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

“All requests are 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]

Runs: on assignments to the variables

\[ x \leftarrow a\ a\ #\ # \]
\[ y \leftarrow a\ a\ a\ a \]

Quantification condition \( \alpha \)

An NFH accepts a language \( L \) if \( L \) satisfies \( \alpha \) w.r.t. \( A \)

NFH: non-det finite word hyperautomaton

Underlying NFA \( A \)

\# padding

“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.

\[ \forall x \text{ low, high} \exists y \text{ low, high} \rightarrow \text{ low}^{\text{dummy}} \]
Realizability

With which quantification condition?

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

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

- Various types of $L$
- Realizability and unrealizability results for various $\alpha$
In this talk

Finite-Word Hyperautomata

- Hyperautomata ✓
- Realizability of \{L\}
  - Finite \(\setminus\) infinite \(L\)
  - Ordered \(L\)
  - Regular \(L\)

Context-Free Hypergrammars

- Hypergrammars
- Synchronous hypergrammars
- Emptiness and membership problems for hypergrammars
Realizability of \{L\}

**Simple \(\alpha\) does not suffice**

\[
\forall x : \text{if } L \text{ is accepted then also } L' \subseteq L \quad \Rightarrow \quad \text{not } \forall\text{-realizable}
\]

\[
\exists x : \text{if } L \text{ is accepted with } x \leftarrow w \text{ then also } L' \text{ for } w \in L' \cap L \quad \Rightarrow \quad \text{not } \exists\text{-realizable}
\]
Realizability of \( \{L\} \): finite \( L \)

Simple \( \alpha \) does not suffice

\[
\forall x \quad A : \text{ if } L \text{ is accepted then also } L' \subset L \quad \Rightarrow \quad \text{not } \forall\text{-realizable}
\]

\[
\exists x \quad A : \text{ if } L \text{ is accepted with } x \leftarrow w \text{ then also } L' \text{ for } w \in L' \cap L \quad \Rightarrow \quad \text{not } \exists\text{-realizable}
\]

If \( L \) is finite then \( \{L\} \) is \( \forall\exists \)-realizable: \( L = \{w_1, \ldots, w_n\} \)

\[
\forall x \exists y \quad \text{It is also } \exists^*\forall^*\text{-realizable}
\]
(Un)Realizability of \( \{L\} \): infinite \( L \)

Simple \( \alpha \) does not suffice

\( \{L\} \) is not \( \forall \exists \)-realizable: Suppose that \( \forall x \exists y \) accepts \( L \)

\[
\forall x \quad w_1 \quad w_2 \quad w_3 \quad \ldots \quad w_i \quad w_{i+1} \quad \ldots \quad w_{j-1} \quad w_j = w_i
\]

\( \{w_i, w_{i+1}, \ldots\} \in \mathcal{L}\{A\} \)

\( \{w_i, w_{i+1}, \ldots, w_j\} \in \mathcal{L}\{A\} \)

It is also not \( \exists^* \forall^* \)-realizable
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:

\[ \exists x \forall y \exists z \]

\[ w_1 \]

\[ w_1 \]

\[ w_2 \]

\[ w_2 \]

\[ w_3 \]

\[ w_3 \]

\[ \vdots \]

\[ \vdots \]

\[ w_i \]

\[ w_i \]

\[ w_{i+1} \]

\[ w_{i+1} \]
Realizability of \( \{L\} \): Partially Ordered \( L \)

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

\[ \exists \text{ relation } R \]

\( u_1' \quad u_2' \quad \ldots \quad u'_k \)

\( u_1 \quad u_2 \quad \ldots \quad u_m \)

\( k \) successors for each word

\( m \) minimal elements

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

\[ \exists x_1 \ldots x_m \; \forall y \exists z_1 \ldots z_k \]

There exists an NFA \( A_R \) for \( R \)

\[ w \quad w' \]

\[ u \quad u' \]

\[ v \quad v' \]

\[ w_1 \quad w_2 \quad \ldots \quad w_m \]

\[ u \quad v_1 \quad v_2 \quad \ldots \quad v_k \]

\[ \in L \]

\[ \text{succ}(u) \]
Realizability of \( \{L\} \): Regular \( L \)

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

\( m \):
Minimal elements - simple paths to accepting states
\( uv \in \text{Min} \)

\( k \):
Successors words - one additional simple cycle
\( uxv \in \text{succ}(uv) \)
In this talk

**Finite-Word Hyperautomata**
- Hyperautomata
- Realizability of \( \{L\} \)
  - Finite \( \backslash \) infinite \( L \)
  - Ordered \( L \)
  - Regular \( L \)

**Context-Free Hypergrammars**
- Hypergrammars
- Synchronous hypergrammars
- Emptiness & membership
A terminal word $w$ is in the language of a CGF $G$ if $w$ can be derived from the initial variable

$$S \Rightarrow a S b \Rightarrow a a S b \Rightarrow a a b b$$
Context-Free Hypergrammars

**CFHG**: context-free hypergrammar

\[
S \rightarrow aSb | A
\]

\[
A \rightarrow a\#A\#\#a\#b
\]

Quantification condition \(\alpha\)

