On the Multiplicative Complexity of Cubic Boolean Functions

Meltem Sönmez Turan and René Peralta

National Institute of Standards and Technology

Presented at BFA2021 – September 2021

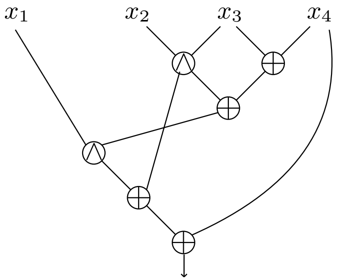
Overview

- Circuit optimization problem
- Multiplicative complexity
- Low MC circuits for cubic Boolean functions

Boolean Circuits

A *Boolean circuit* with n inputs and m outputs is a **directed acyclic graph** (DAG), where

- the inputs and the gates are *nodes*,
- the edges correspond to Boolean-valued *wires*,
- *fanin*/*fanout* of a node is the number of wires going in/out the node,
- the nodes with fanin zero are called *input nodes*
- a node with fanout zero is an *output node*



Boolean Function Complexity

Problem: Given a basis of Boolean gates, construct a circuit that computes a function that is optimal w.r.t. some criteria, such as

- Size: The number of gates in the circuit.
- Depth: The length of the longest path from an input gate to the output gate.

Almost all Boolean functions are complex.

Target metric depends on the application.

- Circuits with small number of gates use less energy and occupy smaller area, and are desired for *lightweight cryptography applications* running on constrained devices.
- Circuits with small number of AND gates are desired for *secure multi-party computation*, *zero-knowledge proofs* and *side channel protection*.
- Circuits with small AND-depth are desired for homomorphic encryption schemes.

Multiplicative Complexity (MC)

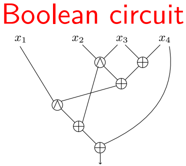
Minimum number of nonlinear gates needed to implement f by a Boolean circuit

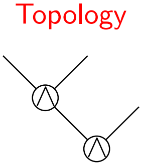
- Min. $\#$ of `AND` gates needed over the basis `(AND, XOR, NOT)`.
- Almost all $f \in B_n$ have MC at least $2^{n/2} - n - 1$ with high probability.
- No specific n-variable function had been proven to have MC larger than n.
- MC of a function with degree d is at least $d - 1$ (degree bound).
- The number of n-variable Boolean fucntions with MC k is at most $2^{k^2-k+2kn+n+1}$
- MC is affine invariant.
  - Boolean functions $f, g \in B_n$ are affine equivalent if there exists a transformation of the form $f(x) = g(Ax + a) + b \cdot x + c$, where $A \in GL(n, 2)$; $a, b \in \mathbb{F}_2^n$, and $c \in \mathbb{F}_2$.
  - The set of affine equivalent functions constitute an equivalence class denoted by $[f]$, where f is an arbitrary function from the class.
  - Affine equivalent Boolean functions have the same MC.

MC of Boolean Functions

Exhaustively construct all Boolean topologies with 1,2, 3, . . . AND gates, and evaluate the topologies until a function from $[f]$ is generated.

- Topology: Abstraction of a Boolean circuit that shows the relations between AND gates



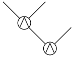


Constructing Topologies [CTP18]

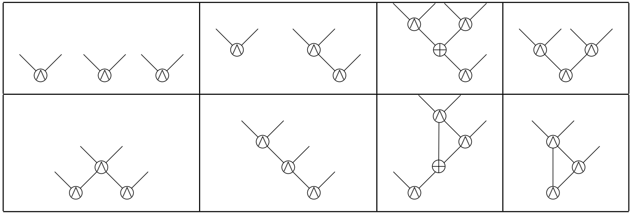
Topologies with 1 AND gate

Topologies with 2 AND gates

and



Topologies with 3 AND gates



Number of topologies with 4 AND gates is 84.

Finding the MC of Boolean functions

Different ways of determining the MC of a Boolean function

- Show that it is affine equivalent to a function whose MC is known.
- Find a circuit that satisfies a lower bound (degree bound).
- Iteratively construct all circuits with increasing #ANDs until the function is generated.

Solved up to 6-variables

- $C_\wedge(f) \leq n-1$ for $f \in B_n, n \leq 5$ (Turan, Peralta, 2014)
- $C_\wedge(f) \leq 6$ for $f \in B_6$ (Çalık et al., 2018)

Known methods are infeasible for $n > 6$, due to the large number of affine equivalence classes and Boolean circuits.

