J. Cryptology (1992) 5: 107–131

Journal of Cryptology

Counting Binary Functions with Certain Cryptographic Properties

Sheelagh Lloyd
Hewlett Packard Laboratories, Filton Road, Stoke Gifford,
Bristol BS12 6QZ, England

Communicated by Ernest F. Brickell

Received 2 February 1990 and revised 5 February 1991

Abstract. This paper investigates the connections between three properties of a binary function. These properties are important in cryptography and are the Strict Avalanche Criterion, balance, and correlation immunity. We derive necessary and sufficient conditions for a function to possess various combinations of these properties, and count the number of such functions.

Key words. Balance, Correlation immunity, Strict Avalanche Criterion, Cryptography, Counting.

1. Introduction

In this paper we investigate the connections between three properties of a binary function: the Strict Avalanche Criterion, balance, and correlation immunity. The Strict Avalanche Criterion was introduced by Webster and Tavares [7] in order to combine the ideas of completeness and the avalanche effect. A cryptographic transformation is said to be complete if each output bit depends on each input bit, and it exhibits the avalanche effect if an average of one-half of the output bits change whenever a single input bit is changed. Forrê [1] extended this notion by defining higher-order Strict Avalanche Criteria. A function is balanced if, when all input vectors are equally likely, then all output vectors are equally likely. This is an important property for many types of cryptographic functions. The idea of correlation immunity is also extremely important, especially in the field of stream ciphers, where combining functions which are not correlation immune are vulnerable to ciphertext-only attacks (see, for example, [5]). The concept of mth-order correlation immunity was introduced by Siegenthaler [4] as a measure of resistance against such an attack.

In a previous paper [2] we found conditions under which a function satisfying the highest possible order Strict Avalanche Criterion was also balanced and/or correlation immune. We found that a function cannot be balanced, correlation immune, and satisfy the highest-order Strict Avalanche Criterion. Since balance and correlation immunity are very important cryptographically, we deduce that the highest-order Strict Avalanche Criterion is too stringent a condition. It is natural, therefore, to look at the next highest-order (that is order $(n-3)$) Strict Avalanche Criterion, and see whether there are any functions satisfying this which are both balanced and correlation immune. We see that such functions do indeed exist, and we are able to formulate necessary and sufficient conditions on a function to satisfy these criteria simultaneously. In doing this, we use the characterization of functions satisfying the Strict Avalanche Criterion of order $(n-3)$ developed in [3]. These new conditions are constructive—a function satisfying the Strict Avalanche Criterion of order $(n-3)$ is determined by its values at vectors of small weight, and we obtain conditions on these values for the function to be balanced and/or correlation immune. This means that constructing such a function becomes merely a matter of selecting a few values from which the remainder of the function may easily be computed. Having established that these functions exist, it is also of interest to determine the number of such functions since, if there were very few, it would not be sensible to recommend their use in cryptographic applications. We also consider here higher orders of correlation immunity to discover whether there is a limit to the amount of correlation immunity possible in a function satisfying the Strict Avalanche Criterion of order $(n-3)$. We find that there is no limit, but obviously the number of functions decreases as the order of correlation immunity increases. We are able to derive necessary and sufficient conditions for each order of correlation immunity, and calculate the number of functions in each case. These conditions are also constructive.

In Section 2 we establish some notation, define the properties to be examined, and state characterizations of functions with the various properties. Section 3 is devoted to some preliminary calculations which enable us to identify conditions the functions must satisfy. We present results on balance in Section 4, on correlation immunity in Section 5, and on simultaneous balance and correlation immunity in Section 6. In each of Sections 4–6 we produce necessary and sufficient conditions, and also expressions for the number of functions satisfying those conditions. In Section 7 we display a table of numbers of functions, for some small values of n, and conclude that there is a sufficient supply of such functions for them to be useful for cryptographic applications.

2. Notation and Definitions

Although we are really dealing with functions of binary vectors of length n which take values in $\{-1, 1\}$, we find it convenient to identify a binary vector with its support, that is the set of positions in which it has a 1. We, therefore, deal instead with functions from subsets of $\{1, 2, \ldots, n\}$ to $\{-1, 1\}$.

Let $\mathscr{S}$ be the set $\{1, 2, \ldots, n\}$ and let $\mathscr{B}_{\mathscr{S}}$ denote the set of functions which takes subsets of $\mathscr{S}$ to $\{-1, 1\}$. We formulate all the definitions and characterizations in terms of such functions.

2.1. *Balance*

This is the simplest of the three properties, and ensures that the number of 1's produced by f is the same as the number of -1's produced.

Definition 2.1.1. Let $f \in \mathcal{B}_{\mathcal{S}}$. Then f is balanced if and only if

$$\sum_{V \subseteq \mathcal{S}} f(V) = 0.$$

2.2. *Correlation Immunity*

Definition 2.2.1. $f \in \mathcal{B}_{\mathcal{S}}$ is said to be first-order correlation immune if, for any $i \in \mathcal{S}$, the probability that $i \in V$, given that V satisfies $f(V) = 1$, is equal to $\frac{1}{2}$.

The definition is extended to higher orders as follows.

Definition 2.2.2. Let m be an integer with $1 \leq m \leq n$. Then $f \in \mathcal{B}_{\mathcal{S}}$ is said to be mth-order correlation immune if, for any $J \subseteq \mathcal{S}$ with $|J| = m$ and any $Y \subseteq J$, the probability that $V \cap J = Y$, given that $f(V) = 1$, is equal to $1/2^m$.

Note that, for any m with $2 \leq m \leq n$, mth-order correlation immunity implies $(m-1)$th-order correlation immunity.

In order to characterize correlation-immune functions, we need to define the Hadamard–Walsh transform.

Definition 2.2.3. The Hadamard–Walsh transform of $f \in \mathcal{B}_{\mathcal{S}}$ is defined by

$$H(U) = \sum_{V \subseteq \mathcal{S}} f(V)(-1)^{|U \cap V|}.$$

There is a well-known formula for inverting the Hadamard–Walsh transform, which we give below:

$$f(W) = \frac{1}{2^n} \sum_{U \subseteq \mathcal{S}} H(U)(-1)^{|U \cap W|} \qquad \text{for all} \quad W \subseteq \mathcal{S}.$$

Xiao and Massey [6] have proved the following theorem characterizing correlation-immune functions in terms of the values of their Hadamard–Walsh transforms.

Theorem 2.2.4. *The function $f \in \mathcal{B}_{\mathcal{S}}$ is mth-order correlation immune if and only if $H(U) = 0$ for all $U \subseteq \mathcal{S}$ with $1 \leq |U| \leq m$.*

Let us define the integer-valued function X by

$$X(W) = \sum_{V \subseteq W} f(V) \qquad \text{for} \quad W \subseteq \mathcal{S}.$$

We will find it more convenient to express the characterization of correlation immunity in terms of the function X. In order to do so, we need the following result.

Lemma 2.2.5. *If X and H are defined as above, then*

$$X(W) = \frac{1}{2^{n-|W|}} \sum_{\substack{U \subseteq \mathscr{S} \\ U \cap W = \varnothing}} H(U) \qquad \textit{for all} \quad W \subseteq \mathscr{S}.$$

Proof. Since H is the Hadamard–Walsh transform of f, we know that

$$f(W) = \frac{1}{2^n} \sum_{U \subseteq \mathscr{S}} H(U)(-1)^{|U \cap W|} \qquad \text{for all} \quad W \subseteq \mathscr{S}.$$

Substituting this into the definition of X, we obtain

$$\begin{aligned} X(W) &= \sum_{V \subseteq W} \frac{1}{2^n} \sum_{U \subseteq \mathscr{S}} H(U)(-1)^{|U \cap V|} \\ &= \frac{1}{2^n} \sum_{U \subseteq \mathscr{S}} H(U) \sum_{V \subseteq W} (-1)^{|U \cap V|}. \end{aligned}$$

For any $V \subseteq W$, we can write $V = A \cup B$ with $A \subseteq (W \cap U)$ and $B \subseteq (W \setminus U)$. So

$$\sum_{V \subseteq W} (-1)^{|U \cap V|} = \sum_{B \subseteq (W \setminus U)} \sum_{A \subseteq (W \cap U)} (-1)^{|A|}.$$

If $W \cap U \neq \varnothing$, there are as many subsets of odd size as of even size, so the sum is 0. If $W \cap U = \varnothing$, then the sum is just $2^{|W|}$. Hence

$$X(W) = \frac{1}{2^{n-|W|}} \sum_{\substack{U \subseteq \mathscr{S} \\ U \cap W = \varnothing}} H(U) \qquad \text{for all} \quad W \subseteq \mathscr{S}.$$

Note that $X(\mathscr{S}) = H(\varnothing)$. □

We now use this to produce a formulation of mth-order correlation immunity in terms of X.

