Department of Mathematics, Computer Science and Physics, University of Udine

The Safety Fragment of Temporal Logics on Infinite Sequences

Lesson 5

Luca Geatti
luca.geatti@uniud.it
Angelo Montanari
angelo.montanari@uniud.it

April 15th, 2024

THE SAFETY FRAGMENT

OF ω-REGULAR LANGUAGES

In this part, we will mainly deal with language of *infinite words* and with logics interpreted over *infinite words*.

Informal definitions:

Safety properties express the fact that "something bad never happens".

E.g.: a deadlock or a simultaneous access to a critical section.

Any violation of a safety property is irremediable.

E.g.: once a deadlock occured, we don't have any hope to do better.

Any violation of a safety property has a finite witness.

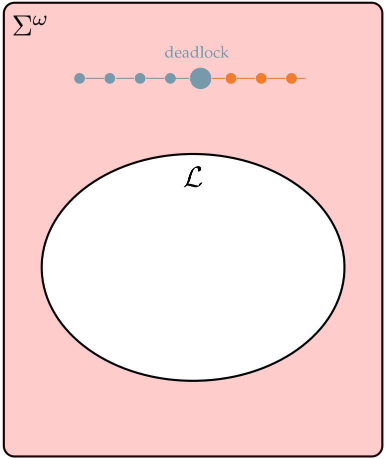
Notation:

- For any $i \in \mathbb{N}$, $\sigma_{[0,i]}$ is the prefix of σ up to position i.
- for any $\sigma \in \Sigma^*$ and for any $\sigma' \in \Sigma^\omega$, $\sigma \cdot \sigma'$ is the *concatenation* of σ' to the end of σ.

Definition (Safety Property)

$\mathcal{L} \subseteq \Sigma^\omega$ is a *safety property* iff, for all $\sigma \notin \mathcal{L}$, there exists an position $i \in \mathbb{N}$ such that $\sigma_{[0,i]} \cdot \sigma' \notin \mathcal{L}$, for all $\sigma' \in \Sigma^\omega$.

$\sigma_{[0,i]}$ is called the *bad prefix* of σ.



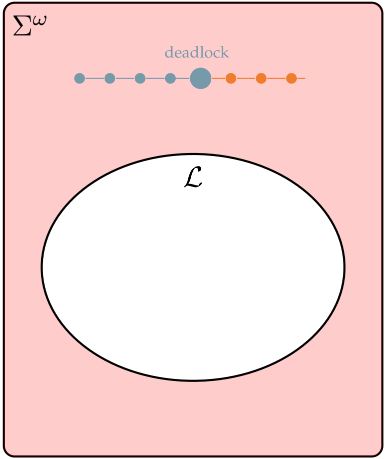
Examples

- $b \cdot (a)^\omega$ is a safety language.
- *"The set of infinite words in which each 'a' is followed by some 'b' "* is <u>not</u> a safety language.

- We denote with $\texttt{bad}(\mathcal{L})$ the set of bad prefixes of $\mathcal{L}$.
- For any safety language $\mathcal{L}$, it holds that:

$$\overline{\mathcal{L}} = \texttt{bad}(\mathcal{L}) \cdot \Sigma^\omega$$

where $\overline{\mathcal{L}}$ is the *complement* of $\mathcal{L}$.



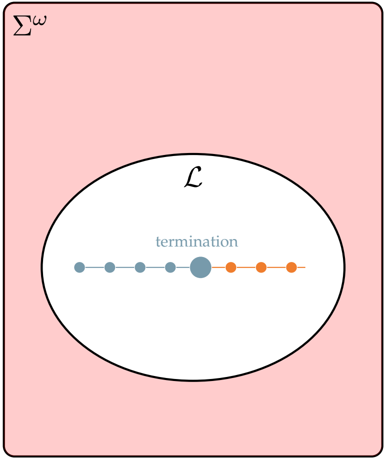
Definition (Cosafety Property)

$\mathcal{L} \subseteq \Sigma^\omega$ is a *cosafety property* iff for all $\sigma \in \mathcal{L}$, there exists an position $i \in \mathbb{N}$ such that $\sigma_{[0,i]} \cdot \sigma' \in \mathcal{L}$, for all $\sigma' \in \Sigma^\omega$.

