Alternation Elimination by Complementation

Christian Dax

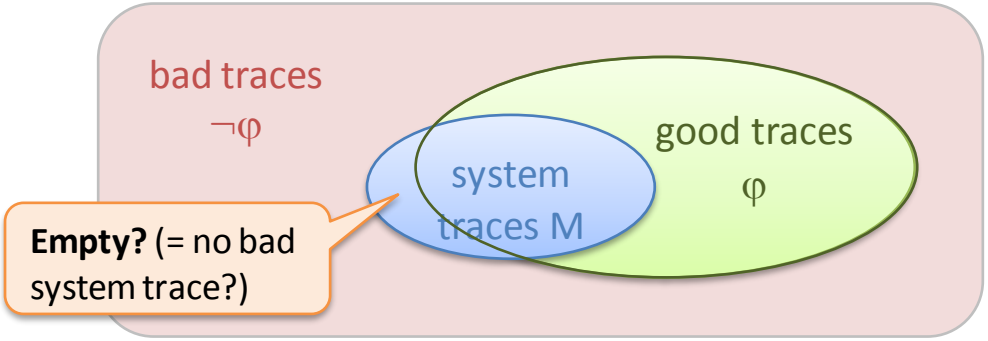
ETH Zurich

Joint work with Felix Klaedtke

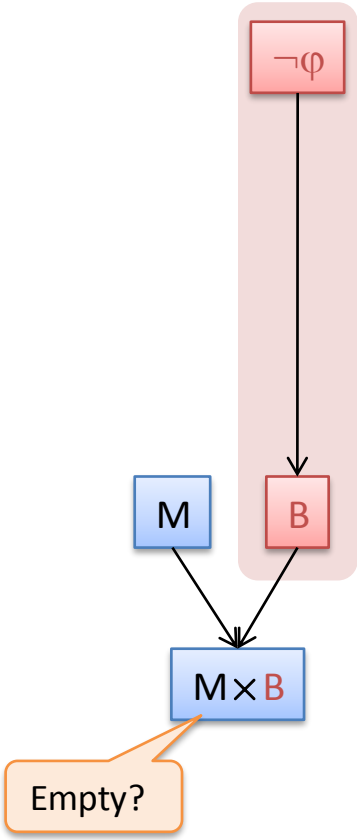
LPAR'08, November 24th, 2008

Motivation: Finite-State Model Checking

- Model-checking problem:
  - Given: finite-state system M (system traces)
  - Given: specification as temporal formula φ **(good traces)** ⇒ ¬φ (bad traces)
  - Question: $M \models \varphi$?

