On the Multiplicative Complexity of Symmetric Boolean Functions

Luís Brandão, Çağdaş Çalık, Meltem Sönmez Turan, René Peralta

National Institute of Standards and Technology, Gaithersburg, MD, USA
{luis.brandao, cagdas.calik, meltem.turan, rene.peralta}@nist.gov

Abstract. The multiplicative complexity $C_\wedge(f)$ of a Boolean function f is the number of AND gates that are necessary and sufficient to implement f over the basis {XOR, AND, NOT}. We provide results related to the multiplicative complexity of Boolean functions with twin variables, where variables x_1 and x_2 are called twins in a function $f(x_1, \ldots, x_n)$ if f can be written as $x_1 x_2 f_1(x_3, \ldots, x_n) + f_2(x_3, \ldots, x_n)$, with f_1 not being the zero function. We show that any nonlinear symmetric Boolean function is affine equivalent to a Boolean function with twin variables. Using the bound $C_\wedge(f) \leq 1 + C_\wedge(x_1 f_1 + f_2)$, we obtain new upper bounds on the multiplicative complexity of symmetric Boolean functions up to 9 variables and answer two open questions posed in [1] about the multiplicative complexity of 8-variable symmetric Boolean functions: the elementary symmetric function Σ^8_4 and the counting function E^8_4 both have multiplicative complexity 6.

Keywords: Symmetric Boolean functions, Multiplicative complexity, Affine equivalence.

References

1. Joan Boyar and Ren Peralta. Tight bounds for the multiplicative complexity of symmetric functions. *Theoretical Computer Science*, 396(1):223 – 246, 2008.