Available online at www.sciencedirect.com
SCIENCE DIRECT®
Discrete Applied Mathematics 149 (2005) 73–86
DISCRETE APPLIED MATHEMATICS
www.elsevier.com/locate/dam

k-th order symmetric SAC boolean functions and bisecting binomial coefficients

T.W. Cusick, Yuan Li

Department of Mathematics, State University of New York at Buffalo, Buffalo, NY 14260-2900, USA

Received 26 January 2004; accepted 21 February 2005
Available online 4 May 2005

Abstract

The Strict Avalanche Criterion (SAC) and symmetry for Boolean functions are important properties in cryptographic applications. High order SAC was first studied by Forré. Based on bisecting binomial coefficients and S. Lloyd's work, we describe a method to find *k*th order symmetric *SAC* functions (*SSAC*(k)). In this paper, we determine all the *SSAC*(k) n-variable functions for $n \leqslant 30$, $k = 1, 2, \ldots, n-2$. Also, for infinitely many n, we give some nontrivial binomial coefficient bisections. The existence of nontrivial bisections makes the problem to find all *SSAC*(k) functions very difficult.

Keywords: Boolean function; Strict Avalanche; Criterion; Cryptography; Symmetry; Binomial coefficients

1. Introduction

The Strict Avalanche Criterion (SAC) was introduced by Webster and Tavares [10] in connection with a study of the design of S-boxes for cryptographic applications. A Boolean function in n variables is said to satisfy *SAC* if complementing any one of the n input bits results in changing the output bit with probability exactly one half. Forré [2] extended this concept by defining the higher order SAC. A Boolean function of n variables satisfies the *SAC* of order k, $0 \leqslant k \leqslant n-2$, if whenever k input bits are fixed arbitrarily, the resulting function of $n-k$ variables satisfies the *SAC*. For brevity, we will say that a function which satisfies *SAC* of order k "is a $SAC(k)$ function", or simply "is *SAC*", if $k = 0$.

E-mail addresses: cusick@buffalo.edu (T.W. Cusick), yuanili@buffalo.edu (Y. Li).

0166-218X/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2005.02.006

A Boolean function of n variables is said to be symmetric if the output bit depends only on the weight of the n-vector of input bits. Symmetry is another important cryptographic property since it guarantees that all of the input bits have equal status in a very strong sense. Symmetric resilient functions were studied by Mitchell [8] and Gopalakrishnan et al. [3]. Maitra and Sarkar [7] investigated nonlinearity for symmetric functions and Savicky [9] studied symmetric bent functions. Here we consider functions which are symmetric and kth order SAC (*SSAC*(k) for short). We give a method for finding *SSAC*(k) functions. This depends on the technique of bisecting binomial coefficients, which was discussed in Mitchell [8]. We say that we have a bisection of the $n+1$ binomial coefficients $C(n, i)$, $i=0, 1, \ldots, n$, if we can find a partition of the $n+1$ coefficients into two subsets whose sums are both 2^{n-1}.

Section 2 contains definitions, notations and some useful lemmas. Section 3 contains the main results of this paper. Some of these depend on congruences which may be of independent interest. In Section 4, we obtain all the binomial coefficient bisections for $n \leqslant 28$. This leads to the determination of all the *SSAC*(k) functions for $n \leqslant 30$. In Section 5, the computed results show that for $n \leqslant 30$, a nonquadratic *SSAC*(k) function exists if and only if $n = 16$. In Section 6, we give some open questions.

2. Preliminaries

In the usual representation, a Boolean function g maps binary vectors of length n to the set $\{0,1\}$. We find it convenient to consider instead the function $f = (-1)^g$ which maps binary n-vectors to $\{-1, 1\}$. Furthermore, we identify a binary n-vector with its support, that is, the set of positions in which the vector has a 1. Therefore, we deal with functions which take subsets of $\{1, 2, \ldots, n\}$ to $\{-1, 1\}$.

Let $I = \{1, 2, \ldots, n\}$, $|U|$=the cardinality of set U, B_I=the set of functions which take subsets of I to $\{-1, 1\}$.

We choose an equivalent description of *SAC* as our definition.

Definition 2.1 (*Lloyd [5, p. 166]*). Let $f \in B_I$, then f satisfies *SAC* iff

$$\Sigma_{V \subseteq I-\{j\}} f(V) f(V \cup \{j\}) = 0 \text{ for all } j, 1 \leqslant j \leqslant n.$$

Definition 2.2. Suppose $f \in B_I$ and U and V are subsets of I. We call f symmetric if $f(U) = f(V)$ whenever $|U| = |V|$.

Since the value of $f(U)$ is determined by the cardinality of U, we may take a symmetric function as a vector $\langle a_0, a_1, \ldots, a_n \rangle$, where $a_{|U|} = f(U) \in \{-1, 1\}$.

Forré [2] first gave the definition of kth order *SAC*. For convenience, we use an equivalent description as our definition.

Definition 2.3 (*Lloyd [5, p. 167] or [6, p. 111]*). If $f \in B_I$, then f satisfies SAC of order $n - r$ $(2 \leqslant r \leqslant n)$ iff

$\Sigma_{T \subseteq V} f(S \cup T) f(S \cup T \cup \{i\}) = 0$ for all $V \subseteq I$, with $|V| = r-1$, and all $S \subseteq I - (\{V \cup \{i\}\})$, $i \in S - V$.