
Radboud University



# Evolutionary Construction of Weightwise Perfectly Balanced Boolean Functions

**Luca Mariot**, Stjepan Picek, Domagoj Jakobovic, Marko Djurasevic, Alberto Leporati

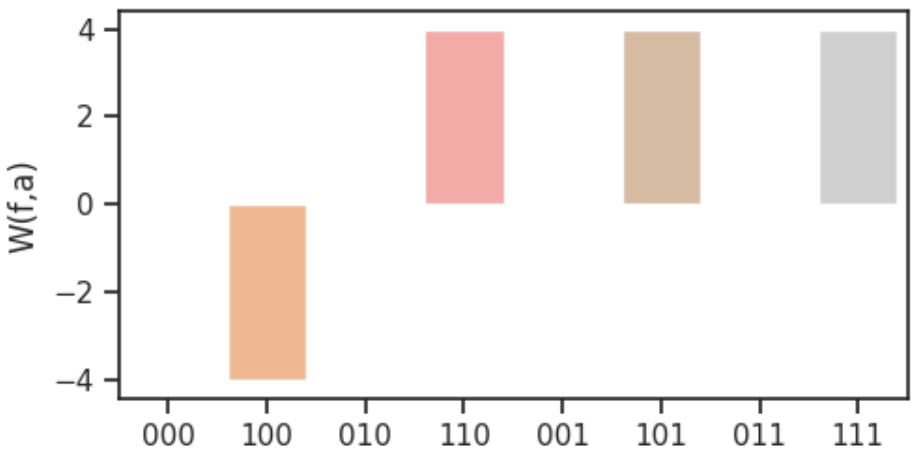
luca.mariot@ru.nl

CEC 2022 – Padova, July 11, 2022

# Boolean Functions

- **Boolean function** of $n$ variables: mapping $f : \{0,1\}^n \to \{0,1\}$
- **Walsh Transform** (WT): correlation of $f$ with linear functions $a \cdot x = a_1 x_1 \oplus \cdots \oplus a_n x_n$

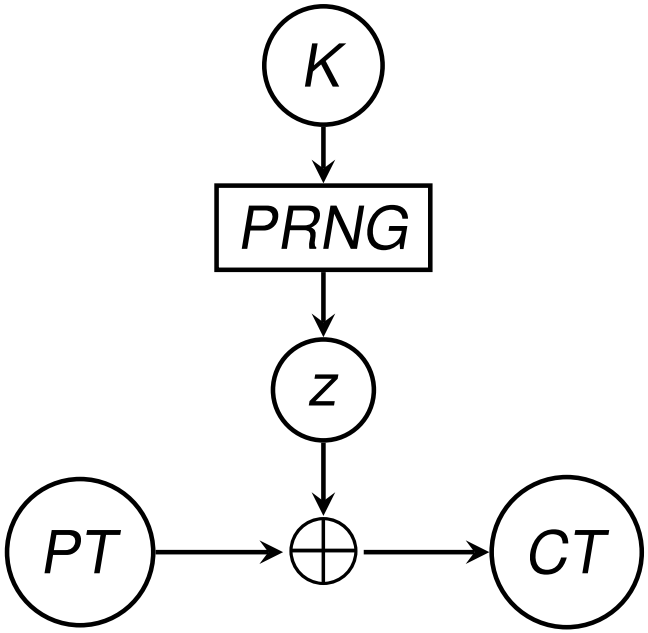
$$W_f(a) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus a \cdot x}$$



