Pieprzyk, Josef; Wang, Huaxiong; Zhang, Xian-Mo
Möbius transforms, coincident Boolean functions and non-coincidence property of Boolean functions. (English) [Zbl 1232.06017]

Boolean functions and their Möbius transforms are involved in logical calculation, digital communications, coding theory and modern cryptography. In this paper, three methods to compute the Möbius transform of a Boolean function are suggested: using matrices, using polynomials and using recursive formulas, and new properties of Möbius transforms are deduced according to the relations between the truth table and the algebraic normal form (ANF) of a Boolean function. A Boolean function which is identical to its Möbius transform is called coincident.

The paper presents characterizations and constructions of coincident functions by matrices, by polynomials, and by recursive formulas, operations of coincident functions, a classification and enumeration of coincident functions, properties of coincident functions and coincident functions with high nonlinearity and high degree. Finally, other related classes of Boolean functions are defined: $h$-non-coincident functions and anti-coincident functions, and some properties of these functions are deduced, e.g., there are precisely $2^{2^n-1}$ coincident functions and the same number of anti-coincident functions of $n$ variables, and the union of these sets of functions is a $(2^{n-1}+1)$-dimensional subspace of the set of all Boolean functions of $n$ variables.

Reviewer: Ioan Tomescu (Bucureşti)

MSC:
06E30 Boolean functions
94A60 Cryptography
94C10 Switching theory, application of Boolean algebra; Boolean functions (MSC2010)

Keywords:
Boolean function; Möbius transform; coincident functions; $h$-non-coincident functions; anti-coincident functions; non-coincident weight

Full Text: DOI

References:
[1] Carlet C., Chapter of the monography 'Boolean Models and Methods in Mathematics, Computer Science, and Engineering'

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.