Lemma 2.2.6. *If H and X are defined as above, then the following three conditions are equivalent:*

(i) *f is mth-order correlation immune.*
(ii) *$H(U) = 0$ for all $U \subseteq \mathscr{S}$ with $1 \leq |U| \leq m$.*
(iii) *$X(W) = 2^{|W|-n} X(\mathscr{S})$ for all $W \subseteq \mathscr{S}$ with $(n - m) \leq |W| \leq (n - 1)$.*

Proof. The equivalence of (i) and (ii) is given by Theorem 2.2.4. We now show the equivalence of (ii) and (iii), using Lemma 2.2.5.

Suppose that (ii) holds. Let $W \subseteq \mathscr{S}$ be such that $(n - m) \leq |W| \leq (n - 1)$, and let $U \subseteq \mathscr{S}$ be such that $W \cap U = \varnothing$. Then $0 \leq |U| \leq (n - |W|) \leq m$, so either $U = \varnothing$ or $H(U) = 0$. So

$$X(W) = \frac{1}{2^{n-|W|}} \sum_{\substack{U \subseteq \mathscr{S} \\ U \cap W = \varnothing}} H(U) = \frac{1}{2^{n-|W|}} H(\varnothing).$$

Now $X(\mathscr{S}) = H(\varnothing)$, so we have (iii).

Now suppose that (iii) holds. We prove (ii) by induction on the size of U. Suppose first that $|U| = 1$. Let $W = \mathscr{S}\backslash U$. Then $V \cap W = \varnothing$ if and only if either $V = \varnothing$ or $V = U$, so

$$X(W) = \tfrac{1}{2}(H(\varnothing) + H(U)).$$

Since $|W| = (n-1)$, we also know that $X(W) = \frac{1}{2}H(\varnothing)$. Hence $H(U) = 0$.

Now suppose that $2 \leq |U| \leq m$ and that $H(V) = 0$ for all V with $1 \leq |V| < |U|$. Let $W = \mathscr{S}\backslash U$, then $V \cap W = \varnothing$ if and only if $V \subseteq U$, so

$$X(W) = \frac{1}{2^{n-|W|}}\left(H(\varnothing) + H(U) + \sum_{V \subset U, V \neq \varnothing} H(V)\right).$$

Now, for any $V \subset U$, $V \neq \varnothing$, we see that $1 \leq |V| < |U|$, so $H(V) = 0$. Since $(n-m) \leq |W| \leq (n-1)$, we also know that $X(W) = 2^{|W|-n}H(\varnothing)$. Thus we may conclude that $H(U) = 0$ as required. □

2.3. *The Strict Avalanche Criterion*

Definition 2.3.1. Let $f \in \mathscr{B}_{\mathscr{S}}$. Then f satisfies the Strict Avalanche Criterion (SAC) if and only if

$$\sum_{V \subseteq (\mathscr{S}\backslash\{j\})} f(V)f(V \cup \{j\}) = 0 \qquad \text{for all } j, \quad 1 \leq j \leq n.$$

We now define the higher-order SAC. The SAC defined above is deemed to be the SAC of order 0, and the SAC of order m for $1 \leq m \leq n-2$ is defined as follows.

Definition 2.3.2 [1]. A function $f \in \mathscr{B}_{\mathscr{S}}$ satisfies the SAC of order m, where $1 \leq m \leq (n-2)$ if and only if, given any subset $\mathscr{T}$ of $\mathscr{S}$ with $|\mathscr{T}| = n - m$ and any subset P of $\mathscr{S}\backslash\mathscr{T}$, the function $g \in \mathscr{B}_{\mathscr{T}}$ obtained from f by setting $g(V) = f(V \cup P)$ for each $V \subseteq \mathscr{T}$ satisfies the SAC.

Let $\bar{f}$ denote the algebraic normal form of f (so $\bar{f}$ also takes subsets of $\mathscr{S}$ to $\{-1, 1\}$). We sometimes find it convenient to write F for the function from $\mathscr{S}$ to $\{1, -1\}$ such that $F(x) = \bar{f}(\{x\})$.

In [3] we proved the following result characterizing functions satisfying the SAC of order $(n-3)$.

Theorem 2.3.3 [3]. *Suppose that $f \in \mathscr{B}_{\mathscr{S}}$. Then f satisfies the SAC of order $(n-3)$ if and only if*

$$f(V) = \prod_{U \subseteq V, |U|<3} \bar{f}(U) \qquad \textit{for all} \quad V \subseteq \mathscr{S}$$

and, for each $x \in \mathscr{S}$, there is at most one $y \in \mathscr{S}$ for which $\bar{f}(\{x, y\}) = 1$.

We were thus able to prove

Theorem 2.3.4 [3]. *The number of functions in $\mathscr{B}_{\mathscr{S}}$ which satisfy the SAC of order*

$(n-3)$ *is*

$$2^{n+1}\sum_{0\le 2m\le n}\frac{n!}{(n-2m)!\,m!\,2^m}.$$

We deduce from Theorem 2.3.3 that if f satisfies the SAC of order $(n-3)$, then we can write any $W\subseteq\mathscr{S}$ as $\{x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_m, x_{2m+1}, \ldots, x_{|W|}\}$ where $\bar{f}(\{x_j, y_j\}) = +1$ for all $1\le j\le m$ and $\bar{f}(\{a, b\}) = -1$ otherwise. We shall find the following notation useful.

Definition 2.3.5. We write $A_W(n, m)$ $(W\subseteq\mathscr{S}, 0\le 2m\le n)$ for the set of functions $f\in\mathscr{B}_{\mathscr{S}}$ satisfying the following conditions: f satisfies the SAC of order $(n-3)$ and there exist $x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_m, x_{2m+1}, \ldots, x_{|W|}$ such that

$$W = \{x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_m, x_{2m+1}, \ldots, x_{|W|}\},$$

and

$$\begin{aligned}\bar{f}(\{x_j, y_j\}) &= +1, & 1\le j\le m,\\ \bar{f}(\{a, b\}) &= -1 & \text{otherwise.}\end{aligned}$$

In what follows we want to distinguish the cases where there exists a pair (x, y), such that $\bar{f}(\{x, y\}) = 1$ and $F(x) = -F(y)$, from those where no such pair exists. In order to be able to state some subsequent results concisely in the cases where no such pair exists, we introduce the following notation.

Definition 2.3.6. We write $C_W(n, m, r, t, q)$ $(W\subseteq\mathscr{S}, 0\le 2m\le n, 0\le r\le m, 0\le t\le n-2m, q = 2r+2t+m-n)$ for the set of functions $f\in\mathscr{B}_{\mathscr{S}}$ satisfying the following conditions: f belongs to $A_W(n, m)$ and

$$\begin{aligned}F(x_j) = F(y_j) &= +1, & 1\le j\le r,\\ F(x_j) = F(y_j) &= -1, & r+1\le j\le m,\\ F(x_j) &= +1, & 2m+1\le j\le 2m+t,\\ F(x_j) &= -1, & 2m+t+1\le j\le |W|.\end{aligned}$$

For ease of notation, we write simply $C(n, m, r, t, q)$ for $C_{\mathscr{S}}(n, m, r, t, q)$. So we see that if $f\in\mathscr{B}_{\mathscr{S}}$ satisfies the SAC of order $(n-3)$, then either there exists a pair (x, y), such that $\bar{f}(\{x, y\}) = 1$, and $F(x) = -F(y)$, or f belongs to $C(n, m, r, t, q)$ for some values of m, r, t, and q. We shall also find the following results useful.

Lemma 2.3.7. *The number of functions belonging to* $C(n, m, r, t, q)$, *where* $0\le 2m\le n, 0\le r\le m, 0\le t\le n-2m$, *and* $q = 2r+2t+m-n$, *is*

$$\frac{2n!}{(n-2m)!\,m!\,2^m}\binom{m}{r}\binom{n-2m}{t}.$$

Proof. We must first choose the m pairs (x_j, y_j), noting that the order within the pair is unimportant. This may be done in $n!/(n-2m)!\,m!\,2^m$ ways. We must now choose r of the m pairs and t of the remaining $(n-2m)$ elements to have $F(x_j) = +1$.