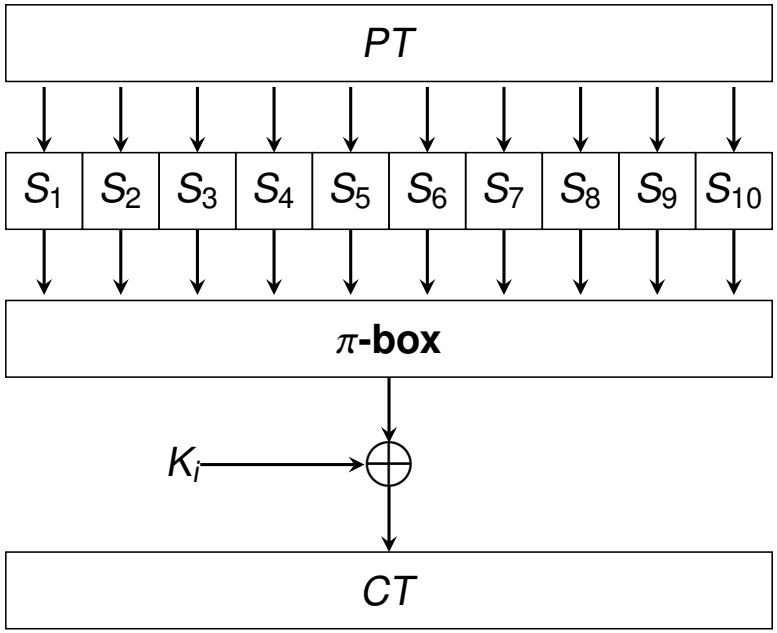

Example: $n = 3$ variables

| $(x_1, x_2, x_3)$ | $f(x)$ | $W_f(a)$ |
|---|---|---|
| 000 | 0 | 0 |
| 001 | 1 | -4 |
| 010 | 1 | 0 |
| 011 | 0 | 4 |
| 100 | 1 | 0 |
| 101 | 0 | 4 |
| 110 | 1 | 0 |
| 111 | 0 | 4 |

# Boolean functions in symmetric crypto




(a) Stream cipher




(b) Block cipher

Used in the design of low-level primitives, e.g. [C21]:

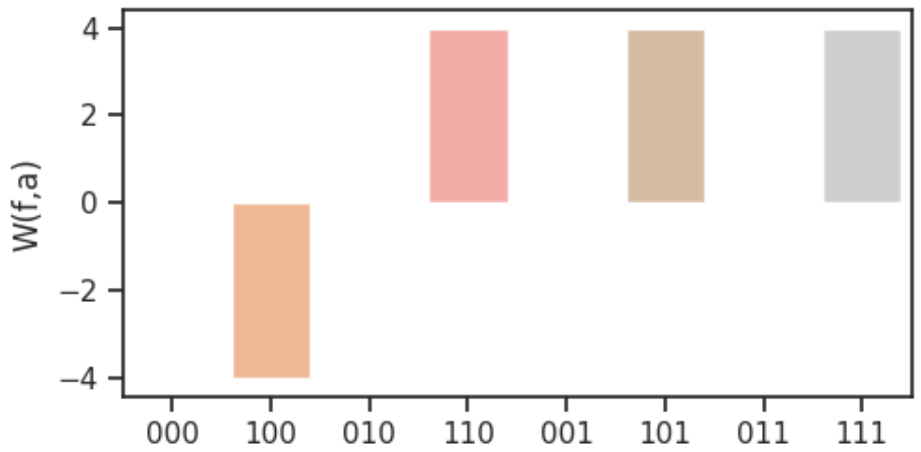
- Pseudorandom number generators (PRNG)
- S-boxes $F : \{0,1\}^n \to \{0,1\}^n$, ...

# Boolean Functions - Cryptographic Properties

To be useful in cryptography, $f : \{0,1\}^n \to \{0,1\}$ should be:

- **Balanced:** TT of $f$ has the same number of 0s and 1s
- **Highly nonlinear:** the nonlinearity of $f$ is given by the WT as:

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \left\{ \left| W_f(a) \right| \right\}$$




Ex: $f$ balanced, $nl(f) = 2^{3-1} - \frac{1}{2} \cdot 4 = 2$

| $(x_1, x_2, x_3)$ | $f(x)$ | $W_f(a)$ |
|---|---|---|
| 000 | 0 | 0 |
| 001 | 1 | -4 |
| 010 | 1 | 0 |
| 011 | 0 | 4 |
| 100 | 1 | 0 |
| 101 | 0 | 4 |
| 110 | 1 | 0 |
| 111 | 0 | 4 |