Boolean functions with MC 1 and 2

Boolean functions with MC 1 [FP02]

- Functions with MC 1 are affine equivalent to x_1x_2.
- The number of n-variable Boolean functions with MC 1 is $2\binom{2^n}{3}$.

Boolean functions with MC 2 [FTT17]

- Functions with MC 2 are affine equivalent to one of the functions from the set $\{x_1x_2x_3,\ x_1x_2x_3 + x_1x_4,\ x_1x_2 + x_3x_4\}$.
- The number of n-variable Boolean functions with MC 2 is

$$2^n(2^n-1)(2^n-2)(2^n-4)\left(\frac{2}{21}+\frac{2^n-8}{12}+\frac{2^n-8}{360}\right).$$

MC of Quadratic Boolean Functions

- The equivalance classes for n-bit quadratic Boolean functions are
  - x_1x_2 (with MC 1)
  - $x_1x_2 + x_3x_4$(with MC 2)
  - $x_1x_2 + x_3x_4 + x_5x_6$ (with MC 3)
  - $\ldots$
  - $x_1x_2 + x_3x_4 + \ldots + x_{n-1}x_n$ (even n) (with MC $\lfloor \frac{n}{2} \rfloor$)
  - $x_1x_2 + x_3x_4 + \ldots + x_{n-2}x_{n-1}$ (odd n) (with MC $\lfloor \frac{n}{2} \rfloor$)

- MC of a quadratic Boolean function is at most $\lfloor \frac{n}{2} \rfloor$.

Dimension of a Boolean function

The following functions are all affine equivalent and have MC=1:

$$x_1x_2$$
$$x_1 + x_2x_3$$
$$(x_1 + x_2)(x_3 + x_4) = x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4$$

It is easier to work on smaller number of variables.

Definition. Let L_f be the number of input variables that appear in the *algebraic normal form* (ANF) of a Boolean function f. The dimension of f is the smallest number of variables that appear in the ANF among the functions that are affine equivalent to f:

$$dim(f) = \min_{g \in [f]} L_g.$$

Example. $dim(x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4) = dim(x_1x_2) = 2$

A New MC Lower Bound based on Dimension

Theorem

For $f \in B_n$, $C_\wedge(f) \geq \lceil \mathrm{dim}(f)/2 \rceil$.

Sketch of the proof.

1. Let $C_\wedge(f) = k$, consider a circuit implementing f with k AND gates.
2. The topology with k AND gates has $2k$ linear function inputs.
3. The rank of $2k$ linear functions can be at most $2k$.
4. Any set of $2k$ linear functions on $n > 2k$ variables can be affine transformed to functions having at most $2k$ variables.
5. Therefore, $dim(f) \leq 2k$, which implies $C_\wedge(f) \geq \lceil dim(f)/2 \rceil$.

Example. Let $f = \Sigma_4^8 = x_1x_2x_3x_4 + \ldots + x_5x_6x_7x_8$. According to the degree bound, $C_\wedge(f) \geq 3$. By dimension bound, $C_\wedge(f) \geq 8/2 = 4$.

Multiplicative Complexity of Cubic Boolean Functions

The following results follow from earlier studies [CTP19, CTP18, TP14, FTT17]

- Let $f \in B_n$ be a Boolean function with MC 2. Then f is affine equivalent to exactly one of the following two functions: $x_1x_2x_3$ and $x_1x_2x_3 + x_1x_4$.
- Let f be an n-variable cubic Boolean function with dimension 5 and MC 3. Then f is affine equivalent to exactly one of the following four functions $x_1x_3x_4 + x_1x_2x_5$, $x_1x_2x_3 + x_4x_5$, $x_3x_4 + x_1x_3x_4 + x_1x_2x_5$ and $x_1x_2x_3 + x_2x_4 + x_1x_5$.
- Let f be an n-variable cubic Boolean function with dimension 6 and MC 3. Then f is affine equivalent to exactly one of the following three functions $x_3x_4 + x_1x_3x_4 + x_1x_2x_5 + x_1x_6$, $x_1x_3x_4 + x_1x_2x_5 + x_1x_6$ and $x_1x_2x_3 + x_4x_5 + x_1x_6$.

Construction Circuits for Cubic Boolean Functions

1. Decompose n-bit cubic Boolean function f such that

$$f = x_n f_1 + f_2$$

   where f_1 is a quadratic function defined on $(x_1, \ldots, x_{n-1})$ and f_2 is a function of degree at most three defined on $(x_1, \ldots, x_{n-1})$.
2. Optimally implement f_1 (with at most $\lfloor \frac{n-1}{2} \rfloor$ `AND` gates).
3. If f_2 is cubic, apply this method recursively. If not cubic, optimally implement f_2 (with at most $\lfloor \frac{n-1}{2} \rfloor$ `AND` gates)
4. Given the implementations of f_1 and f_2, implement f using one additional `AND` gate.

