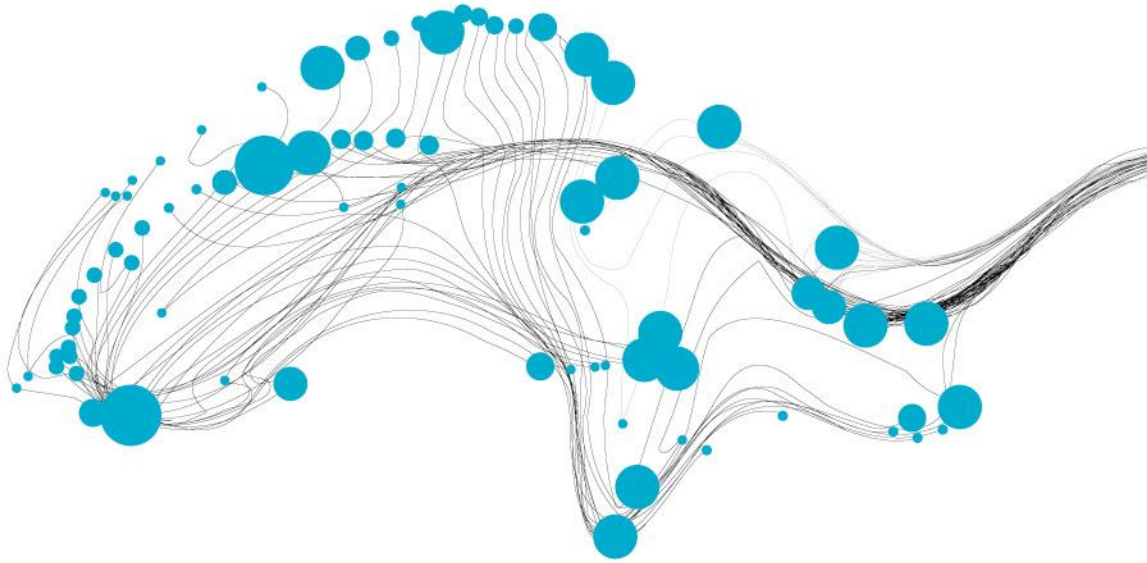
ON COUNTS AND DENSITIES OF HOMOGENEOUS BENT FUNCTIONS: AN EA APPROACH

CLAUDE CARLET, MARKO ĐURASEVIĆ, DOMAGOJ JAKOBOVIC, LUCA MARIOT, STJEPAN PICEK, ALEXANDR POLUJAN



EVOAPPS 2026

TOULOUSE, 8 APRIL 2026

UNIVERSITY OF TWENTE.
Radboud University
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

BOOLEAN FUNCTIONS FOR CRYPTO

- A mapping $f : \{0,1\}^n \to \{0,1\}$ represented by a *truth table*

(x_1, x_2, x_3)	000	001	010	011	100	101	110	111
$f(x_1, x_2, x_3)$	0	1	1	0	1	0	1	1