# Weightwise Perfect Balanced (WPB) functions [Me19]

- $w_H(x)$: **Hamming weight** of $x \Leftrightarrow$ number of 1s in $x$
- $E_{n,k} \subseteq \{0,1\}^n$: set of $n$-bit strings of weight $k$
- **WPB function**: $f$ is balanced on all $E_{n,k}$, for $1 \leq k \leq n-1$
- Exist only if $n = 2^t$ for $t \in \mathbb{N}$
- **Restricted nonlinearity** $nl_k(f)$: WT restricted to $E_{n,k}$

| $\{0,1\}^4$ | $f(x)$ | $k$ | $E_{4,k}$ | $f_{(k)}$ |
|---|---|---|---|---|
| (0,0,0,0) | 0 | 0 | (0,0,0,0) | 0 |
| (0,0,0,1) | 1 | 1 | (0,0,0,1) | 1 |
| (0,0,1,0) | 0 | | (0,0,1,0) | 0 |
| (0,0,1,1) | 1 | | (0,1,0,0) | 0 |
| (0,1,0,0) | 0 | | (1,0,0,0) | 1 |
| (0,1,0,1) | 0 | 2 | (0,0,1,1) | 1 |
| (0,1,1,0) | 1 | | (0,1,0,1) | 0 |
| (0,1,1,1) | 0 | | (0,1,1,0) | 1 |
| (1,0,0,0) | 1 | | (1,0,0,1) | 0 |
| (1,0,0,1) | 0 | | (1,0,1,0) | 1 |
| (1,0,1,0) | 1 | | (1,1,0,0) | 0 |
| (1,0,1,1) | 0 | 3 | (0,1,1,1) | 1 |
| (1,1,0,0) | 1 | | (1,0,1,1) | 0 |
| (1,1,0,1) | 1 | | (1,1,0,1) | 0 |
| (1,1,1,0) | 1 | | (1,1,1,0) | 1 |
| (1,1,1,1) | 1 | 4 | (1,1,1,1) | 1 |

# Constructions of WPB Functions

Search space sizes for various $n = 2^k$:

| | Generic | Balanced | WPB |
|---|---|---|---|
| $n$ | $\#\mathcal{F}_n = 2^{2^n}$ | $\#\mathcal{B}_n = \binom{2^n}{2^{n-1}}$ | $\#\mathcal{W}_n = \prod_{k=1}^{n-1} \binom{\binom{n}{k}}{\frac{1}{2}\cdot\binom{n}{k}}$ |
| 2 | 16 | 6 | 2 |
| 4 | 65536 | 12870 | 720 |
| 8 | $1.16 \cdot 10^{77}$ | $5.77 \cdot 10^{76}$ | $5.28 \cdot 10^{70}$ |
| 16 | $2.01 \cdot 10^{19729}$ | $6.24 \cdot 10^{19727}$ | $1.84 \cdot 10^{19704}$ |

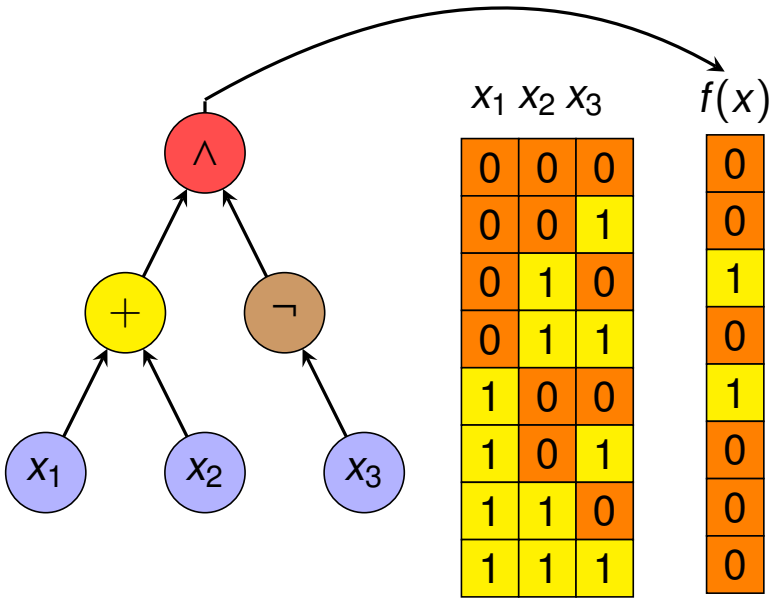
- $\Rightarrow$ too huge for exhaustive search when $n > 4$!
- **Goal**: use GA and GP to construct WPB functions with high restricted nonlinearity