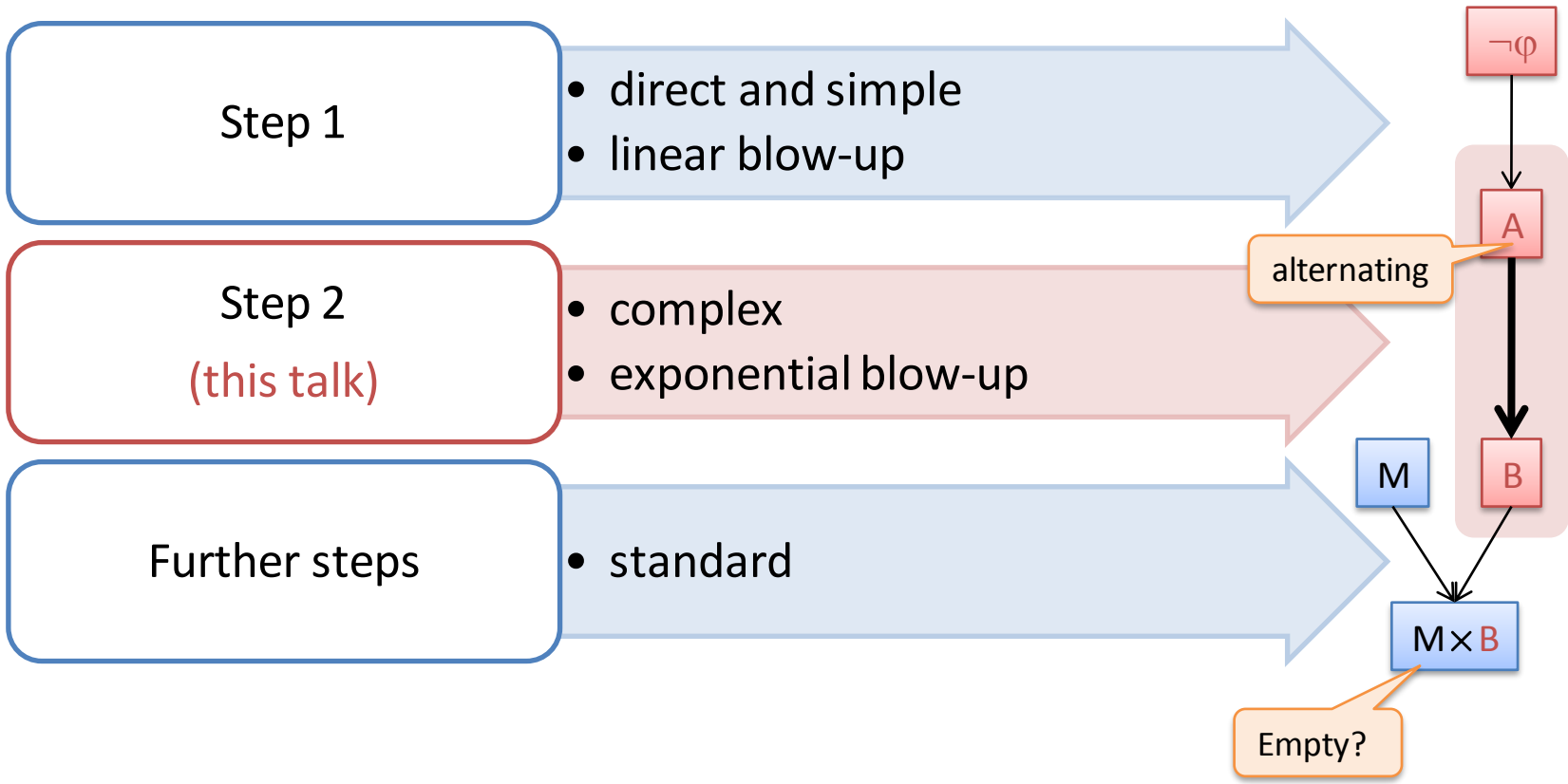


- Automata-based approach:
  1. Represent sets by automata
  2. Represent intersection by product automaton



Motivation: Alternation Elimination

- Alternating automata as intermediate step

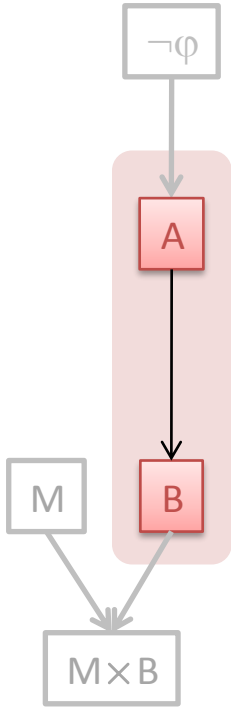


Outline

1. Background

2. Alternation elimination scheme

3. Instance with new complementation construction



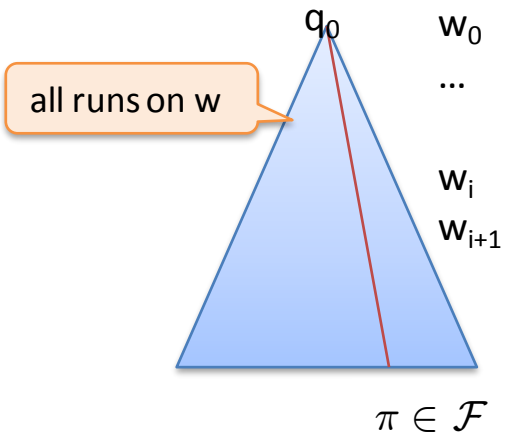
Background on Automata

Nondeterministic Automaton (NA)

- An **NA** is a tuple $(Q, \Sigma, \delta, q_0, \mathcal{F})$
  - $\delta: Q \times \Sigma \to 2^Q$ transition function
  - $\mathcal{F} \subseteq Q^\omega$ acceptance condition
    (state sequences that are considered to be accepting)