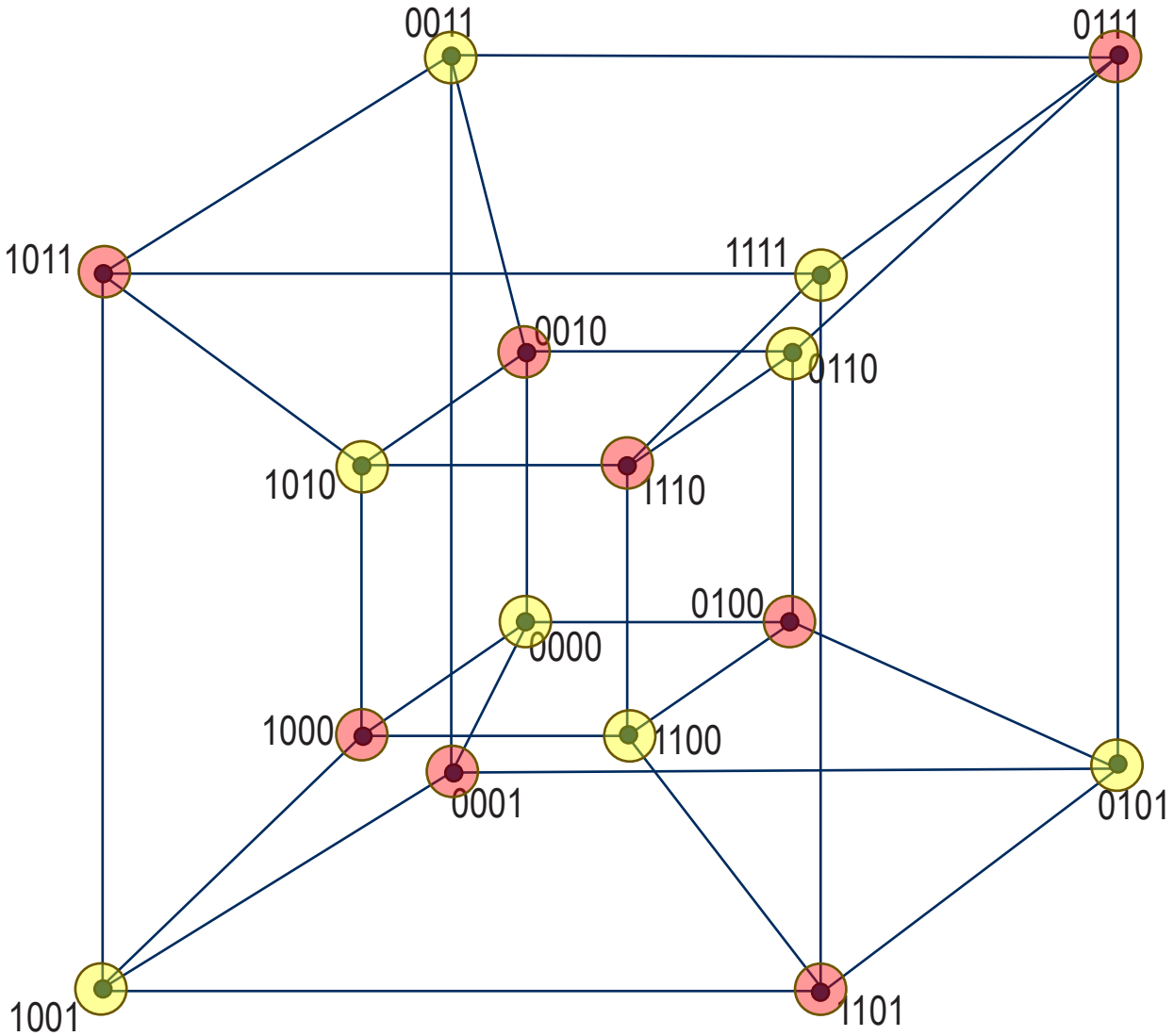
- In cryptography, f must satisfy some properties to resist specific attacks [2]:
  - High **Nonlinearity**: high Hamming distance from **linear** functions:

$$L_a(x) = a \cdot x = a_1 x_1 \oplus \ldots \oplus a_n x_n, \quad a_i, x_i \in \{0,1\}$$

  - High **Algebraic Degree** in the **Algebraic Normal Form (ANF)** of f:

$$f(x) = x_1 + x_2 + x_3 + x1x2 + x_1 x_2 x_3, \Rightarrow deg(f) = 3$$

NONLINEARITY – GEOMETRIC INTUITION



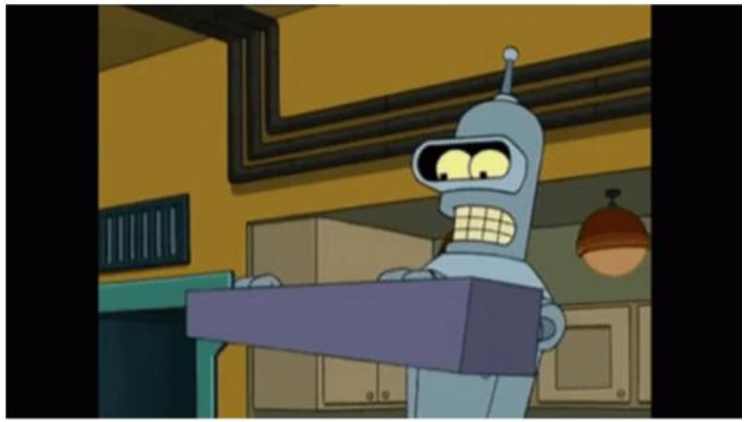
- **Example**: $n = 2$ variables (truth tables of $2^2 = 4$ bits, 16 functions in total)
- Linear functions and complements:

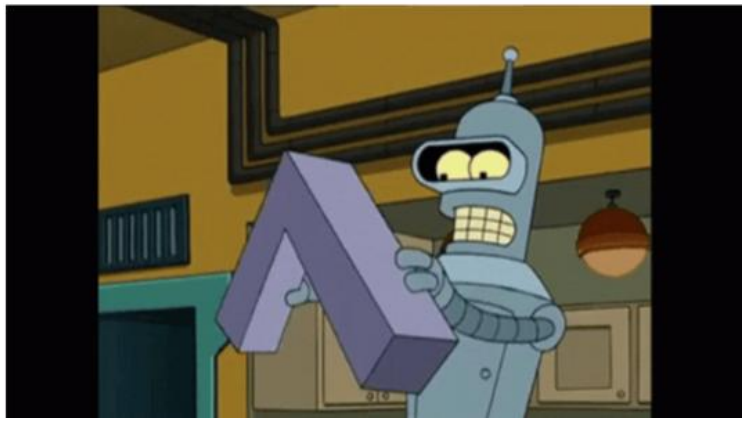
$a_1x_1 \oplus a_2x_2$	TT	TT $\oplus 1$
0	0000	1111
x_1	0011	1100
x_2	0101	1010
$x_1 \oplus x_2$	0110	1001

- **Walsh transform** to compute $nl(f)$:

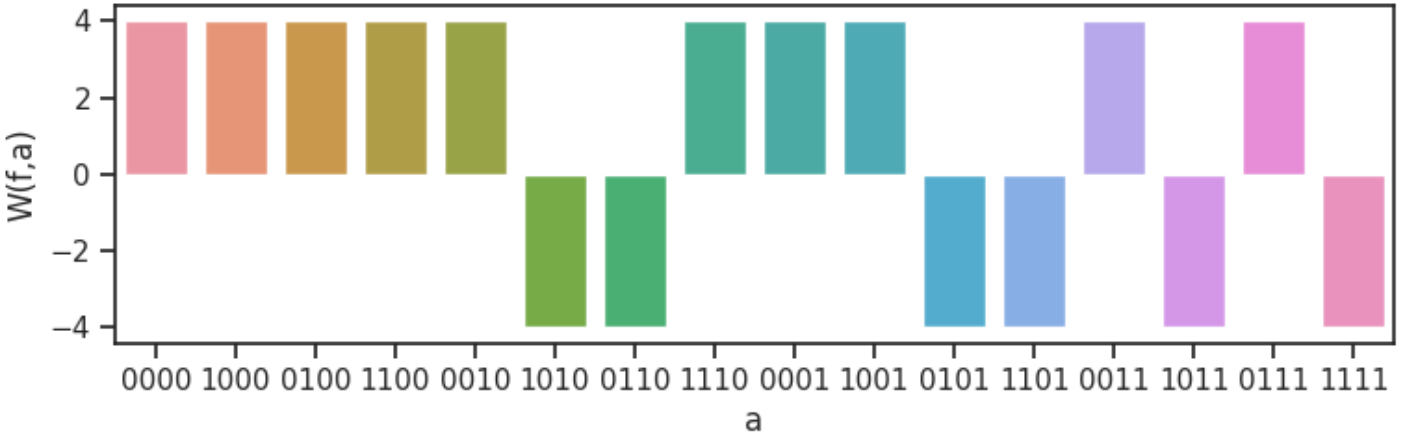
$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus a \cdot x}$$