This may be done in $\binom{m}{r}\binom{n-2m}{t}$ ways. Finally, we must choose a value for $f(\varnothing)$, which may be done in two ways. □

Lemma 2.3.8. *The number of functions* $f \in \mathscr{B}_{\mathscr{S}}$ *which satisfy the SAC of order* $(n-3)$, *and for which there exist exactly p pairs* (x, y) *for which* $\bar{f}(\{x, y\}) = 1$, *and* $F(x) = -F(y)$ *is*

$$\sum_{2p \leq 2m \leq n} \frac{n!}{(n-2m)!\, m!} 2^{n-2m+1} \binom{m}{p}.$$

Proof. The number m of pairs (x, y) for which $\bar{f}(\{x, y\}) = 1$ must be at least p and at most the integer part of $n/2$. If we fix m, then we must first choose the m pairs (x_j, y_j), noting that the order within the pair is unimportant. This may be done in $n!/(n-2m)!\, m!\, 2^m$ ways. We must now choose p of the m pairs to have $F(x) = -F(y)$, and this may be done in $\binom{m}{p}$ ways. We may then choose $F(x)$ for one member of each of the m pairs (since then it is fixed for the other member). This may be done in 2^m ways. We then choose $F(x)$ for each of the remaining $(n-2m)$ elements, and finally choose $f(\varnothing)$. This may be done in 2^{n-2m+1} ways. Summing over m, we obtain the desired expression. □

3. Preliminary Calculations

We want to express $f(V \cup \{x\})$ in terms of $f(V)$. We know that, given x and V, if f satisfies the SAC of order $(n-3)$, then there is at most one z in V with $\bar{f}(\{x, z\}) = 1$. We first deal with the case where no such z exists.

Proposition 3.1. *Suppose that* $f \in \mathscr{B}_{\mathscr{S}}$ *satisfies the SAC of order* $(n-3)$. *Suppose further that* $x \notin V$ *and that* $\bar{f}(\{x, y\}) = -1$ *for all* $y \in V$. *Then*

$$f(V \cup \{x\}) = (-1)^{|V|} f(V) F(x).$$

Proof. Since f satisfies the SAC of order $(n-3)$, we know that

$$f(S) = \prod_{\substack{T \subseteq S \\ |T| < 3}} \bar{f}(T) \qquad \text{for all} \quad S \subseteq \mathscr{S}.$$

Using this to calculate $f(V \cup \{x\})$, we obtain

$$\begin{aligned} f(V \cup \{x\}) &= \prod_{\substack{T \subseteq (V \cup \{x\}) \\ |T| < 3}} \bar{f}(T) \\ &= \prod_{\substack{T \subseteq V \\ |T| < 3}} \bar{f}(T) \prod_{\substack{T \subseteq V \\ |T| < 2}} \bar{f}(T \cup \{x\}) \\ &= f(V) F(x) \prod_{y \in V} \bar{f}(\{x, y\}) \\ &= f(V) F(x) (-1)^{|V|} \\ &= (-1)^{|V|} f(V) F(x) \end{aligned}$$

as required. □

We turn now to the case where there is a unique element z in V with $\bar{f}(\{x, z\}) = 1$.

Proposition 3.2. *Suppose that $f \in \mathscr{B}_{\mathscr{S}}$ satisfies the SAC of order $(n-3)$. Suppose further that $x \notin V$, and that $\bar{f}(\{x, z\}) = 1$ (so $\bar{f}(\{x, y\}) = -1$ for all $y \in V$, $y \neq z$). Then*

$$f(V \cup \{x\}) = (-1)^{|V|-1} f(V) F(x).$$

Proof. As in the proof of Proposition 3.1, we have

$$\begin{aligned} f(V \cup \{x\}) &= f(V)F(x) \prod_{y \in V} \bar{f}(\{x, y\}) \\ &= f(V)F(x)(-1)^{|V|-1} \\ &= (-1)^{|V|-1} f(V)F(x) \end{aligned}$$

as required. □

We are now able to produce an expression for $X(W) = \sum_{V \subseteq W} f(V)$ in terms of the values of $\bar{f}$. In order to prove this, we also need to produce the corresponding expression for $\sum_{V \subseteq W}(-1)^{|V|} f(V)$ as well.

Theorem 3.3. *Suppose that $W \subseteq \mathscr{S}$ and that f belongs to $A_W(n, m)$. Let i denote the square root of -1 and let*

$$G_W = f(\emptyset) \prod_{j=1}^{m} (1 + F(x_j)F(y_j) + i(F(x_j) + F(y_j))) \prod_{j=2m+1}^{|W|} (1 + iF(x_j)),$$

then

$$\sum_{V \subseteq W} f(V) = \Re(G_W) + \Im(G_W)$$

and

$$\sum_{V \subseteq W} (-1)^{|V|} f(V) = \Re(G_W) - \Im(G_W),$$

where $\Re(x)$ and $\Im(x)$ denote the real and imaginary parts of x, respectively.

Proof. The proof is by induction on the size of W.

Firstly, we assume that $|W| = 0$, so that $W = \emptyset$. Then

$$G_W = f(\emptyset), \qquad \sum_{V \subseteq W} f(V) = f(\emptyset), \quad \text{and} \quad \sum_{V \subseteq W} (-1)^{|V|} f(V) = f(\emptyset),$$

so we have the desired relation.

Now suppose the result true for all W with $|W| \leq K$, and let W be such that $|W| = K + 1$. Choose $x \in W$, and let $U = W \backslash \{x\}$. We split the proof into two cases. Either $x = x_j$ for some j with $2m + 1 \leq j \leq K + 1$, or $x = x_j$ or $x = y_j$ for some j with $1 \leq j \leq m$.

Suppose that the first case holds. Now

$$\sum_{V \subseteq W} f(V) = \sum_{V \subseteq U} f(V) + \sum_{V \subseteq U} f(V \cup \{x\}).$$

By the inductive hypothesis, since $|U| = K$, we have

$$\sum_{V \subseteq U} f(V) = \Re(G_U) + \Im(G_U).$$

To calculate the second sum, note that in this case $\bar{f}(\{x, y\}) = -1$ for all $y \in U$, so we may use Proposition 3.1 to obtain

$$\begin{aligned}\sum_{V \subseteq U} f(V \cup \{x\}) &= \sum_{V \subseteq U} (-1)^{|V|} f(V) F(x)\\ &= F(x) \sum_{V \subseteq U} (-1)^{|V|} f(V)\\ &= F(x)(\Re(G_U) - \Im(G_U)) \qquad \text{by the inductive hypothesis.}\end{aligned}$$

So

$$\sum_{V \subseteq W} f(V) = \Re(G_U) + \Im(G_U) + F(x)(\Re(G_U) - \Im(G_U)) = \Re(G_W) + \Im(G_W),$$

since $G_W = (1 + iF(x))G_U$ in this case.

We may now calculate $\sum_{V \subseteq W} (-1)^{|V|} f(V)$ in the same way:

$$\sum_{V \subseteq W} (-1)^{|V|} f(V) = \sum_{V \subseteq U} (-1)^{|V|} f(V) - \sum_{V \subseteq U} (-1)^{|V|} f(V \cup \{x\})$$

and

$$\sum_{V \subseteq U} (-1)^{|V|} f(V) = \Re(G_U) - \Im(G_U).$$

Using Proposition 3.1 again, we have

$$\sum_{V \subseteq U} (-1)^{|V|} f(V \cup \{x\}) = F(x)(\Re(G_U) + \Im(G_U)).$$

Hence

$$\begin{aligned}\sum_{V \subseteq W} (-1)^{|V|} f(V) &= (\Re(G_U) - \Im(G_U)) - F(x)(\Re(G_U) + \Im(G_U))\\ &= \Re(G_W) - \Im(G_W).\end{aligned}$$

We now turn to the case where $x = x_j$ or $x = y_j$ for some j with $1 \le j \le m$. Without loss of generality, let us assume that $x = x_1$. We write y for y_1, U for $W \backslash \{x, y\}$, U_x for $U \cup \{x\}$ $(= W \backslash \{y\})$, and U_y for $U \cup \{y\}$ $(= W \backslash \{x\})$. In the same way as before, we have

$$\sum_{V \subseteq W} f(V) = \sum_{V \subseteq U_y} f(V) + \sum_{V \subseteq U_y} f(V \cup \{x\})$$

and

$$\sum_{V \subseteq U_y} f(V) = \Re(G_{U_y}) + \Im(G_{U_y}) = \Re(G_U) + \Im(G_U) + F(y)(\Re(G_U) - \Im(G_U)),$$

since $G_{U_y} = (1 + iF(y))G_U$.

