The Cayley-Graph of the Queue Monoid: Logic and Decidability

38th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science 2018, Ahmedabad

Faried Abu Zaid[1,2] Chris Köcher[2]

[1] Camelot Management Consultants, Munich

[2] Automata and Logics Group, Technische Universität Ilmenau

December 12, 2018

Motivation

Question

Is the Queue Monoid automatic?

- Queue Monoid is algebraic description of a queue's behavior
- Automatic structures have nice properties
  - e.g. decidable FO-theory [Khoussainov, Nerode 1995]
- The Queue Monoid's FO-theory is undecidable

Answer

No!

Motivation

Question (Huschenbett, Kuske, Zetzsche 2014)

Is the Cayley-graph of the Queue Monoid automatic?

- Queue Monoid is algebraic description of a queue's behavior
- Automatic structures have nice properties
  - e.g. decidable FO-theory [Khoussainov, Nerode 1995]
- The Queue Monoid's FO-theory is undecidable

Possible Approach

Prove that the FO-theory of the Queue Monoid's Cayley-graph is undecidable.

Question (Huschenbett, Kuske, Zetzsche 2014)

Is the Cayley-graph of the Queue Monoid automatic?

- Queue Monoid is algebraic description of a queue's behavior
- Automatic structures have nice properties
  - e.g. decidable FO-theory [Khoussainov, Nerode 1995]
- The Queue Monoid's FO-theory is undecidable

Here

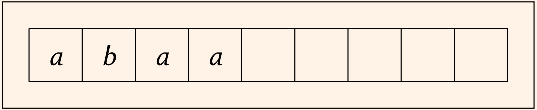
The FO-theory of the Queue Monoid's Cayley-graph is decidable.

Queues

- Let A be an alphabet ($|A| \geq 2$).
- two actions for each $a \in A$:
  - write letter a, denoted: a
  - read letter a, denoted: $\overline{a}$
- $\Sigma := \{a, \overline{a} \mid a \in A\}$

Example

$q = abaa$ $\qquad$ $t = b\overline{a}b\overline{b}$

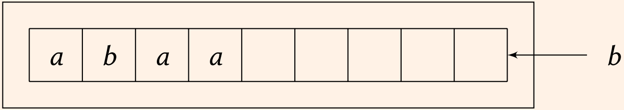


Queues

- Let A be an alphabet ($|A| \geq 2$).
- two actions for each $a \in A$:
  - write letter a, denoted: a
  - read letter a, denoted: $\overline{a}$
- $\Sigma := \{a, \overline{a} \mid a \in A\}$

Example

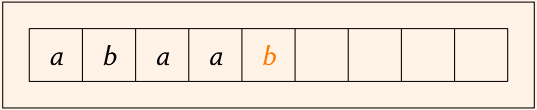
$q = abaa$ $\qquad$ $t = b\overline{a}b\overline{b}$



- Let A be an alphabet ($|A| \geq 2$).
- two actions for each $a \in A$:
  - write letter a, denoted: a
  - read letter a, denoted: $\overline{a}$
- $\Sigma := \{a, \overline{a} \mid a \in A\}$

Example

$q = abaa$ $\qquad$ $t = b\overline{a}b\overline{b}$

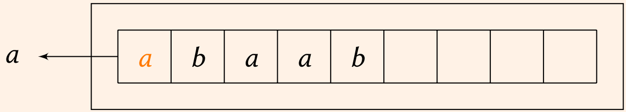


Queues

- Let A be an alphabet ($|A| \geq 2$).
- two actions for each $a \in A$:
  - write letter a, denoted: a
  - read letter a, denoted: $\overline{a}$
- $\Sigma := \{a, \overline{a} \mid a \in A\}$

Example

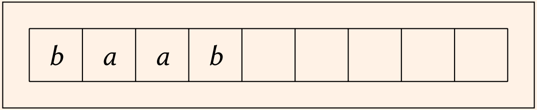
$q = abaa$ $\qquad$ $t = b\overline{a}b\overline{b}$



- Let A be an alphabet ($|A| \geq 2$).
- two actions for each $a \in A$:
  - write letter a, denoted: a
  - read letter a, denoted: $\overline{a}$
- $\Sigma := \{a, \overline{a} \mid a \in A\}$

