Boolean functions satisfying a higher order strict avalanche criterion

Thomas W. Cusick

Department of Mathematics
State University of New York at Buffalo
106 Diefendorf Hall
Buffalo, New York 14214
e–mail: V360EAKB@UBVMS.CC.BUFFALO.EDU

Abstract. The Strict Avalanche Criterion (SAC) for Boolean functions was introduced by Webster and Tavares in connection with a study of the design of S–boxes. Later Forré extended this notion by defining strict avalanche criteria of order k for Boolean functions of n variables, where $0 \leq k \leq n-2$; the case $k = 0$ is the original SAC. Recent work by Lloyd, Preneel and others has been concerned with the problem of counting the functions which satisfy SAC of various orders. If the order is $n-2$ or $n-3$, this problem has been completely solved; the work in these cases is made easier by the fact that only quadratic Boolean functions occur. In this paper, we give good estimates for the number of Boolean functions which satisfy the SAC of order $n-4$. We also give a detailed description of the functions which satisfy SAC of order $n-4$, so the actual construction of these functions for cryptographic applications is made easy.

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; a Boolean function is said to satisfy the SAC if complementing a single input bit results in changing the output bit with probability one half. Forré [3] extended this concept by defining higher order strict avalanche criteria. A Boolean function on n variables satisfies the SAC of order k , $0 \leq k \leq n-2$, if whenever k input bits are fixed arbitrarily, the resulting function of $n-k$ variables satisfies the SAC. It is easy to see (Lloyd [5]) that if a function satisfies the SAC of order $k > 0$, then it also satisfies the SAC of order j for any $j = 0, 1, \ldots, k-1$. As is the case with any Boolean function criterion of cryptographic significance, it is of interest to count the functions which satisfy the criterion. A number of recent papers have dealt, wholly or in part, with counting functions that satisfy the SAC of various orders, for example, Lloyd [5, 6, 7] and Preneel et al. [8]. In all of these papers, when the number of variables is large only quadratic Boolean functions (that is, functions whose algebraic normal

T. Helleseth (Ed.): Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 102-117, 1994.

form contains only terms of degree ≤ 2) are counted. The simplest cases involve the functions satisfying the SAC of order $n-2$ or $n-3$; in these cases, no non–quadratic function can satisfy the criteria, so a complete count is obtained.

The problem of counting the functions which satisfy the SAC of order $\leq n-4$ is difficult, because many of the functions in these cases are non–quadratic. In this paper we apply some methods from group theory and combinatorics to give good estimates for the number of functions which satisfy the SAC of order $n-4$. It is known (see Lemma 2 below) that all such functions have degree ≤ 3. We also give a detailed characterization of the quadratic and cubic functions which can occur in this case, so the actual construction of such functions is made routine.

2. Preliminaries

We define the degree of a Boolean function $f(x_1,\dots,x_n)$ (notation: deg(f)) to be the maximum of the degrees of the terms which occur in the algebraic normal form

$$f(x_1,\dots,x_n) = a_0 \oplus \sum_{1\leq i\leq n} a_i x_i \oplus \sum_{1\leq i<j\leq n} a_{ij} x_i x_j \oplus \dots \oplus a_{12\dots n} x_1 x_2 \dots x_n$$

(Here $\oplus$ denotes addition modulo 2. Some writers use the term "nonlinear order" instead of degree.) We say the Boolean function f is linear if it has degree one with no constant term a_0 and we say f is affine if it has degree one. We say f is quadratic or cubic if it has degree 2 or 3, respectively.

We use the abbreviation SAC(k) for the Strict Avalanche Criterion of order k. Our first lemma states the simple result that in testing whether a Boolean function f satisfies SAC(k), we can discard the affine terms (if any) in f.

Lemma 1. If a Boolean function f of n variables satisfies SAC(k) for some $k, 0 \leq k \leq n-2$, then so does $f \oplus g$, where g is any affine function of n variables.

Two fundamental results on Boolean functions satisfying SAC(k) were given by Preneel et al. [8].

Lemma 2 (Preneel et al. [8, Th. 10, p. 169]) Suppose f is a Boolean function of $n \geq 2$ variables. If f satisfies SAC$(n-2)$, then f has degree 2. If f satisfies SAC(k), $0 \leq k \leq n-3$, then $\deg(f) \leq n-k-1$.

