

1079-11-314

**Ivelisse Rubio\*** (iverubio@gmail.com), **Francis N. Castro** and **Luis A. Medina**. *Application of the Covering Method to Divisibility of Boolean Functions.*

The *covering method* is a combinatorial method introduced by Moreno-Moreno that provides an elementary way to estimate the divisibility of exponential sums over the binary field. Using this method, they improved Ax's theorem for the binary case. Recently, Castro-Randriam-Rubio-Mattson generalized the use of the covering method to any finite field providing an elementary approach to compute the  $p$ -divisibility of exponential sums of polynomials over prime fields. Castro-Medina-Rubio used this method to compute the exact 2-divisibility of exponential sums of boolean functions with prescribed leading monomials and, as an application, families of boolean functions that are not balanced, and sufficient conditions for the solvability of systems of boolean equations were given.

In this paper we consider families of boolean functions where the number of minimal coverings is greater than one. This case is much harder than the cases previously considered, where the families have only one minimal covering. Using the covering method, we compute the exact 2-divisibility of exponential sums of polynomials where the leading monomials are symmetric. Also, we compute the exact 2-divisibility of exponential sums of deformations of symmetric or homogeneous boolean functions. (Received January 17, 2012)