By Propositions 3.1 and 3.2, we know that

$$f(V \cup \{x\}) = \begin{cases}(-1)^{|V|} f(V) F(x) & \text{if } y \notin V,\\ (-1)^{|V|-1} f(V) F(x) & \text{if } y \in V.\end{cases}$$

So we have

$$\begin{aligned}\sum_{V\subseteq U_y} f(V\cup\{x\}) &= \sum_{\substack{V\subseteq U_y\\ y\notin V}} (-1)^{|V|} f(V)F(x) + \sum_{\substack{V\subseteq U_y\\ y\in V}} (-1)^{|V|-1} f(V)F(x)\\ &= F(x)\sum_{V\subseteq U}(-1)^{|V|}f(V) + F(x)\sum_{V\subseteq U}(-1)^{|V|}f(V\cup\{y\})\\ &= F(x)(\Re(G_U) - \Im(G_U)) + F(x)\sum_{V\subseteq U}(-1)^{|V|}f(V\cup\{y\}).\end{aligned}$$

Applying Proposition 3.1 again, since $\bar{f}(\{y,z\}) = -1$ for all $z \in U$, we have

$$\sum_{V\subseteq U}(-1)^{|V|}f(V\cup\{y\}) = \sum_{V\subseteq U} f(V)F(y) = F(y)(\Re(G_U) + \Im(G_U)).$$

So

$$\sum_{V\subseteq U_y} f(V\cup\{x\}) = F(x)(\Re(G_U) - \Im(G_U)) + F(x)F(y)(\Re(G_U) + \Im(G_U))$$

and, therefore,

$$\begin{aligned}\sum_{V\subseteq W} f(V) &= \Re(G_U) + \Im(G_U) + (F(x) + F(y))(\Re(G_U) - \Im(G_U))\\ &\quad + F(x)F(y)(\Re(G_U) + \Im(G_U))\\ &= \Re(G_W) + \Im(G_W),\end{aligned}$$

since, in this case, $G_W = (1 + F(x)F(y) + i(F(x) + F(y)))G_U$.

Similarly,

$$\sum_{V\subseteq W}(-1)^{|V|}f(V) = \sum_{V\subseteq U_y}(-1)^{|V|}f(V) - \sum_{V\subseteq U_y}(-1)^{|V|}f(V\cup\{x\})$$

and

$$\begin{aligned}\sum_{V\subseteq U_y}(-1)^{|V|}f(V) &= \Re(G_{U_y}) - \Im(G_{U_y})\\ &= \Re(G_U) - \Im(G_U) - F(y)(\Re(G_U) + \Im(G_U)),\end{aligned}$$

since $G_{U_y} = (1 + iF(y))G_U$.

We also have, by Propositions 3.1 and 3.2,

$$\begin{aligned}\sum_{V\subseteq U_y}(-1)^{|V|}f(V\cup\{x\}) &= \sum_{\substack{V\subseteq U_y\\ y\notin V}} f(V)F(x) - \sum_{\substack{V\subseteq U_y\\ y\in V}} f(V)F(x)\\ &= F(x)\sum_{V\subseteq U} f(V) - F(x)\sum_{V\subseteq U} f(V\cup\{y\})\\ &= F(x)(\Re(G_U) + \Im(G_U)) - F(x)\sum_{V\subseteq U} f(V\cup\{y\}).\end{aligned}$$

Applying Proposition 3.1 again, since $\bar{f}(\{y,z\}) = -1$ for all $z \in U$, we have

$$\begin{aligned}\sum_{V\subseteq U} f(V\cup\{y\}) &= \sum_{V\subseteq U}(-1)^{|V|}f(V)F(y)\\ &= F(y)(\Re(G_U) - \Im(G_U)).\end{aligned}$$

So

$$\sum_{V\subseteq U_y}(-1)^{|V|}f(V\cup\{x\}) = F(x)(\Re(G_U) + \Im(G_U)) - F(x)F(y)(\Re(G_U) - \Im(G_U))$$

and, therefore,

$$\begin{aligned}\sum_{V\subseteq W}(-1)^{|V|}f(V) &= \Re(G_U)-\Im(G_U)-(F(x)+F(y))(\Re(G_U)+\Im(G_U))\\&\quad+F(x)F(y)(\Re(G_U)-\Im(G_U))\\&=\Re(G_W)-\Im(G_W),\end{aligned}$$

since, in this case, $G_W = (1 + F(x)F(y) + i(F(x) + F(y)))G_U$. □

Corollary 3.4. *Suppose that f belongs to $A_W(n, m)$. Suppose further that, for some j, $1 \le j \le m$, we have $F(x_j) = -F(y_j)$. Then $\sum_{V\subseteq W} f(V) = 0$.*

Proof. Suppose, without loss of generality, that $F(x_1) = -F(y_1)$. Then by Theorem 3.3, $\sum_{V\subseteq W} f(V) = \Re(G) + \Im(G)$, where

$$G = f(\varnothing)\prod_{j=1}^{m}(1 + F(x_j)F(y_j) + i(F(x_j) + F(y_j)))\prod_{j=2m+1}^{|W|}(1 + iF(x_j)).$$

However, $1 + F(x_1)F(y_1) + i(F(x_1) + F(y_1)) = 0$, since $F(x_1) = -F(y_1)$, so $G = 0$. Hence $\sum_{V\subseteq W} f(V) = 0$. □

Corollary 3.5. *Suppose that f belongs to $C_W(n, m, r, t, q)$. Write k for $|W|$; then*

$$\sum_{V\subseteq W} f(V) = \begin{cases} f(\varnothing)(-1)^{q/4}2^{(m+k)/2}, & q \equiv 0 \pmod 4,\\ f(\varnothing)(-1)^{(q-1)/4}2^{(m+k+1)/2}, & q \equiv 1 \pmod 4,\\ f(\varnothing)(-1)^{(q-2)/4}2^{(m+k)/2}, & q \equiv 2 \pmod 4,\\ 0, & q \equiv 3 \pmod 4.\end{cases}$$

Proof. Let G be defined as above; we examine each term in turn. Now if $1 \le j \le m$, then

$$(1 + F(x_j)F(y_j) + iF(x_j) + iF(y_j)) = \begin{cases} 2(1+i) & \text{if } F(x_j) = 1,\\ 2(1-i) & \text{if } F(x_j) = -1\end{cases}$$

and if $2m + 1 \le n$, then

$$(1 + iF(x_j)) = \begin{cases} 1+i & \text{if } F(x_j) = 1,\\ 1-i & \text{if } F(F_j) = -1.\end{cases}$$

So

$$\begin{aligned}G &= f(\varnothing)2^r(1+i)^r 2^{m-r}(1-i)^{m-r}(1+i)^t(1-i)^{k-2m-t}\\&= f(\varnothing)2^m(1+i)^{r+t}(1-i)^{k-m-r-t}\\&= f(\varnothing)2^{k-r-t}(1+i)^{2r+2t+m-k}.\end{aligned}$$

Now if $0 \le b \le 3$, then

$$\Re(1+i)^{4a+b} + \Im(1+i)^{4a+b} = \begin{cases}(-4)^a & \text{if } b = 0,\\ 2(-4)^a & \text{if } b = 1,\\ 2(-4)^a & \text{if } b = 2,\\ 0 & \text{if } b = 3.\end{cases}$$

Now $2r + 2t + m - k = q$, and so

$$\sum_{V \subseteq W} f(V) = \begin{cases} f(\varnothing)2^{k-r-t}(-4)^{q/4} & \text{if} \quad q \equiv 0 \pmod 4, \\ f(\varnothing)2^{k-r-t+1}(-4)^{(q-1)/4} & \text{if} \quad q \equiv 1 \pmod 4, \\ f(\varnothing)2^{k-r-t+1}(-4)^{(q-2)/4} & \text{if} \quad q \equiv 2 \pmod 4, \\ 0 & \text{if} \quad q \equiv 3 \pmod 4, \end{cases}$$

$$= \begin{cases} f(\varnothing)(-1)^{q/4}2^{(m+k)/2} & \text{if} \quad q \equiv 0 \pmod 4, \\ f(\varnothing)(-1)^{(q-1)/4}2^{(m+k+1)/2} & \text{if} \quad q \equiv 1 \pmod 4, \\ f(\varnothing)(-1)^{(q-2)/4}2^{(m+k)/2} & \text{if} \quad q \equiv 2 \pmod 4, \\ 0 & \text{if} \quad q \equiv 3 \pmod 4) \end{cases}$$

as required. □

4. Balance

We use the results of the preceding section to obtain necessary and sufficient conditions for a function satisfying the SAC of order $(n - 3)$ to be balanced.