Example

$q = abaa$ $\qquad$ $t = b\overline{a}b\overline{b}$

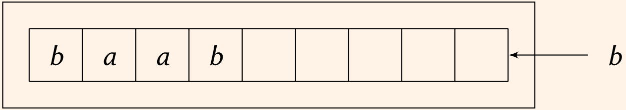


Queues

- Let A be an alphabet ($|A| \geq 2$).
- two actions for each $a \in A$:
  - write letter a, denoted: a
  - read letter a, denoted: $\overline{a}$
- $\Sigma := \{a, \overline{a} \mid a \in A\}$

Example

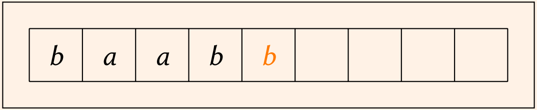
$q = abaa$ $\qquad$ $t = b\overline{a}b\overline{b}$



- Let A be an alphabet ($|A| \geq 2$).
- two actions for each $a \in A$:
  - write letter a, denoted: a
  - read letter a, denoted: $\overline{a}$
- $\Sigma := \{a, \overline{a} \mid a \in A\}$

Example

$q = abaa$ $\qquad$ $t = b\overline{a}b\overline{b}$

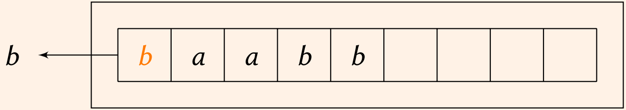


Queues

- Let A be an alphabet ($|A| \geq 2$).
- two actions for each $a \in A$:
  - write letter a, denoted: a
  - read letter a, denoted: $\overline{a}$
- $\Sigma := \{a, \overline{a} \mid a \in A\}$

Example

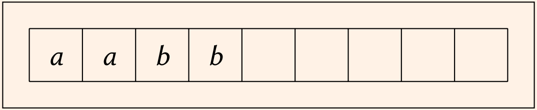
$q = abaa$ $t = b\overline{a}b\overline{b}$



- Let A be an alphabet ($|A| \geq 2$).
- two actions for each $a \in A$:
  - write letter a, denoted: a
  - read letter a, denoted: $\overline{a}$
- $\Sigma := \{a, \overline{a} \mid a \in A\}$

Example

$q = abaa$ $\qquad$ $t = b\overline{a}b\overline{b}$



The Queue Monoid

TECHNISCHE UNIVERSITÄT ILMENAU

Definition

$s, t \in \Sigma^*$ act equally (in symbols $s \equiv t$) if, and only if,

$$\forall p, q \in A^* : p \xrightarrow{s} q \iff p \xrightarrow{t} q \,.$$

Theorem (Huschenbett, Kuske, Zetzsche 2014)

$\equiv$ is the least congruence on Σ^* satisfying the following equations:

1. $a\overline{b} \equiv \overline{b}a$ *if* $a \neq b$
2. $a\overline{ac} \equiv \overline{a}a\overline{c}$
3. $ca\overline{a} \equiv c\overline{a}a$

for each $a, b, c \in A$.

Definition

$\mathcal{Q} := \Sigma^* /_{\equiv}$ is called the queue monoid.

Characteristics

TECHNISCHE UNIVERSITÄT ILMENAU

Definition

Let $[w]_\equiv \in \mathcal{Q}$. A characteristic of $[w]_\equiv$ is a triple $(\lambda, a_1 \ldots a_m, \rho) \in (A^*)^3$ with

$$\overline{\lambda} \cdot a_1\overline{a_1}a_2\overline{a_2} \ldots a_m\overline{a_m} \cdot \rho \equiv w\,.$$

Example

Let $t = [\overline{abac}abacaba\overline{aba}]_\equiv$.

- $\overline{abac}a\overline{a}b\overline{b}a\overline{a}caba \equiv \overline{abac}abacaba\overline{aba}$
- $(abac, aba, caba)$ is a characteristic of t

Definition

Let $[w]_\equiv \in \mathcal{Q}$. A characteristic of $[w]_\equiv$ is a triple $(\lambda, a_1 \ldots a_m, \rho) \in (A^*)^3$ with

$$\overline{\lambda} \cdot a_1\overline{a_1}a_2\overline{a_2} \ldots a_m\overline{a_m} \cdot \rho \equiv w\,.$$

Proposition (cf. Huschenbett, Kuske, Zetzsche 2014)

Each $t \in \mathcal{Q}$ has exactly one characteristic.

Definition

Let $t \in \mathcal{Q}$ and (w_L, w_M, w_R) be its characteristic. We denote the second component by $\mu(t) := w_M$.