Upper bounds on the MC of Cubic Boolean Functions

The method provides an upper bound on the MC of n-variable cubic Boolean functions, denoted $\text{MaxMC}(B_n^c)$, using the following relation

$$\text{MaxMC}(B_n^c) \leq \text{MaxMC}(B_{n-1}^c) + \lfloor \frac{n-1}{2} \rfloor + 1. \tag{1}$$

We experimentally showed that MC of cubic Boolean function for $n = 7$ is at most 8.

$$\text{MaxMC}(B_n^c) \leq \frac{1}{2}(\lfloor \frac{n-1}{2} \rfloor^2 + \lfloor \frac{n-1}{2} \rfloor + (\lfloor \frac{n}{2} \rfloor - 1)\lfloor \frac{n}{2} \rfloor + 2(n-8)). \tag{2}$$

Upper bounds

Table: Upper bounds on the MC of n-variable Boolean functions

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Cubic functions	-	2	2	4	5	8	12	16	20	25	30	36	41	48	54
All functions	1	2	3	4	6	13	26	41	57	88	120	183	247	374	502

Upper bounds

The $\#$ of functions in B_n with MC $\leq k$ is bounded above by $2^{k^2+2kn+n+2}$.
$|B_n^c| = (2^{\binom{n}{3}} - 1)2^{\binom{n}{2}+n+1}$.
Let $\tau = \text{MaxMC}(B_n^c)$, we have

$$\begin{aligned}(2^{\binom{n}{3}} - 1)2^{\binom{n}{2}+n+1} &\leq 2^{\tau^2+2\tau n+n+2} \\ \binom{n}{3} + \binom{n}{2} + n &\leq \tau^2 + 2\tau n + n + 2 \\ n^3 - n &\leq 6\tau^2 + 12\tau n + 12\end{aligned}$$

$$\frac{\sqrt{6}}{6}(n^3 + 6n^2 - n - 12)^{\frac{1}{2}} - n \leq \tau, \tag{3}$$

which shows that $\text{MaxMC}(B_n^c)$ is $\Omega(n^{3/2})$. Thus

$$\Omega(n^{3/2}) \leq \text{MaxMC}(B_n^c) \leq O(n^2). \tag{4}$$

Closing this gap is an interesting open problem.

Conclusion

- Studied the MC of cubic Boolean functions
- Enumerated the exhaustive list of equivalence functions with MC ≤ 4.
- Presented a method to implement cubic Boolean functions that decomposes the function into an expression of functions defined on smaller number of variables.
- Provided an upper bounds on the MC of cubic Boolean functions, significantly better than the upper bounds for random Boolean functions.

More Information

- **NIST Circuit Complexity Project Webpage:**
  https://csrc.nist.gov/Projects/Circuit-Complexity
- **GitHubLink:**
  https://github.com/usnistgov/Circuits/
- **Contact email:**
  circuit_complexity@nist.gov

References

BPP00 J. Boyar, R. Peralta, and D. Pochuev, "On the multiplicative complexity of Boolean functions over the basis $(\wedge, \oplus, 1)$, Theoretical Computer Science, vol. 235, no. 1, pp. 43 – 57, 2000.

CTP18 Ç. Çalık, M. Sönmez Turan, R. Peralta, The Multiplicative Complexity of 6-variable Boolean Functions, Cryptography and Communications 2018.

FP02 M. J. Fischer and R. Peralta. Counting Predicates of Conjunctive Complexity One. Yale Technical Report 1222, February 2002.

FTT17 M. G. Find, D. Smith-Tone, M. Sönmez Turan, The Number of Boolean Functions with Multiplicative Complexity 2, International Journal of Information and Coding Theory, 2017.

Lai94 X. Lai, Additive and Linear Structures of Cryptographic Functions, FSE 1994, LNCS 1008, Springer-Verlag, pp. 75–85, 1994.

TP14 M. Sönmez Turan and R. Peralta. The Multiplicative Complexity of Boolean functions on Four and Five Variables. LightSec 2014, Turkey.

CTP19 Ç. Çalık, M. Sönmez Turan, R. Peralta, Boolean Functions with Multiplicative Complexity 3 and 4, Cryptography and Communications 2019.