Complexity, Computability, Cryptography with Reaction Systems

Rocco Ascone

UNIVERSITÀ DEGLI STUDI DI TRIESTE

Universidad Adolfo Ibáñez, 10/12/2025

Reactions

Definition (Reaction)

Given a finite set S, a *reaction* a over S is a triple (R, I, P) of subsets of S:

- R is the set of *reactants*,
- I is the set of *inhibitors*,
- P is the set of *products*.

Reactions

Definition (Reaction)

Given a finite set S, a *reaction* a over S is a triple (R, I, P) of subsets of S:

- R is the set of *reactants*,
- I is the set of *inhibitors*,
- P is the set of *products*.

Definition (Enabled)

(R, I, P) is *enabled* in a *state* $T \subseteq S$ when:

$$R \subseteq T \quad \text{and} \quad I \cap T = \varnothing.$$

Reaction Systems

Definition (Reaction System)

A *reaction system* (RS) is a pair $\mathcal{A} = (S, A)$ where:

- S is a finite set of *symbols* or *entities*, called the *background set*;
- A is a set of reactions over S.

A *state* of $\mathcal{A}$ is a subset of S.

Reaction Systems

Definition (Reaction System)

A *reaction system* (RS) is a pair $\mathcal{A} = (S, A)$ where:

- S is a finite set of *symbols* or *entities*, called the *background set*;
- A is a set of reactions over S.

A *state* of $\mathcal{A}$ is a subset of S.

Any reaction system induces a discrete dynamical system where the state set is 2^S (all the subsets of S).

Example of RS

Background set: $S = \{\bigstar, \Diamond\}$

Set of reactions: $r_1 = (\varnothing, \{\bigstar, \Diamond\}, \{\Diamond\})$

$r_2 = (\{\Diamond\}, \{\bigstar\}, \{\bigstar, \Diamond\})$

Example of RS

Background set: $S = \{\bigstar, \diamondsuit\}$

Set of reactions: $r_1 = (\varnothing, \{\bigstar, \diamondsuit\}, \{\diamondsuit\})$

$r_2 = (\{\diamondsuit\}, \{\bigstar\}, \{\bigstar, \diamondsuit\})$

State: $T = \{\diamondsuit\}$

Example of RS

Background set: $S = \{\bigstar, \diamondsuit\}$

Set of reactions: $r_1 = (\varnothing, \{\bigstar, \diamondsuit\}, \{\diamondsuit\}) \leftarrow$

$r_2 = (\{\diamondsuit\}, \{\bigstar\}, \{\bigstar, \diamondsuit\})$

State: $T = \{\diamondsuit\}$

$$\varnothing \subseteq T, \quad \{\bigstar, \diamondsuit\} \cap T = \{\diamondsuit\} \quad \Rightarrow \quad \mathrm{res}_{r_1}(T) = \varnothing$$

Example of RS

Background set: $S = \{\bigstar, \diamondsuit\}$

Set of reactions: $r_1 = (\varnothing, \{\bigstar, \diamondsuit\}, \{\diamondsuit\})$

$r_2 = (\{\diamondsuit\}, \{\bigstar\}, \{\bigstar, \diamondsuit\}) \leftarrow$

State: $T = \{\diamondsuit\}$

$$\varnothing \subseteq T, \quad \{\bigstar, \diamondsuit\} \cap T = \{\diamondsuit\} \quad \Rightarrow \quad \mathrm{res}_{r_1}(T) = \varnothing$$

$$\{\diamondsuit\} \subseteq T, \quad \{\bigstar\} \cap T = \varnothing \quad \Rightarrow \quad \mathrm{res}_{r_2}(T) = \{\bigstar, \diamondsuit\}$$

Example of RS

Background set: $S = \{\bigstar, \diamondsuit\}$

Set of reactions: $r_1 = (\varnothing, \{\bigstar, \diamondsuit\}, \{\diamondsuit\})$

$r_2 = (\{\diamondsuit\}, \{\bigstar\}, \{\bigstar, \diamondsuit\})$

State: $T = \{\diamondsuit\}$

$$\varnothing \subseteq T, \quad \{\bigstar, \diamondsuit\} \cap T = \{\diamondsuit\} \quad \Rightarrow \quad \mathrm{res}_{r_1}(T) = \varnothing$$

$$\{\diamondsuit\} \subseteq T, \quad \{\bigstar\} \cap T = \varnothing \quad \Rightarrow \quad \mathrm{res}_{r_2}(T) = \{\bigstar, \diamondsuit\}$$

Result function on T:

$$\mathrm{res}_{\mathcal{A}}(T) = \mathrm{res}_{r_1}(T) \cup \mathrm{res}_{r_2}(T)$$

Example of RS

Background set: $S = \{\bigstar, \diamondsuit\}$

Set of reactions: $r_1 = (\varnothing, \{\bigstar, \diamondsuit\}, \{\diamondsuit\})$

$r_2 = (\{\diamondsuit\}, \{\bigstar\}, \{\bigstar, \diamondsuit\})$

State: $T = \{\diamondsuit\}$

$$\varnothing \subseteq T, \quad \{\bigstar, \diamondsuit\} \cap T = \{\diamondsuit\} \quad \Rightarrow \quad \mathrm{res}_{r_1}(T) = \varnothing$$

$$\{\diamondsuit\} \subseteq T, \quad \{\bigstar\} \cap T = \varnothing \quad \Rightarrow \quad \mathrm{res}_{r_2}(T) = \{\bigstar, \diamondsuit\}$$

Result function on T:

$$\mathrm{res}_{\mathcal{A}}(T) = \mathrm{res}_{r_1}(T) \cup \mathrm{res}_{r_2}(T) = \varnothing \cup \{\bigstar, \diamondsuit\} = \{\bigstar, \diamondsuit\}$$

Example of RS

Background set: $S = \{\bigstar, \diamondsuit\}$

Set of reactions: $r_1 = (\varnothing, \{\bigstar, \diamondsuit\}, \{\diamondsuit\})$

$r_2 = (\{\diamondsuit\}, \{\bigstar\}, \{\bigstar, \diamondsuit\})$

State: $T = \{\diamondsuit\}$

$$\varnothing \subseteq T, \quad \{\bigstar, \diamondsuit\} \cap T = \{\diamondsuit\} \quad \Rightarrow \quad \mathrm{res}_{r_1}(T) = \varnothing$$

$$\{\diamondsuit\} \subseteq T, \quad \{\bigstar\} \cap T = \varnothing \quad \Rightarrow \quad \mathrm{res}_{r_2}(T) = \{\bigstar, \diamondsuit\}$$

Result function on T:

$$\mathrm{res}_{\mathcal{A}}(\{\diamondsuit\}) = \{\bigstar, \diamondsuit\}$$

Example of RS

Background set: $S = \{\bigstar, \Diamond\}$

Set of reactions: $r_1 = (\varnothing, \{\bigstar, \Diamond\}, \{\Diamond\})$

$r_2 = (\{\Diamond\}, \{\bigstar\}, \{\bigstar, \Diamond\})$

State: $T = \{\Diamond\}$

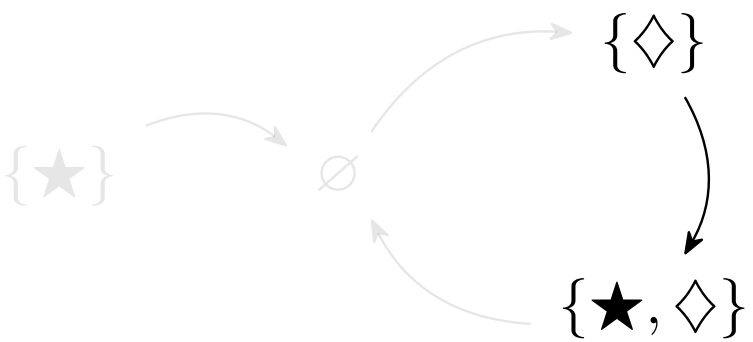
$$\varnothing \subseteq T, \quad \{\bigstar, \Diamond\} \cap T = \{\Diamond\} \quad \Rightarrow \quad \mathrm{res}_{r_1}(T) = \varnothing$$

$$\{\Diamond\} \subseteq T, \quad \{\bigstar\} \cap T = \varnothing \quad \Rightarrow \quad \mathrm{res}_{r_2}(T) = \{\bigstar, \Diamond\}$$

Result function on T:

$$\mathrm{res}_{\mathcal{A}}(\{\Diamond\}) = \{\bigstar, \Diamond\}$$

Representation of the dynamics:



Example of RS

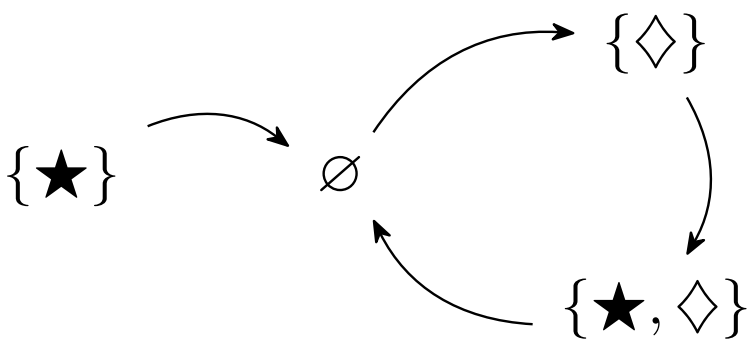
Cycle

Background set: $S = \{\bigstar, \Diamond\}$

Set of reactions: $r_1 = (\varnothing, \{\bigstar, \Diamond\}, \{\Diamond\})$

$r_2 = (\{\Diamond\}, \{\bigstar\}, \{\bigstar, \Diamond\})$

Discrete dynamical system:



Example of RS

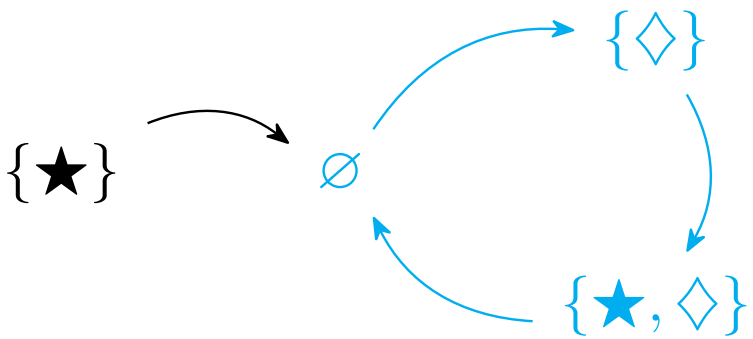
Cycle

Background set: $S = \{\bigstar, \Diamond\}$

Set of reactions: $r_1 = (\varnothing, \{\bigstar, \Diamond\}, \{\Diamond\})$

$r_2 = (\{\Diamond\}, \{\bigstar\}, \{\bigstar, \Diamond\})$

Discrete dynamical system:



Example of RS

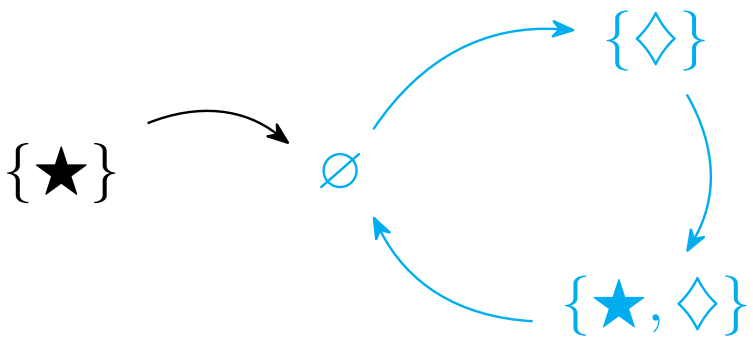
Cycle

Background set: $S = \{\bigstar, \Diamond\}$

Set of reactions: $r_1 = (\varnothing, \{\bigstar, \Diamond\}, \{\Diamond\})$

$r_2 = (\{\Diamond\}, \{\bigstar\}, \{\bigstar, \Diamond\})$

Discrete dynamical system:



Cycle global attractor: $\varnothing, \{\Diamond\}, \{\bigstar, \Diamond\}$

Example of RS

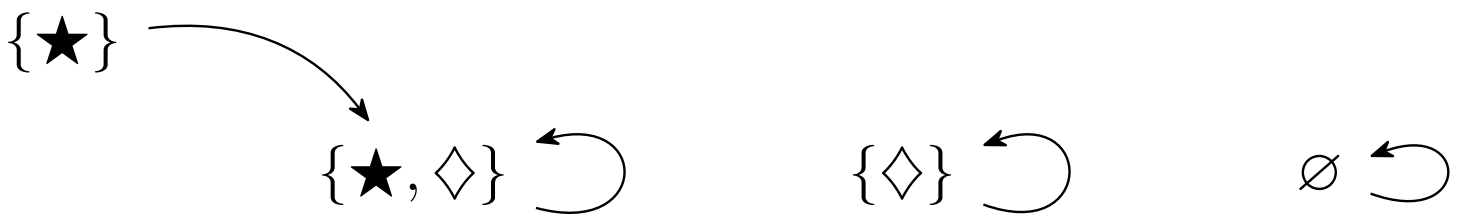
Fixed points

Background set: $S = \{\bigstar, \diamondsuit\}$

Set of reactions: $r_3 = (\{\bigstar\}, \varnothing, \{\bigstar, \diamondsuit\})$

$r_4 = (\{\diamondsuit\}, \{\bigstar\}, \{\diamondsuit\})$

Discrete dynamical system:



Example of RS

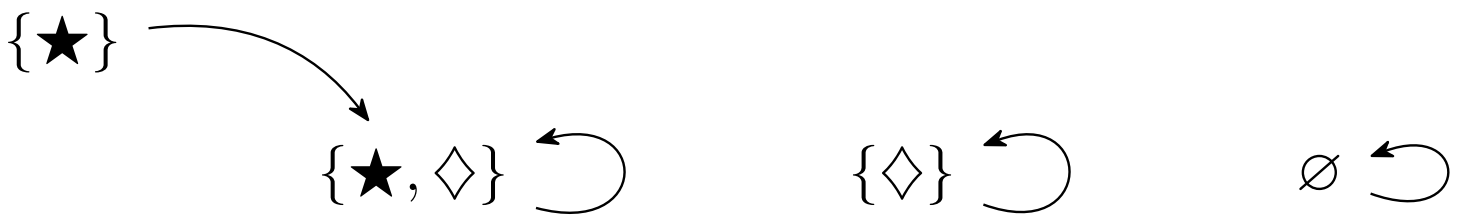
Fixed points

Background set: $S = \{\bigstar, \Diamond\}$

Set of reactions: $r_3 = (\{\bigstar\}, \varnothing, \{\bigstar, \Diamond\})$

$r_4 = (\{\Diamond\}, \{\bigstar\}, \{\Diamond\})$

Discrete dynamical system:



Fixed points: $\{\bigstar, \Diamond\}, \{\Diamond\}, \varnothing$

Example of RS

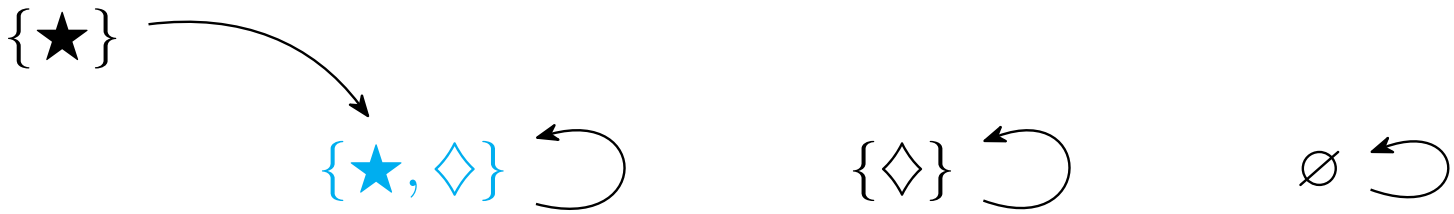
Fixed points

Background set: $S = \{\bigstar, \lozenge\}$

Set of reactions: $r_3 = (\{\bigstar\}, \varnothing, \{\bigstar, \lozenge\})$

$r_4 = (\{\lozenge\}, \{\bigstar\}, \{\lozenge\})$

Discrete dynamical system:



Fixed points: $\{\bigstar, \lozenge\}, \{\lozenge\}, \varnothing$

Fixed points attractor: $\{\bigstar, \lozenge\}$

Example of RS

Fixed points

Background set: $S = \{\bigstar, \lozenge\}$

Set of reactions: $r_3 = (\{\bigstar\}, \varnothing, \{\bigstar, \lozenge\})$

$r_4 = (\{\lozenge\}, \{\bigstar\}, \{\lozenge\})$

Discrete dynamical system:

Fixed points: $\{\bigstar, \lozenge\}, \{\lozenge\}, \varnothing$

Fixed points attractor: $\{\bigstar, \lozenge\}$

Fixed points not attractor: $\{\lozenge\}, \varnothing$

Problems regarding dynamical properties

Given a reaction system $\mathcal{A} = (S, A)$:

- $\exists$ a fixed point?
- $\exists$ global fixed point attractor?
- $\exists$ global cycle attractor?
- ecc. . .

Problems regarding dynamical properties

Given a reaction system $\mathcal{A} = (S, A)$:

- $\exists$ a fixed point? **NP**-complete[1]
- $\exists$ global cycle attractor? **PSPACE**-complete[2]
- ecc. . .

[1] Formenti, Manzoni, and Porreca 2014b.
[2] Formenti, Manzoni, and Porreca 2014a.

Resource-bounded systems

Class of RS	Type of reactions
$\mathcal{RS}(\infty, \infty)$	$(\{a, b\}, \{c\}, \{\dots\})$
$\mathcal{RS}(0, \infty)$	$(\varnothing, \{a, b\}, \{\dots\})$
$\mathcal{RS}(\infty, 0)$	$(\{a, b\}, \varnothing, \{\dots\})$
$\mathcal{RS}(1, 0)$	$(\{a\}, \varnothing, \{\dots\})$

Resource-bounded systems: classification[3]

Class of RS	Type of reactions	Subclass of $2^S \to 2^S$
$\mathcal{RS}(\infty, \infty)$	$(\{a, b\}, \{c\}, \{\dots\})$	all
$\mathcal{RS}(0, \infty)$	$(\varnothing, \{a, b\}, \{\dots\})$	antitone
$\mathcal{RS}(\infty, 0)$	$(\{a, b\}, \varnothing, \{\dots\})$	monotone
$\mathcal{RS}(1, 0)$	$(\{a\}, \varnothing, \{\dots\})$	additive

[3] Manzoni, Pocas, and Porreca 2014.