Theorem 4.1. *Suppose that $f \in \mathscr{B}_{\mathscr{S}}$ satisfies the SAC of order $(n - 3)$. Then f is balanced if and only if either*

(i) *there exist x and y with $\bar{f}(\{x, y\}) = 1$ and $F(x) = -F(y)$ or*
(ii) *f belongs to $C(n, m, r, t, q)$ and $q \equiv 3 \pmod 4$.*

Proof. Since f satisfies the SAC of order $(n - 3)$, we know that either (i) holds or there exist m, r, t, and q such that f belongs to $C(n, m, r, t, q)$. We recall that f is balanced if and only if $\sum_{V \subseteq \mathscr{S}} f(V) = 0$. If (i) holds, then, by Corollary 3.4, we know that $\sum_{V \subseteq \mathscr{S}} f(V) = 0$. If (ii) holds, then, by Corollary 3.5, we have

$$\sum_{V \subseteq \mathscr{S}} f(V) = \begin{cases} f(\varnothing)(-1)^{q/4}2^{(m+n)/2} & \text{if} \quad q \equiv 0 \pmod 4, \\ f(\varnothing)(-1)^{(q-1)/4}2^{(m+n+1)/2} & \text{if} \quad q \equiv 1 \pmod 4, \\ f(\varnothing)(-1)^{(q-2)/4}2^{(m+n)/2} & \text{if} \quad q \equiv 2 \pmod 4, \\ 0 & \text{if} \quad q \equiv 3 \pmod 4. \end{cases}$$

So, in this case, f is balanced if and only if $q \equiv 3 \pmod 4$, since $f(\varnothing) = +1$ or -1. □

Theorem 4.2. *The number of functions $f \in \mathscr{B}_{\mathscr{S}}$ which are balanced and satisfy the SAC of order $(n - 3)$ is*

$$\sum_{0 \leq 2m \leq n} \frac{n!}{(n-2m)!\, m!} 2^{n-2m+1}(2^m - 1) + \sum_{\substack{0 \leq 2m \leq n \\ m \not\equiv n \pmod 2}} \frac{n!}{(n-2m)!\, m!} 2^{n-2m}.$$

Proof. By Lemma 2.3.8, the number of functions satisfying condition (i) of Theorem 4.1 is

$$\sum_{2\le 2p\le n}\ \sum_{2p\le 2m\le n}\frac{n!}{(n-2m)!\,m!}2^{n-2m+1}\binom{m}{p}$$
$$=\sum_{2\le 2m\le n}\frac{n!}{(n-2m)!\,m!}2^{n-2m+1}\sum_{1\le p\le m}\binom{m}{p}$$
$$=\sum_{2\le 2m\le n}\frac{n!}{(n-2m)!\,m!}2^{n-2m+1}(2^m-1)$$
$$=\sum_{0\le 2m\le n}\frac{n!}{(n-2m)!\,m!}2^{n-2m+1}(2^m-1).$$

By Lemma 2.3.7, the number of functions satisfying condition (ii) of Theorem 4.1 is

$$\sum_{0\le 2m\le n}\ \sum_{0\le r\le m}\ \sum_{\substack{0\le t\le n-2m\\ q\equiv 3 \pmod 4}}\frac{2n!}{(n-2m)!\,m!\,2^m}\binom{m}{r}\binom{n-2m}{t}.$$

Now if $m\equiv n \pmod 2$, then $q\not\equiv 3 \pmod 4$, while if $m\not\equiv n \pmod 2$, then $q\equiv 3 \pmod 4$ if and only if $t\equiv \frac{1}{2}(3-m+n-2r) \pmod 2$. So the number of functions satisfying (ii) is

$$\sum_{\substack{0\le 2m\le n\\ m\not\equiv n \pmod 2}}\frac{2n!}{(n-2m)!\,m!\,2^m}\sum_{0\le r\le m}\binom{m}{r}\sum_{\substack{0\le t\le n-2m\\ t\equiv(3-m+n-2r)/2 \pmod 2}}\binom{n-2m}{t}.$$

We shall need the well-known combinatorial identity

$$\sum_{\substack{0\le j\le N\\ j\equiv 1 \pmod 2}}\binom{N}{j}=\sum_{\substack{0\le j\le N\\ j\equiv 0 \pmod 2}}\binom{N}{j}=\tfrac{1}{2}2^N$$

if $N>0$. Applying this to the sum over t, we see that if $2m<n$, then

$$\sum_{\substack{0\le t\le n-2m\\ t\equiv(3-m+n-2r)/2 \pmod 2}}\binom{n-2m}{t}=\tfrac{1}{2}2^{n-2m}.$$

In this case, therefore, we deduce that

$$\sum_{0\le r\le m}\binom{m}{r}\sum_{\substack{0\le t\le n-2m\\ q\equiv 3 \pmod 4}}\binom{n-2m}{t}=2^m\cdot\tfrac{1}{2}2^{n-2m}=2^{n-m-1}.$$

If $n=2m$, then t must be zero, and so $q\equiv 3 \pmod 4$ if and only if $r\equiv\frac{1}{2}(3+m) \pmod 2$. In this case, therefore, we have

$$\sum_{0\le r\le m}\binom{m}{r}\sum_{\substack{0\le t\le n-2m\\ q\equiv 3 \pmod 4}}\binom{n-2m}{t}=\sum_{0\le r\le m}\binom{m}{r}\sum_{\substack{t=0\\ q\equiv 3 \pmod 4}}\binom{0}{t}$$
$$=\sum_{\substack{0\le r\le m\\ q\equiv 3 \pmod 4}}\binom{m}{r}$$

$$= \sum_{\substack{0\le r\le m\\ r\equiv(3+m)/2 \ (\mathrm{mod}\ 2)}} \binom{m}{r}$$
$$= 2^{m-1}.$$

However, since $n = 2m$, this is the same as 2^{n-m-1}. Hence the sum over r and t is the same in both cases. So the number of functions satisfying (ii) is

$$\sum_{\substack{0\le 2m\le n\\ m\not\equiv n \ (\mathrm{mod}\ 2)}} \frac{2n!}{(n-2m)!\,m!\,2^m} \sum_{0\le r\le m} \binom{m}{r} \sum_{\substack{0\le t\le n-2m\\ q\equiv 3 \ (\mathrm{mod}\ 4)}} \binom{n-2m}{t}$$
$$= \sum_{\substack{0\le 2m\le n\\ m\not\equiv n \ (\mathrm{mod}\ 2)}} \frac{2n!}{(n-2m)!\,m!\,2^m} 2^{n-m-1}$$
$$= \sum_{\substack{0\le 2m\le n\\ m\not\equiv n \ (\mathrm{mod}\ 2)}} \frac{n!}{(n-2m)!\,m!} 2^{n-2m}.$$

□

5. Correlation Immunity

We now obtain necessary and sufficient conditions for a function satisfying the SAC of order $(n - 3)$ to be correlation immune.

Proposition 5.1. *Suppose $f \in \mathscr{B}_{\mathscr{S}}$ satisfies the SAC of order $(n - 3)$. Suppose there are exactly p pairs (x_j, y_j) such that $\bar{f}(\{x_j, y_j\}) = 1$ and $F(x_j) = -F(y_j)$. Then f is exactly $(p - 1)$*th*-order correlation immune.*

Proof. By Corollary 3.4, $X(W) = 0$ whenever there exists j, $1 \le j \le p$, with x_j, $y_j \in W$. Any W with $|W| > n - p$ must contain at least one such pair, so $X(W) = 0$ for any such W (including $\mathscr{S}$). By Lemma 2.2.6, therefore, f is at least $(p - 1)$th-order correlation immune.

Let $U = \mathscr{S}\backslash\{x_1, y_1, y_2, \ldots, y_p\}$. Then U contains no pairs (x_j, y_j), and so $G_U \ne 0$. Let us write x for x_1 and y for y_1, and let $U_x = U \cup \{x\}$ and $U_y = U \cup \{y\}$. Since $F(x) = -F(y)$, we may assume without loss of generality that $F(x) = 1$ and $F(y) = -1$. Now

$$G_{U_x} = (1 + iF(x))G_U = (1 + i)G_U,$$

so

$$X(U_x) = \mathfrak{R}(G_U) + \mathfrak{I}(G_U) + \mathfrak{R}(G_U) - \mathfrak{I}(G_U) = 2\mathfrak{R}(G_U).$$

On the other hand,

$$G_{U_y} = (1 + iF(y))G_U = (1 - i)G_U,$$

so

$$X(U_y) = \mathfrak{R}(G_U) + \mathfrak{I}(G_U) - \mathfrak{R}(G_U) + \mathfrak{I}(G_U) = 2\mathfrak{I}(G_U).$$

If f is pth-order correlation immune, then $X(U_x) = X(U_y) = 0$. This forces $G_U = 0$, which is not true. Hence f is not pth-order correlation immune. □

We now prove some results on the values of $X(W)$. In the four lemmas which follow, we assume that f belongs to $C_{W_j}(n, m_j, r_j, t_j, q_j)$ for $j = 1, 2$ and that $|W_j| = k_j$ for $j = 1, 2$. We calculate the relationship between $X(W_1)$ and $X(W_2)$ for various values of W_1 and W_2. The proofs of these results rely heavily on Corollary 3.5.