# Solutions Encoding

- classic GA: **Truth table encoding** [M97, M98]:

$$C = (c_0, \cdots, c_{2^n-1}) \in \{0,1\}^{2^n}$$

- GP: **tree encoding of TT** [P16, M18, M19]

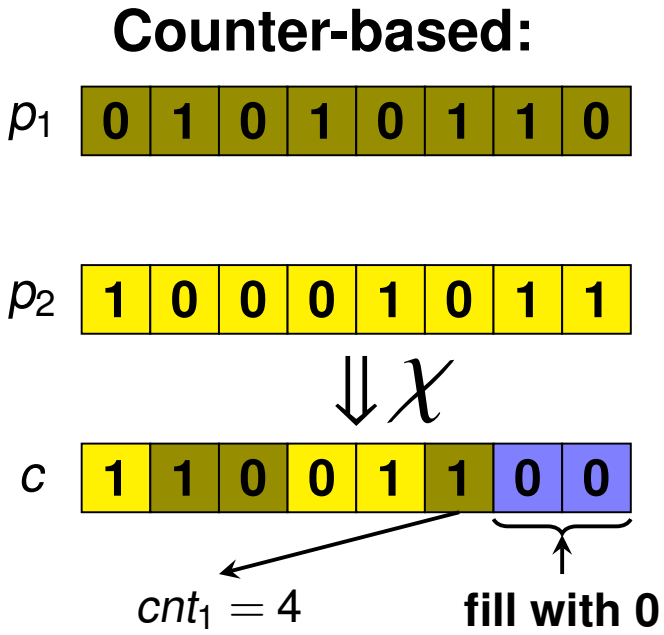


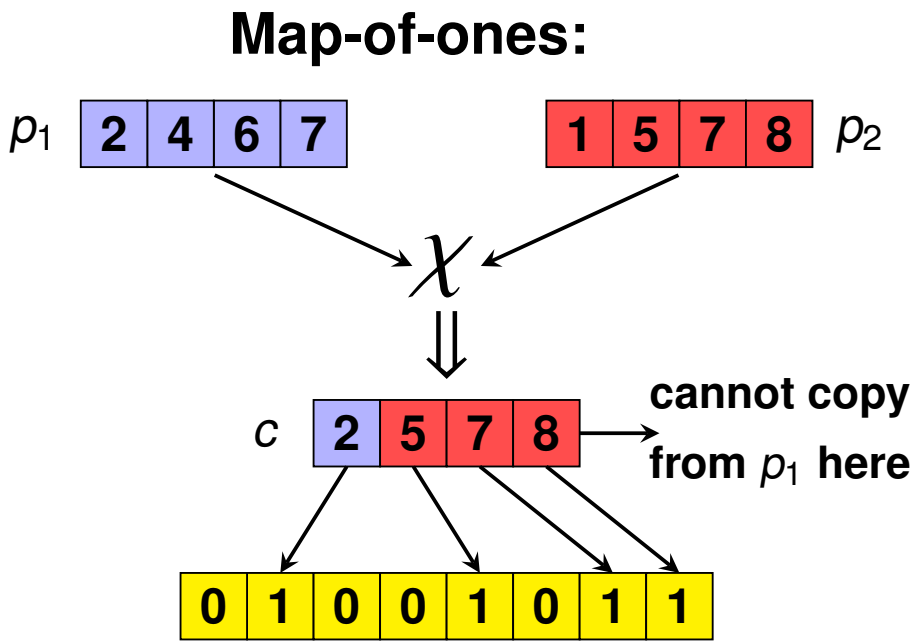

- Balanced GA: **balanced encoding** [M15, M20, M21]:

$$C = \left\{ c_{n,k} \in \{0,1\}^{\binom{n}{k}} : \ 1 \leq k \leq n-1, \ w_H(c_{n,k}) = \frac{1}{2}\binom{n}{k} \right\}$$