Resource-bounded systems: classification

Class of RS	**Subclass of** $2^S \to 2^S$
$\mathcal{RS}(\infty, \infty)$	all
$\mathcal{RS}(0, \infty)$	antitone
$\mathcal{RS}(\infty, 0)$	monotone
$\mathcal{RS}(1, 0)$	additive

Resource-bounded systems: classification

Class of RS	**Subclass of** $2^S \to 2^S$
$\mathcal{RS}(\infty, \infty)$	all
$\mathcal{RS}(0, \infty)$	antitone: $T \subseteq T' \Rightarrow \mathrm{res}(T) \supseteq \mathrm{res}(T')$
$\mathcal{RS}(\infty, 0)$	monotone
$\mathcal{RS}(1, 0)$	additive

Resource-bounded systems: classification

Class of RS	**Subclass of** $2^S \to 2^S$
$\mathcal{RS}(\infty, \infty)$	all
$\mathcal{RS}(0, \infty)$	antitone: $T \subseteq T' \Rightarrow \mathrm{res}(T) \supseteq \mathrm{res}(T')$
$\mathcal{RS}(\infty, 0)$	monotone: $T \subseteq T' \Rightarrow \mathrm{res}(T) \subseteq \mathrm{res}(T')$
$\mathcal{RS}(1, 0)$	additive

Resource-bounded systems: classification

Class of RS	**Subclass of $2^S \to 2^S$**
$\mathcal{RS}(\infty, \infty)$	all
$\mathcal{RS}(0, \infty)$	antitone: $T \subseteq T' \Rightarrow \mathrm{res}(T) \supseteq \mathrm{res}(T')$
$\mathcal{RS}(\infty, 0)$	monotone: $T \subseteq T' \Rightarrow \mathrm{res}(T) \subseteq \mathrm{res}(T')$
$\mathcal{RS}(1, 0)$	additive: $\mathrm{res}(T \cup T') = \mathrm{res}(T) \cup \mathrm{res}(T')$

∃ fixed point

Problem	$\mathcal{RS}(\infty, \infty)$	$\mathcal{RS}(0, \infty)$	$\mathcal{RS}(\infty, 0)$
∃ fixed point	**NP-c**[1]	**NP-c**[2]	**P** [3]

[1] Formenti, Manzoni, and Porreca 2014b

[2] Ascone, Bernardini, and Manzoni 2024b

[3] Knaster-Tarski Theorem

Our results: Fixed Points

Problem	$\mathcal{RS}(\infty,\infty)$	$\mathcal{RS}(0,\infty)$	$\mathcal{RS}(\infty,0)$	$\mathcal{RS}(1,0)$
A given state is a fixed point attractor	**NP**-c[1]	**NP**-c[2]	**NP**-c[2]	**P** [4]
$\exists$ fixed point	**NP**-c[1]	**NP**-c[2]	**P** [3]	
$\exists$ common fixed point	**NP**-c[1]	**NP**-c[2]	**NP**-c[2]	**P** [4]
sharing all fixed points	**coNP**-c[1]	**coNP**-c[2]	**coNP**-c[2]	**P** [4]
$\exists$ fixed point attractor	**NP**-c[1]	**NP**-c[2]	Unknown	**P** [4]
$\exists$ common fixed point attractor	**NP**-c[1]	**NP**-c[2]	**NP**-c[2]	**P** [4]
sharing all fixed points attractor	$\mathbf{\Pi}_2^{\mathbf{P}}$-c[1]	$\mathbf{\Pi}_2^{\mathbf{P}}$-c[2]	$\mathbf{\Pi}_2^{\mathbf{P}}$-c[2]	**P** [4]
$\exists$ fixed point not attractor	$\mathbf{\Sigma}_2^{\mathbf{P}}$-c[2]	$\mathbf{\Sigma}_2^{\mathbf{P}}$-c[2]	$\mathbf{\Sigma}_2^{\mathbf{P}}$-c[2]	**P** [4]
$\exists$ common fixed point not attractor	$\mathbf{\Sigma}_2^{\mathbf{P}}$-c[2]	$\mathbf{\Sigma}_2^{\mathbf{P}}$-c[2]	$\mathbf{\Sigma}_2^{\mathbf{P}}$-c[2]	**P** [4]
sharing all fixed points not attractor	**coNP**-c[2]	**coNP**-c[2]	**coNP**-c[2]	**P** [4]
$\mathrm{res}_{\mathcal{A}} = \mathrm{res}_{\mathcal{B}}$	**coNP**-c[2]	**P** [2]	**P** [2]	
res bijective	**coNP**-c [1]	**P** [2]	**P** [2]	

1 Formenti, Manzoni, and Porreca 2014b

2 Ascone, Bernardini, and Manzoni 2024b

3 Knaster-Tarski Theorem

4 Ascone, Bernardini, and Manzoni 2024a

Our results: Cycles and Global Attractors

Problem		$\mathcal{RS}(\infty,\infty)$	$\mathcal{RS}(0,\infty)$	$\mathcal{RS}(\infty,0)$
A given state is a global attractor		**PSPACE**-c[5]	**P**	**P**
$\exists$ global fixed point attractor		**PSPACE**-c[5]	**P**	**P**
$\exists$ global cycle attractor of length at least k	$k=2$	**PSPACE**-c[6]	**PSPACE**-c	$\nexists$
	$k>2$	**PSPACE**-c[6]	$\nexists$	$\nexists$
A given state is part of a cycle		**PSPACE**-c[5]	**PSPACE**-c	**PSPACE**-c
$\exists$ common cycle		**PSPACE**-c[5]	**PSPACE**-c	**PSPACE**-c
sharing all cycles		**PSPACE**-c[5]	**PSPACE**-c	**PSPACE**-c

[5] Formenti, Manzoni, and Porreca 2014a

[6] Dennunzio et al. 2019

Ascone, Bernardini, and Manzoni 2025

Our results: Cycles and Global Attractors

Problem		$\mathcal{RS}(\infty,\infty)$	$\mathcal{RS}(0,\infty)$	$\mathcal{RS}(\infty,0)$
A given state is a global attractor		**PSPACE**-c[5]	**P**	**P**
$\exists$ global fixed point attractor		**PSPACE**-c[5]	**P**	**P**
$\exists$ global cycle attractor of length at least k	$k=2$	**PSPACE**-c[6]	**PSPACE**-c	$\notin$
	$k>2$	**PSPACE**-c[6]	$\notin$	$\notin$
A given state is part of a cycle		**PSPACE**-c[5]	**PSPACE**-c	**PSPACE**-c
$\exists$ common cycle		**PSPACE**-c[5]	**PSPACE**-c	**PSPACE**-c
sharing all cycles		**PSPACE**-c[5]	**PSPACE**-c	**PSPACE**-c

[5] Formenti, Manzoni, and Porreca 2014a

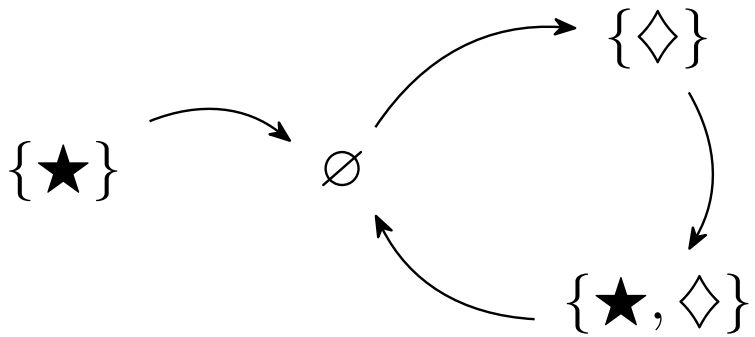
[6] Dennunzio et al. 2019

Ascone, Bernardini, and Manzoni 2025

Future research: study the last three problems for $\mathcal{RS}(1,0)$.

$\nexists$ global 3-cycle attractor in $\mathcal{RS}(0,\infty)$ or $\mathcal{RS}(\infty,0)$

The discrete dynamical system:



is associated to the RS

$$(\varnothing, \{\bigstar, \lozenge\}, \{\lozenge\})$$
$$(\{\lozenge\}, \{\bigstar\}, \{\bigstar, \lozenge\}).$$

Remark: we cannot achieve the same dynamics (3-cycle global attractor) with only reactions of the type $(\varnothing, \{\dots\}, \{\dots\})$ or only reactions of the type $(\{\dots\}, \varnothing, \{\dots\})$.

Reaction Systems $\mapsto$ Pure Reaction Automata

Form the standard definition of RS, we change the following features:

- sets $\rightarrow$ multisets
- allow inputs
- choose a manner to select reactions.

We get a non deterministic automaton called *Pure Reaction Automaton* (PRA).

Reaction Systems $\mapsto$ Pure Reaction Automata

Form the standard definition of RS, we change the following features:

- sets $\rightarrow$ multisets
- allow inputs
- choose a manner to select reactions.

We get a non deterministic automaton called *Pure Reaction Automaton* (PRA).

Chemical Pure Reaction Automata (CPRA) are PRA without inhibitors in each reaction (equivalent to $\mathcal{RS}(\infty, 0)$).

Reaction Systems $\mapsto$ Pure Reaction Automata

Form the standard definition of RS, we change the following features:

- sets $\rightarrow$ multisets
- allow inputs
- choose a manner to select reactions.

We get a non deterministic automaton called *Pure Reaction Automaton* (PRA).

Chemical Pure Reaction Automata (CPRA) are PRA without inhibitors in each reaction (equivalent to $\mathcal{RS}(\infty, 0)$).

Question

Do we achieve Turing universality with those new models?

Chemical Reactions

no inhibitors

Definition

Given a finite set S, a *chemical reaction* over S is a pair $(R, \varnothing, P)$ of multisets of S:

- R is the multiset of *reactants*,
- P is the multiset of *products*.