BENT FUNCTIONS



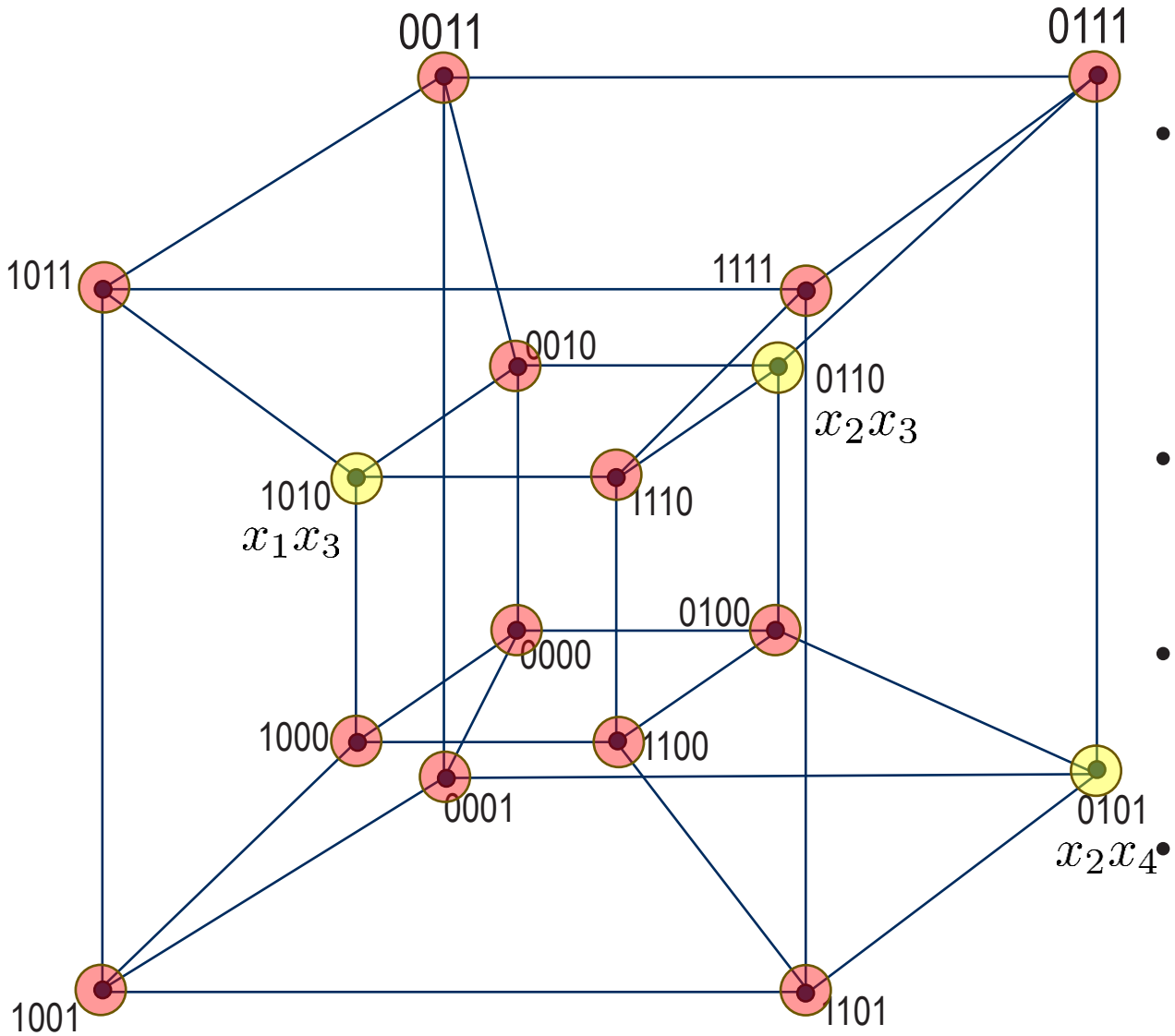


- Only two spectral values: $W_f(a) \in \{-2^{\frac{n}{2}}, +2^{\frac{n}{2}}\}$
- **PRO**: highest possible nonlinearity $nl_f = 2^{n-1} - 2^{\frac{n}{2}-1}$
- **CONS**: unbalanced, exist only for n even [2]



Example with $n = 4$ variables

HOMOGENEOUS BENT FUNCTIONS – THE PROBLEM



- For efficiency, one wants a **homogeneous** ANF (all monomials with same degree)

$$f(x) = x_1x_3 + x_2x_3 + x_2x_4$$
$$\Rightarrow deg(f) = 2,\ nl(f) = 6$$

- **Quadratic homogeneous bent functions:** well-characterized mathematically [5]
- **Cubic homogeneous bent functions:** only one known algebraic construction [12]
- **Optimization goal:** use EA to evolve bent homogeneous functions [3, 7]

UNIVERSITY OF TWENTE.

