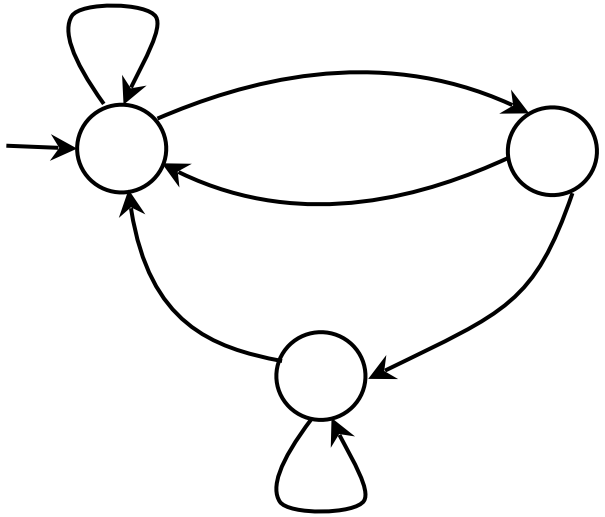
Realizable and Context-Free Hyperlanguages

Hadar Frenkel, CISPA Helmholtz Center for Information Security, Germany

Sarai Sheinvald, Braude College of Engineering, Israel

Hyperproperties [Clarkson & Schneider '10]

Standard Properties: behavior of the traces of the system



"Every request is eventually granted"

Property = a set of traces. LTL, Regular expressions, …

Hyperproperties: behavior of the system in its entirety

"**For every** trace with high-security signals,
there exists a trace in which they are unobservable"

Hyperproperty = a set of sets of traces. HyperLTL

In this talk

Finite-Word Hyperautomata

- Hyperautomata
- Realizability of hyperlanguages

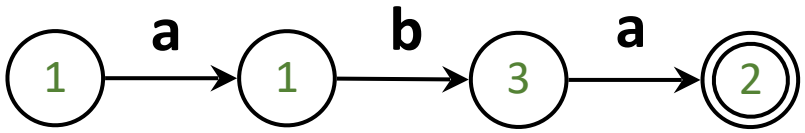
Context-Free Hypergrammars

- Hypergrammars
- Synchronous hypergrammars
- Emptiness and membership problems for hypergrammars

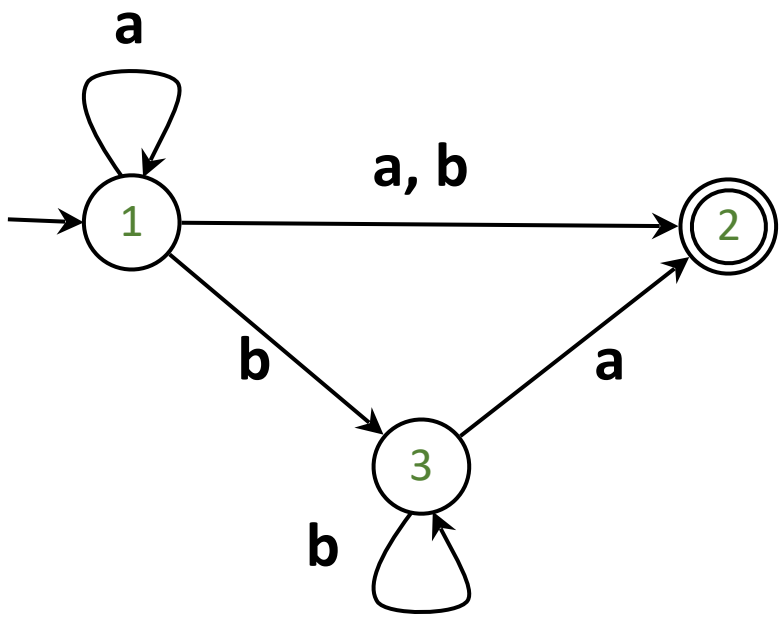
Finite-word automata

NFA: non-det finite word **automaton**

Runs: on **words**



Accepts a word **w** if **w** can reach an accepting state



The **language** of an NFA **A**: the set of all words that **A** accepts

NFA: regular languages

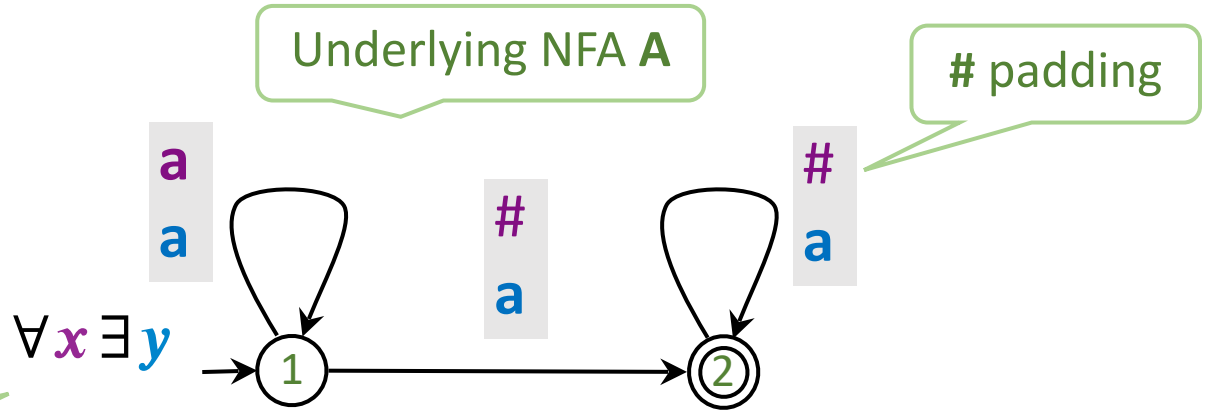
Hyperautomata [Bonakdarpour & Sheinvald '21]

NFH: non-det finite word **hyperautomaton**

Runs: on **assignments** to the **variables**

x ← **a a** # #

y ← **a a a a**



An NFH accepts a **language** L if L satisfies α w.r.t. A

NFH: regular hyperlanguages

"For every word there exists a longer word"

Hyperlanguage: all infinite languages over $\{a\}$

$$\{L \mid L \text{ is infinite}\}$$

Set of sets of words

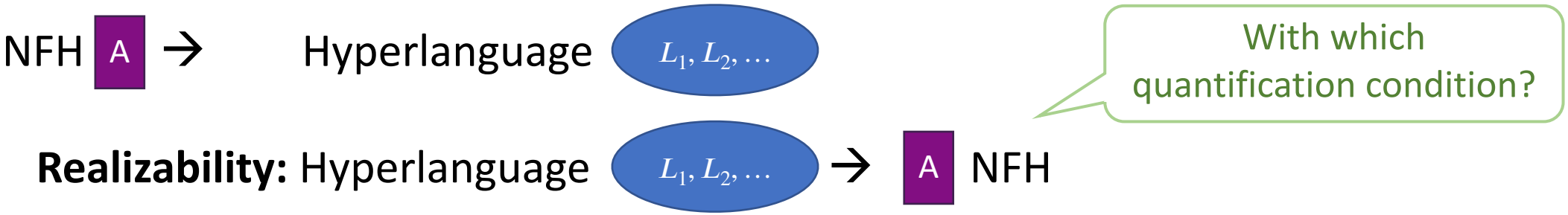
Hyperautomata

Can express regular hyperproperties:

Noninference: replacing high-security commands with dummy value does not affect the low-security observable data.

$$\begin{matrix}\forall x \\ \exists y\end{matrix}\left(\begin{matrix}low,\ high \\ low,\ high \rightarrow low^{dummy}\end{matrix}\right)^{*}$$

Realizability



Def: $\mathscr{L}$ = $L_1, L_2, \ldots$ is **α-realizable** if there is an **α-NFH** for $\mathscr{L}$

We study the basic case of singleton hyperlanguages: $\mathscr{L} = \{L\}$

- Various types of L
- Realizability and unrealizability results for various α

In this talk

Finite-Word Hyperautomata

- Hyperautomata
- Realizability of $\{L\}$ ✓
  - Finite \ infinite L
  - Ordered L
  - Regular L

Context-Free Hypergrammars

- Hypergrammars
- Synchronous hypergrammars
- Emptiness and membership problems for hypergrammars

Realizability of $\{L\}$

Simple α does not suffice

$\forall x$ A : if L is accepted then also $L' \subset L$ $\Rightarrow$ **not ∀-realizable**

$\exists x$ A : if L is accepted with $x \leftarrow w$ then also L' for $\mathrm{w} \in L' \cap L$ $\Rightarrow$ **not ∃-realizable**

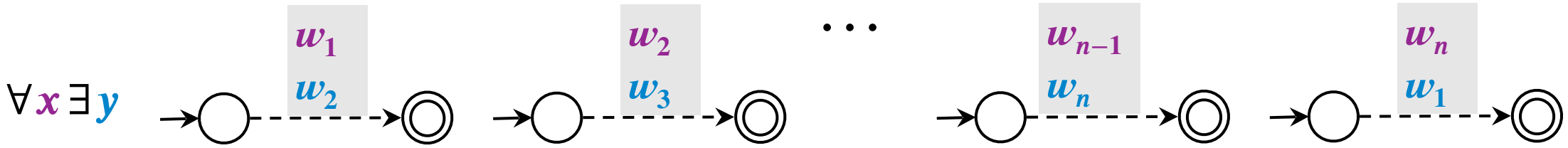
Realizability of $\{L\}$: finite L

Simple α does not suffice

$\forall x$ A : if L is accepted then also $L' \subset L$ $\Rightarrow$ **not ∀-realizable**

$\exists x$ A : if L is accepted with $x \leftarrow w$ then also L' for $w \in L' \cap L$ $\Rightarrow$ **not ∃-realizable**

<u>If L is finite then $\{L\}$ is $\forall\exists$-realizable</u>: $L = \{w_1, \ldots w_n\}$

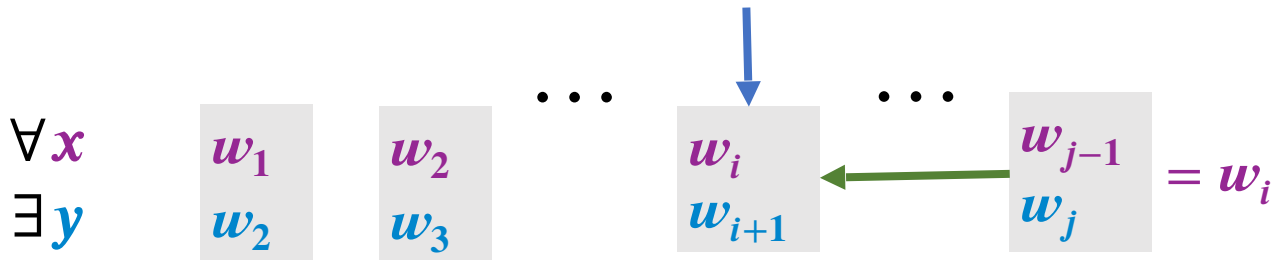


It is also
$\exists^*\forall^*$-realizable

(Un)Realizability of $\{L\}$: infinite L

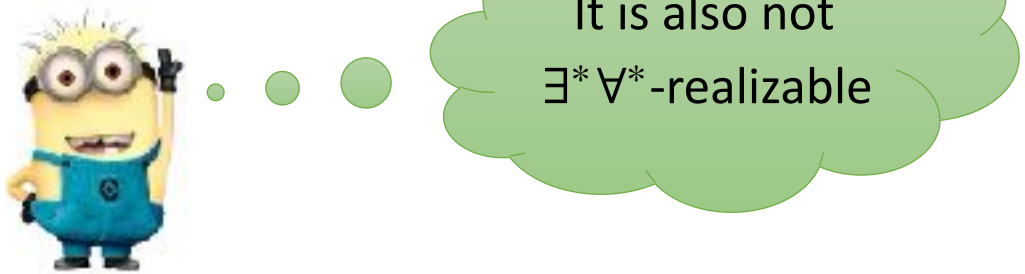
Simple α does not suffice

$\{L\}$ is **not $\forall\exists$-realizable:** Suppose that $\forall x \exists y$ A accepts L



$$\{w_i, w_{i+1}, \dots\} \in \mathscr{L}\{A\}$$

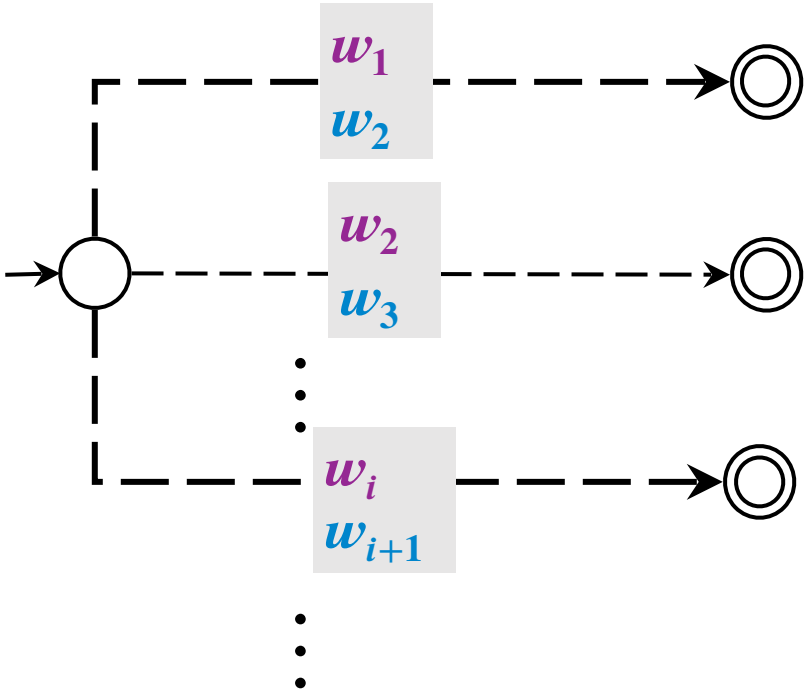
$$\{w_i, w_{i+1}, \dots, w_j\} \in \mathscr{L}\{A\}$$



Realizability of $\{L\}$: Ordered L

Def: L is **ordered** if:

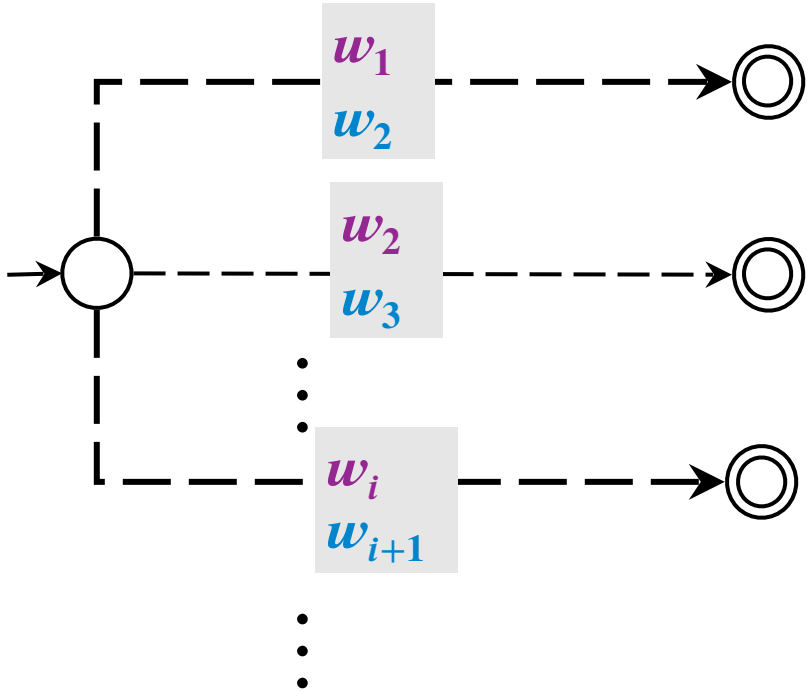
$L = \{w_1, w_2, \ldots\}$ and there exists an NFA A_L



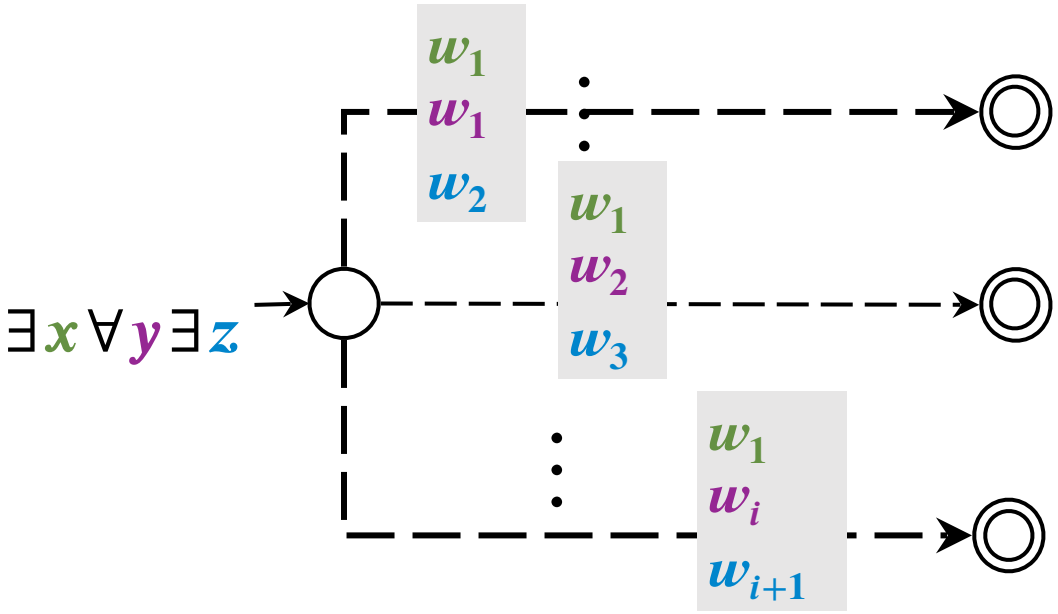
Realizability of $\{L\}$: Ordered L

Def: L is **ordered** if:

$L = \{w_1, w_2, \ldots\}$ and there exists an NFA A_L:

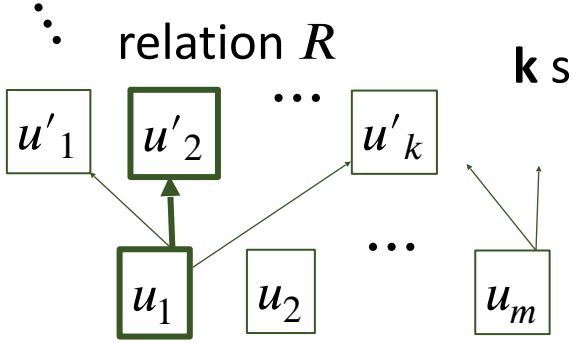


If L is ordered then $\{L\}$ is $\exists\forall\exists$ -realizable:



Realizability of $\{L\}$: Partially Ordered L

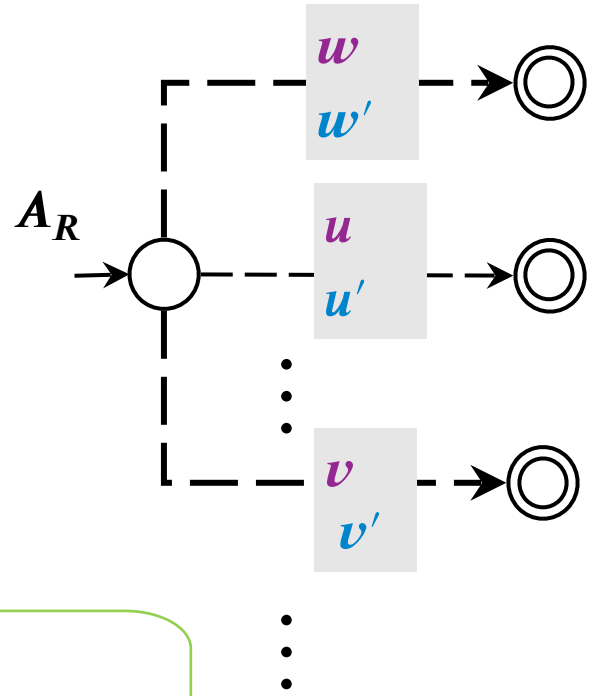
Def: L is **(m,k)-ordered** if: $L = \{w_1, w_2, \ldots\}$