$(R, \varnothing, P)$ is *enabled* in a *state* $T \in S^{\#}$ when $R \leq T$.

Chemical Reactions

no inhibitors

Definition

Given a finite set S, a *chemical reaction* over S is a pair $(R, \varnothing, P)$ of multisets of S:

- R is the multiset of *reactants*,
- P is the multiset of *products*.

$(R, \varnothing, P)$ is *enabled* in a *state* $T \in S^{\#}$ when $R \leq T$.

The reaction $(\{a\}, \varnothing, \{b\})$ is enabled by $\{a, a, b\}$ since

$$\{a\} \leq \{a, a, b\}$$

Chemical Reactions

no inhibitors

Definition

Given a finite set S, a *chemical reaction* over S is a pair $(R, \varnothing, P)$ of multisets of S:

- R is the multiset of *reactants*,
- P is the multiset of *products*.

$(R, \varnothing, P)$ is *enabled* in a *state* $T \in S^{\#}$ when $R \leq T$.

The reaction $(\{a\}, \varnothing, \{b\})$ is enabled by $\{a, a, b\}$ since

$$\{a\} \leq \{a, a, b\}$$

but $(\{a, a, a\}, \varnothing, \{b, b, b\})$ is not enabled by $\{a, a, b\}$ since

$$\{a, a, a\} \not\leq \{a, a, b\}.$$

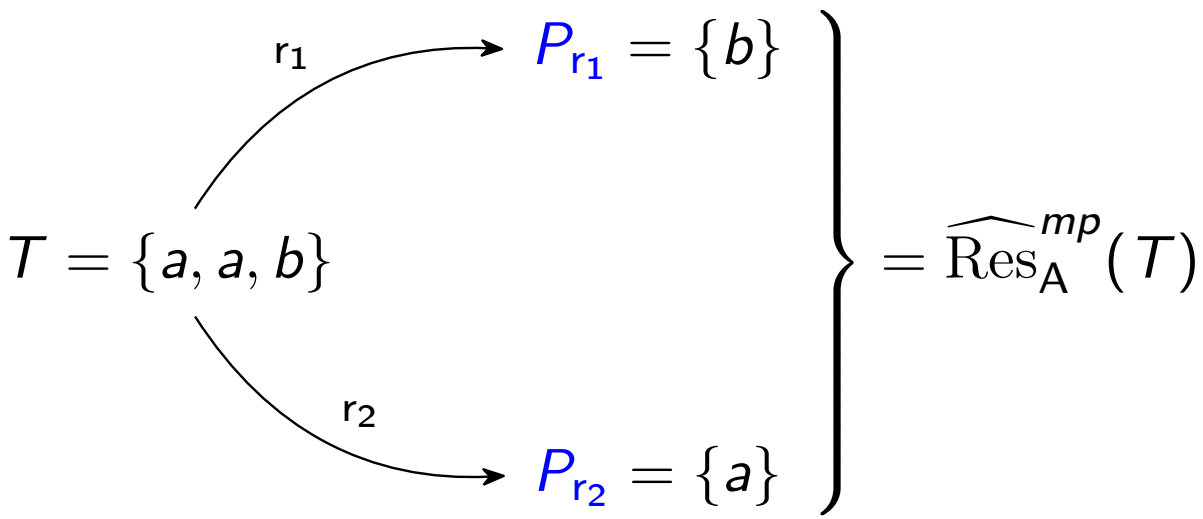
Pure Result[4]

$$\mathsf{A} = \{\mathsf{r}_1 = (\{a, a\}, \varnothing, \{b\}),$$
$$\mathsf{r}_2 = (\{a, a, b\}, \varnothing, \{a\})\}$$
$$T = \{a, a, b\}$$
$$\mathrm{En}_{\mathsf{A}}^{mp}(T) = \{\mathsf{r}_1, \mathsf{r}_2\} \leftarrow \text{reactions } \textit{maximally parallel} \text{ enabled}$$

[4] Ascone, Bernardini, Formenti, et al. 2024.

Pure Result[4]

$$\mathrm{A} = \{\mathsf{r}_1 = (\{a, a\}, \varnothing, \{b\}),$$
$$\mathsf{r}_2 = (\{a, a, b\}, \varnothing, \{a\})\}$$
$$T = \{a, a, b\}$$
$$\mathrm{En}_{\mathrm{A}}^{mp}(T) = \{\mathsf{r}_1, \mathsf{r}_2\} \leftarrow \text{reactions } \textit{maximally parallel} \text{ enabled}$$



[4] Ascone, Bernardini, Formenti, et al. 2024.

How powerful are CPRA?[5]

Results summary (Ascone, Bernardini, Leiter, et al. 2025)

- Non deterministic CPRA are Turing complete.
- Deterministic CPRA are not Turing complete.

[5] Rocco Ascone, Giulia Bernardini, Francesco Leiter, et al. (2025). "Chemical Pure Reaction Automata in Maximally Parallel Manner". In: *J. Membr. Comput.*, pp. 1–10. DOI: 10.1007/s41965-024-00176-7.

How powerful are CPRA?[5]

Results summary (Ascone, Bernardini, Leiter, et al. 2025)

- Non deterministic CPRA are Turing complete.
- Deterministic CPRA are not Turing complete.

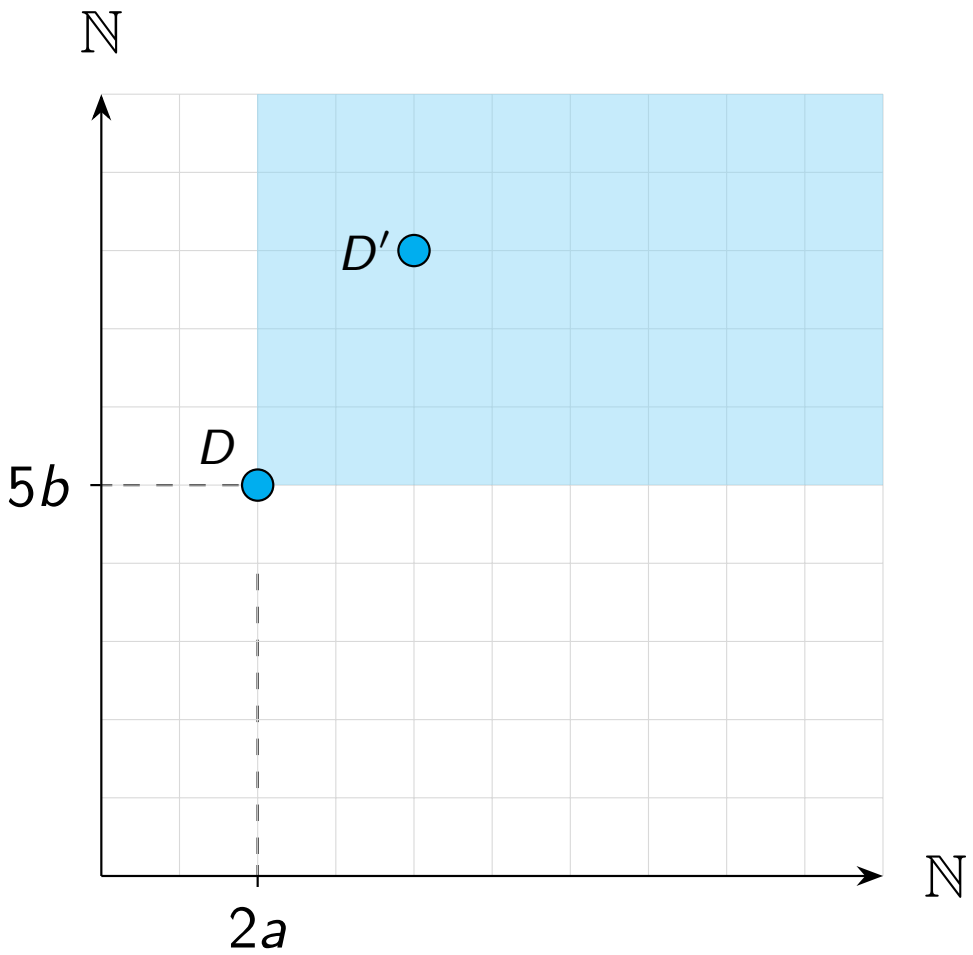
Actually CPRA recognize exactly regular languages.

[5] Rocco Ascone, Giulia Bernardini, Francesco Leiter, et al. (2025). "Chemical Pure Reaction Automata in Maximally Parallel Manner". In: *J. Membr. Comput.*, pp. 1–10. DOI: 10.1007/s41965-024-00176-7.