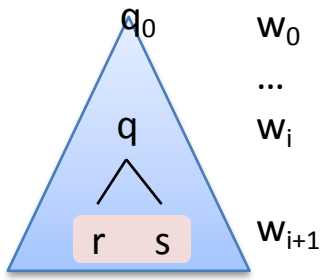
- Remark: **Büchi** and **coBüchi** condition given as $F \subseteq Q$
  - $\mathcal{F} = \{\pi \in Q^\omega \mid$ **an** F-state **occurs** ∞-often in $\pi\}$
  - $\mathcal{F} = \{\pi \in Q^\omega \mid$ no F-state occurs ∞-often in $\pi\}$

- For a word $w = w_0 w_1 \ldots$
  - A **run** $q_0 q_1 \ldots$ is a sequence of states with $q_{i+1} \in \delta(q_i, w_i)$
  - w is **accepted** $:\Leftrightarrow$ there is a run on w that is in $\mathcal{F}$



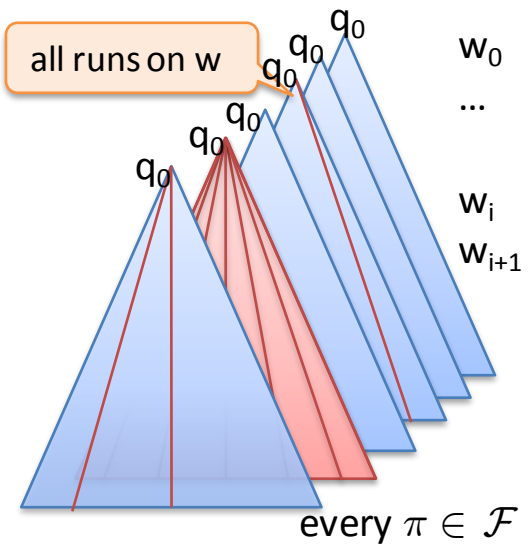
Alternating Automata (AA)

- An **AA** is a tuple $(Q, \Sigma, \delta, q_0, \mathcal{F})$
  - $\delta: Q \times \Sigma \to \mathcal{B}^+(Q)$ transition function
  - $\mathcal{B}^+(Q)$ positive boolean combination of formulas in DNF