Lemma 5.2. *Suppose that $W_1 \subseteq \mathscr{S}$ and that $x, y \in W_1$ are such that $\bar{f}(\{x, y\}) = +1$. Let $W_2 = W_1 \backslash \{x\}$, then $X(W_2) = \frac{1}{2}X(W_1)$.*

Proof. Suppose first that $F(x) = +1$. Then

$$k_2 = k_1 - 1, \qquad m_2 = m_1 - 1, \qquad r_2 = r_1 - 1, \qquad t_2 = t_1 + 1, \qquad q_2 = q_1,$$

and $m_2 + k_2 = m_1 + k_1 - 2$, so $X(W_2) = \frac{1}{2}X(W_1)$. Suppose now that $F(x) = -1$. Then

$$k_2 = k_1 - 1, \qquad m_2 = m_1 - 1, \qquad r_2 = r_1, \qquad t_2 = t_1, \qquad q_2 = q_1,$$

and $m_2 + k_2 = m_1 + k_1 - 2$, so $X(W_2) = \frac{1}{2}X(W_1)$. □

Lemma 5.3. *Suppose that $W_1 \subseteq \mathscr{S}$ and that $x \in W_1$ is such that $\bar{f}(\{x, y\}) = -1$ for all $y \in W_1$, and that $F(x) = +1$. Let $W_2 = W_1 \backslash \{x\}$. Then*

$$X(W_1)/X(W_2) = \begin{cases} \infty, & q_1 \equiv 0 \pmod 4, \\ 2, & q_1 \equiv 1 \pmod 4, \\ 1, & q_1 \equiv 2 \pmod 4, \\ 0, & q_1 \equiv 3 \pmod 4. \end{cases}$$

Proof. By Corollary 3.5,

$$X(W_1) = \begin{cases} f(\varnothing)(-1)^{q_1/4}2^{(m_1+k_1)/2}, & q_1 \equiv 0 \pmod 4, \\ f(\varnothing)(-1)^{(q_1-1)/4}2^{(m_1+k_1+1)/2}, & q_1 \equiv 1 \pmod 4, \\ f(\varnothing)(-1)^{(q_1-2)/4}2^{(m_1+k_1)/2}, & q_1 \equiv 2 \pmod 4, \\ 0, & q_1 \equiv 3 \pmod 4. \end{cases}$$

Since $F(x) = 1$, we have

$$k_2 = k_1 - 1, \qquad m_2 = m_1, \qquad r_2 = r_1, \qquad t_2 = t_1 - 1, \qquad q_2 = q_1 - 1,$$

and therefore

$$X(W_2) = \begin{cases} f(\varnothing)(-1)^{q_2/4}2^{(m_2+k_2)/2}, & q_2 \equiv 0 \pmod 4, \\ f(\varnothing)(-1)^{(q_2-1)/4}2^{(m_2+k_2+1)/2}, & q_2 \equiv 1 \pmod 4, \\ f(\varnothing)(-1)^{(q_2-2)/4}2^{(m_2+k_2)/2}, & q_2 \equiv 2 \pmod 4, \\ 0, & q_2 \equiv 3 \pmod 4, \end{cases}$$

$$= \begin{cases} f(\varnothing)(-1)^{(q_1-1)/4}2^{(m_1+k_1-1)/2}, & q_2 \equiv 0 \pmod 4, \\ f(\varnothing)(-1)^{(q_1-2)/4}2^{(m_1+k_1)/2}, & q_2 \equiv 1 \pmod 4, \\ f(\varnothing)(-1)^{(q_1-3)/4}2^{(m_1+k_1-1)/2}, & q_2 \equiv 2 \pmod 4, \\ 0, & q_2 \equiv 3 \pmod 4, \end{cases}$$

$$= \begin{cases} 0, & q_1 \equiv 0 \pmod 4, \\ f(\varnothing)(-1)^{(q_1-1)/4}2^{(m_1+k_1-1)/2}, & q_1 \equiv 1 \pmod 4, \\ f(\varnothing)(-1)^{(q_1-2)/4}2^{(m_1+k_1)/2}, & q_1 \equiv 2 \pmod 4, \\ f(\varnothing)(-1)^{(q_1-3)/4}2^{(m_1+k_1-1)/2}, & q_1 \equiv 3 \pmod 4. \end{cases}$$

Hence

$$X(W_1)/X(W_2) = \begin{cases} \infty, & q_1 \equiv 0 \pmod 4, \\ 2, & q_1 \equiv 1 \pmod 4, \\ 1, & q_1 \equiv 2 \pmod 4, \\ 0, & q_1 \equiv 3 \pmod 4. \end{cases}$$ □

Lemma 5.4. *Suppose that $W_1 \subseteq \mathscr{S}$ and that $x \in W_1$ is such that $\bar{f}(\{x, y\}) = -1$ for all $y \in W_1$, and that $F(x) = -1$. Let $W_2 = W_1 \backslash \{x\}$. Then*

$$X(W_1)/X(W_2) = \begin{cases} 1, & q_1 \equiv 0 \pmod 4, \\ 2, & q_1 \equiv 1 \pmod 4, \\ \infty, & q_1 \equiv 2 \pmod 4, \\ 0, & q_1 \equiv 3 \pmod 4. \end{cases}$$

Proof. This may be proved in a similar way to Lemma 5.3, using Corollary 3.5, and noting that

$$k_2 = k_1 - 1, \qquad m_2 = m_1, \qquad r_2 = r_1, \qquad t_2 = t_1, \qquad q_2 = q_1 + 1.$$ □

Corollary 5.5. *Suppose that $W_1 \subseteq \mathscr{S}$ and that $x \in W_1$ is such that $\bar{f}(\{x, y\}) = -1$ for all $y \in W_1$. Let $W_2 = W_1 \backslash \{x\}$. Then*

$$X(W_2) = \tfrac{1}{2}X(W_1) \qquad \textit{if and only if} \quad q_1 \equiv 1 \pmod 4.$$

Lemma 5.6. *Suppose that $W_1 \subseteq \mathscr{S}$ and that $x, y \in W_1$ are such that $\bar{f}(\{x, y\}) = +1$, and $F(x) = F(y) = +1$. Let $W_2 = W_1 \backslash \{x, y\}$, then*

$$X(W_1)/X(W_2) = \begin{cases} \infty, & q_1 \equiv 0 \pmod 4, \\ 2^2, & q_1 \equiv 1 \pmod 4, \\ 2, & q_1 \equiv 2 \pmod 4, \\ 0, & q_1 \equiv 3 \pmod 4. \end{cases}$$

Proof. This may be proved in a similar way to Lemma 5.3, using Corollary 3.5, and noting that

$$k_2 = k_1 - 2, \qquad m_2 = m_1 - 1, \qquad r_2 = r_1 - 1, \qquad t_2 = t_1, \qquad q_2 = q_1 - 1. \quad \square$$

Lemma 5.7. *Suppose that $W_1 \subseteq \mathscr{S}$ and that $x, y \in W_1$ are such that $\bar{f}(\{x, y\}) = +1$, and $F(x) = F(y) = -1$. Let $W_2 = W_1 \backslash \{x, y\}$, then*

$$X(W_1)/X(W_2) = \begin{cases} 2, & q_1 \equiv 0 \pmod 4, \\ 2^2, & q_1 \equiv 1 \pmod 4, \\ \infty, & q_1 \equiv 2 \pmod 4, \\ 0, & q_1 \equiv 3 \pmod 4. \end{cases}$$

Proof. This may be proved in a similar way to Lemma 5.3, using Corollary 3.5, and noting that

$$k_2 = k_1 - 2, \qquad m_2 = m_1 - 1, \qquad r_2 = r_1, \qquad t_2 = t_1, \qquad q_2 = q_1 + 1. \quad \square$$

Corollary 5.8. *Suppose that $W_1 \subseteq \mathscr{S}$ and that $x, y \in W_1$ are such that $\bar{f}(\{x, y\}) = +1$. Let $W_2 = W_1 \backslash \{x, y\}$, then*

$$X(W_2) = \frac{1}{2^2} X(W_1) \qquad \textit{if and only if} \quad q_1 \equiv 1 \pmod 4.$$

Proposition 5.9. *Suppose that f belongs to $C(n, m, r, t, q)$. If $2m < n$ and $q \not\equiv 1$ (mod 4), then f is not correlation immune.*

Proof. We must find W with $|W| = n - 1$, and $X(W) \neq \frac{1}{2}X(\mathscr{S})$. Let $W = \mathscr{S} \backslash \{x_n\}$. Since $2m < n$, we may apply Corollary 5.5, with $W_1 = \mathscr{S}$. Since $q \not\equiv 1$ (mod 4), we deduce that $X(W) \neq \frac{1}{2}X(\mathscr{S})$. So f is not correlation immune. □