# padding
Underlying CFG $G$

Quantification condition $\alpha$

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

Hyperlanguage: all infinite languages $\subseteq \{a^n b^n | n \in \mathbb{N}\}$

CFHG: context-free hypergrammar

A GFHG accepts a language $L$ if $L$ satisfies $\alpha$ w.r.t. $G$

Derives: assignments to the variables

$x \leftarrow a a \# \# b b$

$y \leftarrow a a a b b b$

# padding

Set of sets of words
Context-Free Hypergrammars

∀ x ∈ y  S → a a  S b b  |  A

A → # a  A # b  |  # # a b
Context-Free Hypergrammars

\[
\forall x \exists y \quad S \rightarrow a \quad S \quad b \quad | \quad A
\]

\[
A \rightarrow \# \quad A \quad | \quad \# \quad \# \quad a \quad b
\]

\[
S \Rightarrow a \quad S \quad b \quad \Rightarrow \quad a \quad a \quad S \quad b \quad b \quad \Rightarrow \quad a \quad a \quad a \quad a \quad b \quad b \quad \Rightarrow \quad a \quad a \quad A \quad b \quad b \quad \Rightarrow \quad a \quad a \quad a \quad A \quad b \quad b \quad \Rightarrow \quad a \quad a \quad a \quad a \quad A \quad b \quad b \quad \Rightarrow \quad a \quad a \quad a \quad a \quad b \quad b \quad b \quad \Rightarrow \quad a \quad a \quad a \quad a \quad b \quad b \quad b \quad \Rightarrow \quad a \quad a \quad a \quad a \quad b \quad b \quad b \quad \Rightarrow \quad a \quad a \quad a \quad a \quad b \quad b \quad b \quad \Rightarrow \quad a \quad a \quad a \quad a \quad b \quad b \quad b \quad \Rightarrow \quad a \quad a \quad a \quad a \quad b \quad b \quad b \quad \Rightarrow \quad a \quad a \quad a \quad a \quad b \quad b \quad b \quad \Rightarrow \quad a \quad a \quad a \quad a \quad b \quad b \quad b
\]
Context-Free Hypergrams

∀x ∃y \quad S \rightarrow a \quad S \quad b \quad \mid A

A \rightarrow \# \quad A \quad \mid \# \quad \# \quad \# \quad \#
Synchronous Context-Free Hypergrammars

Easy solution:

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

$$G \cap \sum^* \cdot \{\#\}^*$$

Result: only the synchronous part of $G$

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

\[
S \rightarrow AB
\]

\[
A \rightarrow \begin{array}{l}
a \\ 
\text{#} \\
a \\ 
b \\
a \\ 
b \\
\end{array}
\]

\[
B \rightarrow \begin{array}{l}
\text{#} \\
\text{#} \\
\text{#} \\
c \\
c \\
\end{array}
\]

\[
S \Rightarrow \begin{array}{l}
a \\
\text{#} \\
\text{#} \\
a \\
b \\
\end{array}
\Rightarrow 
\begin{array}{l}
a \\
\text{#} \\
\text{#} \\
\text{#} \\
\text{#} \\
\text{#} \\
\text{c} \\
\text{c} \\
\end{array}
\]

Rgt(w) \subseteq 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
Can we define a hypergrammar that is inherently synchronous?

S → aSb | A
A → #A#b | #aba

Lft(X) = \( \cap_{X \rightarrow \alpha} \) Lft(\( \alpha \))
Rgt(X) = \( \cup_{X \rightarrow \alpha} \) Rgt(\( \alpha \))
Can we define a hypergrammar that is inherently synchronous?

\[ S \rightarrow \begin{cases} a & \text{S} \\ b & \text{A} \end{cases} \]

\[ A \rightarrow \begin{cases} # & \text{A} \\ b & \# \\ a & \# \end{cases} \]

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

Rgt(X) = \bigcup_{X \rightarrow \alpha} \text{Rgt}(\alpha)
Can we define a hypergrammar that is inherently synchronous?

S → a S b | A
A → # A # b | # #

R_{w} \subseteq L_{w'}
Synchronous Context-Free Hypergrammars

Can we define a hypergrammar that is inherently synchronous?

Rgt(S) = \{1\} \not\subseteq Lft(\text{bb}) = \{\}

Lft = \{\} Rgt = \{1\}

Rgt(w) \subseteq Lft(w')
In this talk

Finite-Word Hyperautomata
- Hyperautomata
- Realizability of \{L\}
  - Finite \(\setminus\) infinite \(L\)
  - Ordered \(L\)
  - Regular \(L\)

Context-Free Hypergrammars
- Hypergrammars ✓
- Synchronous hypergrammars ✓
- Emptiness & membership
Emptiness: $\forall^* \text{syncCFHG}$

$\forall x \forall y \ G : \text{if } L \text{ is accepted then also } L' \subset L \implies$

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

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

Check emptiness of the underlying grammar
Emptiness: Undecidable for $\forall^*\text{CFHG}$

Reduction from Post correspondence problem

$S \rightarrow \text{a#} \ \text{ba} \ \text{a} \ \text{ab} \ \text{aa} \ \text{bb} \ \text{bba} \ \text{ab} \ \text{aa} \ \text{bba} \ \text{bb#}$

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

EXPTIME for $\exists^*(\text{sync})\text{CFHG}$

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

Undecidable for $\forall^*(\text{sync})\text{CFHG}$

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 \( \setminus \) 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]