Deterministic CPRA in *mp* are *monotone*

Lemma

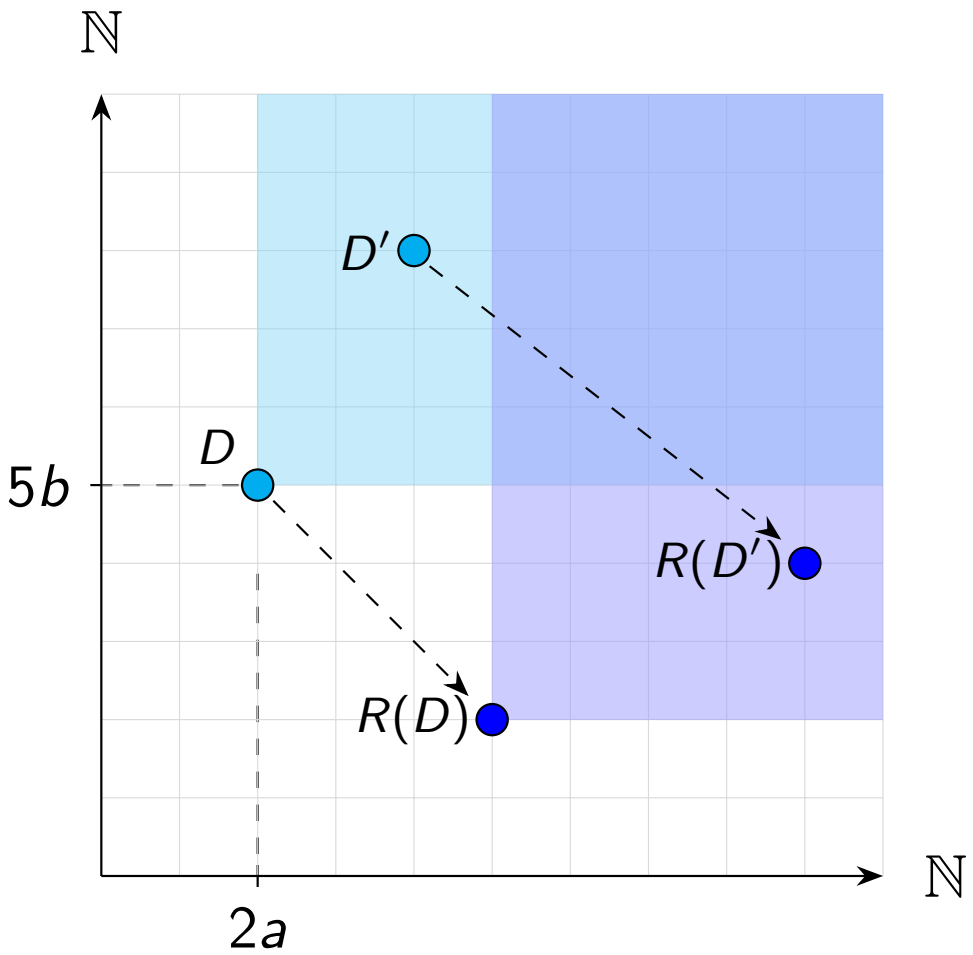
Let D, D' multisets such that $D \leq D'$, then $R(D) \leq R(D')$.



Deterministic CPRA in *mp* are *monotone*

Lemma

Let D, D' multisets such that $D \leq D'$, then $R(D) \leq R(D')$.



Pure Reaction Automata[6]

Inhibitors rule

What happens if we use also inhibitors in the reactions?

[6] Rocco Ascone, Giulia Bernardini, Enrico Formenti, et al. (2024). "Pure reaction automata". In: *Nat. Comput.* 23.2. DOI: 10.1007/S11047-024-09980-7.

Pure Reaction Automata[6]

Inhibitors rule

What happens if we use also inhibitors in the reactions?

Results summary (Ascone, Bernardini, Formenti, et al. 2024)

Both in the deterministic and non deterministic case, PRA are Turing complete.

[6] Rocco Ascone, Giulia Bernardini, Enrico Formenti, et al. (2024). "Pure reaction automata". In: *Nat. Comput.* 23.2. DOI: 10.1007/S11047-024-09980-7.

Cryptographic properties: nonlinearity and balanced

Let $\mathbb{F}_2 = \{0, 1\}$.

- *Linear boolean functions*: for any $a \in \mathbb{F}_2^n$, we define $\ell_a : \mathbb{F}_2^n \to \mathbb{F}_2$ as

$$\ell_a(x) = x_1 \cdot a_1 \oplus x_2 \cdot a_2 \oplus \cdots \oplus x_n \cdot a_n,$$

  where the product is AND logic operation and the sum is the XOR logic operation.

Cryptographic properties: nonlinearity and balanced

Let $\mathbb{F}_2 = \{0, 1\}$.

- *Linear boolean functions*: for any $a \in \mathbb{F}_2^n$, we define $\ell_a : \mathbb{F}_2^n \to \mathbb{F}_2$ as

$$\ell_a(x) = x_1 \cdot a_1 \oplus x_2 \cdot a_2 \oplus \cdots \oplus x_n \cdot a_n,$$

  where the product is AND logic operation and the sum is the XOR logic operation.
- The *nonlinearity* of $f : \mathbb{F}_2^n \to \mathbb{F}_2$ measures the Hamming distance of the function from the set of all linear functions.

Cryptographic properties: nonlinearity and balanced

Let $\mathbb{F}_2 = \{0, 1\}$.

- *Linear boolean functions*: for any $a \in \mathbb{F}_2^n$, we define $\ell_a : \mathbb{F}_2^n \to \mathbb{F}_2$ as

$$\ell_a(x) = x_1 \cdot a_1 \oplus x_2 \cdot a_2 \oplus \cdots \oplus x_n \cdot a_n,$$

  where the product is AND logic operation and the sum is the XOR logic operation.
- The *nonlinearity* of $f : \mathbb{F}_2^n \to \mathbb{F}_2$ measures the Hamming distance of the function from the set of all linear functions.
- A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called *balanced* if its truth table contains an equal number of zeros and ones.

Example of Boolean function

Let $\varphi : \mathbb{F}_2^3 \to \mathbb{F}_2$ defined as $\varphi(x) := (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2 \wedge x_3)$.

$x_1x_2x_3$	φ
000	0
001	0
010	0
011	1
100	1
101	1
110	0
111	0

Example of Boolean function

Let $\varphi : \mathbb{F}_2^3 \to \mathbb{F}_2$ defined as $\varphi(x) := (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2 \wedge x_3)$.

$x_1x_2x_3$	φ
000	0
001	0
010	0
011	1
100	1
101	1
110	0
111	0

Since there are 3 ones and 5 zeros the function is not balanced.

Example of Boolean function

Let $\varphi : \mathbb{F}_2^3 \to \mathbb{F}_2$ defined as $\varphi(x) := (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2 \wedge x_3)$.

$x_1x_2x_3$	φ	ℓ_{110}
000	0	0
001	0	0
010	0	1
011	1	1
100	1	1
101	1	1
110	0	0
111	0	0

Example of Boolean function

Let $\varphi : \mathbb{F}_2^3 \to \mathbb{F}_2$ defined as $\varphi(x) := (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2 \wedge x_3)$.

$x_1x_2x_3$	φ	ℓ_{110}
000	0	0
001	0	0
010	0	1
011	1	1
100	1	1
101	1	1
110	0	0
111	0	0

The minimum Hamming distance between φ and the linear functions is achieved with $\ell_{110} = x_1 \oplus x_2$. Therefore the nonlinearity of φ is 1.

Balanced highly nonlinear functions

Research question

Find balanced functions with the highest nonlinearity.

Balanced highly nonlinear functions

Research question

Find balanced functions with the highest nonlinearity.

For $n \geq 8$, it is **not** known which is the exact highest value of nonlinearity a balanced function can reach.

Balanced highly nonlinear functions

Research question

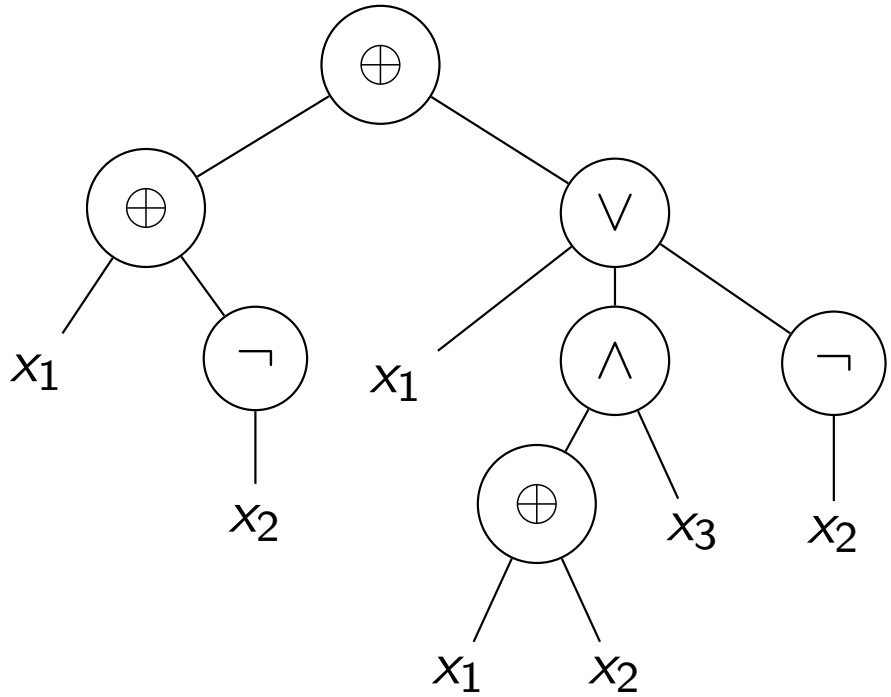
Find balanced functions with the highest nonlinearity.

For $n \geq 8$, it is **not** known which is the exact highest value of nonlinearity a balanced function can reach.

Solution? Evolutionary algorithms.

Encodings

Three different encodings for a Boolean function $f : \mathbb{F}_2^3 \to \mathbb{F}_2$ given by $f(x) = (x_1 \oplus \neg x_2) \oplus (x_1 \vee ((x_1 \oplus x_2) \wedge x_3) \vee \neg x_2)$:

Strategy	**Encoding**
Genetic Programming	
Genetic Algorithm	$[0, 0, 0, 1, 1, 1, 0, 0]$

RS and DNF formulas

RS can encode Boolean functions in Disjunctive Normal Form (DNF).