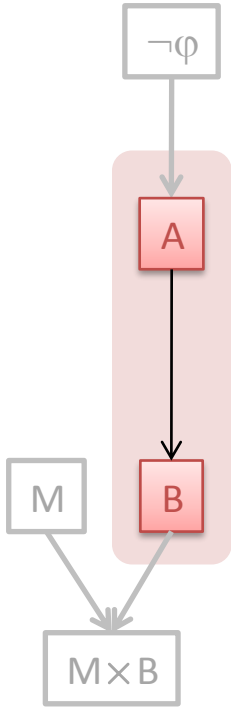


$\delta(q, w_i) = (r \wedge s) \vee (s \wedge t)$

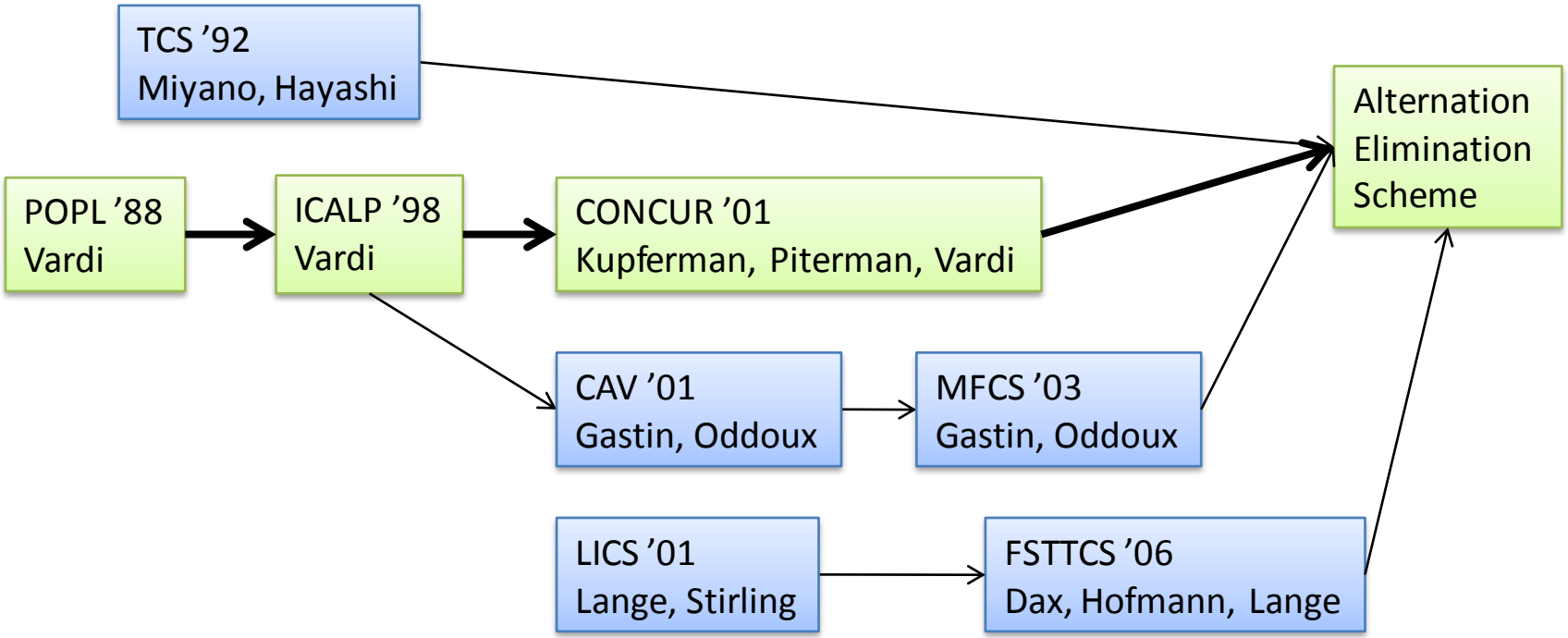
- For a word $w = w_0 w_1 \ldots$
  - A **run** is a Q-labeled tree, where
    - the root is labeled by q_0, and
    - a q-labeled node in level i has children labeled by states of one of the monomials of $\delta(q, w_i)$
  - w is **accepted**
    $:\Leftrightarrow$ there is a run such that every path is in $\mathcal{F}$



From Alternating to Nondeterministic Automata



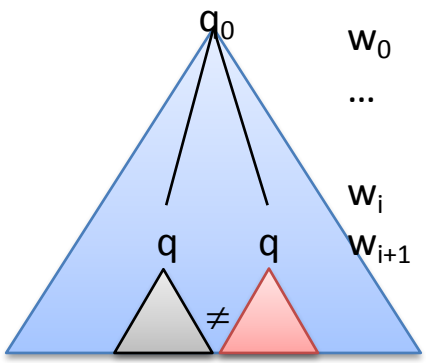
Related Work



- Alternation Elimination Scheme:
  - Improves and generalizes approach used in **green boxes**
  - Unifies + simplifies constructions and proofs of blue boxes that can now be seen as instances

Alternation Elimination (1/2) : Runs as Words

- We consider only automata with memoryless runs
  - Examples: Büchi, co-Büchi, Parity, Rabin automata
  - Equally-labeled nodes in same level can be merged



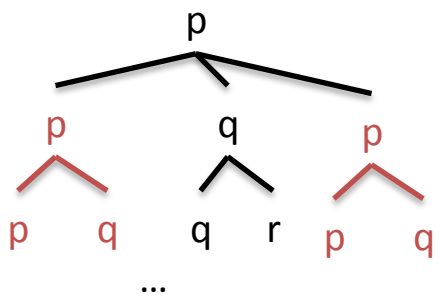
not memoryless

- Encode run as sequence $r_0 r_1 r_2 \ldots \in (Q \to 2^Q)^\omega$ of successor functions
  - $r_i(q)$: 'labels of children of q-labeled node in level i'
  - Example:

$r_0(p) = \{p, q\}$

$r_1(p) = \{p, q\}, r_1(q) = \{q, r\}$

$r_2(p) = \ldots, r_2(q) = \ldots, r_2(r) = \ldots$



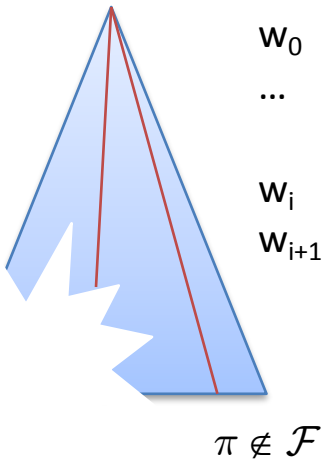
Alternation Elimination (2/2) : Complementation