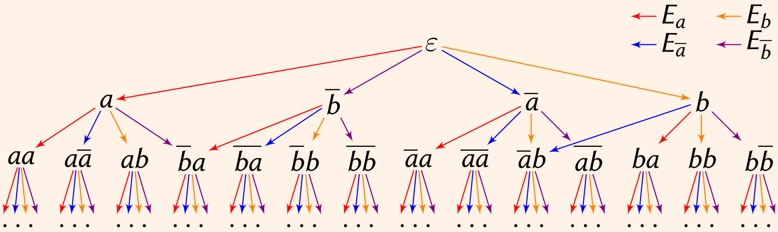
TECHNISCHE UNIVERSITÄT ILMENAU

Definition

The queue monoid's Cayley-graph is the Σ-labeled graph $\mathfrak{C} := (\mathcal{Q}, (E_\alpha)_{\alpha\in\Sigma})$ with

$$E_\alpha = \{(t, t\alpha) \mid t \in \mathcal{Q}\}\,.$$

Example ($A = \{a, b\}$)



Properties of the Cayley-Graph

Proposition

1. *$\mathfrak{C}$ is an acyclic graph with root ε.*
2. *$\mathfrak{C}$ has bounded out-degree and unbounded in-degree.*
3. *$\mathfrak{C}$ contains an infinite 2-dimensional grid as induced subgraph.*

Corollary (cf. Seese 1991)

The MSO-theory of $\mathfrak{C}$ is undecidable.

Main Theorem

Theorem

The FO-theory of $\mathfrak{C}$ is primitive recursive.

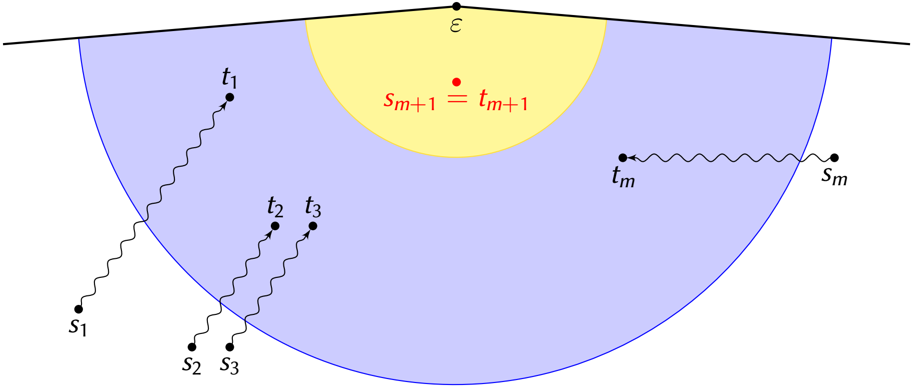
Idea (cf. Ferrante, Rackoff 1979)

For each element from $\mathcal{Q}$, find another one which is equivalent and close to the root ε.

- We prove this by induction on quantifier depth of an FO-formula.

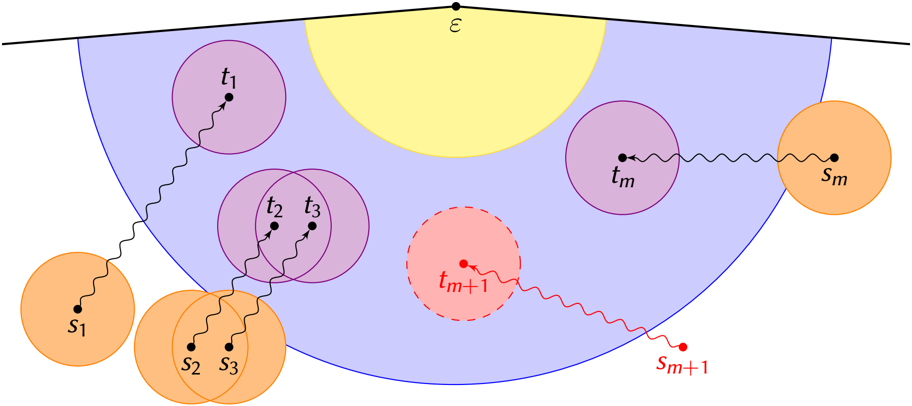
TECHNISCHE UNIVERSITÄT ILMENAU

- Let $\phi(\vec{y}) = \exists x\colon \psi(\vec{y}, x) \in \mathrm{FO}$ with m free variables and quantifier rank $\leq r + 1$.
- Let $\vec{s}, \vec{t} \in \mathcal{Q}^m$ with $(\mathfrak{C}, \vec{s}) \models \phi$ and $(\mathfrak{C}, \vec{t}) \models \phi$; and let $s_{m+1} \in \mathcal{Q}$ with $(\mathfrak{C}, \vec{s}, s_{m+1}) \models \psi$.
- Find "small" t_{m+1} with $(\mathfrak{C}, \vec{t}, t_{m+1}) \models \psi$.
  - first case:



Induction Step

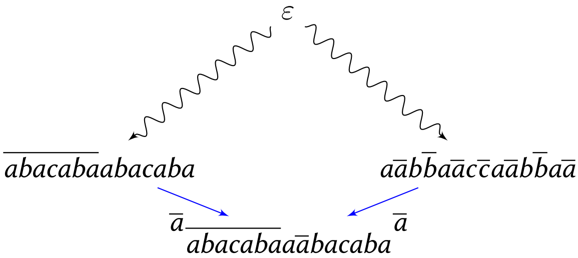
- Let $\phi(\vec{y}) = \exists x\colon \psi(\vec{y}, x) \in \mathrm{FO}$ with m free variables and quantifier rank $\leq r + 1$.
- Let $\vec{s}, \vec{t} \in \mathcal{Q}^m$ with $(\mathfrak{C}, \vec{s}) \models \phi$ and $(\mathfrak{C}, \vec{t}) \models \phi$; and let $s_{m+1} \in \mathcal{Q}$ with $(\mathfrak{C}, \vec{s}, s_{m+1}) \models \psi$.
- Find "small" t_{m+1} with $(\mathfrak{C}, \vec{t}, t_{m+1}) \models \psi$.
  - second case:



- Consider the transformations having *abacaba* as subsequence of write and read actions:

$$(abacaba, \varepsilon, abacaba) \rightsquigarrow \overline{abacaba}abacaba$$
$$(abacab, a, bacaba) \rightsquigarrow \overline{abacab}a\bar{a}bacaba$$
$$(abac, aba, caba) \rightsquigarrow \overline{abac}a\bar{a}b\bar{b}a\bar{a}caba$$
$$(\varepsilon, abacaba, \varepsilon) \rightsquigarrow a\bar{a}b\bar{b}a\bar{a}c\bar{c}a\bar{a}b\bar{b}a\bar{a}$$

- Shortest path between $\overline{abacaba}abacaba$ and $a\bar{a}b\bar{b}a\bar{a}c\bar{c}a\bar{a}b\bar{b}a\bar{a}$?



- Consider the transformations having *abacaba* as subsequence of write and read actions:

$$\begin{array}{ccc} (abacaba, \varepsilon, abacaba) & \rightsquigarrow & \overline{abacaba}abacaba \\ (abacab, a, bacaba) & \rightsquigarrow & \overline{abacab}a\bar{a}bacaba \\ (abac, aba, caba) & \rightsquigarrow & \overline{abac}a\bar{a}b\bar{b}a\bar{a}caba \\ (\varepsilon, abacaba, \varepsilon) & \rightsquigarrow & a\bar{a}b\bar{b}a\bar{a}c\bar{c}a\bar{a}b\bar{b}a\bar{a} \end{array}$$

Definition

Let $v, w \in A^*$.

- v is a border of w if it is a prefix and a suffix of w.
- The border-decomposition $(w_0, \ldots, w_n)$ of w is the sequence of all borders of w in length-increasing order.

Skeletons & Instantiations

TECHNISCHE UNIVERSITÄT ILMENAU

- Recall $\vec{w} = (\varepsilon, a, aba, abacaba)$ is the border-decomposition of *abacaba*.
- Here: $w_{i+1} = w_i x_i w_i$ for each $0 \leq i < 3$ and some $x_i \in A^*$

Definition

Let $(w_0, \ldots, w_n)$ be the border-decomposition of $w \in A^*$ and $r \in \mathbb{N}$. The *r*-skeleton $\mathcal{S}_r(w)$ of w is the sequence $(s_0, \ldots, s_{n-1})$ where s_i is the maximal prefix of length at most r of $w_i^{-1}w$.