Background set: $S = \{x_0, x_1, x_2, \text{True}\}$
Set of reactions: $r_1 = (\{x_0\}, \{x_1, x_2\}, \{\text{True}\})$
$r_2 = (\{x_1\}, \{x_0, x_2\}, \{\text{True}\})$
$r_3 = (\{x_1, x_2\}, \{x_0\}, \{\text{True}\})$

$$f(x) = (x_0 \wedge \neg x_1 \wedge \neg x_2) \vee (x_1 \wedge \neg x_0 \wedge \neg x_2) \vee (x_1 \wedge x_2 \wedge \neg x_0)$$

RS and DNF formulas

RS can encode Boolean functions in Disjunctive Normal Form (DNF).

Background set: $S = \{x_0, x_1, x_2, \text{True}\}$
Set of reactions: $r_1 = (\{x_0\}, \{x_1, x_2\}, \{\text{True}\})$
$r_2 = (\{x_1\}, \{x_0, x_2\}, \{\text{True}\})$
$r_3 = (\{x_1, x_2\}, \{x_0\}, \{\text{True}\})$

$$f(x) = (x_0 \wedge \neg x_1 \wedge \neg x_2) \vee (x_1 \wedge \neg x_0 \wedge \neg x_2) \vee (x_1 \wedge x_2 \wedge \neg x_0)$$

Idea

Construct an evolutionary algorithm to find highly nonlinear boolean functions encoded by RS.

RS and DNF formulas

RS can encode Boolean functions in Disjunctive Normal Form (DNF).

Background set: $S = \{x_0, x_1, x_2, \text{True}\}$
Set of reactions: $r_1 = (\{x_0\}, \{x_1, x_2\}, \{\text{True}\})$
$r_2 = (\{x_1\}, \{x_0, x_2\}, \{\text{True}\})$
$r_3 = (\{x_1, x_2\}, \{x_0\}, \{\text{True}\})$

$$f(x) = (x_0 \wedge \neg x_1 \wedge \neg x_2) \vee (x_1 \wedge \neg x_0 \wedge \neg x_2) \vee (x_1 \wedge x_2 \wedge \neg x_0)$$

Idea

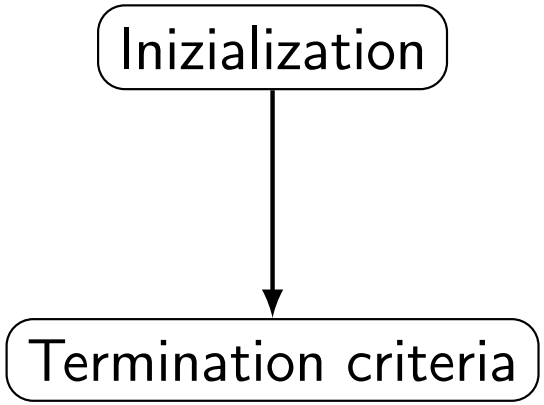
Construct an evolutionary algorithm to find highly nonlinear boolean functions encoded by RS.

$\Rightarrow$ **Evolutionary Boolean Reaction System** (EvoBRS)