Lemma 3 (Preneel et al. [8, Th. 11, p. 170]) Suppose f is a quadratic Boolean function of $n \geq 2$ variables. Then f satisfies SAC(k), $0 \leq k \leq n-2$, if and only if every variable x_i occurs in at least $k+1$ second degree terms of the algebraic normal form.

If we define

$$q(x_1,\dots,x_n) = \sum_{1 \leq i < j \leq n} x_i x_j, \tag{1}$$

then each variable x_i occurs in exactly $n-1$ terms. It follows immediately from Lemmas 1 to 3 that any Boolean function on n variables which satisfies SAC$(n-2)$ has nonaffine part equal to $q(x_1,\dots,x_n)$, so we have:

Lemma 4. There are 2^{n+1} Boolean functions of $n \geq 2$ variables which satisfy SAC$(n-2)$; they are exactly the functions $q(x_1,\dots,x_n) \oplus g(x_1,\dots,x_n)$, where g is affine.

The count in Lemma 4 was first found in a less direct way by Lloyd [5].

It is possible to use Lemmas 1 to 3 to count the Boolean functions which satisfy SAC$(n-3)$:

Lemma 5. Define the sequence $\{w_i\}$ of integers by $w_1 = 1$, $w_2 = 2$, $w_n = w_{n-1} + (n-1)w_{n-2}$ for $n \geq 3$. The number of Boolean functions of $n \geq 3$ variables which satisfy SAC$(n-3)$ is $2^{n+1}w_n$.

Proof. By Lemma 1, it suffices to show that the number of functions which satisfy SAC$(n-3)$ and have no affine terms is w_n. By Lemmas 2 and 3, any such function is obtained by deleting zero or more terms from the sum in (1) in such a way that the remaining sum has the property that every variable x_i occurs in at least $n-2$ terms. Thus S is a set of terms which we are allowed to delete if and only if no subscript i occurs in a term x_ix_j in S more than once. It is easy to find a recursion for the number w_n of such sets S: Obviously $w_1 = 1$ (the empty set) and $w_2 = 2$. Clearly any set of terms $T = \{x_ix_j\}$ which is counted in w_{n-1} is also a set which must be counted in w_n, and this includes all sets which do not contain any term w_iw_n. If we have any set T which includes $\leq n-2$ variables from $x_1,\ldots,x_{n-1}$, we may add a term x_kx_n to T and get a set to be counted in w_n if and only if x_k does not already occur in a term in T. There are w_{n-2} such sets T, by our definitions, so we count w_{n-2} sets for each k, $1 \leq k \leq n-1$. Hence $w_n = w_{n-1} + (n-1)w_{n-2}$ and the lemma is proved.

The numbers w_n have been previously studied in a combinatorial setting because w_n is the number of permutations in the symmetric group S_n whose square is the identity. In particular, Chowla et al. [2, p. 333] gave the following asymptotic formula for w_n:

$$w_n \sim (e^{1/4}\sqrt{2})^{-1} e^{\sqrt{n}} (n/e)^{n/2} \quad \text{as } n \to \infty . \tag{2}$$

It is not difficult to use Lemmas 1 to 3 to deduce the expression

$$2^{n+1} \sum_{0\leq i\leq n/2} \frac{n!}{(n-2i)!i!2^i} \tag{3}$$

for the number of Boolean functions of $n \geq 3$ variables which satisfy SAC$(n-3)$. This expression is more complicated to compute with than the recursion for w_n and it does not seem simple to deduce the nice asymptotic result (2) from (3). Formula (3) was found in a more complicated way by Lloyd [6, p. 171].

3. Orbits of Boolean functions of 4 variables

Our goal is to find good estimates for the number of Boolean functions of n variables which satisfy SAC$(n-4)$. By Lemma 1, we lose no generality in confining ourselves to functions which have no affine terms; for brevity, we shall sometimes call such a function "affineless". We define t_n for $n \geq 4$ by

t_n = number of affineless Boolean functions of n variables which satisfy $SAC(n-4)$.

