Evolving Cryptographic Boolean Functions with Reaction Systems

Rocco Ascone, Luca Manzoni, Luca Mariot, Gloria Pietropolli

Problem

- **BENT**: find maximally *non-linear* Boolean functions.
- **BAL**: find maximally non-linear *balanced* Boolean functions.

Application ⟶ Cryptography

Challenges

- Huge search space $\mathcal{O}(2^{2^n})$
- **Compact** and **interpretable** representation
- Designing independent solutions

Idea : Boolean Reaction System

Boolean Reaction Systems are a natural way to encode Boolean functions in their **DNF** (Disjunctive Normal Form) representation.

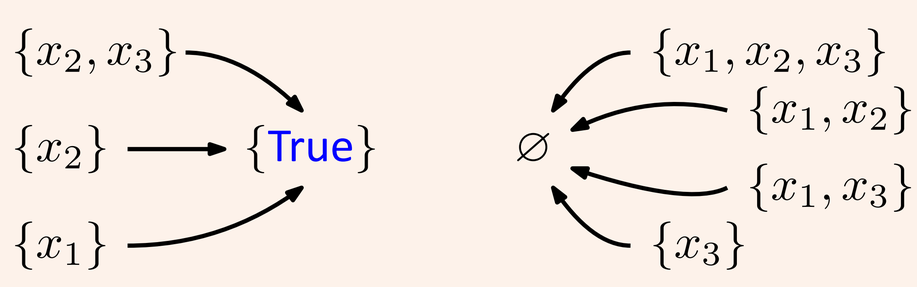
Encoding

Boolean function in DNF:

$$(x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (x_2 \wedge \neg x_1 \wedge \neg x_3) \vee (x_2 \wedge x_3 \wedge \neg x_1)$$

Set of clauses:	Reaction System:
$(x_2 \wedge x_3 \wedge \neg x_1)$	$(\{x_2, x_3\}, \{x_1\}, \{\text{True}\})$
$(x_2 \wedge \neg x_1 \wedge \neg x_3)$	$(\{x_2\}, \{x_1, x_3\}, \{\text{True}\})$
$(x_1 \wedge \neg x_2 \wedge \neg x_3)$	$(\{x_1\}, \{x_2, x_3\}, \{\text{True}\})$

Discrete Dynamical System:



Evolutionary Boolean Reaction Systems (EvoBRS)

Crossover

Reaction System $\mathcal{A}$	Reaction System $\mathcal{B}$	
$(\{x_2\}, \{x_1, x_4\}, \{\text{True}\})$		size 3
$(\{x_5\}, \{x_2, x_4\}, \{\text{True}\})$		
	$(\{x_2, x_3\}, \{x_4\}, \{\text{True}\})$	size 3
$(\{x_2, x_3\}, \{x_1, x_5\}, \{\text{True}\})$	$(\{x_5\}, \{x_1, x_3, x_4\}, \{\text{True}\})$	size 4
	$(\{x_4, x_5\}, \{x_2, x_3\}, \{\text{True}\})$	size 4
$(\{x_1, x_2, x_5\}, \{x_3, x_4\}, \{\text{True}\})$		size 5
	$(\{x_2, x_4\}, \{x_1, x_3, x_5\}, \{\text{True}\})$	size 5
	$(\{x_3, x_4\}, \{x_1, x_2, x_5\}, \{\text{True}\})$	size 5

Mutation

Reaction System $\mathcal{A}$	Reaction System $\mathcal{A}'$	
$(\{x_2, x_3\}, \{x_4\}, \{\text{True}\})$	$(\{x_2\}, \{x_1, x_4\}, \{\text{True}\})$	size 3
$(\{x_5\}, \{x_1, x_3, x_4\}, \{\text{True}\})$	$(\{x_5\}, \{x_1, x_3, x_4\}, \{\text{True}\})$	
$(\{x_4, x_5\}, \{x_2, x_3\}, \{\text{True}\})$	$(\{x_4, x_5\}, \{x_2, x_3\}, \{\text{True}\})$	
$(\{x_2, x_4\}, \{x_1, x_3, x_5\}, \{\text{True}\})$	$(\{x_1, x_2, x_5\}, \{x_3, x_4\}, \{\text{True}\})$	size 5
$(\{x_3, x_4\}, \{x_1, x_2, x_5\}, \{\text{True}\})$	$(\{x_3, x_4\}, \{x_1, x_2, x_5\}, \{\text{True}\})$	