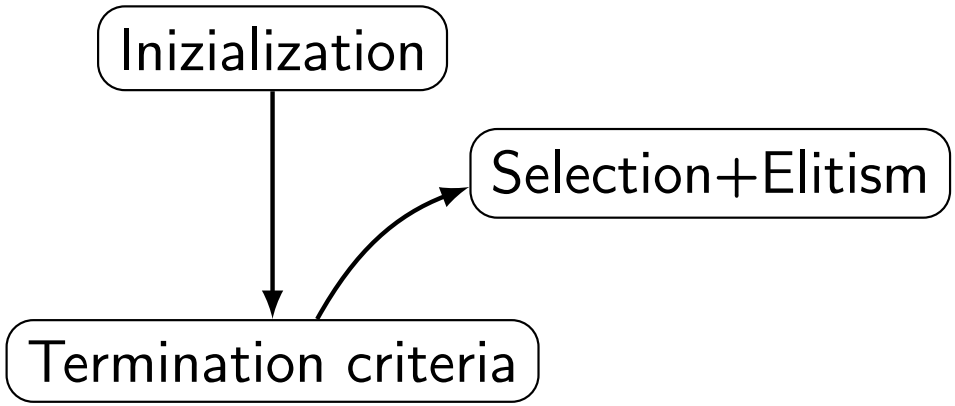
Evolution cycle of EvoBRS

Inizialization

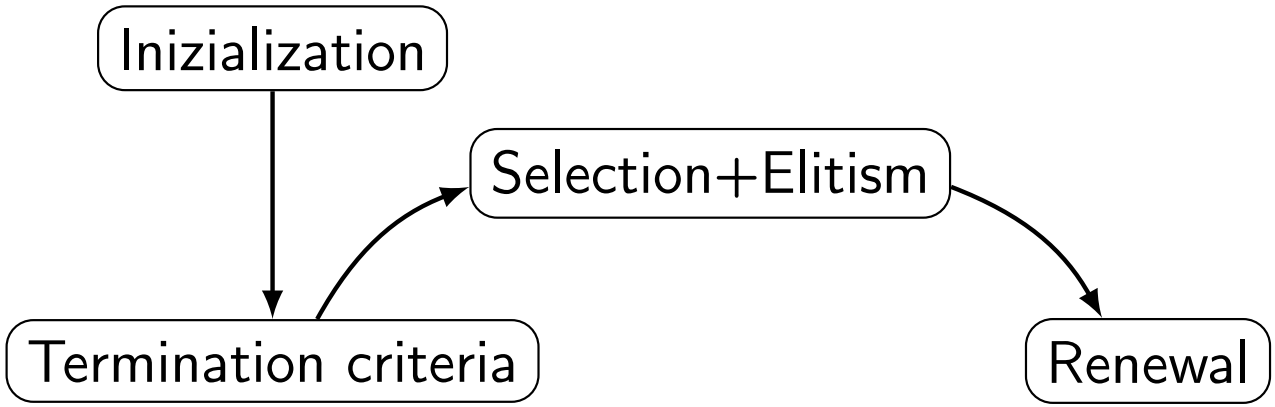
Evolution cycle of EvoBRS



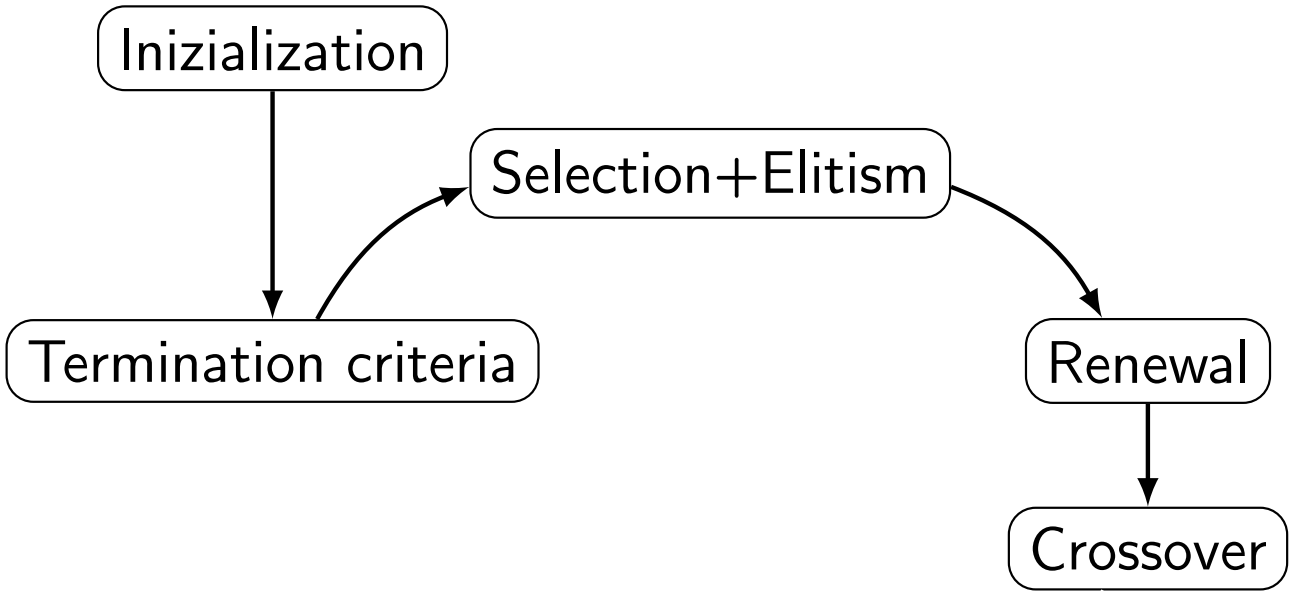
Evolution cycle of EvoBRS



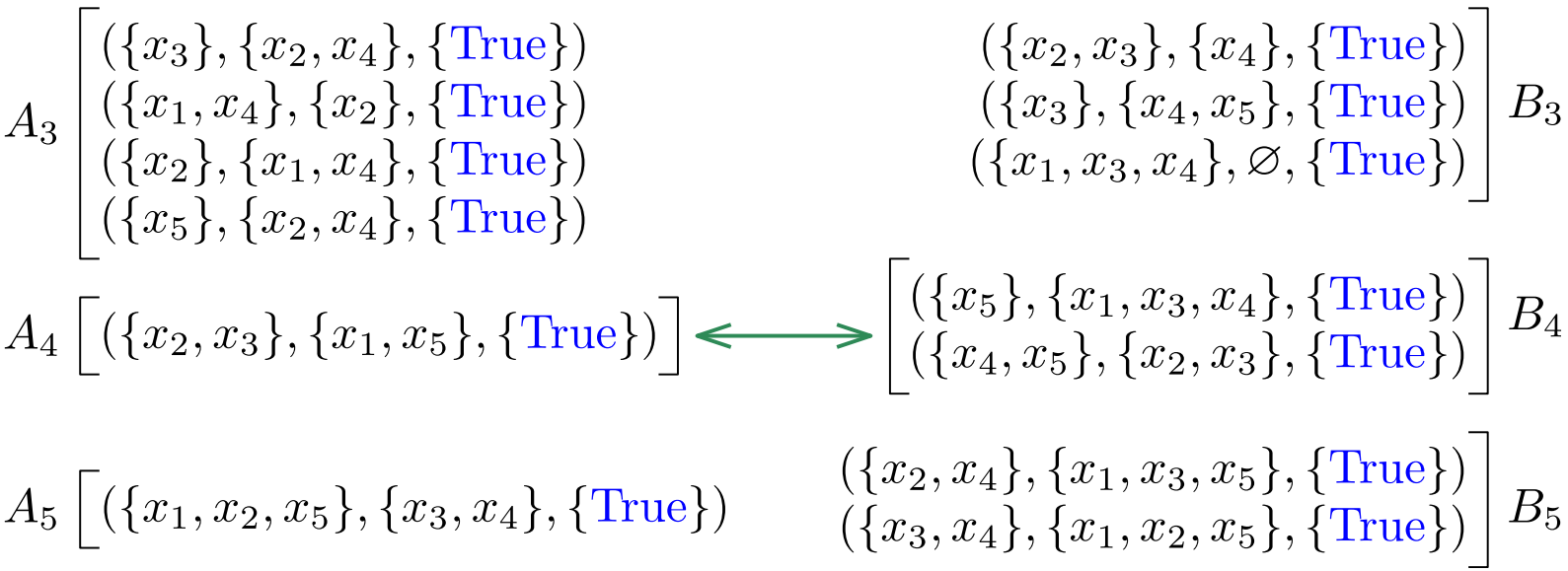
Evolution cycle of EvoBRS



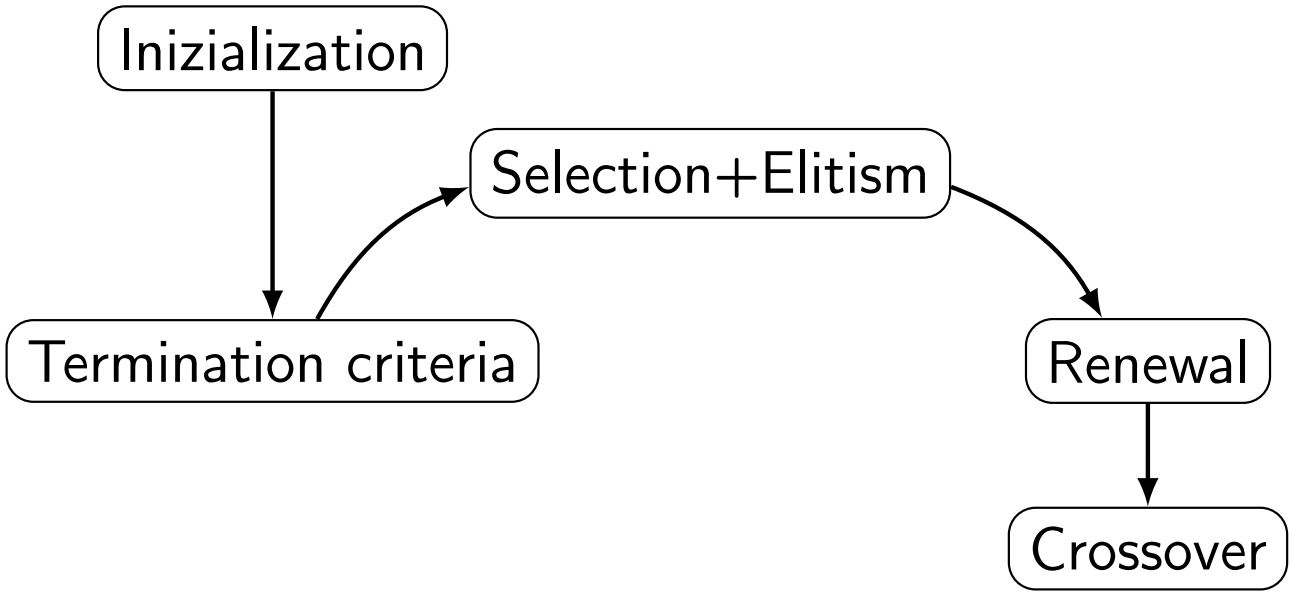
Evolution cycle of EvoBRS



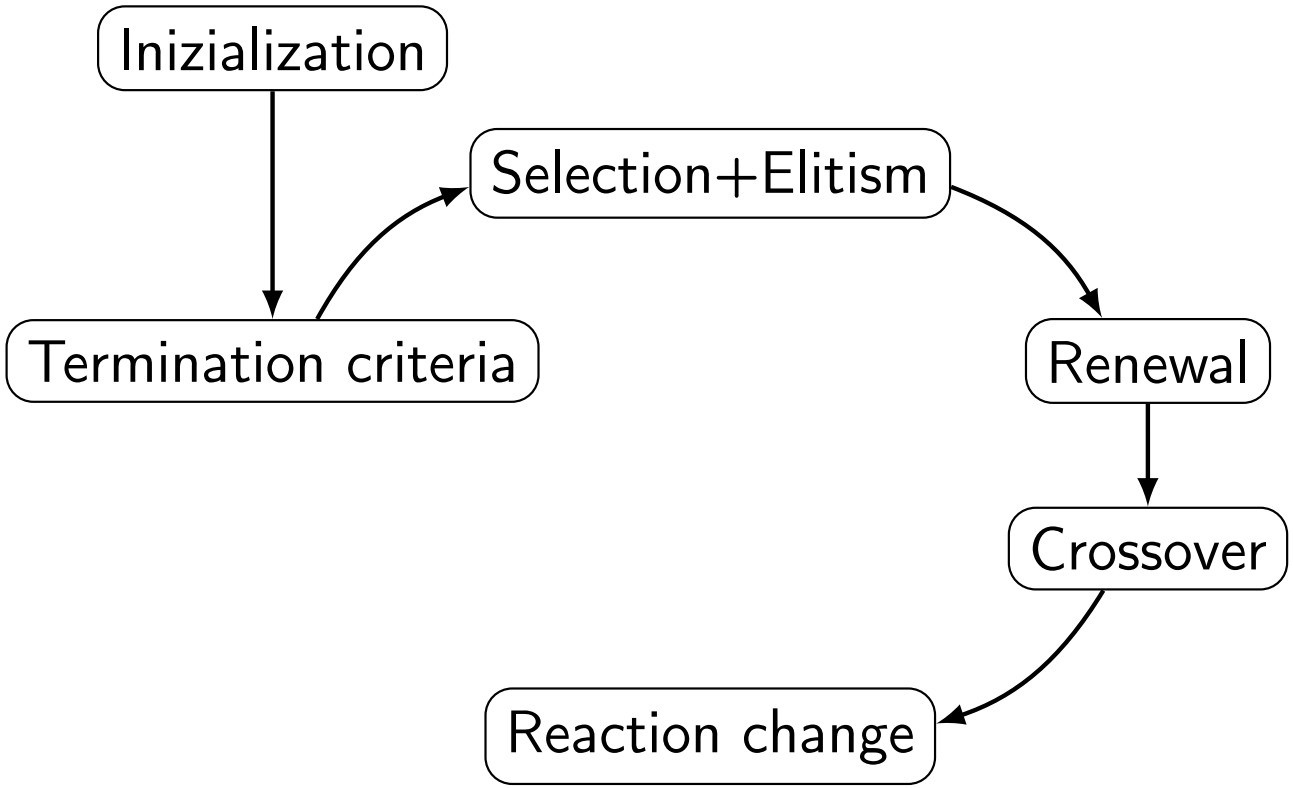
Crossover


$\mathcal{A} = (S, A)$
$\mathcal{B} = (S, B)$
A_3
$(\{x_3\}, \{x_2, x_4\}, \{\text{True}\})$
$(\{x_1, x_4\}, \{x_2\}, \{\text{True}\})$
$(\{x_2\}, \{x_1, x_4\}, \{\text{True}\})$
$(\{x_5\}, \{x_2, x_4\}, \{\text{True}\})$
$(\{x_2, x_3\}, \{x_4\}, \{\text{True}\})$
$(\{x_3\}, \{x_4, x_5\}, \{\text{True}\})$
$(\{x_1, x_3, x_4\}, \varnothing, \{\text{True}\})$
B_3
A_4
$(\{x_2, x_3\}, \{x_1, x_5\}, \{\text{True}\})$
$(\{x_5\}, \{x_1, x_3, x_4\}, \{\text{True}\})$
$(\{x_4, x_5\}, \{x_2, x_3\}, \{\text{True}\})$
B_4
A_5
$(\{x_1, x_2, x_5\}, \{x_3, x_4\}, \{\text{True}\})$
$(\{x_2, x_4\}, \{x_1, x_3, x_5\}, \{\text{True}\})$
$(\{x_3, x_4\}, \{x_1, x_2, x_5\}, \{\text{True}\})$
B_5