- Let $\mathcal{A} = (Q, \Sigma, \delta, q_0, \mathcal{F})$ be an AA and $\Gamma := Q \to 2^Q$
- $\mathcal{A}$ accepts the word w
  - $\Leftrightarrow$ there is a run on w s.t. every path is in $\mathcal{F}$
  - $\Leftrightarrow \exists$ r: r $\in$ runs(w) $\wedge \forall \pi \in$ r: $\pi \in \mathcal{F}$
  - $\Leftrightarrow \exists$ r: $\neg$ (r $\notin$ runs(w) $\vee \exists \pi \in$ r: $\pi \notin \mathcal{F}$) ★
  - $\Leftrightarrow \exists$ r: $\neg \mathcal{B}$(w, r)

'refuter's strategy'

- It is easy to build an NA $\mathcal{B}$ over $\Sigma \times \Gamma$ for ★
  - $\mathcal{B} := (Q, \Sigma \times \Gamma, \eta, q_0, Q^\omega \setminus \mathcal{F})$
  - $\eta(q, (a,r)) := \begin{cases} r(q) & r(q) \text{ is monomial in } \delta(q, a) \\ \{\text{acc-sink}\} & \text{otherwise} \end{cases}$

- Finally: complement the NA $\mathcal{B}$ and project it on Σ.

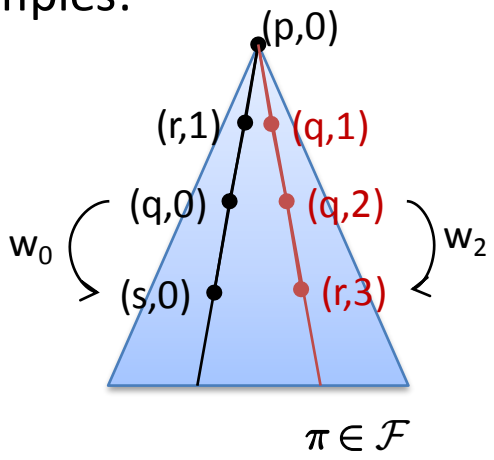


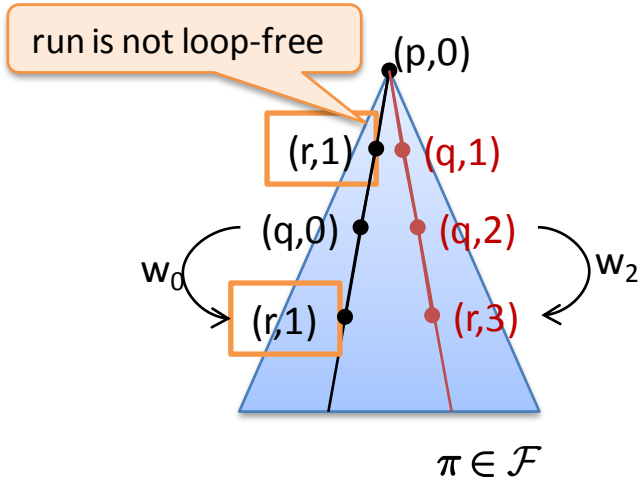
Scheme for 2-Way Automata

- In our paper: scheme also works for **2-way automata**
  - 2-way automata can move the read-only head in both directions.
  - Configuration consists of a state and the position of the read-only head

- Loop-freeness
  - A run is **loop-free** :⇔ for every path, no configuration occurs twice
  - An AA is **loop-free** :⇔ every run is loop-free

- Examples:





Some Instances

- Translations from **different AAs** to 1-way NBAs

- Resulting sizes:

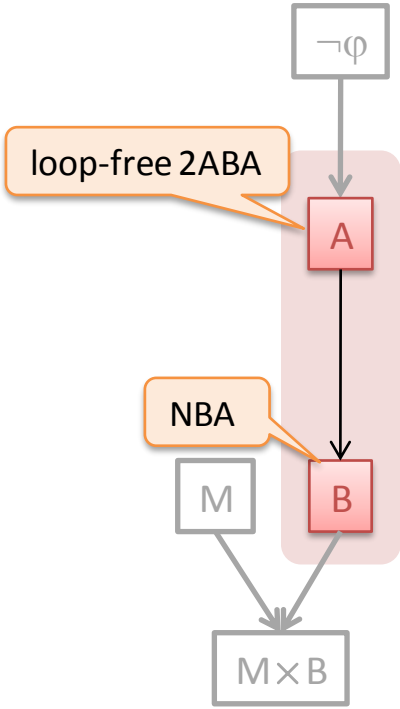
alternating automata

old/new	1-Weak Büchi LTL (+ Past)	Büchi PSL (+ Past)	Parity μLTL (+ Past)	Rabin
1-way	$O(n2^n)$/ ○	$O(2^{2n})$/ ○	$2^{O(nk \log n)}$/ ◯	--/**$O(2^{nk \log nk})$**
2-way	--/**$O(n2^{3n})$**	$2^{O(n*n)}$/ ◯	$2^{O(nk*nk)}$/ ◯	
2-way + loop-free	$O(n2^{2n})$/ ○	--/**$O(2^{4n})$**	--/in progress	--/in progress

