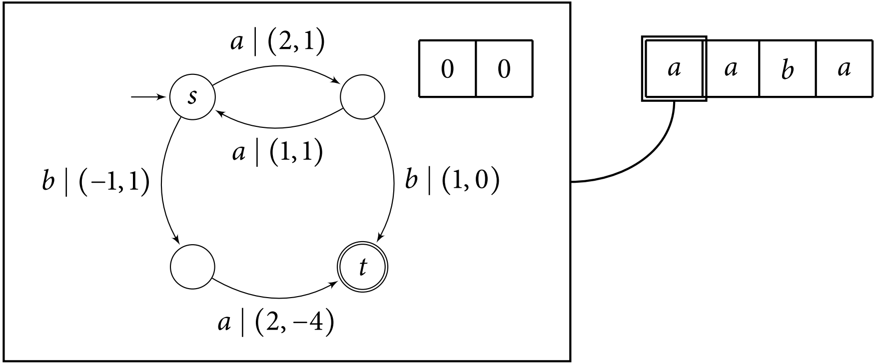
# Regular Separators for VASS Coverability Languages

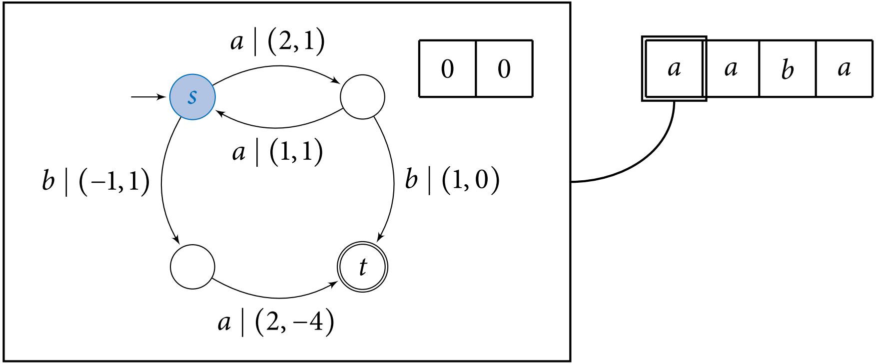
Chris Köcher    Georg Zetzsche

Max Planck Institute for Software Systems, Kaiserslautern

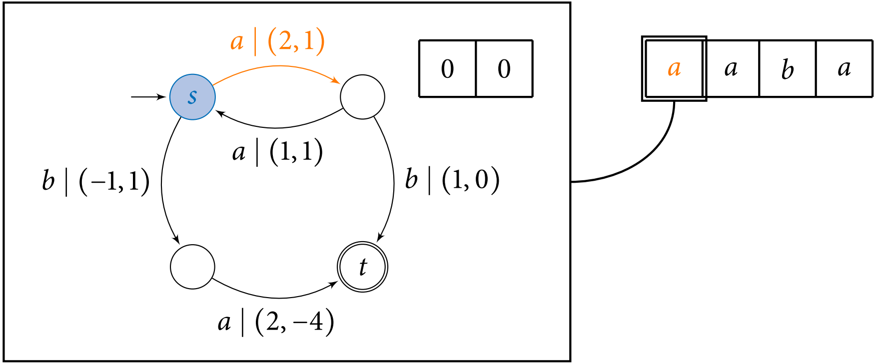
# Vector Addition Systems with States (VASS)



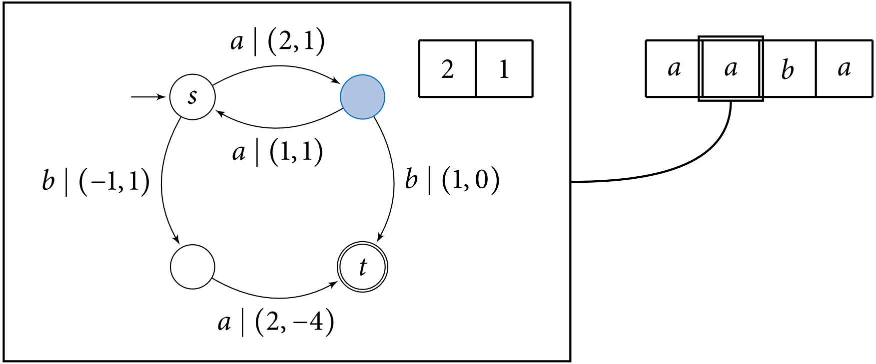
# Vector Addition Systems with States (VASS)