k succesors for each word

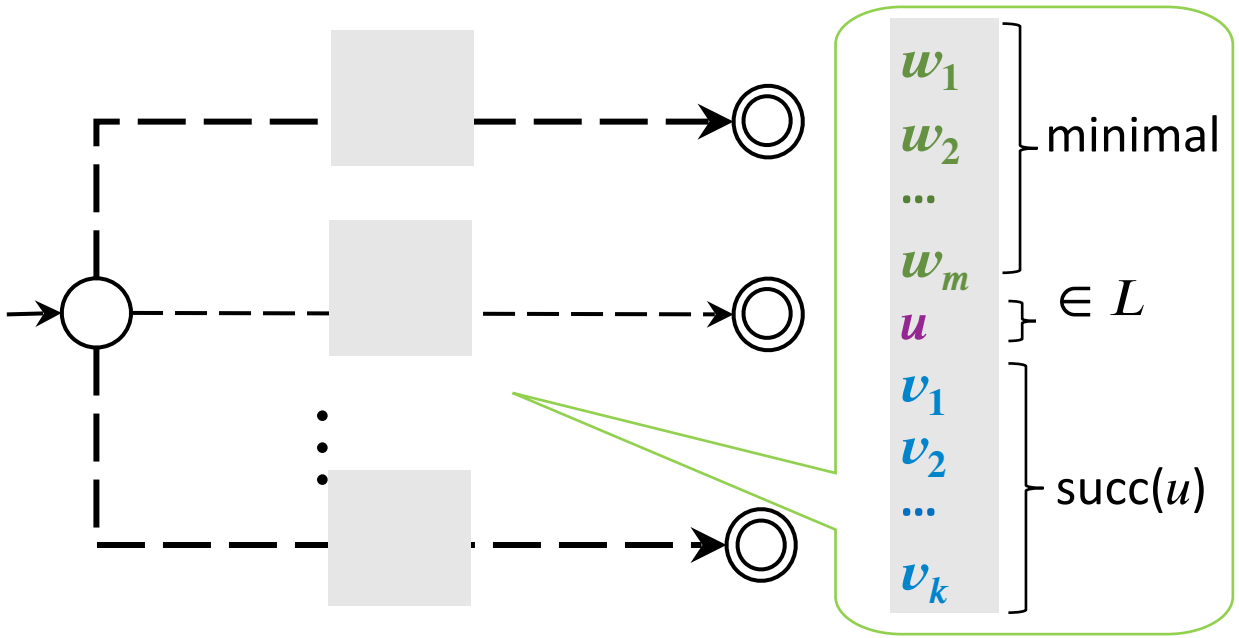
m minimal elements

There exists an NFA A_R for R



If L is (m,k)-ordered then $\{L\}$ is $\exists^m \forall \exists^k$ -realizable:

$$\exists x_1 \ldots x_m \forall y \exists z_1 \ldots z_k$$



Realizability of $\{L\}$: Regular L

If L is regular then $\{L\}$ is **(m,k)**-ordered and $\exists^m \forall \exists^k$ -realizable

$\exists \forall \exists$ Realizable proof: automatic structures

m:

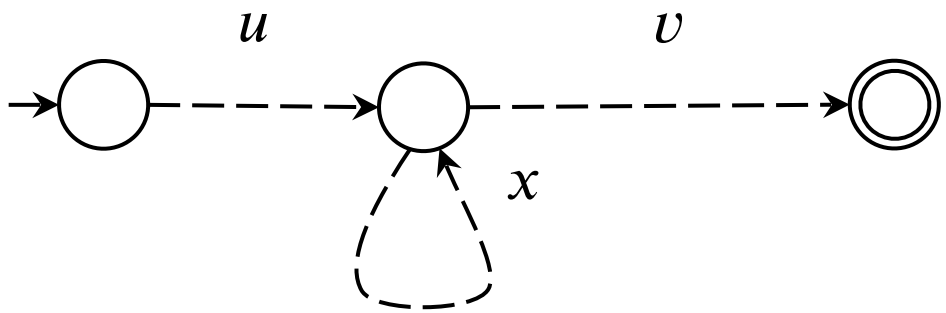
Minimal elements - simple paths to accepting states

$uv \in \mathrm{Min}$

k:

Successors words - one additional simple cycle

$uxv \in succ(uv)$



In this talk

Finite-Word Hyperautomata

- Hyperautomata
- Realizability
  - Finite \ infinite
  - Ordered
  - Regular

Context-Free Hypergrammars

- Hypergrammars
- Synchronous hypergrammars
- Emptiness & membership

Context-Free Grammars (CGF)

Terminal word

Derives: **words**

$S \Rightarrow a\ S\ b \Rightarrow a\ a\ S\ b\ b \Rightarrow a\ a\ b\ b$

Derivation rule

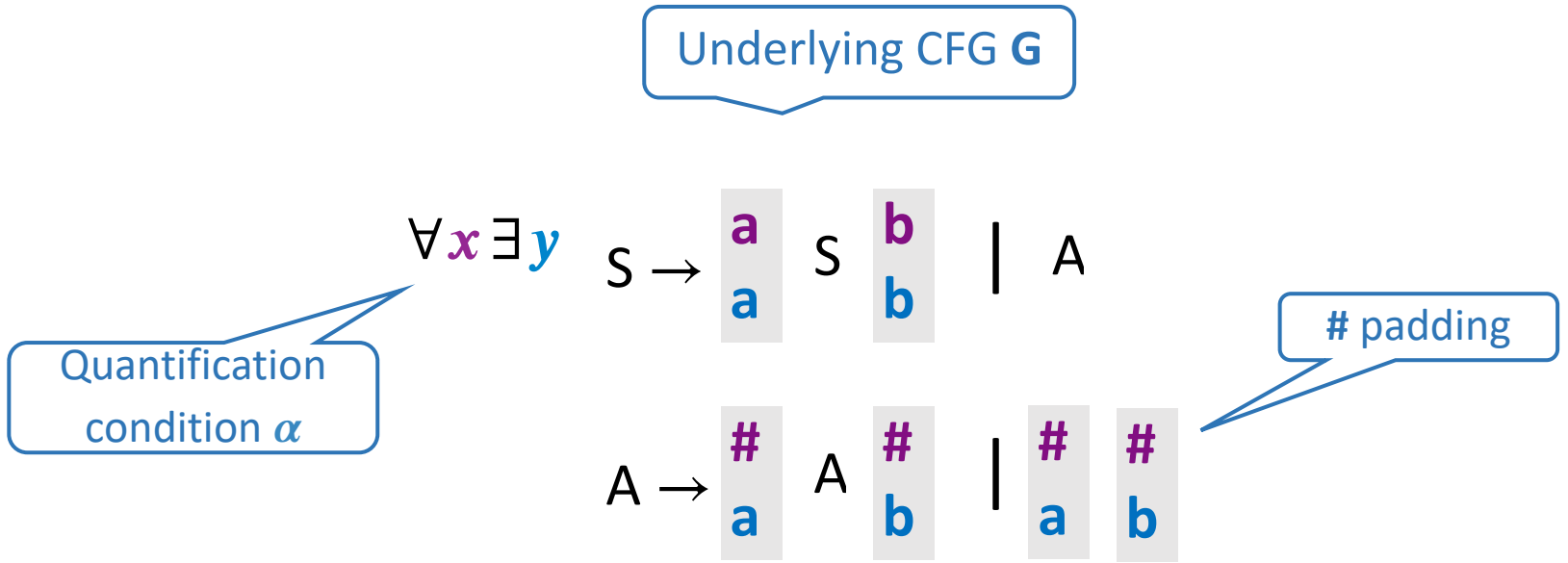
(initial) variable

$S \rightarrow a\ S\ b \mid \epsilon$

A terminal word **w** is in the **language** of a CGF **G**
if **w** can be derived from the initial variable