$\sigma_{[0,i]}$ is called the *good prefix* of σ.

Property:

$\mathcal{L}$ is a cosafety property iff $\overline{\mathcal{L}}$ is a safety property.

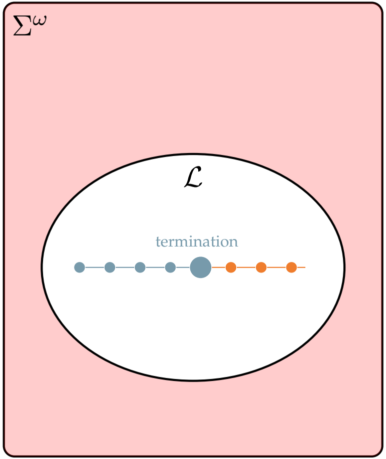


Examples

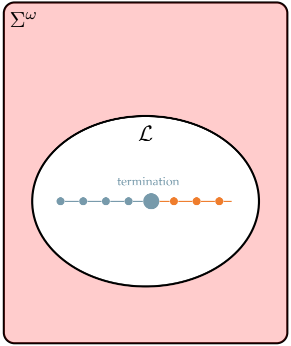
- *"The set of infinite words in which there is an 'a' that is followed by some 'b' "* is a cosafety language.
- *"The set of infinite words in which each 'a' is followed by some 'b' "* is not a cosafety language.

- We denote with $\mathsf{good}(\mathcal{L})$ the set of good prefixes of $\mathcal{L}$.
- For any cosafety language $\mathcal{L}$, it holds that:

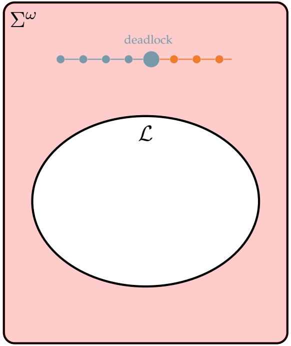
$$\mathcal{L} = \mathsf{good}(\mathcal{L}) \cdot \Sigma^\omega$$



We denote with coSAFETY the set of all cosafety ω-regular languages.



We denote with SAFETY the set of all safety ω-regular languages.



We denote with coSAFETY the set of all cosafety ω-regular languages.

ω-Regular Expressions

coSAFETY is characterized by the following type of ω-regular expressions:

$$K \cdot \Sigma^\omega$$

where $K \in \mathsf{REG}$.

We denote with SAFETY the set of all safety ω-regular languages.

ω-Regular Expressions

SAFETY is characterized by the following type of ω-regular expressions:

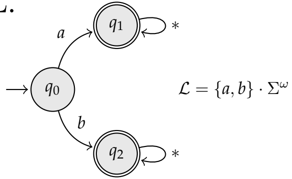
$$\overline{K \cdot \Sigma^\omega}$$

where $K \in \mathsf{REG}$.

We denote with coSAFETY the set of all cosafety ω-regular languages.

Automata

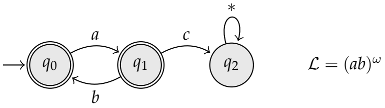
coSAFETY is characterized by the following type of automata: *terminal deterministic Büchi automata* (tDBA, for short), that is DBAs in which each final state has self-loop labeled with each letter in Σ.



We denote with SAFETY the set of all safety ω-regular languages.

Automata

SAFETY is characterized by the following type of automata: *deterministic safety automata* (DSA, for short). Accepting condition: visit *only* final states.



We denote with coSAFETY the set of all cosafety ω-regular languages.

S1S

To the best of our knowledge, no characterizations of coSAFETY in terms of S1S have been studied.

We denote with SAFETY the set of all safety ω-regular languages.