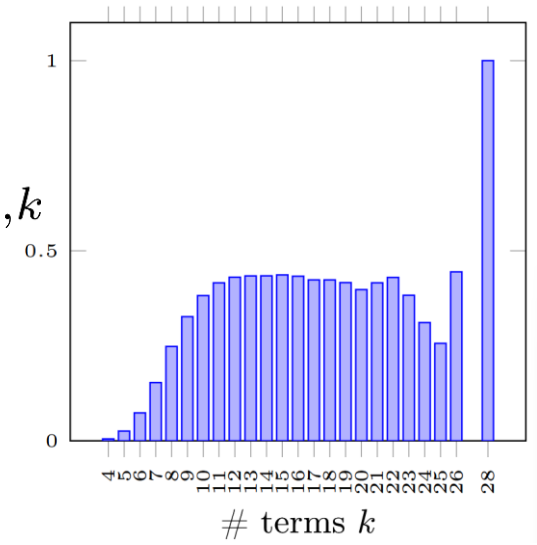
SEARCH SPACE EMPIRICAL ANALYSIS

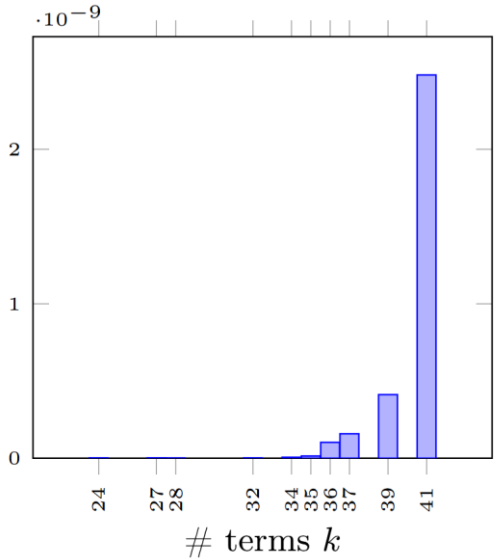
- **Idea:** investigate the empirical *density* of homogeneous bent Boolean functions

$$\Rightarrow \quad \delta_{n,d,k} = \frac{|\mathcal{HB}_{n,d,k}|}{\binom{\binom{n}{d}}{k}} \Longrightarrow$$

Ratio of homogeneous bent functions in n variables, degree d and k monomials against all homogeneous functions

$\delta_{8,2,k}$



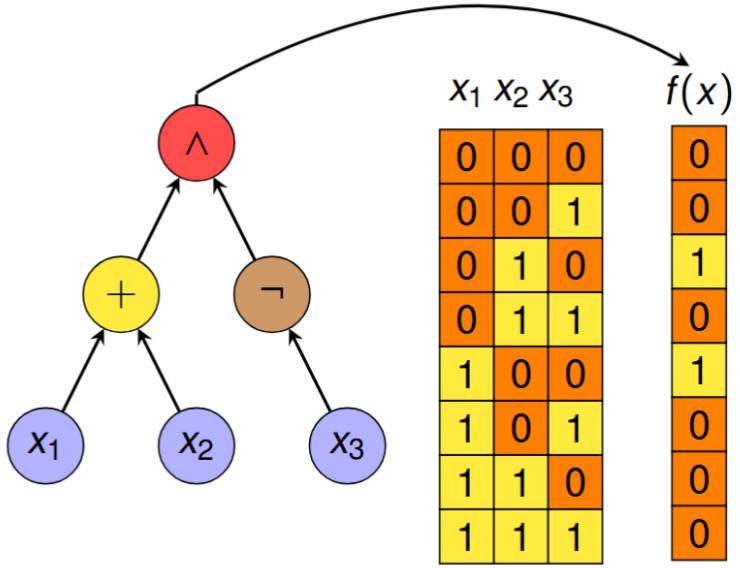


$\delta_{8,3,k}$

- **Main finding:** cubic homogeneous bent functions are much rarer than quadratic ones! ⇒ Use this to *inform* the design of the EA later

UNIVERSITY OF TWENTE.

SOLUTIONS ENCODING - GP



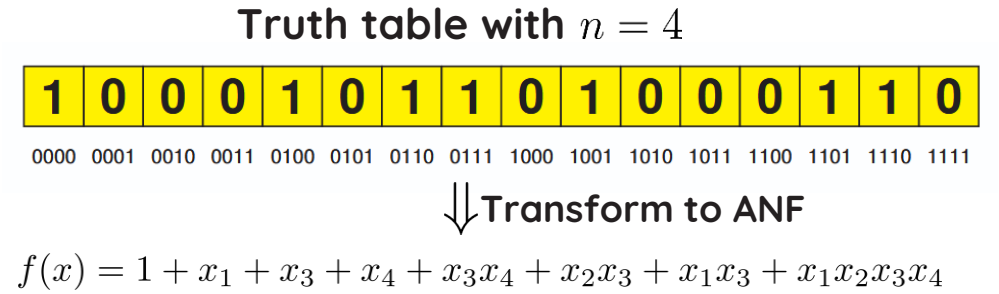
$$f(x) = x_1 \oplus x_2 \oplus x_1x_3 \oplus x_2x_3$$

