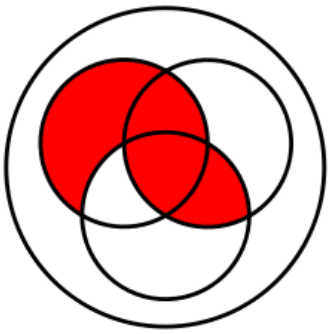
University of Puerto Rico Mayaguez Campus
Faculty of Arts and Sciences
Department of Mathematical Sciences
call box 9000, Mayagüez, P.R. 00681

THE DEPARTMENT OF MATHEMATICAL SCIENCES PROUDLY PRESENTS

COLLOQUIUM

Fall 2022

A characterization of k-rotations Boolean functions



Dr. Luis E. Medina
UPR - Río Piedras

Nov-17-2022
10:30 am

Anfiteatro Física B

Abstract

Rotation symmetric Boolean functions were introduced by Pieprzyk and Qu in the late 1990's. They showed that these functions are useful, among other things, in the design of fast hashing algorithms with strong cryptographic properties. The concept of rotation symmetric Boolean functions has been generalized to a class of functions known as k-rotation Boolean functions, where k divides n and n is the number of variables of the Boolean function. Analogous to the case of regular rotation symmetric Boolean functions, a monomial k-rotation Boolean function is called long cycle if the number of terms coincides with n/k and short k-cycle if the number of terms is less than n/k. In this work we characterize short k-cycles by providing specific generators for them.

Anfiteatro Física B

Refrigerios, 15 minutos antes.

Ph.D. in CISE
University of Puerto Rico