S1S

To the best of our knowledge, no characterizations of SAFETY in terms of S1S have been studied.

We denote with coSAFETY the set of all cosafety ω-regular languages.

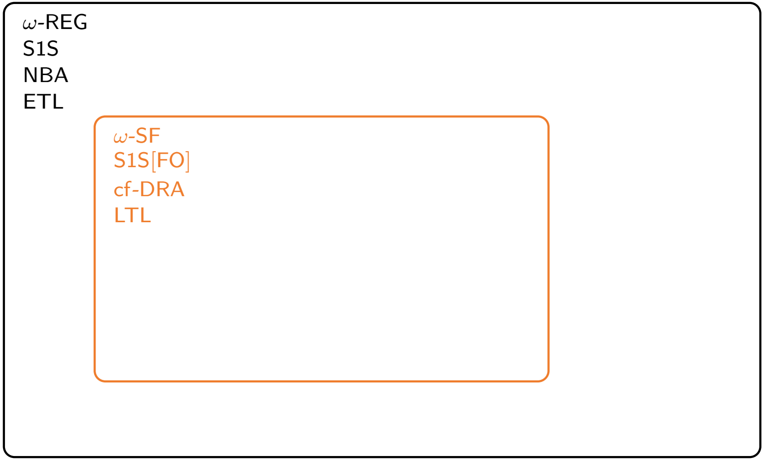
Temporal Logics

To the best of our knowledge, no characterizations of coSAFETY in terms of temporal logics have been studied.

We denote with SAFETY the set of all safety ω-regular languages.

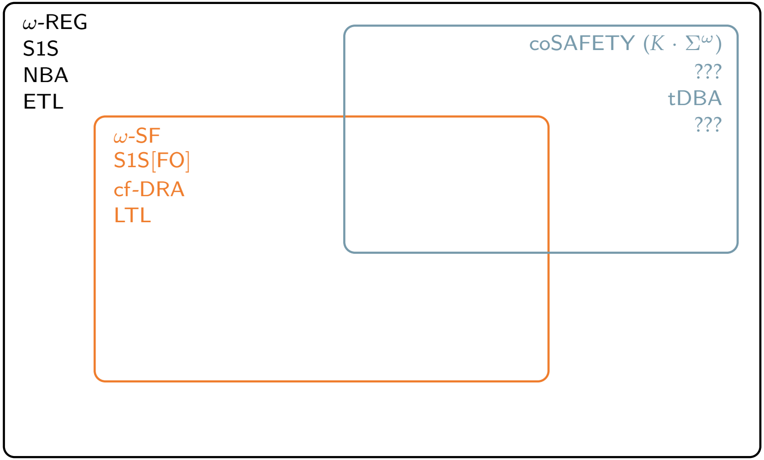
Temporal Logics

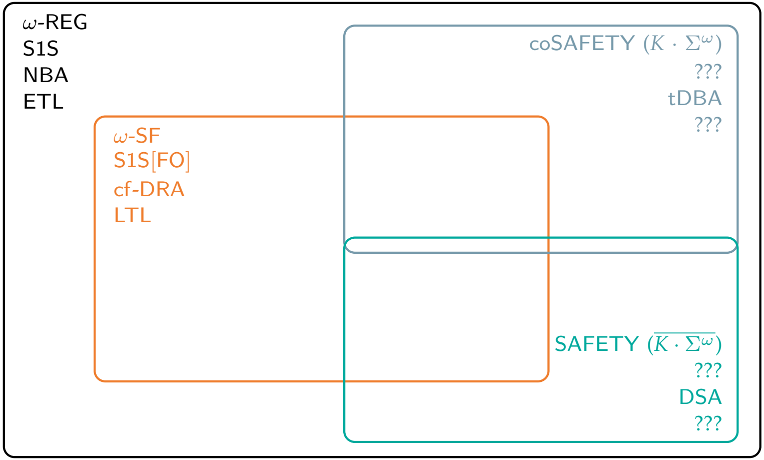
To the best of our knowledge, no characterizations of SAFETY in terms of temporal logics have been studied.