# Crossover Operators

- **Classic GA and GP**: one-point and subtree crossover
- **Balanced GA**: counter-based and map-of-ones crossovers applied weightwise [M20]



# Fitness Functions

- **Penalty**: deviation from balancedness for each weight $k$

$$pen(f) = \sum_{k=1}^{n-1} unb_k(f), \text{ where } unb_k(f) = \left| \frac{\#E_{n,k}}{2} - w_H(f_{(k)}) \right|$$

- **Fitness 1:** Maximize *sum* of nonlinearities

$$fit_1(f) = \delta_{pen} \cdot \left( \sum_{k=2}^{n/2} nl_k(f) \right) - pen(f)$$

- **Fitness 2:** Maximize *minimum* nonlinearity

$$fit_2(f) = \delta_{pen} \cdot \left( \min_{2 \le k \le n/2} \{nl_k(f)\} \right) - pen(f)$$

where $\delta_{pen} = 1$ if $pen(f) = 0$ and 0 otherwise

# Experimental Settings

**Common Parameters:**

- Instance: $n = 8$
- Fitness Evals.: 500 000
- Breeding: Steady-state

**GP-related parameters:**

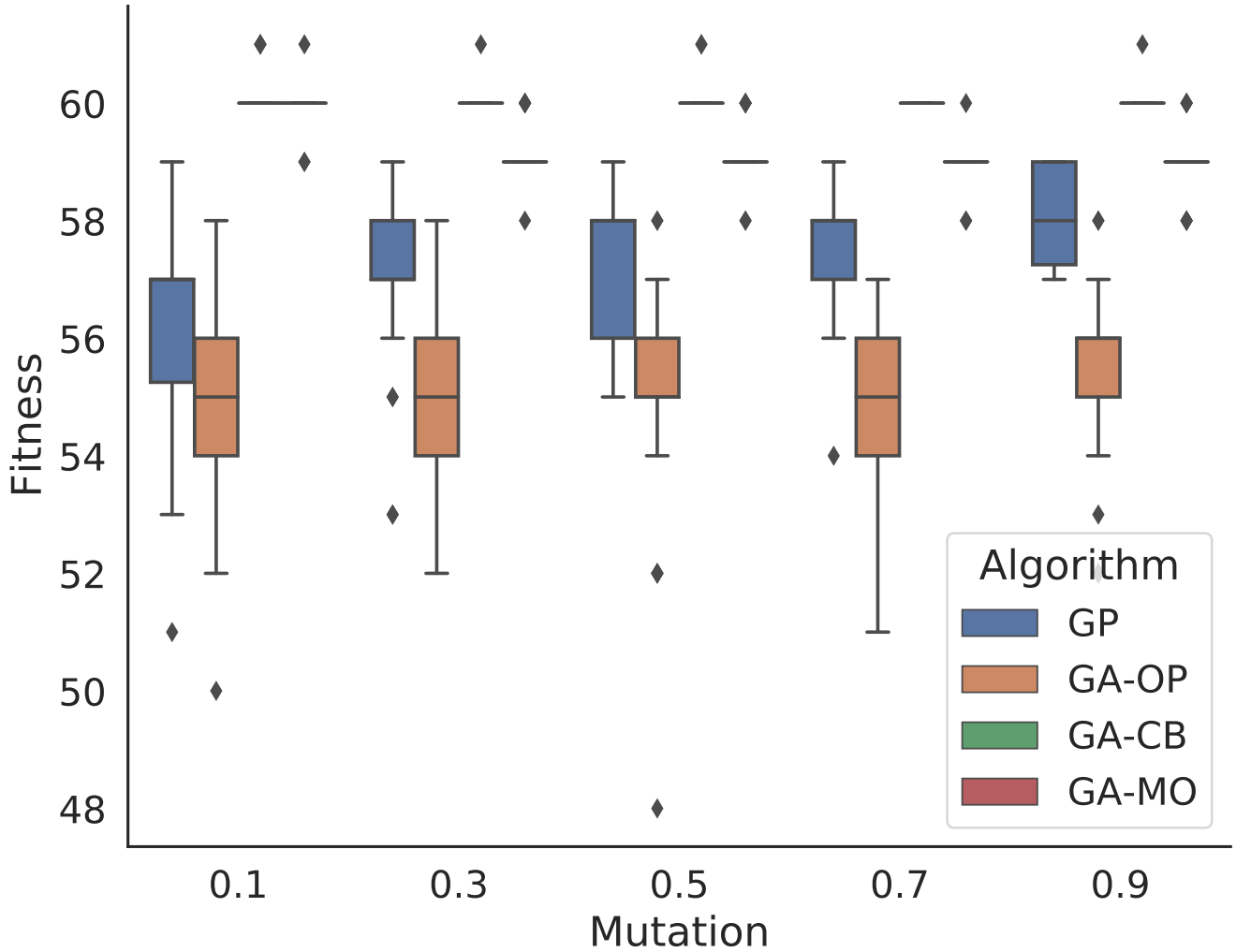
- Population size: 1000
- Max tree depth: 5
- Tournament size: 3
- Mutation rates: 0.1 – 0.9
- Independent Runs: 30