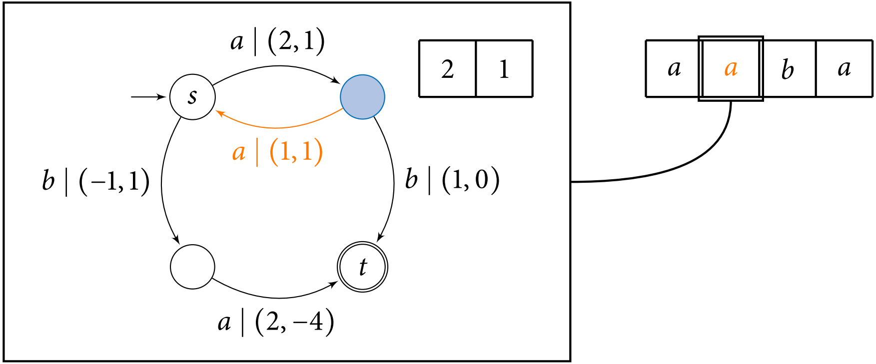
# Vector Addition Systems with States (VASS)



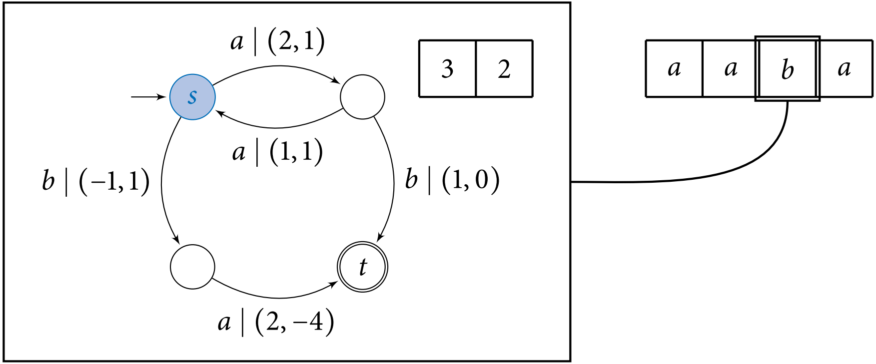
# Vector Addition Systems with States (VASS)



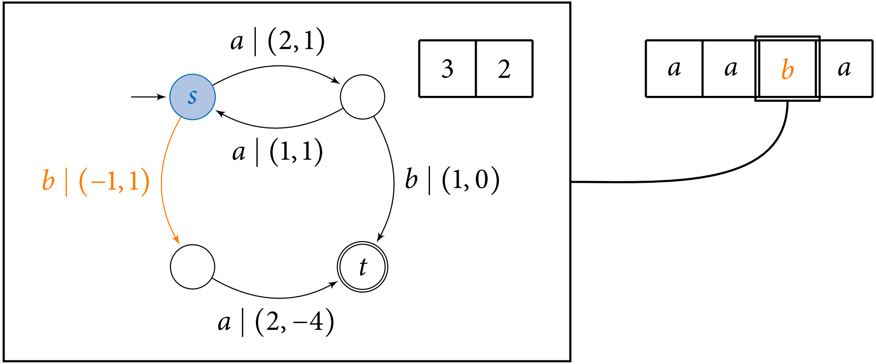
# Vector Addition Systems with States (VASS)



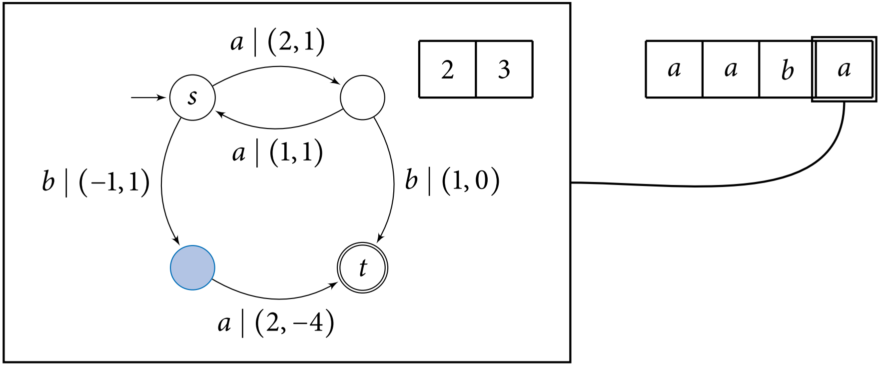
# Vector Addition Systems with States (VASS)