Proposition 5.10. *Suppose that f belongs to $C(2m, m, r, 0, q)$. If $q \not\equiv 1$ (mod 4), then f is exactly first-order correlation immune.*

Proof. We show first that if $|W| = n - 1$, then $X(W) = \frac{1}{2}X(\mathscr{S})$. Let W be such that $|W| = n - 1$. Then either $W = \mathscr{S} \backslash \{x_j\}$ for some j or $W = \mathscr{S} \backslash \{y_j\}$ for some j. By Lemma 5.2, therefore, with $W_1 = \mathscr{S}$, $X(W) = \frac{1}{2}X(\mathscr{S})$. So we have shown that f is at least first-order correlation immune. We now need to find W with $|W| = n - 2$, and $X(W) \neq (1/2^2)X(\mathscr{S})$. We take $W = \mathscr{S} \backslash \{x_1, y_1\}$. Then we may use Corollary 5.8, with $W_1 = \mathscr{S}$. Since $q \not\equiv 1$ (mod 4), $X(W) \neq (1/2^2)X(\mathscr{S})$. So f is not second-order correlation immune.

We turn now to the case where $q \equiv 1$ (mod 4).

Lemma 5.11. *Suppose that f belongs to $C(n, m, r, t, q)$ and that $q \equiv 1$ (mod 4). Then f is first-order correlation immune.*

Proof. We must show that $X(W) = \frac{1}{2}X(\mathscr{S})$ for any W with $|W| = n - 1$. Choose any such W. Then we have the following possibilities for W:

$$\begin{array}{lll} W = \mathscr{S}\backslash\{x_j\} & \text{for some } j, \quad 1 \le j \le m, & \text{or} \\ W = \mathscr{S}\backslash\{y_j\} & \text{for some } j, \quad 1 \le j \le m, & \text{or} \\ W = \mathscr{S}\backslash\{x_j\} & \text{for some } j, \quad 2m + 1 \le j \le n. & \end{array}$$

In either of the first two cases, we may apply Lemma 5.2, to obtain $X(W) = \frac{1}{2}X(\mathscr{S})$, while in the third case we may apply Corollary 5.5 to obtain $X(W) = \frac{1}{2}X(\mathscr{S})$. Hence f is first-order correlation immune. □

Lemma 5.12. *Suppose that f belongs to $C(n, m, r, t, q)$ and that $q \equiv 1 \pmod 4$. Then f is second-order correlation immune if and only if $2m \ge n - 1$.*

Proof. We already know that f is first-order correlation immune. We must show that $X(W) = (1/2^2)X(\mathscr{S})$ for any W with $|W| = n - 2$. Choose any such W. Then we have the following possibilities for W:

$$\begin{array}{lll} W = \mathscr{S}\backslash\{x_j, y_k\}, & j \ne k, & 1 \le j, k \le m, \\ W = \mathscr{S}\backslash\{x_j, x_k\}, & j \ne k, & 1 \le j, k \le m, \\ W = \mathscr{S}\backslash\{y_j, y_k\}, & j \ne k, & 1 \le j, k \le m, \\ W = \mathscr{S}\backslash\{x_j, y_j\}, & 1 \le j \le m, & \\ W = \mathscr{S}\backslash\{x_j, x_k\}, & 1 \le j \le m, & 2m + 1 \le k \le n, \\ W = \mathscr{S}\backslash\{y_j, x_k\}, & 1 \le j \le m, & 2m + 1 \le k \le n, \\ W = \mathscr{S}\backslash\{x_j, x_k\}, & j \ne k, & 2m + 1 \le j, k \le n. \end{array}$$

In the first case, we may first apply Lemma 5.2 with $W_1 = \mathscr{S}$ and $W_2 = \mathscr{S}\backslash\{x_j\}$, and then apply Lemma 5.2 again with $W_1 = \mathscr{S}\backslash\{x_j\}$ and $W_2 = W$ to obtain $X(W) = \frac{1}{2}X(\mathscr{S}\backslash\{x_j\}) = (1/2^2)X(\mathscr{S})$ as required. This may also be done in the second and third cases. In the fourth case, we may apply Corollary 5.8, with $W_1 = \mathscr{S}$, to obtain $X(W) = (1/2^2)X(\mathscr{S})$, as required. In the fifth and sixth cases, we may proceed in a similar manner as in the first case, applying Lemma 5.2, and then Corollary 5.5 to obtain the result (noting that q is unchanged after applying Lemma 5.2). When we come to the seventh case, however, we see that if we apply Corollary 5.5 with $W_1 = \mathscr{S}$ and $W_2 = \mathscr{S}\backslash\{x_j\}$, we obtain $X(W_2) = \frac{1}{2}X(W_1)$, but when we come to apply Corollary 5.5 again with $W_1 = \mathscr{S}\backslash\{x_j\}$ and $W_2 = W$, we now have $q_1 \equiv 0 \pmod 4$ or $q_1 \equiv 2 \pmod 4$, according as $j \le 2m_1 + t_1$ or $j > 2m_1 + t_1$, and so $X(W) \ne (1/2^2)X(\mathscr{S})$ in this case. This case can only occur when $2m + 1 < n$, so f is second-order correlation immune if and only if $2m \ge n - 1$. □

Lemma 5.13. *Suppose that f belongs to $C(n, m, r, t, q)$ and that $q \equiv 1 \pmod 4$. Then f is third-order correlation immune if and only if $2m = n$.*

Proof. We already know that f is second-order correlation immune, since $2m \ge n - 1$. We must show that $X(W) = (1/2^3)X(\mathscr{S})$ for any W with $|W| = n - 3$. Let W be such that $|W| = n - 3$. If $W = \mathscr{S}\backslash\{x_j, x_k, x_l\}$, with j, k, and l all different, and

$1 \le j, k, l \le m$, then we may apply Lemma 5.2 three times to obtain the result. The same method will also work in the cases $W = \mathcal{S}\backslash\{x_j, x_k, y_l\}$, $W = \mathcal{S}\backslash\{x_j, y_k, y_l\}$, and $W = \mathcal{S}\backslash\{y_j, y_k, y_l\}$. The cases $W = \mathcal{S}\backslash\{x_j, y_j, x_k\}$ and $W = \mathcal{S}\backslash\{x_j, y_j, y_k\}$, where $1 \le j, k \le m$, may each be dealt with using first Corollary 5.8 and then Lemma 5.2. This means that when $2m = n$, f is third-order correlation immune.

When, however, $2m < n$, we must consider the case $W = \mathcal{S}\backslash\{x_1, y_1, x_n\}$. We apply Corollary 5.8 with $W_1 = \mathcal{S}$ and $W_2 = \mathcal{S}\backslash\{x_1, y_1\}$, and then apply Corollary 5.5 with $W_1 = \mathcal{S}\backslash\{x_1, y_1\}$ and $W_2 = W$. However, this time either $q_1 \equiv 0 \pmod 4$ or $q_1 \equiv 2 \pmod 4$ according as $r > 0$ or $r = 0$. So in this case, f is not third-order correlation immune.

Lemma 5.14. *Suppose that f belongs to $C(n, m, r, t, q)$ and that $q \equiv 1 \pmod 4$. Then f is not fourth-order correlation immune.*

Proof. We shall produce W with $X(W) \neq (1/2^4)X(\mathcal{S})$. We take

$$W = \mathcal{S}\backslash\{x_1, y_1, x_2, y_2\}.$$

Let us also denote $\mathcal{S}\backslash\{x_1, y_1\}$ by U. Then, by Corollary 5.8, we see that $X(U) = (1/2^2)X(\mathcal{S})$, since $q_1 \equiv 1 \pmod 4$. We now apply Corollary 5.8 with $W_1 = U$. This time, however, we have $q_1 \equiv 0 \pmod 4$ or $q_1 \equiv 2 \pmod 4$ (according as $r \ge 1$ or not), so $X(W) \neq (1/2^2)X(U)$, and therefore $X(W) \neq (1/2^4)X(\mathcal{S})$. Hence f is not fourth-order correlation immune.

We thus have, combining the preceding four lemmas,

Corollary 5.15. *Suppose that f belongs to $C(n, m, r, t, q)$ and that $q \equiv 1 \pmod 4$. Then*

(i) *if $2m < n - 1$, then f is exactly first-order correlation immune,*
(ii) *if $2m = n - 1$, then f is exactly second-order correlation immune, and*
(iii) *if $2m = n$, then f is exactly third-order correlation immune.*

Combining all the results of this section, we have the following theorems and corollaries.