**GA-related parameters:**

- Population size: 200

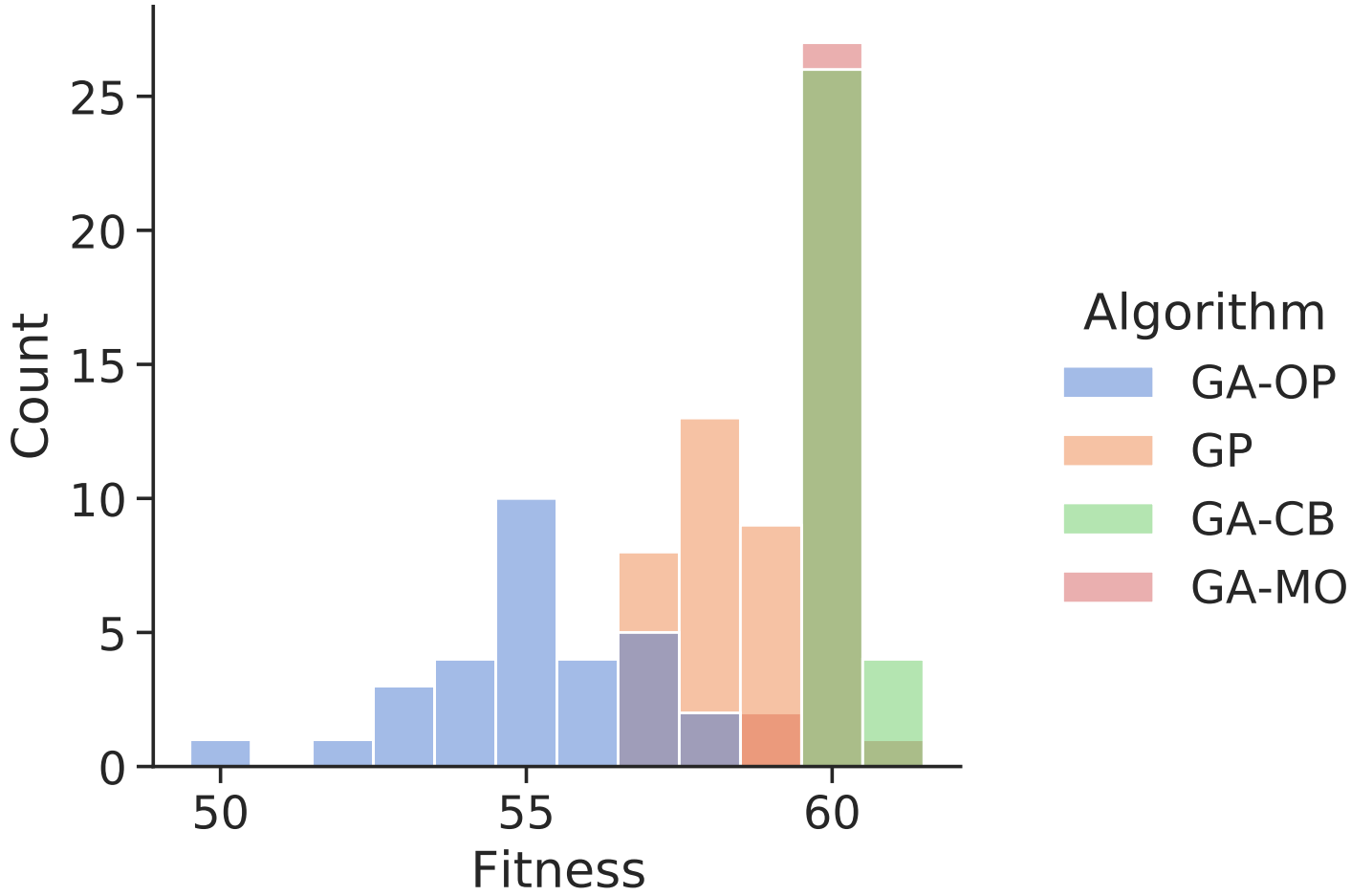
# Results (1/2)