Context-Free Hypergrammars

CFHG: context-free **hypergrammar**



Context-Free Hypergrammars

CFHG: context-free **hypergrammar**

Derives: **assignments** to the **variables**

x ← **a a # # b**
b

y ← **a a a b b**
b

Underlying CFG **G**

$\forall x \exists y$

Quantification condition α

$S \rightarrow \begin{matrix}a\\a\end{matrix} S \begin{matrix}b\\b\end{matrix} \mid A$

$A \rightarrow \begin{matrix}\#\\a\end{matrix} A \begin{matrix}\#\\b\end{matrix} \mid \begin{matrix}\#\\a\end{matrix} \begin{matrix}\#\\b\end{matrix}$

padding

A GFHG accepts a **language** L if L satisfies α w.r.t. G

"For every word of type $a^n b^n$ there exists a longer word"

Hyperlanguage: all infinite languages

$\subseteq \{a^n b^n \mid n \in \mathbb{N}\}$

Set of sets of words

Context-Free Hypergrammars

$\forall x \exists y$

$$S \rightarrow \begin{matrix}\mathbf{a}\\\mathbf{a}\end{matrix} \; S \; \begin{matrix}\mathbf{b}\\\mathbf{b}\end{matrix} \mid A$$

$$A \rightarrow \begin{matrix}\mathbf{\#}\\\mathbf{a}\end{matrix} \; A \; \begin{matrix}\mathbf{\#}\\\mathbf{b}\end{matrix} \mid \begin{matrix}\mathbf{\#}\\\mathbf{a}\end{matrix} \; \begin{matrix}\mathbf{\#}\\\mathbf{b}\end{matrix}$$

Context-Free Hypergrammars

$\forall x \exists y$

$$S \rightarrow \begin{matrix}a\\a\end{matrix}\ S\ \begin{matrix}b\\b\end{matrix} \mid A$$

$$A \rightarrow \begin{matrix}\#\\a\end{matrix}\ A\ \begin{matrix}\#\\b\end{matrix} \mid \begin{matrix}\#\\a\end{matrix}\ \begin{matrix}\#\\b\end{matrix}$$

$$S \Rightarrow \begin{matrix}a\\a\end{matrix}\ S\ \begin{matrix}b\\b\end{matrix} \Rightarrow \begin{matrix}a\\a\end{matrix}\ \begin{matrix}a\\a\end{matrix}\ S\ \begin{matrix}b\\b\end{matrix}\ \begin{matrix}b\\b\end{matrix} \Rightarrow \begin{matrix}a\\a\end{matrix}\ \begin{matrix}a\\a\end{matrix}\ A\ \begin{matrix}b\\b\end{matrix}\ \begin{matrix}b\\b\end{matrix} \Rightarrow \begin{matrix}a\\a\end{matrix}\ \begin{matrix}a\\a\end{matrix}\ \begin{matrix}\#\\a\end{matrix}\ A\ \begin{matrix}\#\\b\end{matrix}\ \begin{matrix}b\\b\end{matrix}\ \begin{matrix}b\\b\end{matrix} \Rightarrow \begin{matrix}a\\a\end{matrix}\ \begin{matrix}a\\a\end{matrix}\ \begin{matrix}\#\\a\end{matrix}\ \begin{matrix}\#\\b\end{matrix}\ \begin{matrix}b\\b\end{matrix}\ \begin{matrix}b\\b\end{matrix}$$

$$\begin{matrix}a\\a\end{matrix}\ \begin{matrix}a\\a\end{matrix}\ \begin{matrix}b\\a\end{matrix}\ \begin{matrix}b\\b\end{matrix}\ b\ b$$

Context-Free Hypergrammars

$\forall x \exists y$

$$S \to \begin{matrix}\mathbf{a}\\\mathbf{a}\end{matrix}\ S\ \begin{matrix}\mathbf{b}\\\mathbf{b}\end{matrix} \mid A$$

$$A \to \begin{matrix}\mathbf{\#}\\\mathbf{a}\end{matrix}\ A\ \begin{matrix}\mathbf{\#}\\\mathbf{b}\end{matrix} \mid \begin{matrix}\mathbf{\#}\\\mathbf{a}\end{matrix}\ \begin{matrix}\mathbf{\#}\\\mathbf{b}\end{matrix}$$

$$S \Rightarrow \begin{matrix}a\\a\end{matrix}\ S\ \begin{matrix}b\\b\end{matrix} \Rightarrow \begin{matrix}a\\a\end{matrix}\ \begin{matrix}a\\a\end{matrix}\ S\ \begin{matrix}b\\b\end{matrix}\ \begin{matrix}b\\b\end{matrix} \Rightarrow \begin{matrix}a\\a\end{matrix}\ \begin{matrix}a\\a\end{matrix}\ A\ \begin{matrix}b\\b\end{matrix}\ \begin{matrix}b\\b\end{matrix} \Rightarrow \begin{matrix}a\\a\end{matrix}\ \begin{matrix}a\\a\end{matrix}\ \begin{matrix}\#\\a\end{matrix}\ A\ \begin{matrix}\#\\b\end{matrix}\ \begin{matrix}b\\b\end{matrix}\ \begin{matrix}b\\b\end{matrix} \Rightarrow \begin{matrix}a\\a\end{matrix}\ \begin{matrix}a\\a\end{matrix}\ \begin{matrix}\#\\a\end{matrix}\ \begin{matrix}\#\\b\end{matrix}\ \begin{matrix}b\\b\end{matrix}\ \begin{matrix}b\\b\end{matrix}$$

at the middle of words leads to *asynchronization*

Synchronous Context-Free Hypergrammars

Easy solution:

hypergrammar G: $\forall x \exists y$ G

G $\cap$ $\begin{matrix} \Sigma^* \cdot \{\#\}^* \\ \Sigma^* \cdot \{\#\}^* \end{matrix}$

Avoid # at the middle of the word

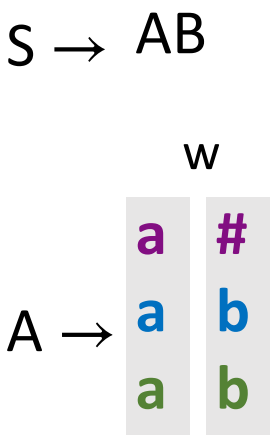
a	a	#	#	b	b
a	a	a	b	b	b

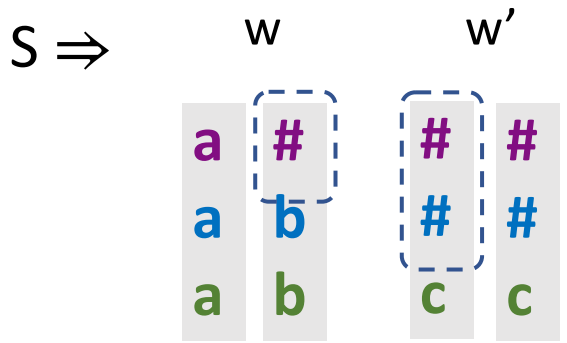
Result: only the synchronous part of G

Can we define a hypergrammar that is **inherently** synchronous?

Synchronous Context-Free Hypergrammars

Can we define a hypergrammar that is **inherently** synchronous?