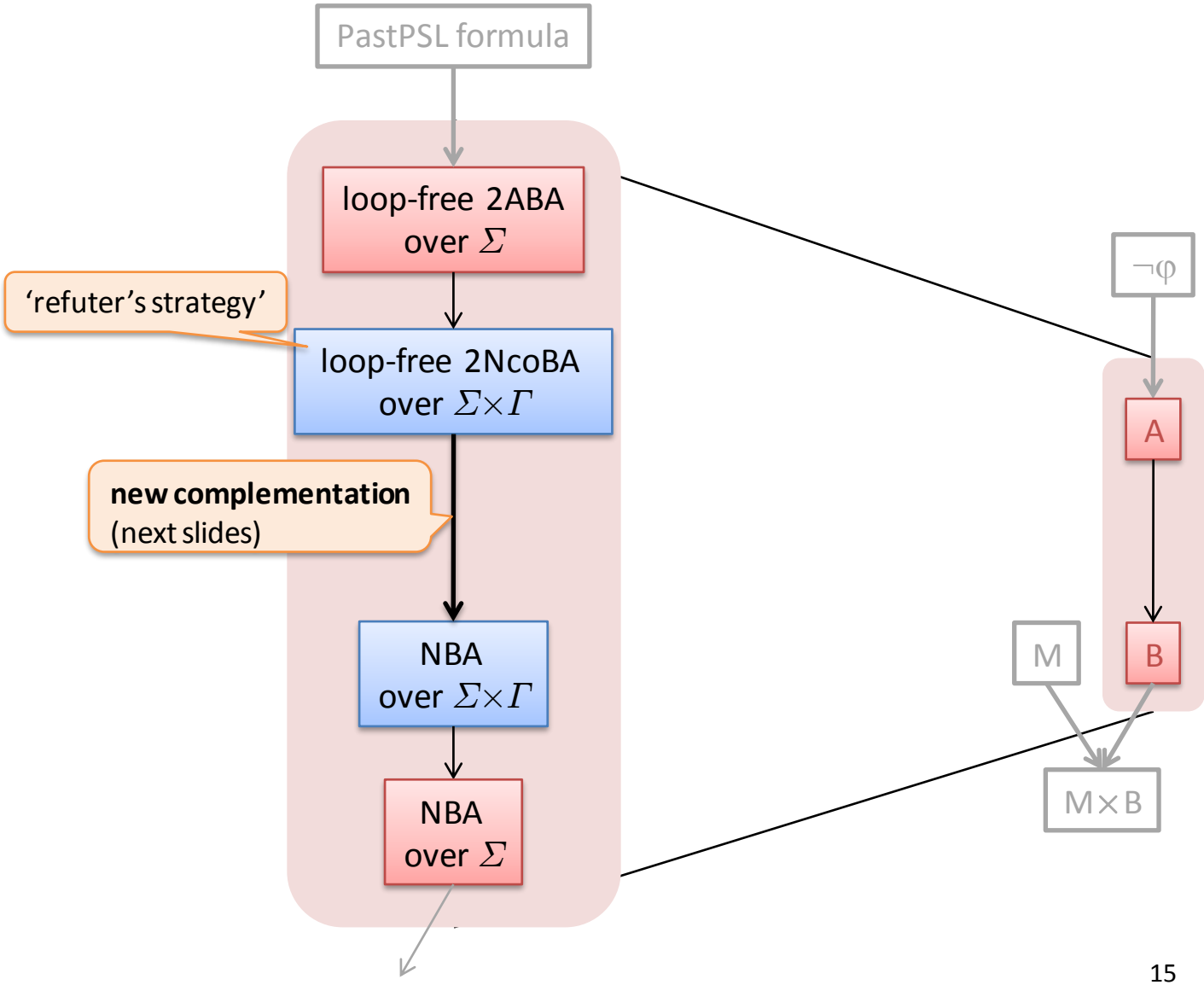
next slides

◯ **smaller constant** (hidden in O notation)
○ **same size** but construction **more modular**

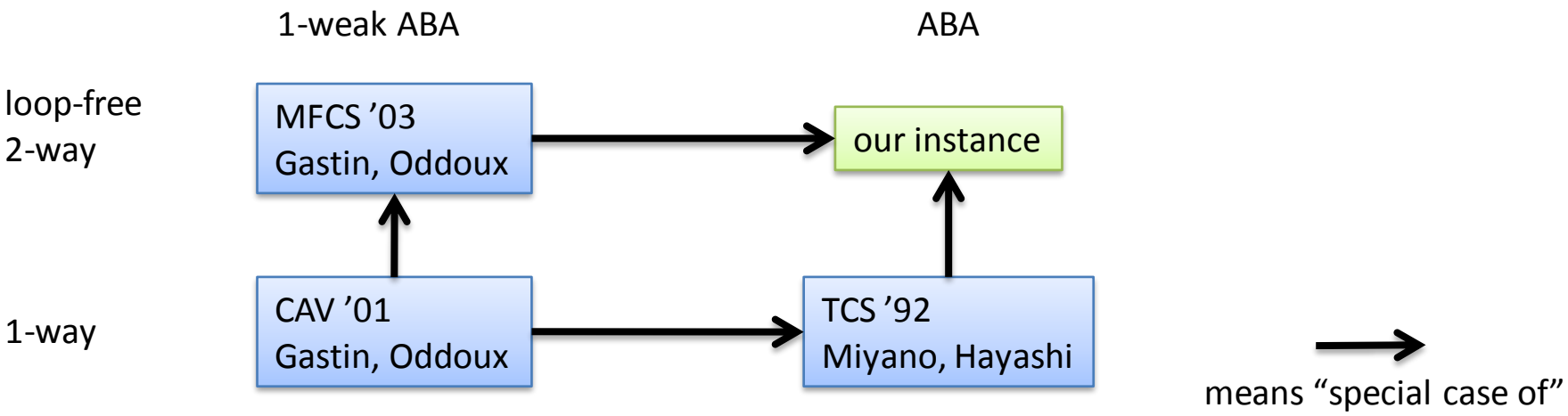
Novel Instance of the Scheme



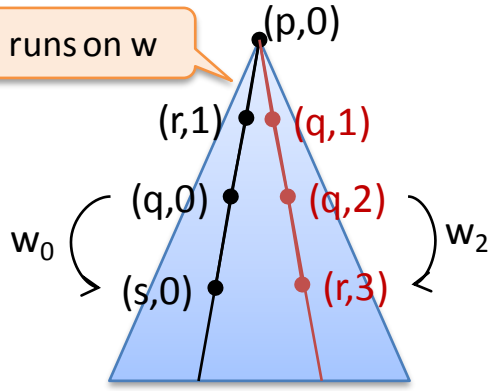
Outline: From Loop-Free 2ABA to NBA



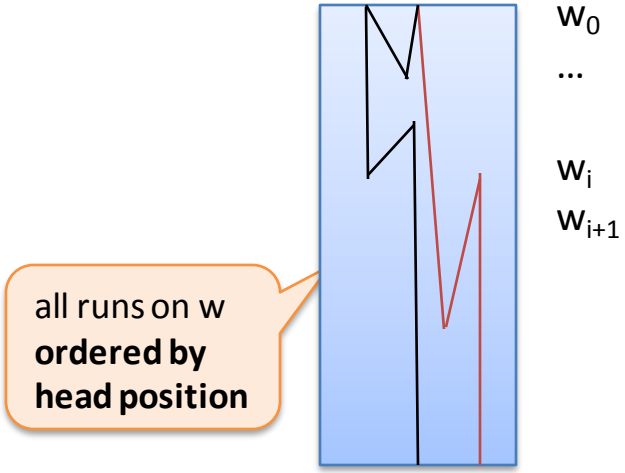
Related Work



- Requirement for **instance**: 2NcoBA complementation
  - Based on Miyano/Hayashi: "breakpoint construction"
  - Based on Vardi's idea in [IPL'89]: representation of bidirectional runs