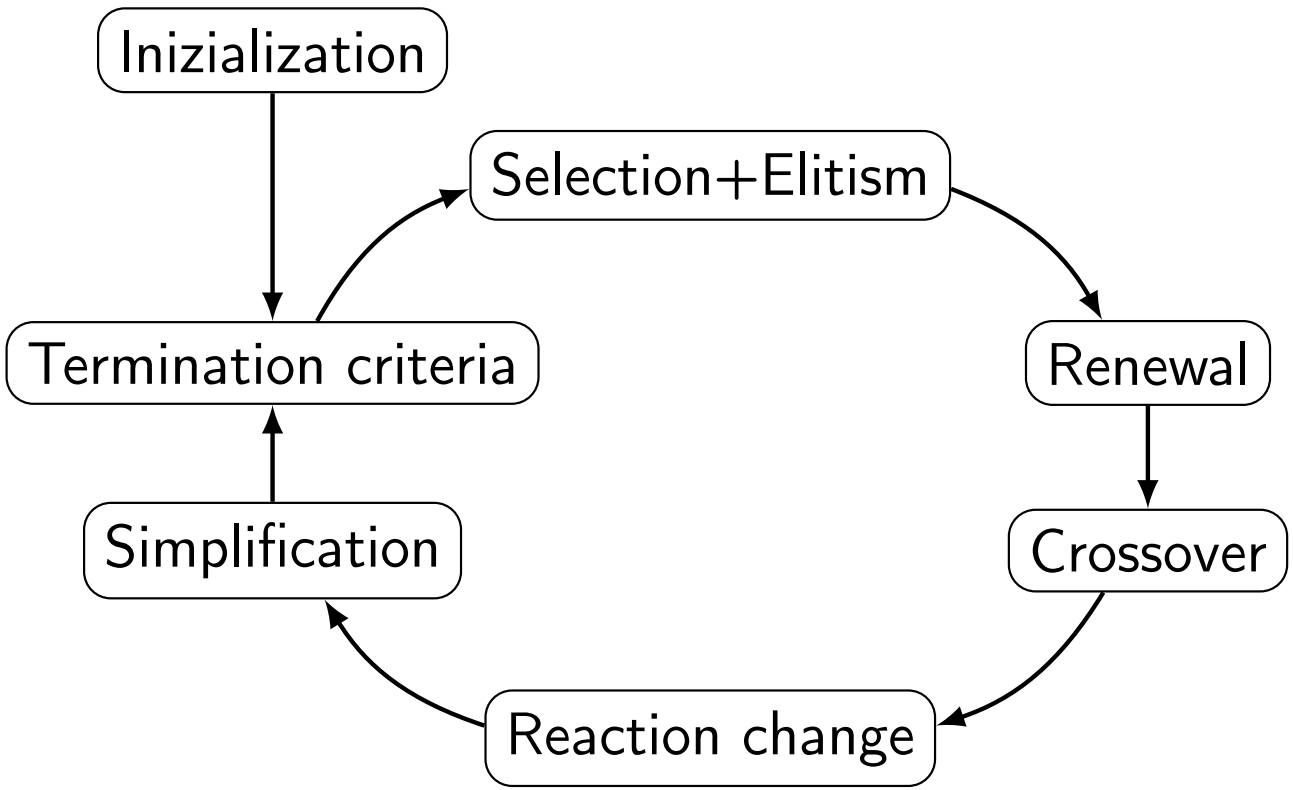
Evolution cycle of EvoBRS



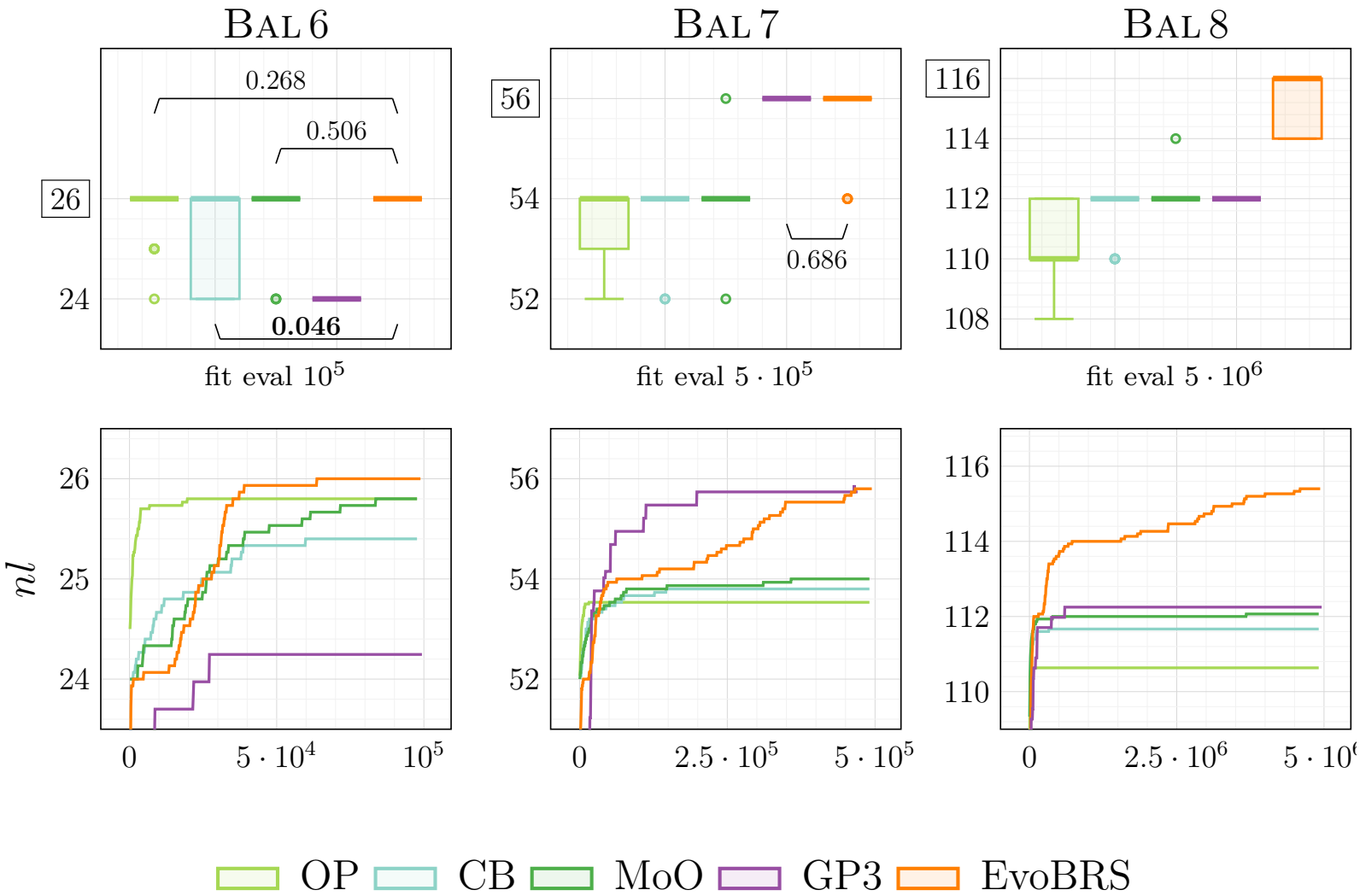
Evolution cycle of EvoBRS



Evolution cycle of EvoBRS



Results


Bal 6
Bal 7
Bal 8
0.268
0.506
0.046
0.686
26
24
56
54
52
116
114
112
110
108
fit eval 10^5
fit eval $5 \cdot 10^5$
fit eval $5 \cdot 10^6$
nl
25
0
$5 \cdot 10^4$
10^5
$2.5 \cdot 10^5$
$5 \cdot 10^5$
$2.5 \cdot 10^6$
OP
CB
MoO
GP3
EvoBRS

Gracias por su atención!

References (Complexity and Computability)

- Rocco Ascone, Giulia Bernardini, and Luca Manzoni (2024b). "Fixed points and attractors of reactantless and inhibitorless reaction systems". In: *Theoretical Computer Science* 984. DOI: 10.1016/j.tcs.2023.114322
- Rocco Ascone, Giulia Bernardini, and Luca Manzoni (2024a). "Fixed points and attractors of additive reaction systems". In: *Natural Computing*. DOI: 10.1007/s11047-024-09977-2
- Rocco Ascone, Giulia Bernardini, and Luca Manzoni (2025). "Cycles and global attractors of reactantless and inhibitorless reaction systems". In: *Theor. Comput. Sci.* 1045. DOI: 10.1016/J.TCS.2025.115300
- Rocco Ascone, Giulia Bernardini, Enrico Formenti, et al. (2024). "Pure reaction automata". In: *Nat. Comput.* 23.2. DOI: 10.1007/S11047-024-09980-7
- Rocco Ascone, Giulia Bernardini, Francesco Leiter, et al. (2025). "Chemical Pure Reaction Automata in Maximally Parallel Manner". In: *J. Membr. Comput.*, pp. 1–10. DOI: 10.1007/s41965-024-00176-7

References (Cryptography and other research)

- Rocco Ascone, Luca Mariot, et al. (2025). "Evolving Cryptographic Boolean Functions with Reaction Systems". In: *Proceedings of the Genetic and Evolutionary Computation Conference Companion*, pp. 195–198. DOI: 10.1145/3712255.3726685
- Rocco Ascone, Giulia Bernardini, Alessio Conte, Massimo Equi, et al. (2024). "A Unifying Taxonomy of Pattern Matching in Degenerate Strings and Founder Graphs". In: *24th International Workshop on Algorithms in Bioinformatics (WABI 2024)*. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 14:1–14:21. DOI: 10.4230/LIPIcs.WABI.2024.14
- Rocco Ascone, Giulia Bernardini, Alessio Conte, Veronica Guerrini, et al. (2025). "Are Depth-2 Regular Expressions Hard to Intersect?" In: *arXiv preprint*. DOI: 10.48550/arXiv.2507.03593