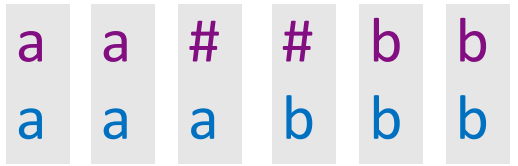


Rgt(w) ⊆ Lft(w')

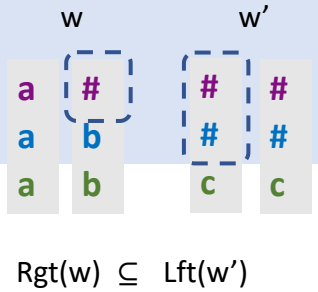
set of indices in which w contains # on the right

set of indices in which w' contains # on the left

Avoid # at the middle of the word



Synchronous Context-Free Hypergrammars



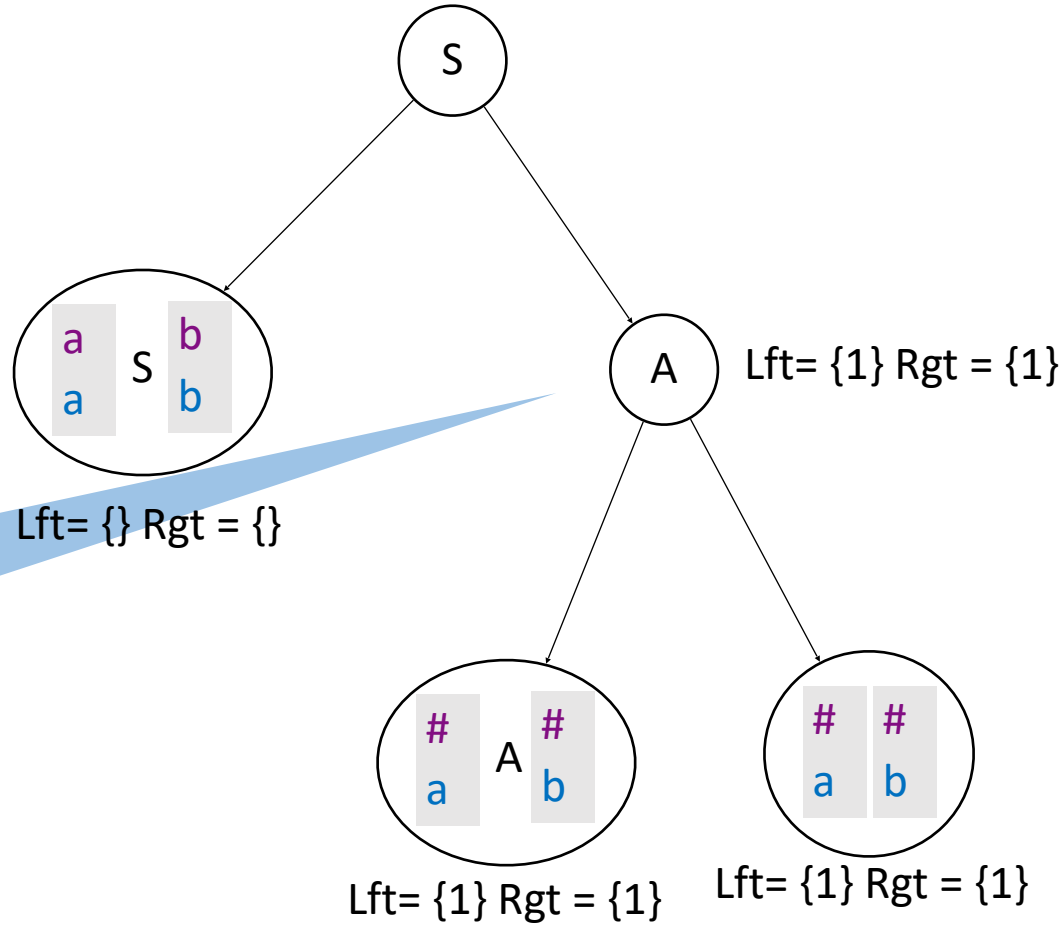
Can we define a hypergrammar that is **inherently** synchronous?

$$S \rightarrow \begin{matrix} a \\ a \end{matrix} \; S \; \begin{matrix} b \\ b \end{matrix} \mid A$$

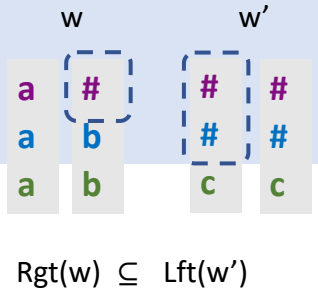
$$A \rightarrow \begin{matrix} \# \\ a \end{matrix} \; A \; \begin{matrix} \# \\ b \end{matrix} \mid \begin{matrix} \# \\ a \end{matrix} \; \begin{matrix} \# \\ b \end{matrix}$$

$$\text{Lft}(X) = \bigcap_{X \rightarrow \alpha} \text{Lft}(\alpha)$$

$$\text{Rgt}(X) = \bigcup_{X \rightarrow \alpha} \text{Rgt}(\alpha)$$



Synchronous Context-Free Hypergrammars



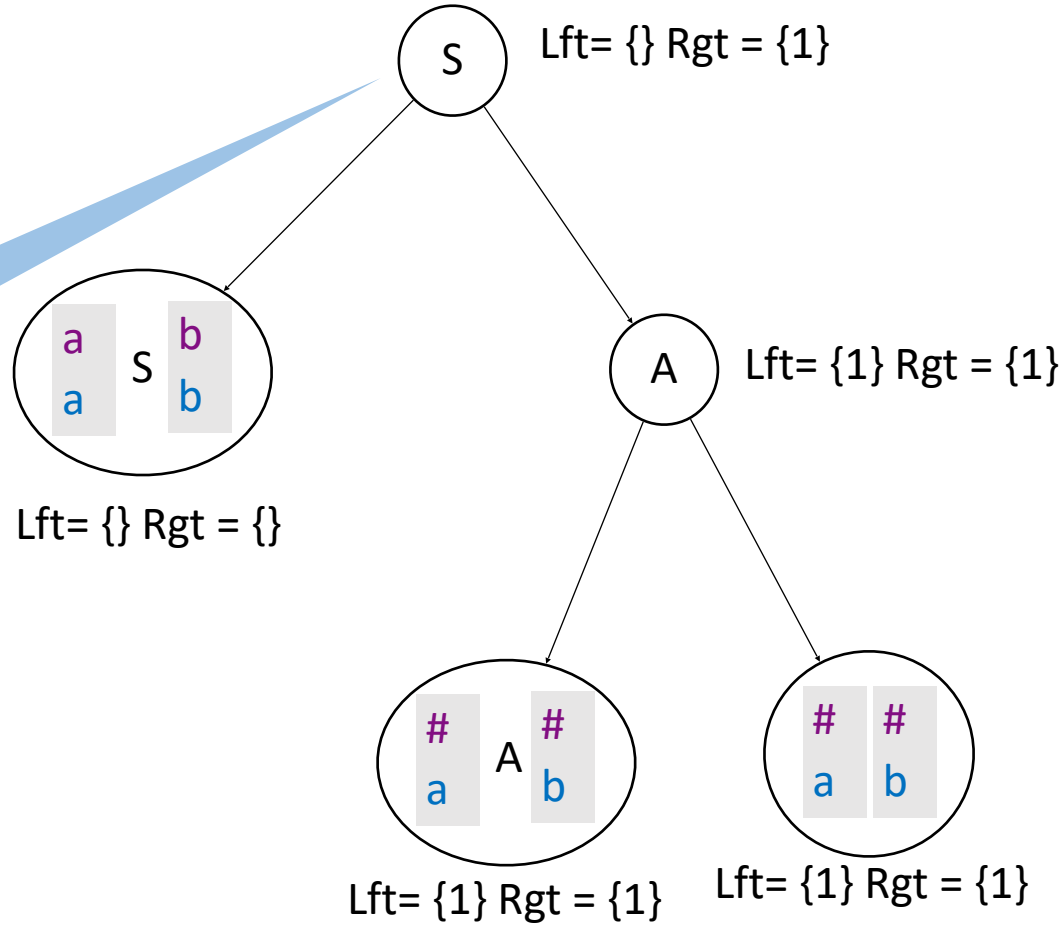
Can we define a hypergrammar that is **inherently** synchronous?