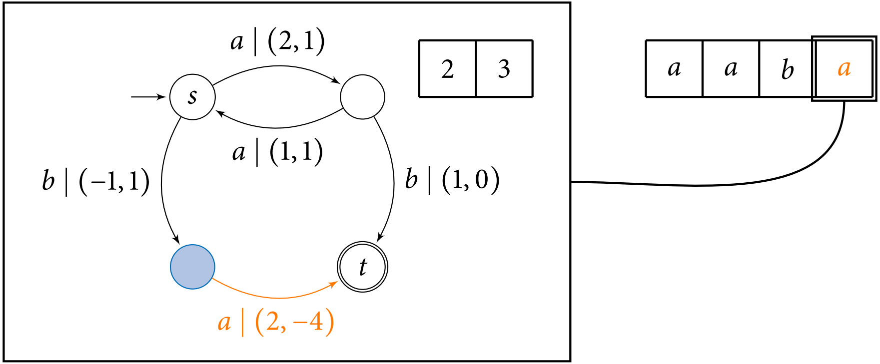
# Vector Addition Systems with States (VASS)



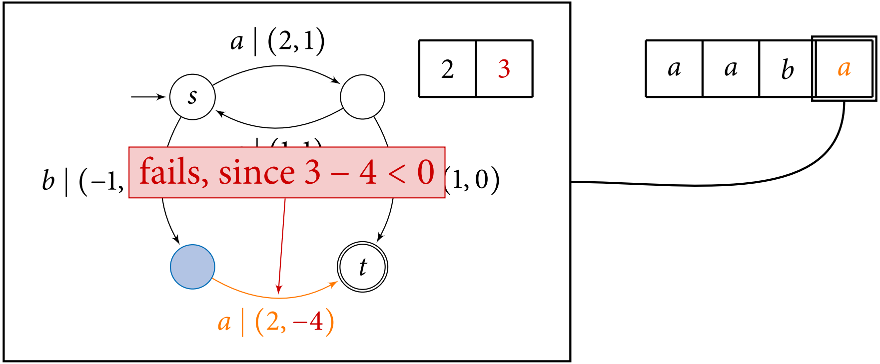
# Vector Addition Systems with States (VASS)



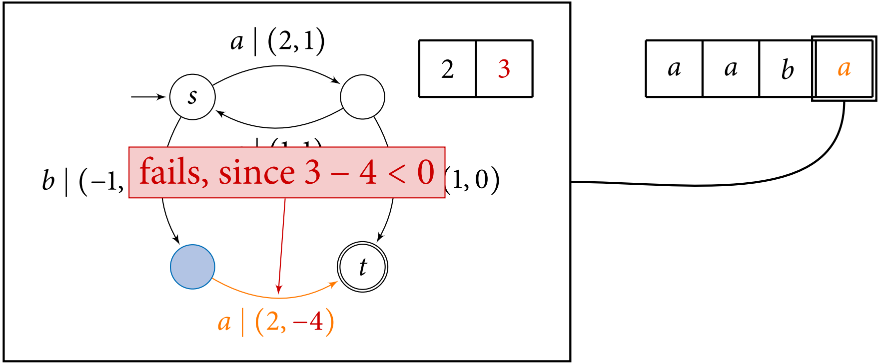
# Vector Addition Systems with States (VASS)



# Vector Addition Systems with States (VASS)



# Vector Addition Systems with States (VASS)

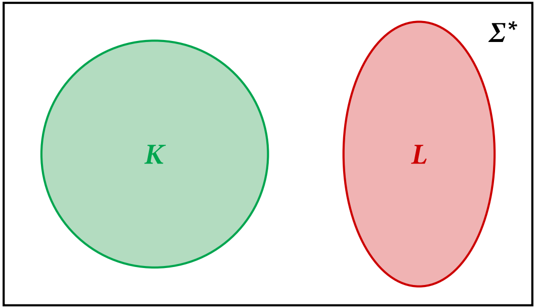



- $L(\mathfrak{V}) = \{w \in \Sigma^* \mid \exists \vec{v} \in \mathbb{N}^d \colon (s, \vec{0}) \xrightarrow{w}_{\mathfrak{V}} (t, \vec{v}) \geq (t, \vec{0})\}$

# Regular Separability (1)

## Problem

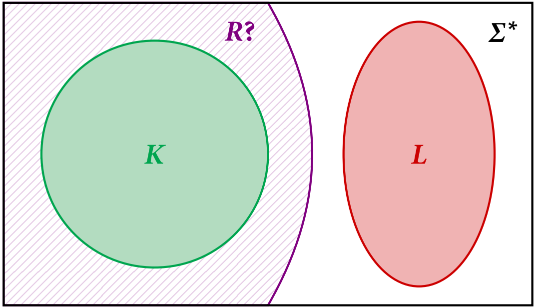
- Given two languages $K, L \subseteq \Sigma^*$.



