bar{y} \land x > \bar{x}) \lor (q_2 \land \bar{x} = \bar{k})$

$p_0 \xrightarrow{a} p_1 \lor y \neq k$

$p_1 \xrightarrow{a} p_1 \lor \bar{x} > \bar{y}$

Emptiness Checking of ADA

Impact Example

$q_0 \wedge p_0$

$\downarrow a$

$q_1 \wedge p_1 \wedge k \leq y$

$\downarrow a$

$(q_1 \vee p_1) \wedge (q_2 \vee (((p_1 \wedge k \leq y) \vee 2 \leq x - k) \wedge q_1))$

$\downarrow a$

$(q_1 \vee p_1) \wedge (q_2 \vee (((p_1 \wedge k \leq y) \vee 2 \leq x - k \vee 3 \leq x - k) \wedge q_1))$

$\downarrow a$

$q_1 \vee p_1$

Initial State: $q_0 \wedge p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \wedge y = k$

$q_1 \xrightarrow{a} (q_1 \wedge k = \overline{k} \wedge y \geq \overline{y} \wedge x > \overline{x}) \vee (q_2 \wedge \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \vee y \neq k$

$p_1 \xrightarrow{a} p_1 \vee \overline{x} > \overline{y}$

Emptiness Checking of ADA

Impact Example

$q_0 \land p_0$

$\downarrow a$

$q_1 \land p_1 \land k \leq y$

$\downarrow a$

$(q_1 \lor p_1) \land (q_2 \lor (((p_1 \land k \leq y) \lor 2 \leq x - k) \land q_1))$

$\downarrow a$

$(q_1 \lor p_1) \land (q_2 \lor (((p_1 \land k \leq y) \lor 2 \leq x - k \lor 3 \leq x - k) \land q_1))$

$\downarrow a$

$q_1 \lor p_1$

empty

Initial State: $q_0 \land p_0$ Set of Final States: $\{q_2, p_0\}$

Transitions:

$q_0 \xrightarrow{a} q_1 \land y = k$

$q_1 \xrightarrow{a} (q_1 \land k = \overline{k} \land y \geq \overline{y} \land x > \overline{x}) \lor (q_2 \land \overline{x} = \overline{k})$

$p_0 \xrightarrow{a} p_1 \lor y \neq k$

$p_1 \xrightarrow{a} p_1 \lor \overline{x} > \overline{y}$

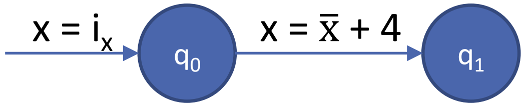
Emptiness Checking of ADA

Experiments

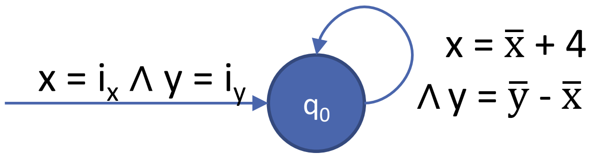
Example	|A| (bytes)	L(A) = ∅ ?	PA (sec)	Impact (sec)	INCLUDER (sec)
simple1	309	no	0.774	0.064	0.076
simple2	504	yes	0.867	0.070	0.070
simple3	214	yes	0.899	0.095	0.095
array shift	874	yes	2.889	0.126	0.078
array simple	3440	yes	timeout	9.998	7.154
array rotation1	1834	yes	7.227	0.331	0.229
array rotation2	15182	yes	timeout	timeout	31.632
abp	6909	no	9.492	0.631	2.288
train	1823	yes	19.237	0.763	0.678
hw1	322	yes	1.861	0.163	0.172
hw2	674	yes	24.111	0.308	0.473

Future Work

Hidden Variables



A



B

$L(A) \subseteq L(B)$ iff:

For each word $w = (a_1,\langle x_1\rangle)(a_2,\langle x_2\rangle)\ldots(a_k,\langle x_k\rangle)$ in $L(A)$, there exists a series of data $Y = y_1, y_2, \ldots, y_k$ such that $(a_1,\langle x_1,y_1\rangle)(a_2,\langle x_2,y_2\rangle)\ldots(a_k,\langle x_k,y_k\rangle)$ is in $L(B)$.