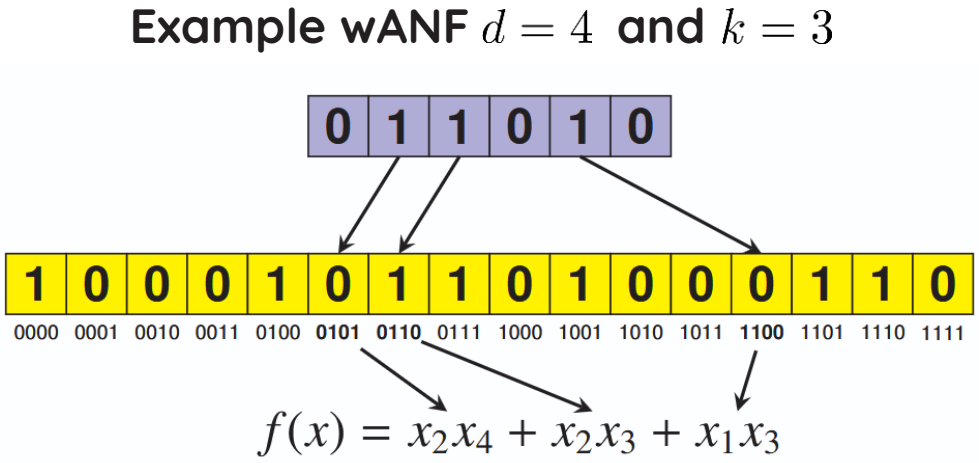
$$\Downarrow$$

$$f(x) = x_1x_3 \oplus x_2x_3$$

- **GP Genotype**: a syntactic tree
  - Leaf nodes: input variables
  - Internal nodes: operators (e.g. AND, OR, NOT, XOR, …)
- **Phenotype:** evaluate the tree to get the truth table, then convert it in ANF and *correct* the expression for homogeneity
- Classic GP operators (subtree crossover and mutation, …) [4, 11]

SOLUTIONS ENCODING - GA





- **Truth table**: fixed-length 2^n-bit strings [11]
- **Reduced ANF (rANF):** bitstring of $\binom{n}{d}$ bits, specifying the ANF monomials of degree d
- **Weighted ANF (wANF):** as reduced ANF, but we set the number k of d- degree monomials
- **GA operators:** classic and balanced crossover and mutation operators [6, 9]

FITNESS FUNCTIONS / EXPERIMENTAL SETTINGS

- **Fitness 1:** maximize nonlinearity and minimize the number of occurrences of the maximum Walsh absolute value [8]:

$$fit_{bent} = nl_f + \frac{2^n - \#max\_values}{2^n}$$

- **Fitness 2:** two-stage fitness optimizing first the requested number of monomials k in the ANF, then Fitness 1:

$$fit_{bent,k} = \begin{cases} -|num\_monomials - k|, \text{ if } num\_monomials \neq k; \\ nl_f + \frac{2^n - \#max\_values}{2^n}, \text{ otherwise.} \end{cases}$$

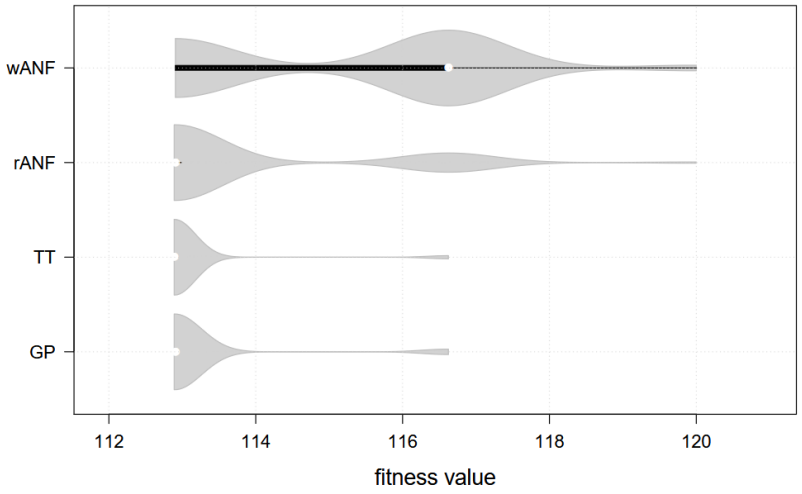
- **Common parameters:** 3-tournament steady-state EA, population size 500, mutation probability 0.5, fitness budget 10^6 evaluations, 30 independent runs