# Regular Separability (1)

## Problem

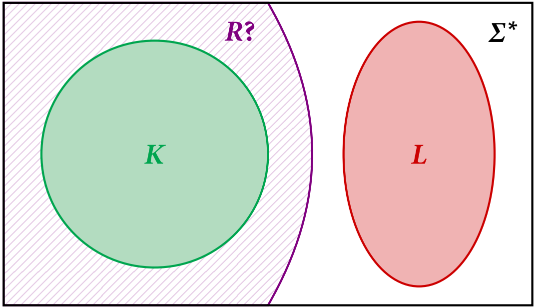
- Given two languages $K, L \subseteq \Sigma^*$.
- Is there a regular language $R \subseteq \Sigma^*$ with $K \subseteq R$ and $L \cap R = \emptyset$?



# Regular Separability (1)

## Problem

- Given two languages $K, L \subseteq \Sigma^*$.
- Is there a regular language $R \subseteq \Sigma^*$ with $K \subseteq R$ and $L \cap R = \varnothing$?




- Note: Regular Separability ≠ Disjointness!

# Regular Separability (2)

**Theorem (Czerwiński et al. @ CONCUR 2018)**

*Let $\mathfrak{V}$ and $\mathfrak{W}$ be two VASS. Then $L(\mathfrak{V})$ and $L(\mathfrak{W})$ are regular separable if, and only if, $L(\mathfrak{V}) \cap L(\mathfrak{W}) = \varnothing$.*

# Regular Separability (2)

**Theorem (Czerwiński et al. @ CONCUR 2018)**

*Let $\mathfrak{V}$ and $\mathfrak{W}$ be two VASS. Then $L(\mathfrak{V})$ and $L(\mathfrak{W})$ are regular separable if, and only if, $L(\mathfrak{V}) \cap L(\mathfrak{W}) = \emptyset$.*

**Question**

What is the size of a regular separator of $L(\mathfrak{V})$ and $L(\mathfrak{W})$?

- Czerwiński et al.: doubly exp. lower bound & triply exp. upper bound

# Regular Separability (2)

**Theorem (Czerwiński et al. @ CONCUR 2018)**

*Let $\mathfrak{V}$ and $\mathfrak{W}$ be two VASS. Then $L(\mathfrak{V})$ and $L(\mathfrak{W})$ are regular separable if, and only if, $L(\mathfrak{V}) \cap L(\mathfrak{W}) = \varnothing$.*

**Question**

What is the size of a regular separator of $L(\mathfrak{V})$ and $L(\mathfrak{W})$?

- Czerwiński et al.: doubly exp. lower bound & triply exp. upper bound

**Theorem (Main Theorem)**

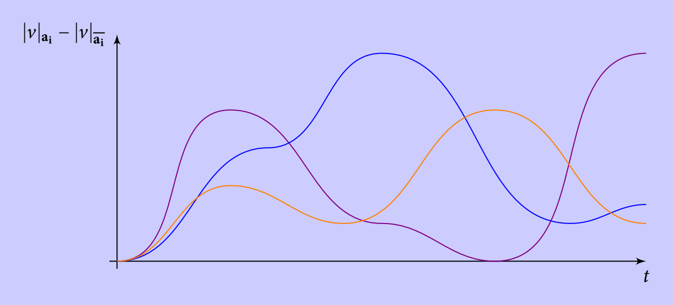
*Let $\mathfrak{V}$ and $\mathfrak{W}$ be two VASS with $\leq n$ states and updates of norm $\leq m$. If $L(\mathfrak{V}) \cap L(\mathfrak{W}) = \varnothing$ then there is an separating NFA with at most $(n+m)^{2^{\mathrm{poly}(d)}}$ many states.*

# Proof (1): Reduce to Counter Instructions

- $\Gamma_d = \{\mathbf{a_i}, \overline{\mathbf{a_i}} \mid 1 \leq i \leq d\}$
  - $\mathbf{a_i}$ increase counter $i$ by 1
  - $\overline{\mathbf{a_i}}$ decrease counter $i$ by 1
- $C_d = \{w \in \Gamma_d^* \mid \forall$ prefixes $v$ of $w, 1 \leq i \leq d\colon |v|_{\mathbf{a_i}} \geq |v|_{\overline{\mathbf{a_i}}}\}$

# Proof (1): Reduce to Counter Instructions

- $\Gamma_d = \{\mathbf{a_i}, \overline{\mathbf{a_i}} \mid 1 \le i \le d\}$
  - $\mathbf{a_i}$ increase counter $i$ by 1
  - $\overline{\mathbf{a_i}}$ decrease counter $i$ by 1
- $C_d = \{w \in \Gamma_d^* \mid \forall$ prefixes $v$ of $w, 1 \le i \le d \colon |v|_{\mathbf{a_i}} \ge |v|_{\overline{\mathbf{a_i}}}\}$