It is clear that the property of satisfying $SAC(n-4)$ is preserved if we apply any permutation of $x_1,\ldots,x_n$ to a Boolean function of n variables which has that property. Thus if we let the symmetric group S_n of permutations of $\{1,2,\ldots,n\}$ act on the set of Boolean functions of n variables in the natural way, either all or none of the functions in any orbit under this action will satisfy $SAC(n-4)$. Therefore in estimating t_n it suffices to estimate the size and the number of the orbits which contain affineless Boolean functions of n variables satisfying $SAC(n-4)$. Given such a function, if we fix any $n-4$ variables we have an affineless function of 4 variables which satisfies SAC. Our first theorem gives a complete description of all of the orbits of these functions of 4 variables. We abbreviate the terms $x_ix_jx_k$ and x_ix_j in such a function by ijk and ij, respectively.

Theorem 1. There are exactly 90 orbits under the action of S_4 on the set of the 2^{10} Boolean functions of 4 variables with no affine terms. The tables below give the following information about these orbits: a representative function for each orbit, the size of the orbit, and whether the functions in the orbit satisfy SAC. The tables group all orbits with representatives having a given number of third degree terms in the algebraic normal form of the Boolean function. Presence of a given second degree term in the representative is indicated by an "x".

Four third degree terms – 11 orbits containing 64 functions

Representative = 123 ⊕ 134 ⊕ 124 ⊕ 234 ⊕ indicated quadratic terms

Orbit	Quadratic terms included						Orbit	SAC
number	12	13	14	23	24	34	size	
1							1	yes
2	x						6	no
3	x					x	3	no
4	x			x			12	no
5	x	x		x			4	yes
6	x	x	x				4	no
7	x			x		x	12	no
8	x	x			x	x	3	yes
9	x	x		x		x	12	no
10	x	x	x	x	x		6	no
11	x	x	x	x	x	x	1	no

Three third degree terms – 20 orbits containing 256 functions

Representative = 123 ⊕ 124 ⊕ 234 ⊕ indicated quadratic terms

Orbit	Quadratic terms included						Orbit	SAC
number	12	13	14	23	24	34	size	
12							4	no
13	x						12	no
14		x					12	no
15	x					x	12	no
16	x			x			12	no
17		x	x				12	no
18	x	x					24	no
19	x			x	x		4	no
20		x	x			x	4	no
21	x	x		x			12	no
22	x	x	x				12	no
23		x	x		x		24	no
24			x	x	x		24	no
25	x	x			x	x	12	no
26		x	x		x	x	12	no
27	x	x		x	x		12	no
28	x	x		x		x	24	no
29	x		x	x	x	x	12	no
30	x	x	x		x	x	12	no
31	x	x	x	x	x	x	4	no

Two third degree terms – 28 orbits containing 384 functions

Representative = 123 ⊕ 234 ⊕ indicated quadratic terms

Orbit	Quadratic	terms	included				Orbit	SAC
number	12	13	14	23	24	34	size	
32							6	no
33			x				6	no
34				x			6	no
35	x						24	no
36			x	x			6	no
37	x					x	12	no
38	x	x					12	no
39	x				x		12	no
40		x		x			24	no
41	x		x				24	no
42	x	x		x			12	no
43	x	x	x				12	yes
44	x		x		x		12	no
45	x			x	x		12	no
46	x			x		x	12	no
47	x		x			x	12	yes
48	x		x	x			24	no
49	x				x	x	24	no
50	x	x			x	x	6	no
51	x		x	x		x	12	yes
52	x	x	x	x			12	yes
53		x	x	x		x	12	no
54	x		x		x	x	24	no
55		x		x	x	x	24	no
56	x	x		x	x	x	6	no
57	x	x	x		x	x	6	no
58		x	x	x	x	x	24	no
59	x	x	x	x	x	x	6	no

No third degree terms – 11 orbits containing 64 functions

Representative = indicated quadratic terms

Orbit	Quadratic	terms	included				Orbit	SAC
number	12	13	14	23	24	34	size	
80							1	no
81	x						6	no
82	x					x	3	yes
83	x			x			12	no
84	x	x		x			4	no
85	x	x	x				4	yes
86	x			x		x	12	yes
87	x	x			x	x	3	yes
88	x	x		x		x	12	yes
89	x	x	x	x	x		6	yes
90	x	x	x	x	x	x	1	yes