**Main Finding**: Balanced GA fares better than classical GA and GP



# Results (2/2)

**Main Finding**: No significant difference between counter-based and map-of-ones crossovers



# Conclusions and Future Works

**Summing up:**

- We applied GA and GP to evolve WPB functions with high restricted nonlinearities
- Curiously, balanced GA performs better than GP (while in previous works on global balancedness it is not the case)

**Future work:**

- Perform Fitness Landscape Analysis to investigate the gap between balanced GA and classic GA/GP [J21]
- Scale to higher number of variables (fitness calculation becomes the bottleneck)

# References


[C21] Carlet, C.: Boolean functions for cryptography and coding theory. Cambridge University Press (2021)

[J21] Jakobovic, D., Picek, S., Martins, M.S.R., Wagner, M.: Toward more efficient heuristic construction of boolean functions. Appl. Soft Comput., 107: 107327 (2021)

[M21] Manzoni, L., Mariot, L., Tuba, E.: Tip the balance: Improving exploration of balanced crossover operators by adaptive bias. In: Proceedings of CANDAR (Workshops) 2021, pp. 234–240 (2021)

[M20] Manzoni, L., Mariot, L., Tuba, E.: Balanced crossover operators in Genetic Algorithms. Swarm Evol. Comput. 54: 100646 (2020)

[M19] Mariot, L., Picek, S., Leporati, A., Jakobovic, D.: Cellular automata based S-boxes. Cryptogr. Commun. 11(1):41–62 (2019)

[M18] Mariot, L., Picek, S., Jakobovic, D., Leporati, A.: Evolutionary Search of Binary Orthogonal Arrays. In: Auger, A., Fonseca, C.M., Lourenço, N., Machado, P., Paquete, L., Whitley, D. (eds.): PPSN 2018 (I). LNCS vol. 11101, pp. 121–133. Springer (2018)

[M15] Mariot, L., Leporati, A.: A Genetic Algorithm for Evolving Plateaued Cryptographic Boolean Functions. In: Proceedings of *TPNC 2015*: 33–45 (2015)

[Me19] Mesnager, S., Zhou, Z., Ding, C.: On the nonlinearity of boolean functions with restricted input. Cryptogr. Commun. 11(1) pp. 63–76 (2019)

[M98] Millan, W., Clark, J., Dawson, E.: Heuristic Design of Cryptographically Strong Balanced Boolean Functions. Proceedings of EUROCRYPT 1998, pp. 489–499 (1998)

[M97] Millan, W., Clark, A.J., Dawson, E.: An effective genetic algorithm for finding highly nonlinear boolean functions. In: Proceedings of ICICS'97, pp. 149–158 (1997)

[P16] Picek, S., Jakobovic, D., Miller, J.F., Batina, L., Cupic, M.: Cryptographic Boolean functions: One output, many design criteria. Appl. Soft Comput. 40: 635–653 (2016)