RESULTS – SUCCESS RATES

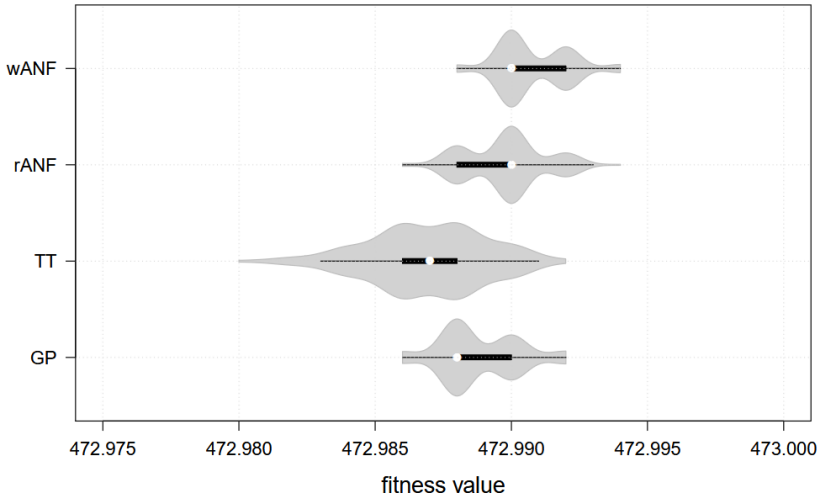
n	weight	GP	TT	rANF	wANF	rANF/LS	wANF/LS
6	unrestricted	21	30	30	–		
	16	24	30	30	30		
8	unrestricted	0	0	0	–	0	–
	24	0	0	0	0	0	0
	27	0	0	0	0	0	0
	28	0	0	0	0	0	0
	32	0	0	0	0	0	0
	34	0	0	0	0	0	0
	35	0	0	0	0	0	0
	36	0	0	0	0	0	0
	37	0	0	0	1	0	1
	39	0	0	1	4	0	2
	41	0	0	1	4	0	2

- Quadratic functions are easy to evolve: EA always converged from $6 < n < 12$
- Cubic ones, are much harder to evolve
- wANF encoding managed to evolve some cubic functions for $n = 8$
- Improvement on previous results [1]