One third degree term – 20 orbits containing 256 functions

Representative = 134 ⊕ indicated quadratic terms

Orbit	Quadratic	terms	included				Orbit	SAC
number	12	13	14	23	24	34	size	
60							4	no
61	x						12	no
62		x					12	no
63	x					x	12	no
64	x			x			12	no
65		x	x				12	no
66	x	x					24	no
67	x			x	x		4	yes
68		x	x			x	4	no
69	x	x		x			12	no
70	x	x	x				12	no
71		x	x		x		24	no
72			x	x	x		24	no
73	x	x			x	x	12	no
74		x	x		x	x	12	no
75	x	x		x	x		12	yes
76	x	x		x		x	24	no
77	x		x	x	x	x	12	yes
78	x	x	x		x	x	12	no
79	x	x	x	x	x	x	4	yes

Proof. The number of orbits can be predicted in advance from the well–known Burnside counting formula (for example, see Artin [1, p. 196]), which says that if a group G with |G| elements acts on a set S then

$$\text{number of orbits} = |G|^{-1} \sum_{g \in G} f(g)\ , \tag{4}$$

where f(g) = the number of elements of S fixed by the action of g . In our case $|G| = |S_4| = 24$ and a computation shows that the sum in (4) is 2160.

Now it is a matter of calculation (we used the Mathematica software system), using the properties of the group action in order to minimize the work, to enumerate the orbits and test whether SAC is satisfied. This proves the theorem.

For our later work, it will be important to have more conceptual descriptions of the 18 orbits containing functions satisfying SAC . These are given in the Corollary below. In every case, the description in the Corollary follows in a straightforward way from the information given in Theorem 1 for the orbit in question.

Corollary to Theorem 1. The 18 orbits in Theorem 1 which contain functions satisfying SAC can be described as follows. The orbit numbers are the same as in Theorem 1. The quadratic terms are described in terms of the digit set $\{1, 2, 3, 4\} = \{h, i, j, k\}$, where the letters can stand for any one of the four numbers.

Orbit number	Orbit size	No. of degree 3 terms	Description of quadratic terms
1	1	4	None
5	4	4	Three terms containing only 3 digits, each twice
8	3	4	Four terms, consisting of two disjoint pairs
43	12	2	hi, hj, hk; h occurs only once in the two cubic terms
47	12	2	hi, hk, jk; h and k occur only once in the two cubic terms
51	12	2	hk and ij and two disjoint pairs, where h and k occur only once in the two cubic terms
52	12	2	hk and three pairs from one of the cubic terms; h and k occur only once in the cubic terms
67	4	1	hi, hj, hk; h does not occur in the cubic term
75	12	1	Four terms, where the two missing terms do not contain the number not in the cubic term
77	12	1	Five terms; the missing term is one of the 3 not containing the number not in the cubic term
79	4	1	All six possible pairs
82	3	0	One disjoint pair, e.g. 12, 34
85	4	0	Three pairs hi, hj, hk
86	12	0	Three pairs hi, ij, jk
87	3	0	Four terms consisting of two disjoint pairs
88	12	0	Four terms, where the two missing terms are not disjoint
89	6	0	Any five pairs
90	1	0	All six possible pairs

4 Functions with no affine terms satisfying SAC(n − 4)

We have already defined t_n $(n \geq 4)$ to be the number of affineless Boolean functions satisfying SAC(n − 4) . By Lemma 2, if f is any such function, then $\deg(f) \leq 3$. We let T(f) denote the set of triples ijk such that $x_i x_j x_k$ is a term in the algebraic normal form of f and we let P(f) denote the corresponding set of pairs ij . Our next two lemmas give conditions that T(f) must satisfy if f satisfies SAC(n − 4) .

Lemma 6. If $f(x_1,\dots,x_n)$ is a Boolean function satisfying SAC(n − 4) , then no more than two triples in T(f) can have exactly two integers in common.