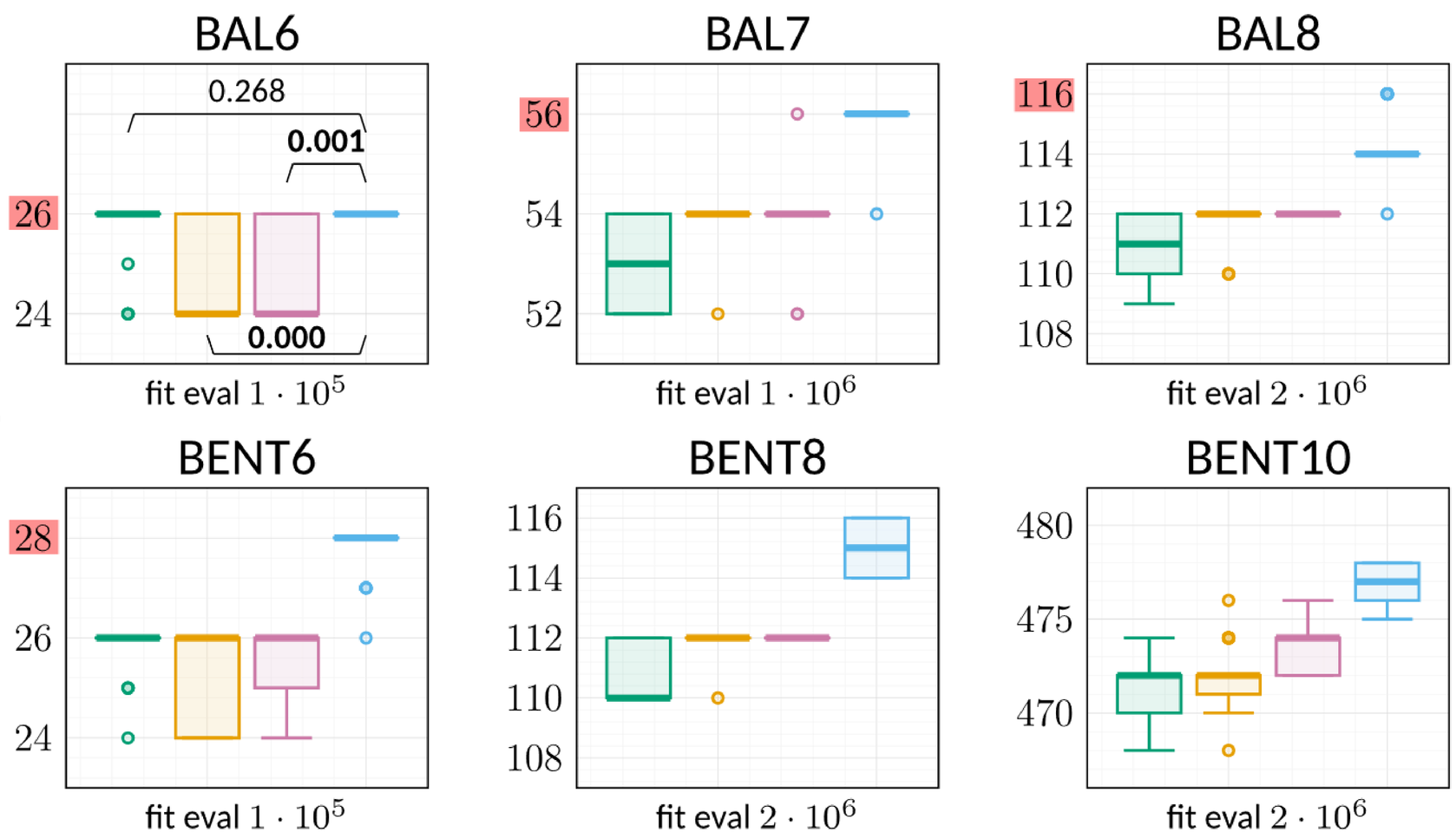
The operators satisfy some **new** theoretical results regarding DNF representation.

Experiments

Final distribution of the non-linearity achieved by the best individual across 30 runs:

GAs using the *truth table* representation

Legend:
- OP
- CP
- MoO
- EvoBRS



C++ implementation

Results

We achieved the maximum known values of non-linearity for **BAL6 (26)**,**BENT6 (28)**, **BAL7 (56)**, **BAL8 (116)**.

Email: rocco.ascone@phd.units.it
Github: @roccoasc1