# Proof (1): Reduce to Counter Instructions

- $\Gamma_d = \{\mathbf{a_i}, \overline{\mathbf{a_i}} \mid 1 \le i \le d\}$
  - $\mathbf{a_i}$ increase counter $i$ by 1
  - $\overline{\mathbf{a_i}}$ decrease counter $i$ by 1
- $C_d = \{w \in \Gamma_d^* \mid \forall$ prefixes $v$ of $w, 1 \le i \le d\colon |v|_{\mathbf{a_i}} \ge |v|_{\overline{\mathbf{a_i}}}\}$

**Lemma (Jantzen 1979)**

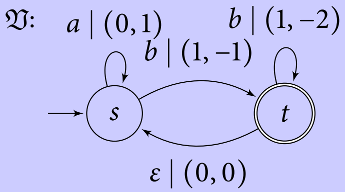
*$L \subseteq \Sigma^*$ is a VASS coverability language iff there is a rational transduction $T$ with $L = T(C_d)$.*

# Proof (1): Reduce to Counter Instructions

- $\Gamma_d = \{\mathbf{a_i}, \overline{\mathbf{a_i}} \mid 1 \leq i \leq d\}$
  - $\mathbf{a_i}$ increase counter $i$ by 1
  - $\overline{\mathbf{a_i}}$ decrease counter $i$ by 1
- $C_d = \{w \in \Gamma_d^* \mid \forall$ prefixes $v$ of $w, 1 \leq i \leq d\colon |v|_{\mathbf{a_i}} \geq |v|_{\overline{\mathbf{a_i}}}\}$

## Lemma (Jantzen 1979)

*$L \subseteq \Sigma^*$ is a VASS coverability language iff there is a rational transduction $T$ with $L = T(C_d)$.*

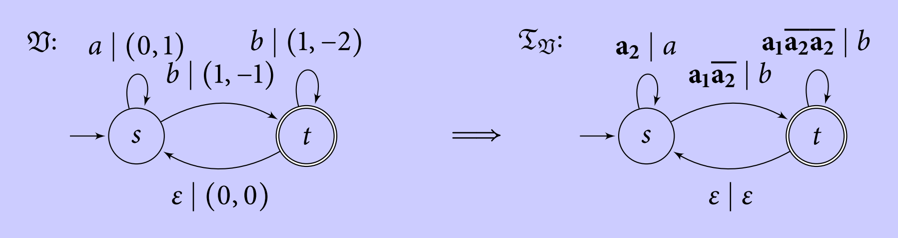


# Proof (1): Reduce to Counter Instructions

- $\Gamma_d = \{\mathbf{a_i}, \overline{\mathbf{a_i}} \mid 1 \leq i \leq d\}$
  - $\mathbf{a_i}$ increase counter $i$ by 1
  - $\overline{\mathbf{a_i}}$ decrease counter $i$ by 1
- $C_d = \{w \in \Gamma_d^* \mid \forall$ prefixes $v$ of $w, 1 \leq i \leq d\colon |v|_{\mathbf{a_i}} \geq |v|_{\overline{\mathbf{a_i}}}\}$

## Lemma (Jantzen 1979)

*$L \subseteq \Sigma^*$ is a VASS coverability language iff there is a rational transduction $T$ with $L = T(C_d)$.*



# Proof (1): Reduce to Counter Instructions

- $\Gamma_d = \{\mathbf{a_i}, \overline{\mathbf{a_i}} \mid 1 \leq i \leq d\}$
  - $\mathbf{a_i}$ increase counter $i$ by 1
  - $\overline{\mathbf{a_i}}$ decrease counter $i$ by 1
- $C_d = \{w \in \Gamma_d^* \mid \forall$ prefixes $v$ of $w, 1 \leq i \leq d \colon |v|_{\mathbf{a_i}} \geq |v|_{\overline{\mathbf{a_i}}}\}$

## Lemma (Jantzen 1979)

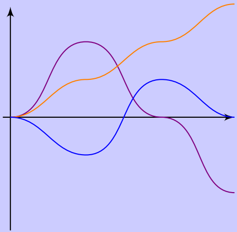
*$L \subseteq \Sigma^*$ is a VASS coverability language iff there is a rational transduction $T$ with $L = T(C_d)$.*

## Corollary

*Let $\mathfrak{V}$ and $\mathfrak{W}$ be two VASS and $T$ be a rational transduction with $L(\mathfrak{W}) = T(C_d)$. Then $L(\mathfrak{V})$ is regularly separable from $L(\mathfrak{W})$ iff $T^{-1}(L(\mathfrak{V}))$ is regularly separable from $C_d$.*