$$S \rightarrow \begin{matrix} a \\ a \end{matrix} \; S \; \begin{matrix} b \\ b \end{matrix} \mid A$$

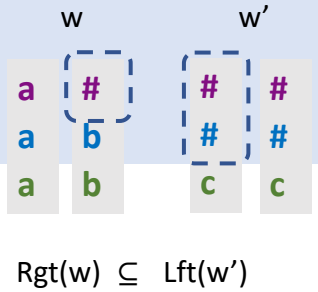
$$A \rightarrow \begin{matrix} \# \\ a \end{matrix} \; A \; \begin{matrix} \# \\ b \end{matrix} \mid \begin{matrix} \# \\ a \end{matrix} \; \begin{matrix} \# \\ b \end{matrix}$$

$$\text{Lft}(X) = \bigcap_{X \rightarrow \alpha} \text{Lft}(\alpha)$$

$$\text{Rgt}(X) = \bigcup_{X \rightarrow \alpha} \text{Rgt}(\alpha)$$



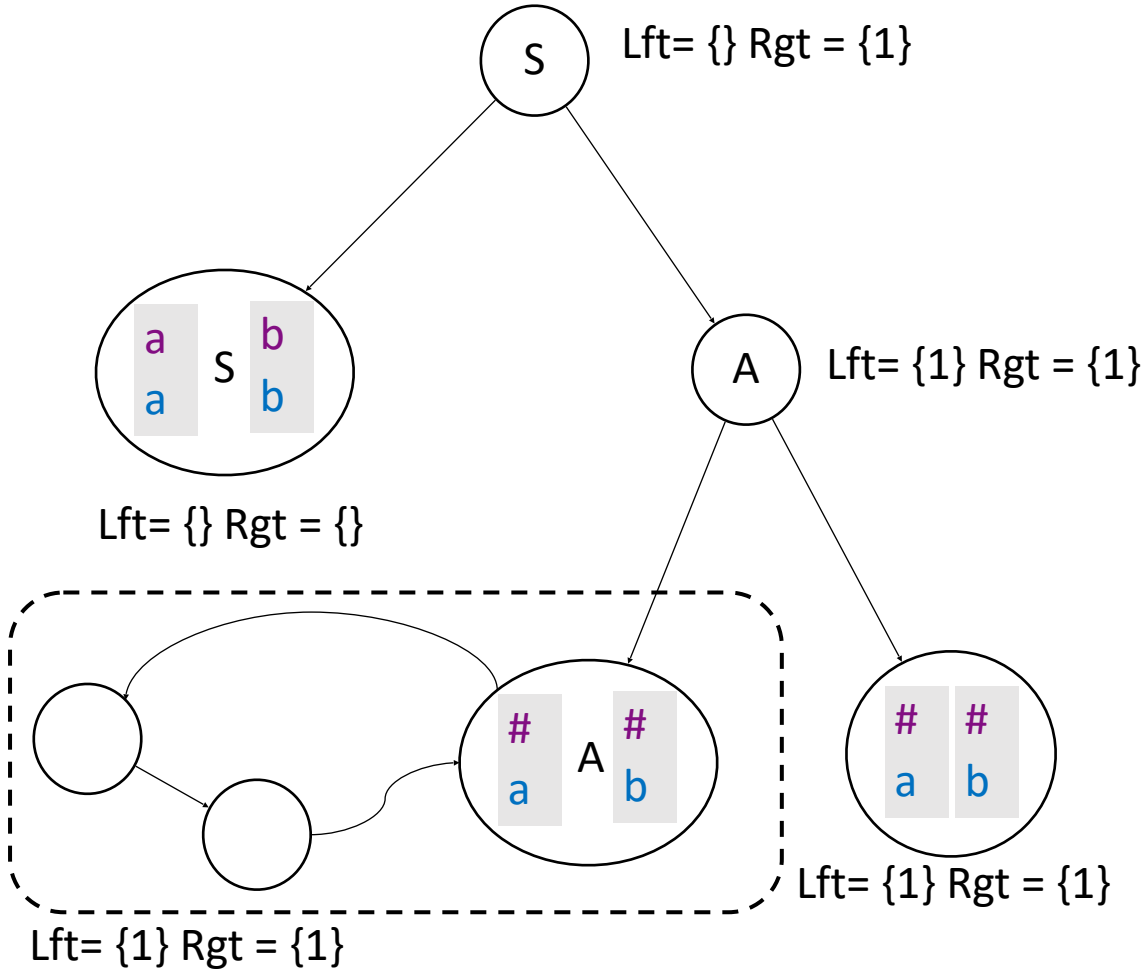
Synchronous Context-Free Hypergrammars



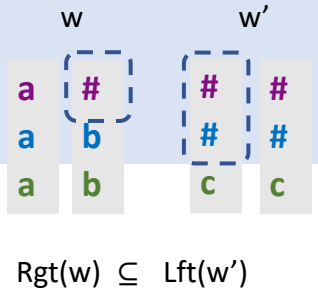
Can we define a hypergrammar that is **inherently** synchronous?

$$S \rightarrow \begin{matrix} a \\ a \end{matrix} \; S \; \begin{matrix} b \\ b \end{matrix} \mid A$$

$$A \rightarrow \begin{matrix} \# \\ a \end{matrix} \; A \; \begin{matrix} \# \\ b \end{matrix} \mid \begin{matrix} \# \\ a \end{matrix} \; \begin{matrix} \# \\ b \end{matrix}$$



