On The Multiplicative Complexity of Boolean Functions over the Basis $(\wedge, \oplus, 1)$

Joan Boyar (joan@imada.ou.dk) ⋆[1] René Peralta (peralta@cs.uwm.edu) ⋆⋆[2]
Denis Pochuev (denis@cs.uwm.edu) ⋆⋆[2]

[1] Department of Mathematics and Computer Science
Odense University, Denmark

[2] Center for Cryptography, Computer, and Network Security
Computer Science Department
University of Wisconsin-Milwaukee

Abstract. The multiplicative complexity $c_\wedge(f)$ of a Boolean function f is the minimum number of AND gates in a circuit representing f which employs only AND, XOR and NOT gates. A constructive upper bound, $c_\wedge(f) = 2^{\frac{n}{2}+1} - n/2 - 2$, for any Boolean function f on n variables (n even) is given. A counting argument gives a lower bound of $c_\wedge(f) = 2^{\frac{n}{2}} - O(n)$. Thus we have shown a separation, by an exponential factor, between worst-case Boolean complexity (which is known to be $\Theta(2^n)$) and worst-case multiplicative complexity. A construction of circuits for symmetric Boolean functions on n variables, requiring less than $n + \frac{3}{2}\sqrt{n}$ AND gates, is described.

This article was processed using the LaTeX macro package with LLNCS style

⋆ Supported in part by SNF (Denmark).

⋆⋆ Supported in part by NSF Grant CCR-9712109