# Proof (1): Reduce to Counter Instructions

$$T^{-1} \Big( \quad S \quad ( \quad C_d \quad )\Big)$$

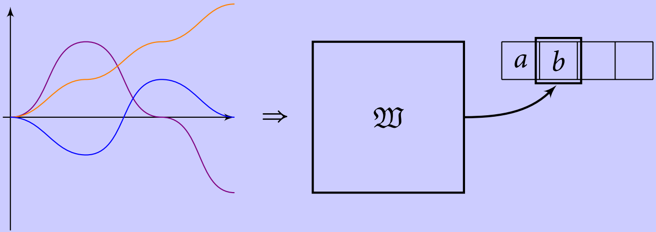


**Corollary**

*Let $\mathfrak{V}$ and $\mathfrak{W}$ be two VASS and $T$ be a rational transduction with $L(\mathfrak{W}) = T(C_d)$. Then $L(\mathfrak{V})$ is regularly separable from $L(\mathfrak{W})$ iff $T^{-1}(L(\mathfrak{V}))$ is regularly separable from $C_d$.*

# Proof (1): Reduce to Counter Instructions

$$T^{-1} \Big( \quad S \quad \big( \quad C_d \quad \big) \Big)$$

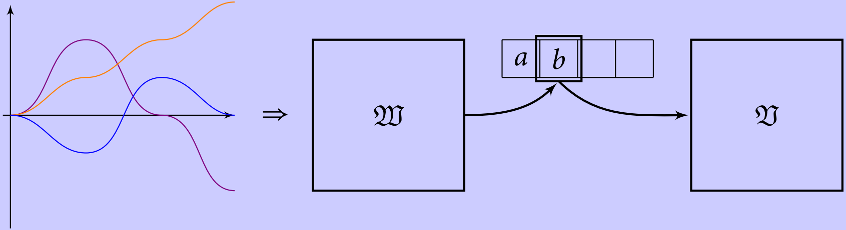



## Corollary

*Let $\mathfrak{V}$ and $\mathfrak{W}$ be two VASS and $T$ be a rational transduction with $L(\mathfrak{W}) = T(C_d)$. Then $L(\mathfrak{V})$ is regularly separable from $L(\mathfrak{W})$ iff $T^{-1}(L(\mathfrak{V}))$ is regularly separable from $C_d$.*

# Proof (1): Reduce to Counter Instructions

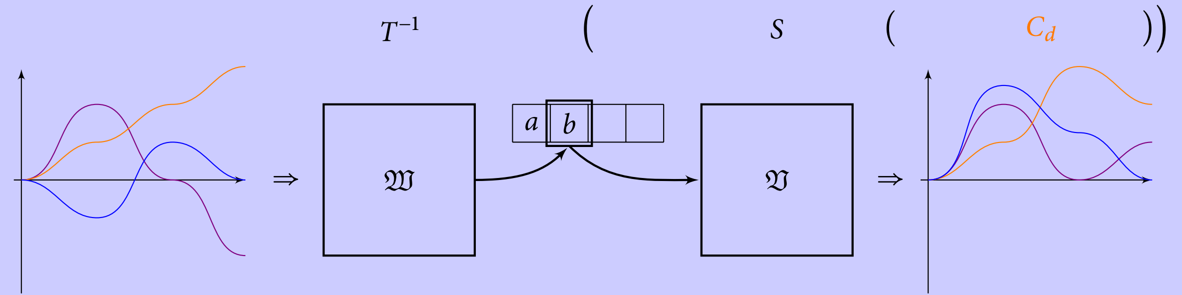
$$T^{-1}\Big( S \big( C_d \big)\Big)$$




## Corollary

*Let $\mathfrak{V}$ and $\mathfrak{W}$ be two VASS and $T$ be a rational transduction with $L(\mathfrak{W}) = T(C_d)$. Then $L(\mathfrak{V})$ is regularly separable from $L(\mathfrak{W})$ iff $T^{-1}(L(\mathfrak{V}))$ is regularly separable from $C_d$.*

# Proof (1): Reduce to Counter Instructions



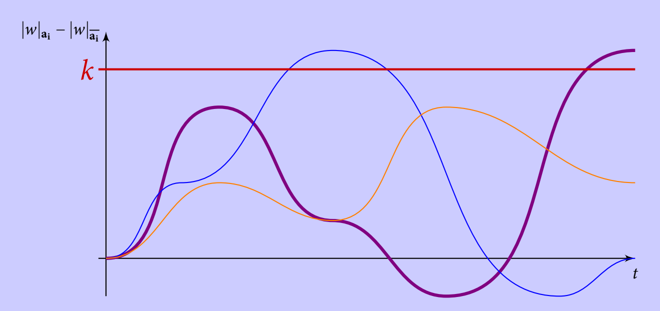

**Corollary**

*Let $\mathfrak{V}$ and $\mathfrak{W}$ be two VASS and $T$ be a rational transduction with $L(\mathfrak{W}) = T(C_d)$. Then $L(\mathfrak{V})$ is regularly separable from $L(\mathfrak{W})$ iff $T^{-1}(L(\mathfrak{V}))$ is regularly separable from $C_d$.*