Example ($w = abacaba$, $r = 2$)

- *abacaba*
- *abacaba*
- *abacaba*

$\Rightarrow \mathcal{S}_2(w) = (ab, ba, ca)$

- Recall $\vec{w} = (\varepsilon, a, aba, abacaba)$ is the border-decomposition of *abacaba*.
- Here: $w_{i+1} = w_i x_i w_i$ for each $0 \leq i < 3$ and some $x_i \in A^*$

Definition

Let $(w_0, \ldots, w_n)$ be the border-decomposition of $w \in A^*$ and $r \in \mathbb{N}$. The r-skeleton $\mathcal{S}_r(w)$ of w is the sequence $(s_0, \ldots, s_{n-1})$ where s_i is the maximal prefix of length at most r of $w_i^{-1} w$.

Definition

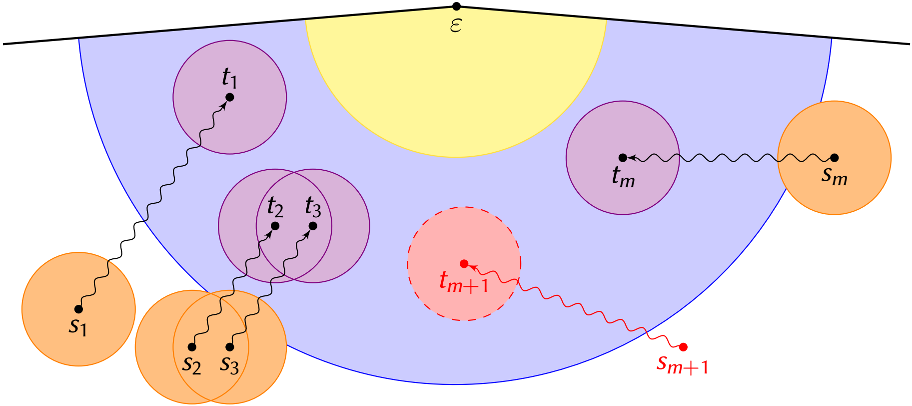
An r-instantiation of an r-skeleton $(s_0, \ldots, s_{n-1})$ is the word v_n with $v_0 = \varepsilon$ and $v_{i+1} = v_i\ s_i y_i\ v_i$ (for some special $y_i \in A^{\mathcal{O}(n+r)}$).

Lemma

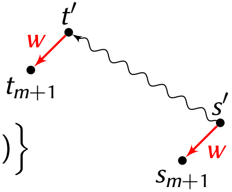
Let v be an r-instantiation of an r-skeleton $(s_0, \ldots, s_{n-1})$. Then $|v| = \mathcal{O}(2^{nr})$ and $\mathcal{S}_r(v) = (s_0, \ldots, s_{n-1})$.

Induction Step

- Let $\phi(\vec{y}) = \exists x\colon \psi(\vec{y}, x) \in$ FO with m free variables and quantifier rank $\leq r + 1$.
- Let $\vec{s}, \vec{t} \in \mathcal{Q}^m$ with $(\mathfrak{C}, \vec{s}) \models \phi$ and $(\mathfrak{C}, \vec{t}) \models \phi$; and let $s_{m+1} \in \mathcal{Q}$ with $(\mathfrak{C}, \vec{s}, s_{m+1}) \models \psi$.
- Find "small" t_{m+1} with $(\mathfrak{C}, \vec{t}, t_{m+1}) \models \psi$.
  - second case:



- find $s' \in \mathcal{Q}$ close to s_{m+1} with
  - $\mu(s')$ has as many borders as possible
  - hence, $\mathcal{S}_{\mathcal{O}(2^{r+m})}(\mu(s'))$ is as long as possible
- we can construct an automaton $\mathcal{A}_{s'}$ with



$$L(\mathcal{A}_{s'}) = \left\{ V \in (A^{\mathcal{O}(2^{r+m})})^* \;\middle|\; V \equiv_{r+1}^{\text{Büchi}} \mathcal{S}_{\mathcal{O}(2^{r+m})}(\mu(s')) \right\}$$

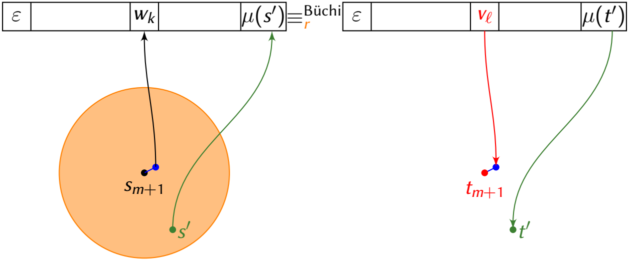
  - $\equiv_{r+1}^{\text{Büchi}}$ is related to Büchi's logic on words
- find some small word $V \in L(\mathcal{A}_{s'})$ and construct an $\mathcal{O}(2^{r+m})$-instantiation v of V
- choose $t' \in \mathcal{Q}$ with $\mu(t') = v$ appropriately
- recall the path from s' to s_{m+1} and go a similar path from t' to new t_{m+1}