Proof. We give a proof by contradiction. Suppose f satisfies SAC(n − 4) and T(f) contains three triples 23i, 23j, 23k . We can assume with no loss of generality that the triples are 123, 234, 23k . If g is the function obtained when all variables except x_i $(1 \leq i \leq 4)$ are set equal to zero, then from Theorem 1 Corollary we see that if g satisfies SAC then P(g) must be one of the eight sets

$$(5)\qquad \begin{array}{llll} \{12, 13, 14\}, & \{12, 14, 34\}, & \{13, 14, 24\}, & \{14, 24, 34\}, \\ \{12, 13, 14, 23\}, & \{12, 14, 23, 34\}, & \{13, 14, 23, 24\}, & \{14, 23, 24, 34\} \end{array}$$

(notice 14 is in every set and the last four sets are just the first four sets with 23 added).

First suppose 12 and 13 occur in P(g) (an analogous argument deals with the case when 24 and 34 occur). If g_1 is the function obtained when all variables except x_2, x_3, x_4 and x_k are set equal to zero, then $P(g_1)$ (which is in the list (5) with 1 replaced by k) must contain both 2k and 3k (otherwise either 24 or 34 is in $P(g_1)$, so P(g) contains 12, 13, 14 and at least one of 24, 34; this contradicts the fact that P(g) is in the list (5)). If g_2 is the function obtained when all variables except x_1, x_2, x_3, x_k are set equal to zero, we now have that $P(g_2)$ (which is in the list (5) with 4 replaced by k) contains at least 1k, 12, 13, 2k and 3k ; this contradicts the fact that $P(g_2)$ can have no more than 4 elements.

Now suppose 12 and 34 occur in $P(g)$ (an analogous argument deals with the case when 13 and 24 occur). It follows that $P(g_1)$ must contain both 2k and 4k (otherwise 24 occurs in $P(g_1)$ and so in $P(g)$, contradicting the fact that $P(g)$ is in the list (5)). This means $P(g_2)$ must contain both 12 and 2k, which is impossible since $P(g_2)$ is in the list (5) with 4 replaced by k. This completes the proof.

Lemma 7. If $f(x_1,\dots,x_n)$ is a Boolean function satisfying $SAC(n-4)$, then no two triples in $T(f)$ can have exactly one integer in common.

Proof. We give a proof by contradiction. Let f satisfy $SAC(n-4)$. Suppose $T(f)$ contains two triples 123 and 14k, $k > 4$, and does not contain any of the triples 124, 134, 234. If g is the function obtained when all variables except x_1, x_2, x_3, x_4 are set equal to zero, then Theorem 1 Corollary shows that if g satisfies SAC, then $P(g)$ must be $\{14, 24, 34\}$ plus any subset of $\{12, 13, 23\}$. If g_1 is the function obtained when all variables except x_1, x_2, x_3, x_4, x_k are set equal to zero and $x_k = 1$, then $T(g_1) = \{123\}$ and $P(g_1)$ does not contain 14. This means g_1 does not satisfy SAC, so f cannot satisfy $SAC(n-4)$.

Now suppose $T(f)$ contains 123, 14k and 234. With g defined as above, we saw in the proof of Lemma 6 that $P(g)$ must be one of the sets in (5). Since 14 is in every set in (5), looking at g_1 defined above again gives a contradiction. A similar argument gives a contradiction in the case where $T(f)$ contains 123, 14k and one of 124, 134.

Finally suppose $T(f)$ contains 123, 14k, 124 and 234 (the case 123, 14k, 134, 234 is similar and other choices of two or more triples from $\{124, 134, 234\}$ are ruled out by Lemma 6). If g is defined as above, then $T(g)$ has three triples and so by Theorem 1 g does not satisfy SAC and f does not satisfy $SAC(n-4)$. This completes the proof of the lemma.

We turn to the quadratic functions which satisfy $SAC(n-4)$. By Lemma 3, such a function is characterized by the property that every variable x_i occurs in at least $n-3$ of the terms $x_i x_j$ in the algebraic normal form. Thus every such function with no affine terms is obtained from the sum in (1) by deleting a set S of zero or more terms in which no subscript i occurs more than twice; hence we can count the functions by counting the corresponding sets S (the same idea was already used in the proof of Lemma 5). In our next lemma we give a proof of an asymptotic formula for the number of these sets. By analogy with the proof of Lemma 5, we define

$$v_n = \text{the number of quadratic functions } \Sigma x_i x_j \text{ of } n \text{ variables}$$
$$\text{such that no variable } x_i \text{ occurs more than twice}$$

Lemma 8. The number of quadratic Boolean functions of $n \geq 4$ variables, with no affine terms, which satisfy $SAC(n-4)$ is v_n. We have

$$v_n \sim (2^{5/2}\pi)^{-1/2} (n+1)^{-3/4} \exp((\tfrac{1}{2}(n+1))^{1/2}) n! \tag{6}$$

as $n \to \infty$.