ω-REG
S1S
NBA
ETL
ω-SF
S1S[FO]
cf-DRA
LTL

Set-theoretic view of (co)safety ω-languages




ω-REG
S1S
NBA
ETL
ω-SF
S1S[FO]
cf-DRA
LTL
coSAFETY $(K \cdot \Sigma^\omega)$
???
tDBA
???
SAFETY $(\overline{K \cdot \Sigma^\omega})$
???
DSA
???

Informal definitions:

> *In a liveness property, no partial execution is irremediable.*

E.g.: *"each request is eventually followed by a grant"* is a liveness property.

Definition (Liveness Property)

$\mathcal{L} \subseteq \Sigma^\omega$ is a *liveness property* iff, for all $\sigma \in \Sigma^*$, there exists a $\sigma' \in \Sigma^\omega$ such that $\sigma \cdot \sigma' \in \mathcal{L}$.

Examples:

- *"The set of infinite words in which each 'a' is followed by some 'b' "* is a liveness language.
- $b \cdot (a)^\omega$ is not a liveness language.

Theorem (Alpern & Schneider (1987))

Each ω-regular property is the intersection of a safety property and a liveness property.

Reference:

Bowen Alpern and Fred B. Schneider (1987). "Recognizing Safety and Liveness". In: *Distributed Comput.* 2.3, pp. 117–126. DOI: 10.1007/BF01782772. URL: https://doi.org/10.1007/BF01782772

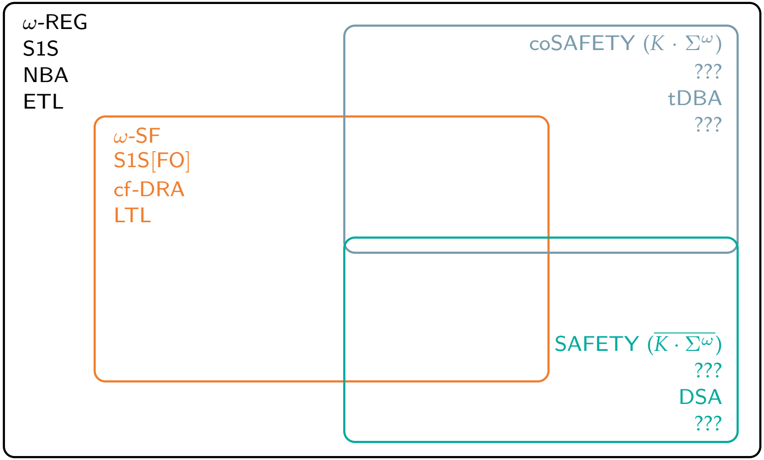
Theorem (Alpern & Schneider (1987))

Each ω-regular property is the intersection of a safety property and a liveness property.

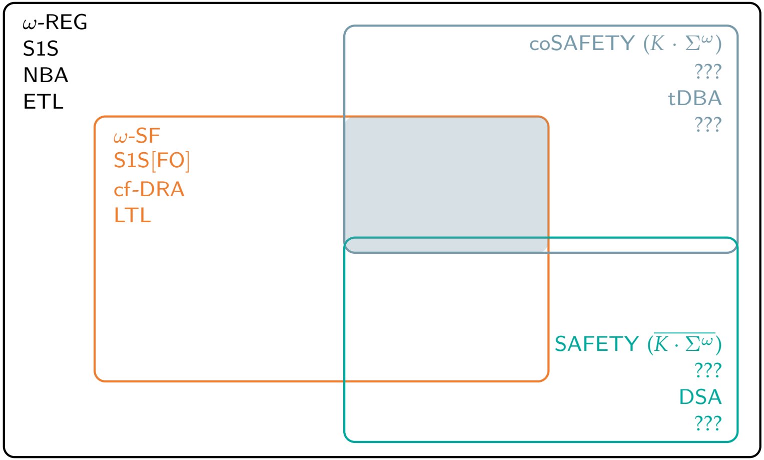
This decomposition can be performed effectively:

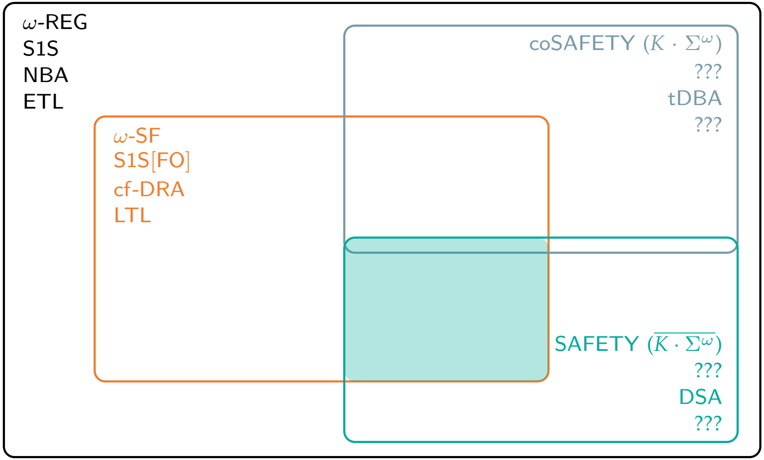
Given a NBA $\mathcal{A}$, there is an algorithm to build two NBA $\mathcal{A}_s$ and $\mathcal{A}_l$ such that:

- $\mathcal{L}(\mathcal{A}_s)$ is safety;
- $\mathcal{L}(\mathcal{A}_l)$ is liveness;
- $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{A}_s) \cap \mathcal{L}(\mathcal{A}_l)$.



ω-REG
S1S
NBA
ETL
coSAFETY $(K \cdot \Sigma^\omega)$
???
tDBA
???
ω-SF
S1S[FO]
cf-DRA
LTL
SAFETY $(\overline{K \cdot \Sigma^\omega})$
???
DSA
???


ω-REG
S1S
NBA
ETL
coSAFETY $(K \cdot \Sigma^\omega)$
???
tDBA
???
ω-SF
S1S[FO]
cf-DRA
LTL
SAFETY $(\overline{K \cdot \Sigma^\omega})$
???
DSA
???


ω-REG
S1S
NBA
ETL
coSAFETY $(K \cdot \Sigma^\omega)$
???
tDBA
???
ω-SF
S1S[FO]
cf-DRA
LTL
SAFETY $(\overline{K \cdot \Sigma^\omega})$
???
DSA
???

THE SAFETY FRAGMENT OF LTL

AND ITS THEORETICAL FEATURES

The cosafety fragment of LTL

Definition

The *cosafety fragment of* LTL is the set of languages in this set:

$$[\![\mathsf{LTL}]\!] \cap \mathsf{coSAFETY}$$

We will see four characterizations in terms of:

- regular expressions
- first-order logic
- automata
- temporal logic

Definition

The *cosafety fragment of* LTL is the set of languages in this set:

$$[\![\mathsf{LTL}]\!] \cap \mathsf{coSAFETY}$$

ω-regular expressions

$\mathsf{SF} \cdot \Sigma^\omega = \{K \cdot \Sigma^\omega \mid K \in \mathsf{SF}\}$

- the "SF " part corresponds to LTL
- the "$\cdot\Sigma^\omega$" part corresponds to being a cosafety fragment

Ina Schiering and Wolfgang Thomas (1996). "Counter-free automata, first-order logic, and star-free expressions extended by prefix oracles". In: *Developments in Language Theory, II (Magdeburg, 1995), Worl Sci. Publishing, River Edge, NJ*, pp. 166–175

Definition

The *cosafety fragment of* LTL is the set of languages in this set:

$$[\![\mathsf{LTL}]\!] \cap \mathsf{coSAFETY}$$

First-order logic

We define coSafety-FO as the fragment of S1S[FO] in which quantifiers are bounded as follows:

- $\exists y \,.\, (x < y \wedge \ldots)$
- $\forall y \,.\, (x < y < z \rightarrow \ldots)$

Alessandro Cimatti et al. (2022). "A first-order logic characterisation of safety and co-safety languages". In: *Foundations of Software Science and Computation Structures - 25th International Conference, FOSSACS 2022, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2022, Munich, Germany, April 2-7, 2022, Proceedings*. Ed. by Patricia Bouyer and Lutz Schröder. Vol. 13242. Lecture Notes in Computer Science. Springer, pp. 244–263. DOI: 10.1007/978-3-030-99253-8_13. URL: https://doi.org/10.1007/978-3-030-99253-8%5C_13

Definition

The *cosafety fragment of* LTL is the set of languages in this set:

$$[\![\mathsf{LTL}]\!] \cap \mathsf{coSAFETY}$$

First-order logic

Example

$\phi(x) := \exists y \,.\, (x < y \wedge P(y) \wedge \forall z \,.\, (x < z < y \rightarrow Q(z)))$

The cosafety fragment of LTL

Definition

The *cosafety fragment of* LTL is the set of languages in this set:

$$[\![\mathsf{LTL}]\!] \cap \mathsf{coSAFETY}$$

First-order logic

- the "first-order" part corresponds to LTL
- the "bounded quantifiers" part corresponds to being a cosafety fragment

Definition

The *cosafety fragment of* LTL is the set of languages in this set:

$$[\![\mathsf{LTL}]\!] \cap \mathsf{coSAFETY}$$

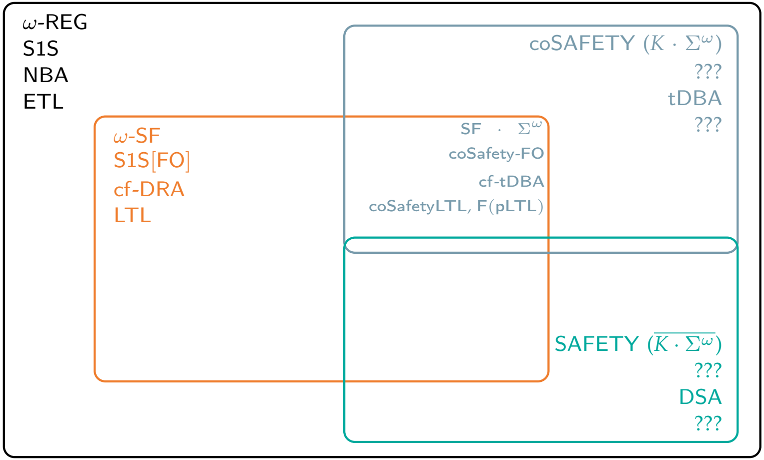
Automata

cf-tDBA = counter-free terminal DBA

- the "counter-free" part corresponds to LTL
- the "terminal" part corresponds to being a cosafety fragment

Ina Schiering and Wolfgang Thomas (1996). "Counter-free automata, first-order logic, and star-free expressions extended by prefix oracles". In: *Developments in Language Theory, II (Magdeburg, 1995), Worl Sci. Publishing, River Edge, NJ*, pp. 166–175

Set-theoretic view of the (co)safety fragment of LTL



The cosafety fragment of LTL

We say that a temporal logic $\mathbb{L}$ is *cosafety* iff, for any $\phi \in \mathbb{L}$, $\mathcal{L}(\phi)$ is *cosafety*.

coSafetyLTL

Definition

$\phi := p \mid \neg p \mid \phi \vee \phi \mid \phi \wedge \phi \mid \mathsf{X}\phi \mid \mathsf{F}\phi \mid \phi \, \mathsf{U} \, \phi$

Example:

$p \, \mathsf{U} \, q$

F(pLTL)

Definition

$\phi := \mathsf{F}(\alpha)$, where $\alpha \in \mathsf{pLTL}$, that is α is a pure-past LTL formula.