Synchronous Context-Free Hypergrammars

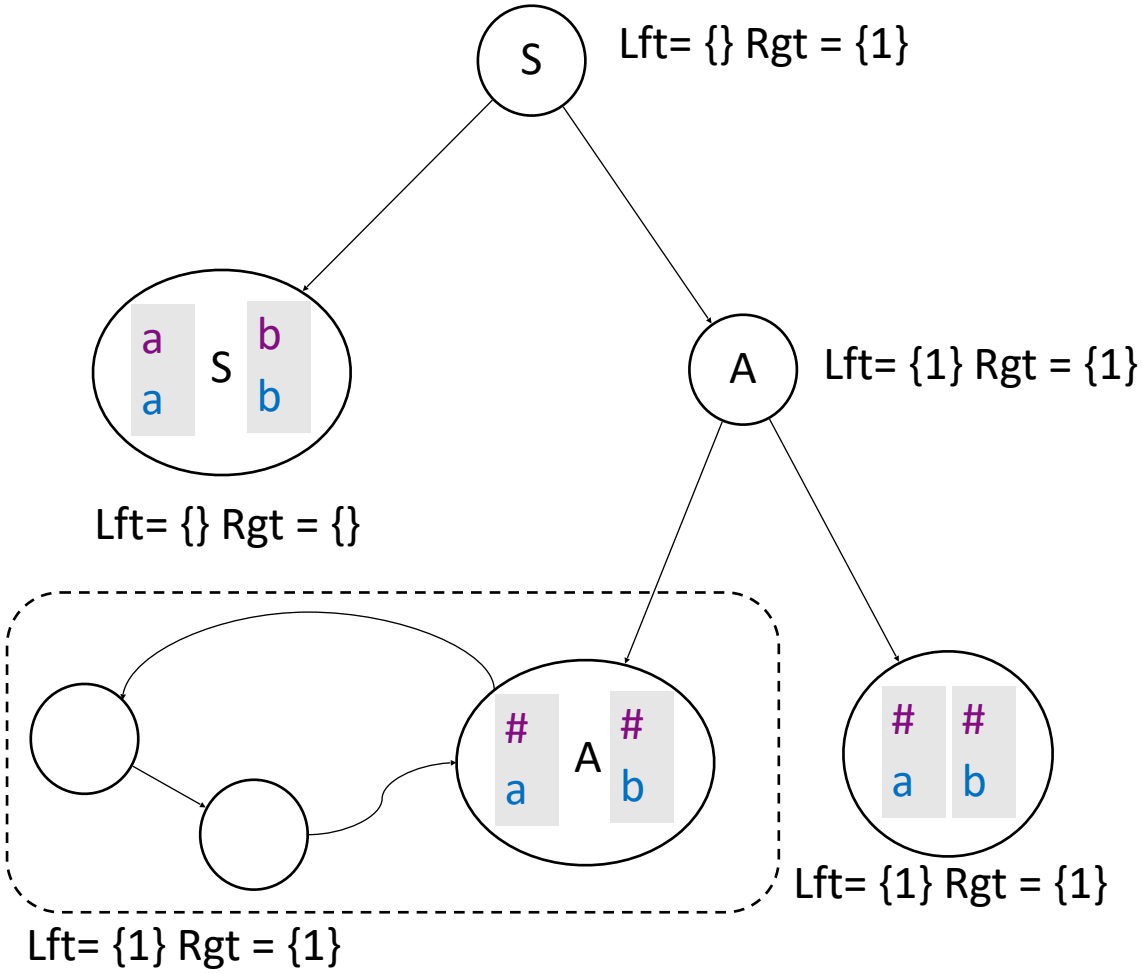


Can we define a hypergrammar that is **inherently** synchronous?

$$S \rightarrow \begin{matrix}a\\a\end{matrix}\ S\ \begin{matrix}b\\b\end{matrix} \mid A$$

$$A \rightarrow \begin{matrix}\#\\a\end{matrix}\ A\ \begin{matrix}\#\\b\end{matrix} \mid \begin{matrix}\#\\a\end{matrix}\ \begin{matrix}\#\\b\end{matrix}$$

$$Rgt(S) = \{1\} \not\subseteq Lft\left(\begin{matrix}b\\b\end{matrix}\right) = \{\}$$



In this talk

Finite-Word Hyperautomata

- Hyperautomata
- Realizability
  - Finite \ infinite
  - Ordered
  - Regular

Context-Free Hypergrammars

- Hypergrammars ✓
- Synchronous hypergrammars ✓
- Emptiness & membership

Emptiness: ∀*syncCFHG

$\forall x \forall y$ G : if L is accepted then also $L' \subset L$ $\Rightarrow$

G is not empty iff is a singleton language $\{w\} \in \mathscr{L}(G)$ $\Rightarrow$ w w G

$\forall x \forall y$ S → a S b | A

Check emptiness of the underlying grammar

A → # # | # #

Same proof also works for $\exists \forall^*$

Emptiness: Undecidable for ∀*CFHG

Reduction from Post correspondence problem

a 1	ab 2	bba 3
baa	aa	bb

→

a##	ab	bba
baa	aa	bb#

3 2 3 1
bba ab bba a
bb aa bb baa

$\forall x \forall y$ S →

a## baa	S	|	a## baa	|
ab aa	S	|	ab aa	|
bba bb#	S	|	bba bb#	

Same proof also works for ∃∀*

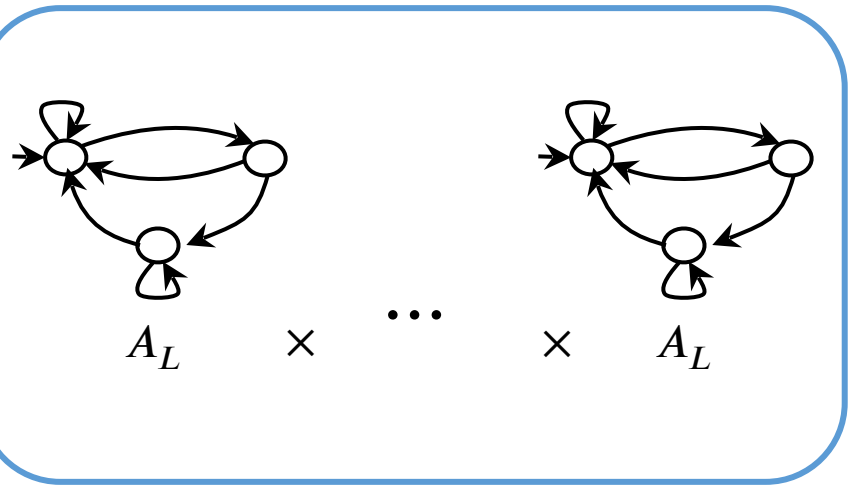
$x \leftarrow$ bba ab bba a

$y \leftarrow$ bb aa bb baa

Regular Membership

EXPTIME for $\exists^*$(sync)CFHG

$L \in \exists x_1 \cdots \exists x_k$ G?

G $\cap$ 

Undecidable for $\forall^*$(sync)CFHG

Reduction from the universality problem of CFG

G is universal $\iff$

$\Sigma^* \subseteq$ G $\iff$

$\Sigma^* \in \forall x$ G

Questions?

Hyperautomata

- Realizability of $\{L\}$ for
  - Finite \ infinite L
  - Ordered L
  - Regular L

Hypergrammars

- Synchronous hypergrammars
- Emptiness $\forall^*$, $\exists\forall^*$
  [in the paper: $\exists^*$, $\exists^*\forall^*$]
- Regular membership $\exists^*$, $\forall^*$
  [in the paper: finite membership]