Proof. The first sentence of the lemma follows from the remarks in the paragraph preceding the lemma. The number v_n is clearly the number of graphs (no multiple edges) on the vertex set $\{1,2,...,n\}$ such that every component is an isolated vertex, an edge, a cycle (of length at least 3) or a path. By well–known combinatorial arguments (see [9, Example 6.5, p. 134] for a similar problem), the exponential generating function is

$$\sum_{n=0}^{\infty} v_n x^n/n! = \exp(-x^2/4 + x/(2(1-x)))(1-x)^{-1/2}$$

This function is "admissible" in the sense of Hayman [4] and it follows from his Theorem I, Corollary II that (6) holds as $n \to \infty$.

Lemma 8 Corollary. The number v_n satisfies

$$\log v_n \sim n \log n \text{ as } n \to \infty .$$

Proof. This follows from (6) and Stirling's formula $n! \sim \sqrt{2\pi n}\ (n/e)^n$.

We are now ready to give our estimates for t_n.

Theorem 2. The following inequalities hold for the number t_n of Boolean functions of n variables which satisfy $SAC(n-4)$ and have no affine terms:

$$n!g(n) < t_n < 3.2\, n^3\, n!\, g(n-4)$$

where

$$g(n) \sim C(n+1)^{-3/4} \exp((\tfrac{1}{2}(n+1))^{1/2})$$

as $n \to \infty$, with $C = (2^{5/2}\pi)^{-1/2} = .237\ldots$.

Proof. We see from the tables after Theorem 1 that there are no orbits which contain functions satisfying SAC and which have three third degree terms. It follows from this and Lemmas 6 and 7 that if f is an affineless Boolean function satisfying $SAC(n-4)$, then the set of triples $T(f)$ is either made up of disjoint triples or is made up of exactly two triples with a common pair of elements, and possibly some further disjoint triples.

We define

$$(7) \qquad g(n) = v_n/n!,$$

where v_n is defined above Lemma 8.

We first consider the case where $T(f)$ contains a single triple, which we may take to be 123. Suppose now that we fix all of the variables except those with subscripts 1, 2, 3 and j for some j, $4 \le j \le n$. The resulting function of 4 variables satisfies SAC and so by Theorem 1 it lies in one of four orbits which contain functions with a single term of degree 3. If 123 is the term of degree 3, then by the Corollary to Theorem 1 the set of pairs for the function of the variables 1,2,3,j is

$$1j,\ 2j,\ 3j \text{ plus some subset of } \{12, 13, 23\};$$

all of the eight possible subsets can occur. It follows from this that the pair set $P(f)$ for the function f of n variables must be some subset of $\{12, 13, 23\}$ plus 14, 24, 34, 15, 25, 35,... ,

ln, 2n, 3n plus more terms involving $x_4,\ldots,x_n$.

Let $r(x_1,\ldots,x_n)$ denote the quadratic function of n variables formed from the terms 15, 25, 35 and all the subsequent terms in the above list. If we fix variables x_1,x_2,x_3 in some way, since our original function f satisfies SAC(n − 4) , the resulting quadratic function r of n − 3 variables must satisfy SAC of order n − 7 = (n − 3) − 4 . Since there is no choice for the affine terms in such a function r , by Lemma 8 the number of such functions n is $\leq v_{n-3}$. Thus the total number of functions f satisfying SAC(n − 4) and with T(f) containing a single triple is less than

$$8\binom{n}{3} g(n-3)(n-3)!\ ;$$

here the binomial coefficient gives the number of ways of choosing the single triple, say ijk ; 8 is the number of ways of choosing the associated subset of {ij, ik, jk} ; and (7) gives the final factors.