# Proof (2): Basic Separators

- For $k \in \mathbb{N}$ let $B_k \subseteq \Gamma_d^*$ be the following language: $w \in B_k$ iff there is $1 \leq i \leq d$ with
  - there is a prefix $v$ of $w$ with $|v|_{\mathbf{a_i}} < |v|_{\overline{\mathbf{a_i}}}$ and
  - each proper prefix $u$ of $v$ satisfies $0 \leq |u|_{\mathbf{a_i}} - |u|_{\overline{\mathbf{a_i}}} \leq k$

- For $k \in \mathbb{N}$ let $B_k \subseteq \Gamma_d^*$ be the following language: $w \in B_k$ iff there is $1 \le i \le d$ with
  - there is a prefix $v$ of $w$ with $|v|_{\mathbf{a_i}} < |v|_{\overline{\mathbf{a_i}}}$ and
  - each proper prefix $u$ of $v$ satisfies $0 \le |u|_{\mathbf{a_i}} - |u|_{\overline{\mathbf{a_i}}} \le k$



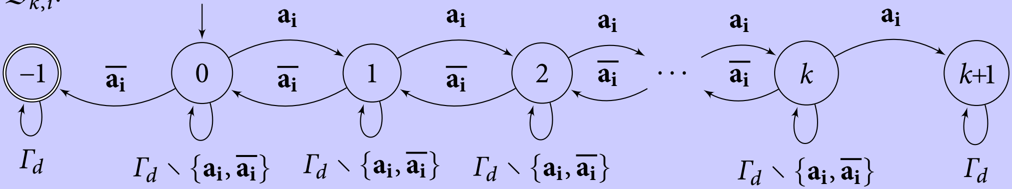
# Proof (2): Basic Separators

- For $k \in \mathbb{N}$ let $B_k \subseteq \Gamma_d^*$ be the following language: $w \in B_k$ iff there is $1 \leq i \leq d$ with
  - there is a prefix $v$ of $w$ with $|v|_{\mathbf{a_i}} < |v|_{\overline{\mathbf{a_i}}}$ and
  - each proper prefix $u$ of $v$ satisfies $0 \leq |u|_{\mathbf{a_i}} - |u|_{\overline{\mathbf{a_i}}} \leq k$
- $B_k$ is accepted by a DFA of size $O(k^d)$.

# Proof (2): Basic Separators

- For $k \in \mathbb{N}$ let $B_k \subseteq \Gamma_d^*$ be the following language: $w \in B_k$ iff there is $1 \leq i \leq d$ with
  - there is a prefix $v$ of $w$ with $|v|_{\mathbf{a_i}} < |v|_{\overline{\mathbf{a_i}}}$ and
  - each proper prefix $u$ of $v$ satisfies $0 \leq |u|_{\mathbf{a_i}} - |u|_{\overline{\mathbf{a_i}}} \leq k$
- $B_k$ is accepted by a DFA of size $O(k^d)$.

$\mathfrak{B}_{k,i}$:




$$B_k = \bigcup_{1 \leq i \leq d} L(\mathfrak{B}_{k,i})$$

# Proof (2): Basic Separators

- For $k \in \mathbb{N}$ let $B_k \subseteq \Gamma_d^*$ be the following language: $w \in B_k$ iff there is $1 \le i \le d$ with
  - there is a prefix $v$ of $w$ with $|v|_{\mathbf{a_i}} < |v|_{\overline{\mathbf{a_i}}}$ and
  - each proper prefix $u$ of $v$ satisfies $0 \le |u|_{\mathbf{a_i}} - |u|_{\overline{\mathbf{a_i}}} \le k$
- $B_k$ is accepted by a DFA of size $O(k^d)$.