Problem

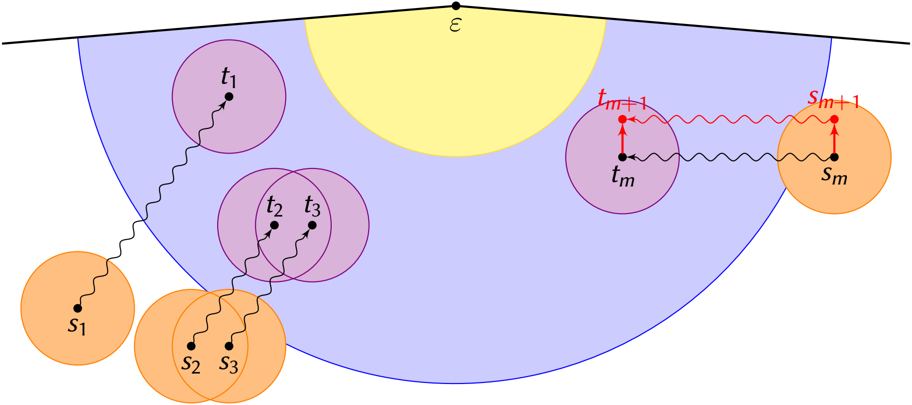
There may be multiple nodes t_{m+1} with path from t' labelled with w.

Choosing the Right Node (1)

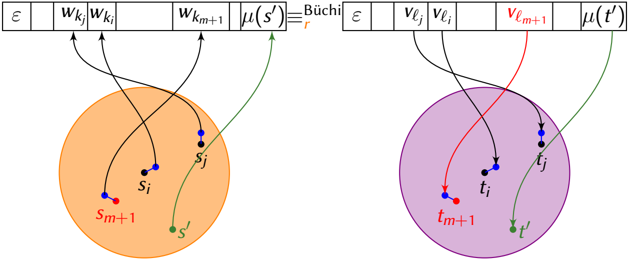
- Let $(w_0, \ldots, w_n)$ and $(v_0, \ldots, v_{n'})$ be the border-decompositions of $\mu(s')$ resp. $\mu(t')$.
- Recall that $\mathcal{S}_{\mathcal{O}(2^{r+m})}(\mu(s')) \equiv^{\text{Büchi}}_{r+1} \mathcal{S}_{\mathcal{O}(2^{r+m})}(\mu(t'))$.
- Let $0 \leq k \leq n$ be maximal such that w_k is a prefix of $\mu(s_{m+1})$.
- Hence, there is ℓ with $(\mathcal{S}_{\mathcal{O}(2^{r+m})}(\mu(s')), k) \equiv^{\text{Büchi}}_{r} (\mathcal{S}_{\mathcal{O}(2^{r+m})}(\mu(t')), \ell)$.
- Find t_{m+1} such that v_ℓ is maximal with v_ℓ is prefix of $\mu(t_{m+1})$.



- Let $\phi(\vec{y}) = \exists x \colon \psi(\vec{y}, x) \in \mathrm{FO}$ with m free variables and quantifier rank $\leq r + 1$.
- Let $\vec{s}, \vec{t} \in \mathcal{Q}^m$ with $(\mathfrak{C}, \vec{s}) \models \phi$ and $(\mathfrak{C}, \vec{t}) \models \phi$; and let $s_{m+1} \in \mathcal{Q}$ with $(\mathfrak{C}, \vec{s}, s_{m+1}) \models \psi$.
- Find "small" t_{m+1} with $(\mathfrak{C}, \vec{t}, t_{m+1}) \models \psi$.
  - third case:



- s_{m+1} is close to s_i ($1 \leq i \leq m$ minimal)
- Let s' and t' be constructed from s_i as in 2nd case.



Conclusion & Open Problems

Theorem

The FO*-theory of* $\mathfrak{C}$ *is primitive recursive.*

Open Problems

1. Is the FO-theory of $\mathfrak{C}$ decidable in elementary time?
2. Is $\mathfrak{C}$ automatic?
3. Is the FO-theory of the (Partially) Lossy Queue Monoid's Cayley-graph decidable?
   - (Partially) Lossy Queues can forget parts of their content at any time.

Thank you!