Now we suppose the set of triples T(f) contains t disjoint triples. A straightforward extension of the argument in the previous paragraph now gives the upper bound

$$8^t \binom{n}{3t} g(n-3t)(n-3t)!$$

for the number of such functions f which satisfy SAC(n − 4) . Summing our estimates, we find that the number of functions f satisfying SAC(n − 4) and having T(f) made up of disjoint triples is less than

$$g(n-3)\sum_{t=1}^{[n/3]} 8^t \binom{n}{3t} (n-3t)! < (e^2-1)n!\, g(n-3)$$

since

$$\sum_{t=1}^{[n/3]} 8^t/(3t)! < \sum_{t=1}^{\infty} 8^{t/3}/t! = e^2 - 1\ .$$

Next we consider the case where T(f) contains two triples with a common pair, which we may take to be 123, 234. Suppose now that we fix all of the variables except those with subscripts 1,2,3,4. The resulting function of 4 variables satisfies SAC and so by Theorem 1 it lies in one of four orbits which contain functions with two terms of degree 3. If we fix x_4 we have a function of $n-1$ variables satisfying SAC$(n-5)$ with triple set 123 only. Thus our above analysis for the case of a singleton triple set applies (with $n-1$ in place of n), and so the number of such functions of $n-1$ variables is less than

$$8\binom{n-1}{3}g(n-4)(n-4)!\,.$$

To return to functions of n variables with two–element triple set made up of two triples with some pair ij in common we must multiply this bound by

$$\binom{n}{3}3\,(n-3)\,;$$

here the binomial coefficient gives the number of ways of choosing the first triple, 3 is the number of ways of choosing ij from the first triple and $n-3$ is the number of ways of choosing the third element in the second triple.

As in our previous work, we can extend the above argument to the case where the triple set is made up of two triples with a common pair plus t more disjoint triples. This gives the following upper bound for the number of functions f satisfying SAC$(n-4)$ and having triple set T(f) containing two triples with a common pair:

$$3(n-3)\binom{n}{3}\sum_{t=1}^{[(n-4)/3]} 8^t\binom{n-1}{3t}g(n-1-3t)(n-1-3t)!$$

$$<\frac{1}{2}(n-1)(n-2)(n-3)n!\,g(n-4)\sum_{t=1}^{[(n-4)/3]} 8t/(3t)!$$

$$<\frac{1}{2}(e^2-1)n^3\,n!\,g(n-4)\,.$$

Since $\frac{1}{2}(e^2-1) = 3.195...$, putting together our estimates and using Lemma 8 gives the upper bound in Theorem 2. The lower bound follows immediately from (7) and Lemma 8.

References

[1] M. Artin, *Algebra*, Prentice–Hall, 1992.

[2] S. Chowla, I. N. Herstein and K. Moore, On recursions connected with symmetric groups I, *Canadian J. Math.* 3 (1951), 328–334.

[3] R. Forré, The strict avalanche criterion: spectral properties of Boolean functions and an extended definition, *Advances in Cryptology – Crypto '88*, Lect. Notes Comp. Sci. 403, Springer–Verlag, 1990, pp. 450–468.

[4] W. K. Hayman, A generalisation of Stirling's formula, J. reine agnew. Math. 196 (1956), 67–95.

[5] S. Lloyd, Counting functions satisfying a higher order strict avalanche criterion, *Advances in Cryptology – Eurocrypt '89*, Lect. Notes Comp. Sci. 434, Springer– Verlag, 1990, pp. 63–74.

[6] S. Lloyd, Characterising and counting functions satisfying the strict avalanche criterion of order $(n - 3)$, in *Cryptography and Coding II*, Clarendon Press, Oxford, 1992, pp. 165–172.

[7] S. Lloyd, Counting binary functions with certain cryptographic properties, *J. Cryptology* 5 (1992), 107–131.

[8] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts and J. Vandewalle, Propagation characteristics of Boolean functions, *Advances in Cryptology – Eurocrypt '90*, Lect. Notes Comp. Sci. 473, Springer–Verlag, 1991, pp. 161–173.

[9] R. P. Stanley, Generating functions, in *Studies in Combinatorics*, MAA Studies 17, Math. Assoc. America, 1978, pp. 100–141.

[10] A. F. Webster and S. E. Tavares, On the design of S–boxes, *Advances in Cryptology – Crypto '85*, Lect. Notes Comp. Sci. 218, Springer–Verlag, 1986, pp. 523–534.