

1102-11-169

**Lavinia Ciungu\*** (lavinia-ciungu@uiowa.edu), The University of Iowa, Department of Mathematics, 14 MacLean Hall, Iowa City, IA 52245. *Results on Rotation Symmetric Boolean Functions.*

Boolean functions, which are functions from the vector space  $F_2^n$  to the two element field  $F_2$ , are an important tool in Cryptography, a few of their applications including pseudo-random generators in stream ciphers, S-boxes in block ciphers, error correcting codes etc. We focus on a particular class of Boolean functions, namely Rotation Symmetric Boolean functions, which are invariant under circular translation of indices. Consider the action of  $Z_n$  on  $F_2^n$  under cyclic permutation, and let  $S$  be the set of orbits of this action. Denote  $(a_i)$  a set of representatives of this action, and consider the matrix  $A = (\sum_{O(a_i)} x_{a_j})_{i,j}$ . This matrix has been intensely studied by authors such as J. Clark, M. Hell, S. Maitra, A. Maximov, P. Stănică. Here we answer an open question regarding the form of the matrix for  $n$  even. In fact we find several properties of this matrix that hold for any  $n$ , such as  $A^2 = 2^n I$  and we prove that the matrix has a general block structure given by its eigenvalues. (Received July 28, 2014)