Example:

$\mathsf{F}(q \wedge \widetilde{\mathsf{Y}}\mathsf{H}p)$

F(pLTL) is the canonical form of coSafetyLTL.

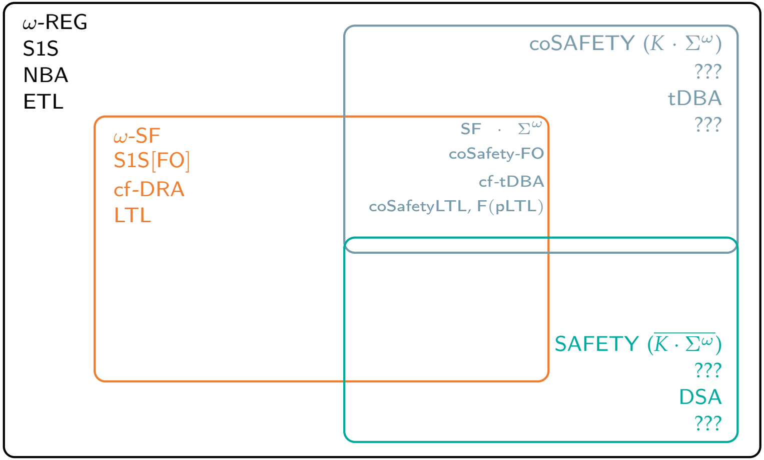
The cosafety fragment of LTL

Theorem

- coSafetyLTL *and* F(pLTL) *are expressively equivalent.*
- coSafetyLTL *and* F(pLTL) *are expressively complete w.r.t.* $[\![\mathsf{LTL}]\!] \cap \mathsf{coSAFETY}$.

Reference:

Edward Y. Chang, Zohar Manna, and Amir Pnueli (1992). "Characterization of Temporal Property Classes". In: *Proceedings of the 19th International Colloquium on Automata, Languages and Programming*. Ed. by Werner Kuich. Vol. 623. Lecture Notes in Computer Science. Springer, pp. 474–486. DOI: 10.1007/3-540-55719-9_97


ω-REG
S1S
NBA
ETL
coSAFETY $(K \cdot \Sigma^\omega)$
???
tDBA
???
ω-SF
S1S[FO]
cf-DRA
LTL
SF $\cdot$ Σ^ω
coSafety-FO
cf-tDBA
coSafetyLTL, F(pLTL)
SAFETY $(\overline{\overline{K} \cdot \Sigma^\omega})$
???
DSA
???

REFERENCES

Bibliography I

Bowen Alpern and Fred B. Schneider (1987). "Recognizing Safety and Liveness". In: *Distributed Comput.* 2.3, pp. 117–126. DOI: 10.1007/BF01782772. URL: https://doi.org/10.1007/BF01782772.

Edward Y. Chang, Zohar Manna, and Amir Pnueli (1992). "Characterization of Temporal Property Classes". In: *Proceedings of the 19th International Colloquium on Automata, Languages and Programming*. Ed. by Werner Kuich. Vol. 623. Lecture Notes in Computer Science. Springer, pp. 474–486. DOI: 10.1007/3-540-55719-9_97.

Bibliography II

Alessandro Cimatti et al. (2022). "A first-order logic characterisation of safety and co-safety languages". In: *Foundations of Software Science and Computation Structures - 25th International Conference, FOSSACS 2022, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2022, Munich, Germany, April 2-7, 2022, Proceedings*. Ed. by Patricia Bouyer and Lutz Schröder. Vol. 13242. Lecture Notes in Computer Science. Springer, pp. 244–263. DOI: 10.1007/978-3-030-99253-8_13. URL: https://doi.org/10.1007/978-3-030-99253-8%5C_13.

Ina Schiering and Wolfgang Thomas (1996). "Counter-free automata, first-order logic, and star-free expressions extended by prefix oracles". In: *Developments in Language Theory, II (Magdeburg, 1995), Worl Sci. Publishing, River Edge, NJ*, pp. 166–175.