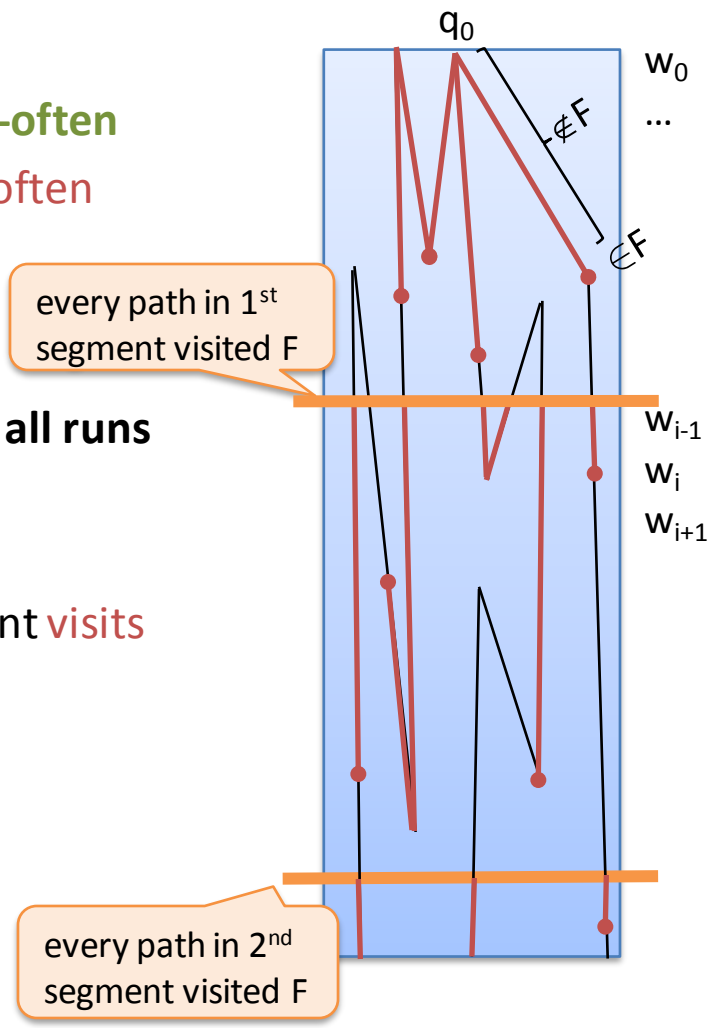
$\pi \in \mathcal{F}$



Complementation Construction

- A loop-free 2NcoBA $\mathcal{A}$ = (Q, Σ, δ, q_0, F)
  - **accepts** w
    :⇔ **ex. run** on w such that **no F-state occurs ∞-often**
  - rejects w ⇔ each run on w visits an F-state ∞-often

- NBA for the complement (sketch)
  1. Guess sequence $R_0R_1\ldots \in (2^Q)^\omega$ that represents **all runs** on w **ordered by head positions**.
  2. Guess **breakpoints**:
     - each run starting at the previous breakpoint visits F before reaching the next breakpoint
  3. Check locally that guesses are correct
  4. Check that **breakpoints** occur ∞-often.



Conclusion

- Construction scheme for translating AAs to NAs
  - Requires complementation construction for NA with co-acceptance condition
  - Requires AA to accept by memoryless runs
  - Previous translations can be seen as instances:
    unifies and simplifies constructions and proofs
- Novel alternation elimination for loop-free 2ABAs
  - Based on novel complementation construction for loop-free 2NcoBA
  - Constructions by Miyano-Hayashi and by Gastin-Oddoux are special cases

- Ongoing and future work
  - Scheme for automata that do not accept by memoryless runs
  - Translations for PSL and μLTL with past operators
  - Practical experiences of translating 2-way AAs to NAs