**Theorem (Czerwiński & Zetzsche @ LICS 2020)**

*Let $\mathfrak{V}$ and $\mathfrak{W}$ be two VASS with $L(\mathfrak{V}) \cap L(\mathfrak{W}) = \emptyset$ and let $T$ be a rational transduction with $L(\mathfrak{W}) = T(C_d)$. Then $B_k$ is a regular separator of $T^{-1}(L(\mathfrak{V}))$ and $C_d$ for a $k \in \mathbb{N}$.*

# Proof (3): Covering

**Theorem (Rackoff 1978)**

*Let $\mathfrak{V}$ be a VASS, $c$ be a configuration of $\mathfrak{V}$, and a vector $\vec{v} \in \mathbb{N}^d$ with $c \to_{\mathfrak{V}}^{*} (t, \vec{v}) \geq (t, \vec{0})$.*
*Then there is $0 \leq \ell \leq \underbrace{(n+m)^{2^{\mathrm{poly}(d)}}}_{=:\mathrm{Rackoff}(\mathfrak{V})}$ and $\vec{w} \in \mathbb{N}^d$ with $c \to_{\mathfrak{V}}^{\ell} (t, \vec{w}) \geq (t, \vec{0})$.*
*Here, $n$ is the number of states in $\mathfrak{V}$ and $m$ is the norm of the counter updates in $\mathfrak{V}$.*

# Proof (3): Covering

## Theorem (Rackoff 1978)

*Let $\mathfrak{V}$ be a VASS, $c$ be a configuration of $\mathfrak{V}$, and a vector $\vec{v} \in \mathbb{N}^d$ with $c \to_{\mathfrak{V}}^{*} (t, \vec{v}) \geq (t, \vec{0})$. Then there is $0 \leq \ell \leq \underbrace{(n+m)^{2^{\mathrm{poly}(d)}}}_{=:\mathrm{Rackoff}(\mathfrak{V})}$ and $\vec{w} \in \mathbb{N}^d$ with $c \to_{\mathfrak{V}}^{\ell} (t, \vec{w}) \geq (t, \vec{0})$.*

*Here, $n$ is the number of states in $\mathfrak{V}$ and $m$ is the norm of the counter updates in $\mathfrak{V}$.*

## Theorem

*Let $\mathfrak{V}$ and $\mathfrak{W}$ be two VASS with $L(\mathfrak{V}) \cap L(\mathfrak{W}) = \emptyset$ and let $T$ be a rational transduction with $L(\mathfrak{W}) = T(C_d)$. Then $B_{\mathrm{Rackoff}(\mathfrak{V}\times\mathfrak{W})}$ is a regular separator of $T^{-1}(L(\mathfrak{V}))$ and $C_d$.*

# Proof (3): Covering

## Theorem (Rackoff 1978)

*Let $\mathfrak{V}$ be a VASS, $c$ be a configuration of $\mathfrak{V}$, and a vector $\vec{v} \in \mathbb{N}^d$ with $c \to_{\mathfrak{V}}^{*} (t, \vec{v}) \geq (t, \vec{0})$. Then there is $0 \leq \ell \leq \underbrace{(n+m)^{2^{\mathrm{poly}(d)}}}_{=:\mathrm{Rackoff}(\mathfrak{V})}$ and $\vec{w} \in \mathbb{N}^d$ with $c \to_{\mathfrak{V}}^{\ell} (t, \vec{w}) \geq (t, \vec{0})$. Here, $n$ is the number of states in $\mathfrak{V}$ and $m$ is the norm of the counter updates in $\mathfrak{V}$.*

## Theorem

*Let $\mathfrak{V}$ and $\mathfrak{W}$ be two VASS with $L(\mathfrak{V}) \cap L(\mathfrak{W}) = \emptyset$ and let $T$ be a rational transduction with $L(\mathfrak{W}) = T(C_d)$. Then $B_{\mathrm{Rackoff}(\mathfrak{V}\times\mathfrak{W})}$ is a regular separator of $T^{-1}(L(\mathfrak{V}))$ and $C_d$.*

- Finally, $T(B_{\mathrm{Rackoff}(\mathfrak{V}\times\mathfrak{W})})$ is a regular separator of $L(\mathfrak{V})$ and $L(\mathfrak{W})$. □

# Conclusion

| | | NFAs | DFAs |
|---|---|---|---|
| $d$ as input | | 2-exp. | 3-exp. |
| $d$ fixed | $d \geq 2$ | | |
| | $d = 1$ | | |

# Conclusion

| | | NFAs | | DFAs | |
|---|---|---|---|---|---|
| | | unary | binary | unary | binary |
| $d$ as input | | 2-exp. | | 3-exp. | |
| $d$ fixed | $d \geq 2$ | poly. | exp. | exp. | 2-exp. |
| | $d = 1$ | poly. | exp. | exp. | exp. |

# Conclusion

| | | NFAs | | DFAs | |
|---|---|---|---|---|---|
| | | unary | binary | unary | binary |
| $d$ as input | | 2-exp. | | 3-exp. | |
| $d$ fixed | $d \geq 2$ | poly. | exp. | exp. | 2-exp. |
| | $d = 1$ | poly. | exp. | exp. | exp. |

Thank you!