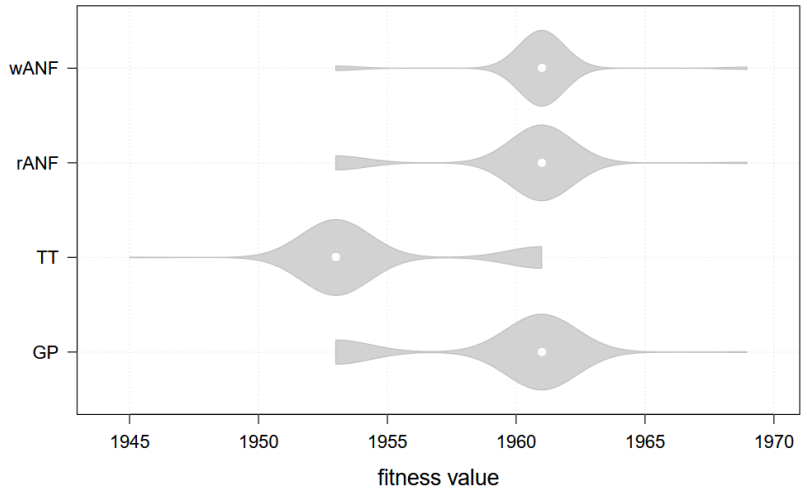
RESULTS – CUMULATIVE FITNESS



(a) 8 variables



(b) 10 variables

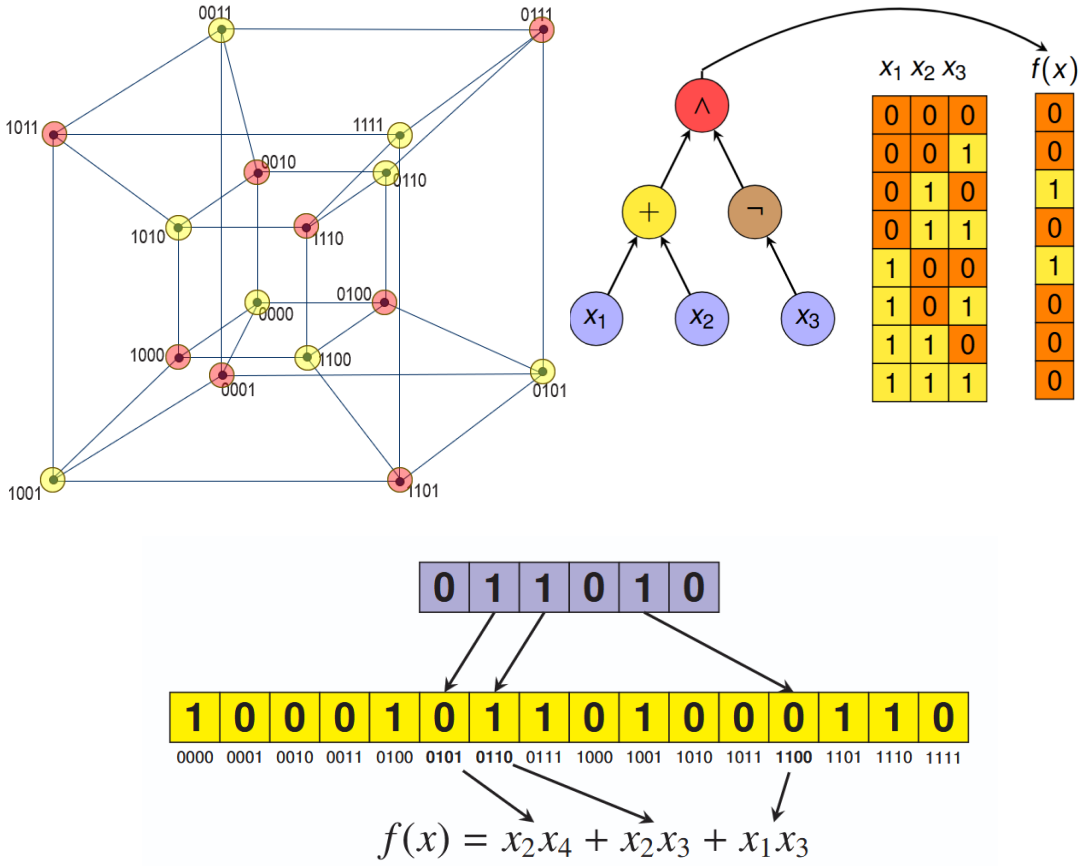


(c) 12 variables

- **Main finding**: TT is the worst encoding, followed by GP tree. Differences among encodings tend to decrease as n grows

CONCLUSIONS

- GP is the worst performing EA (contrary to other similar problems [8, 10, 11])
- We evolved cubic homogeneous bent functions, improving upon previous work [1]
- **Crucially:** this improvement is due to the rANF and wANF encodings, influenced by our density analysis results
- The improvement is more evident when restricting the number of monomials k



UNIVERSITY OF TWENTE.

REFERENCES

1. C. Carlet, M. Durasevic, D. Jakobovic, L. Mariot, S. Picek, S: Degree is important: On evolving homogeneous Boolean functions. Proc. of GECCO ’25 Companion, pp. 795–798 (2025)
2. C. Carlet: Boolean functions for cryptography and coding theory. Cambridge University Press (2021)
3. M. Djurasevic, D. Jakobovic, L. Mariot, S. Picek: A survey of metaheuristic algorithms for the design of cryptographic Boolean functions. Cryptogr. Commun. 15(6): 1171-1197 (2023)
4. J.R. Koza: Genetic programming: A paradigm for genetically breeding populations of computer programs to solve problems (Vol. 34). Stanford, CA: Stanford University, Department of Computer Science (1990)
5. F.J. MacWilliams, N.J.A Sloane: The Theory of Error-Correcting Codes. Elsevier, Amsterdam, North Holland (1977)
6. L. Manzoni, L. Mariot, E. Tuba: Balanced crossover operators in Genetic Algorithms. Swarm Evol. Comput. 54: 100646 (2020)
7. L. Mariot, D. Jakobovic, T. Bäck, J.C. Hernandez-Castro: Artificial Intelligence for the Design of Symmetric Cryptographic Primitives. Security and Artificial Intelligence, pp. 3-24 (2022)
8. L. Mariot, D. Jakobovic, A. Leporati, S. Picek: Hyper-bent Boolean Functions and Evolutionary Algorithms. Proc. of EuroGP 2019, pp. 262-277 (2019)
9. W. Millan, J. Clark, E. Dawson: Heuristic Design of Cryptographically Strong Balanced Boolean Functions. Proc. of EUROCRYPT 1998, pp. 489–499 (1998)
10. Picek, S., Knezevic, K., Mariot, L., Jakobovic, D., Leporati, A.: Evolving bent quaternary functions. Proc. of CEC 2018, pp. 1–8 (2018)
11. S. Picek, D. Jakobovic, J. F. Miller, L. Batina, M. Cupic: Cryptographic Boolean functions: One output, many design criteria. Appl. Soft Comput. 40: 635-653 (2016)
12. J. Seberry, J., T. Xia, J. Pieprzyk: Construction of cubic homogeneous Boolean bent functions. Australas. J. Comb. 22:233–246 (2000)