Theorem 5.16. *If $f \in \mathcal{B}_{\mathcal{S}}$ satisfies the SAC of order $(n - 3)$, then f is not correlation immune if and only if either*

(i) *there is exactly one pair (x, y) with $\bar{f}(\{x, y\}) = 1$ and $F(x) = -F(y)$ or*
(ii) *f belongs to $C(n, m, r, t, q)$ and $2m < n$ and $q \not\equiv 1 \pmod 4$.*

Corollary 5.17. *The number of functions satisfying the SAC of order $(n - 3)$ which are not correlation immune is*

$$\sum_{2 \le 2m \le n} \frac{n!}{(n-2m)!\,(m-1)!} 2^{n-2m+1} + \sum_{\substack{0 \le 2m < n \\ m = n \ (\mathrm{mod}\ 4)}} \frac{n!}{(n-2m)!\, m!} 2^{n-2m+1}$$

$$+ \sum_{\substack{0 \le 2m < n \\ m \not\equiv n \ (\mathrm{mod}\ 4)}} \frac{n!}{(n-2m)!\, m!} 2^{n-2m}.$$

Proof. By Lemma 2.3.8, the number of functions satisfying condition (i) of Theorem 5.16 is

$$\sum_{2\leq 2m\leq n}\frac{n!}{(n-2m)!\,m!}2^{n-2m+1}m=\sum_{2\leq 2m\leq n}\frac{n!}{(n-2m)!\,(m-1)!}2^{n-2m+1}.$$

By Lemma 2.3.7, the number of functions satisfying condition (ii) of Theorem 5.16 is

$$\sum_{0\leq 2m<n}\ \sum_{0\leq r\leq m}\ \sum_{\substack{0\leq t\leq n-2m\\ q\not\equiv 1\ (\mathrm{mod}\ 4)}}\frac{2n!}{(n-2m)!\,m!\,2^m}\binom{m}{r}\binom{n-2m}{t}.$$

If $m\equiv n\ (\mathrm{mod}\ 2)$, then $q\not\equiv 1\ (\mathrm{mod}\ 4)$, while if $m\not\equiv n\ (\mathrm{mod}\ 4)$, then $q\not\equiv 1\ (\mathrm{mod}\ 4)$ if and only if $t\equiv\frac{1}{2}(3-m+n-2r)\ (\mathrm{mod}\ 2)$. So the number of functions satisfying (ii) is

$$\begin{aligned}
&\sum_{\substack{0\leq 2m<n\\ m\equiv n\ (\mathrm{mod}\ 4)}}\ \sum_{0\leq r\leq m}\ \sum_{0\leq t\leq n-2m}\frac{2n!}{(n-2m)!\,m!\,2^n}\binom{m}{r}\binom{n-2m}{t}\\
&\quad+\sum_{\substack{0\leq 2m<n\\ m\not\equiv n\ (\mathrm{mod}\ 4)}}\ \sum_{0\leq r\leq m}\ \sum_{\substack{0\leq t\leq n-2m\\ q\equiv 3\ (\mathrm{mod}\ 4)}}\frac{2n!}{(n-2m)!\,m!\,2^m}\binom{m}{r}\binom{n-2m}{t}\\
&=\sum_{\substack{0\leq 2m<n\\ m\equiv n\ (\mathrm{mod}\ 4)}}\frac{2n!}{(n-2m)!\,m!\,2^m}2^{n-m}+\sum_{\substack{0\leq 2m<n\\ m\not\equiv n\ (\mathrm{mod}\ 4)}}\frac{2n!}{(n-2m)!\,m!\,2^m}2^{n-m-1}\\
&=\sum_{\substack{0\leq 2m<n\\ m\equiv n\ (\mathrm{mod}\ 4)}}\frac{n!}{(n-2m)!\,m!}2^{n-2m+1}+\sum_{\substack{0\leq 2m<n\\ m\not\equiv n\ (\mathrm{mod}\ 4)}}\frac{n!}{(n-2m)!\,m!}2^{n-2m}.
\end{aligned}$$

□

Theorem 5.18. *If $f\in\mathscr{B}_{\mathscr{S}}$ satisfies the SAC of order $(n-3)$, then f is exactly first-order correlation immune if and only if one of the following holds:*

(i) *there are exactly two pairs (x,y) with $\bar{f}(\{x,y\})=1$ and $F(x)=-F(y)$ or*
(ii) *f belongs to $C(n,m,r,t,q)$ and $2m=n$ and $q\not\equiv 1\ (\mathrm{mod}\ 4)$ or*
(iii) *f belongs to $C(n,m,r,t,q)$ and $2m<n-1$ and $q\equiv 1\ (\mathrm{mod}\ 4)$.*

Corollary 5.19. *The number of functions satisfying the SAC of order $(n-3)$ which are exactly first-order correlation immune is*

$$\begin{cases}T(n) & \text{if}\quad n\equiv 1\quad(\mathrm{mod}\ 2),\\[4pt] T(n)+\dfrac{2n!}{(n/2)!} & \text{if}\quad n\equiv 0\quad(\mathrm{mod}\ 4),\\[4pt] T(n)+\dfrac{n!}{(n/2)!} & \text{if}\quad n\equiv 2\quad(\mathrm{mod}\ 4),\end{cases}$$

where

$$T(n)=\sum_{4\leq 2m\leq n}\frac{n!}{(n-2m)!\,(m-2)!}2^{n-2m}+\sum_{\substack{0\leq 2m<n-1\\ m\not\equiv n\ (\mathrm{mod}\ 4)}}\frac{n!}{(n-2m)!\,m!}2^{n-2m}.$$

Proof. By Lemma 2.3.8, the number of functions satisfying condition (i) of Theorem 5.18 is

$$\sum_{4\le 2m\le n} \frac{n!}{(n-2m)!\,m!}2^{n-2m+1}\binom{m}{2} = \sum_{4\le 2m\le n} \frac{n!}{(n-2m)!\,(m-2)!}2^{n-2m}.$$

By Lemma 2.3.7, the number of functions satisfying condition (ii) of Theorem 5.18 is

$$\sum_{\substack{0\le r\le m\\ q\not\equiv 1 \pmod 4}} \frac{2(2m)!}{m!\,2^m}\binom{m}{r}.$$

Now $q = 2r - m$, so if $m \equiv 0 \pmod 2$, then $q \not\equiv 1 \pmod 4$. If $m \equiv 1 \pmod 4$, then $q \not\equiv 1 \pmod 4$ if and only if $r \equiv \frac{1}{2}(3 + m) \pmod 2$. So the number of functions satisfying (ii) is

$$\begin{cases} \dfrac{2(2m)!}{m!\,2^m}2^m & \text{if} \quad n \equiv 0 \quad (\text{mod } 4),\\[2ex] \dfrac{2(2m)!}{m!\,2^m}2^{m-1} & \text{if} \quad n \equiv 2 \quad (\text{mod } 4),\\[2ex] 0 & \text{if} \quad n \equiv 1 \quad (\text{mod } 2), \end{cases}$$

or

$$\begin{cases} \dfrac{2n!}{(n/2)!} & \text{if} \quad n \equiv 0 \quad (\text{mod } 4),\\[2ex] \dfrac{n!}{(n/2)!} & \text{if} \quad n \equiv 2 \quad (\text{mod } 4),\\[2ex] 0 & \text{if} \quad n \equiv 1 \quad (\text{mod } 2). \end{cases}$$

By Lemma 2.3.7, the number of functions satisfying condition (iii) of Theorem 5.18 is

$$\sum_{0\le 2m<n-1}\ \sum_{0\le r\le m}\ \sum_{\substack{0\le t\le n-2m\\ q\equiv 1 \pmod 4}} \frac{2n!}{(n-2m)!\,m!\,2^m}\binom{m}{r}\binom{n-2m}{t}.$$

If $m \equiv n \pmod 2$, then $q \not\equiv 1 \pmod 4$, while if $m \not\equiv n \pmod 4$, then $q \equiv 1 \pmod 4$ if and only if $t \equiv \frac{1}{2}(1 - m + n - 2r) \pmod 2$. So the number of functions satisfying (iii) is

$$\sum_{\substack{0\le 2m<n-1\\ m\not\equiv n \pmod 4}}\ \sum_{0\le r\le m}\ \sum_{\substack{0\le t\le n-2m\\ q\equiv 1 \pmod 4}} \frac{2n!}{(n-2m)!\,m!\,2^m}\binom{m}{r}\binom{n-2m}{t}$$

$$= \sum_{\substack{0\le 2m<n-1\\ m\not\equiv n \pmod 4}} \frac{2n!}{(n-2m)!\,m!\,2^m}2^{n-m-1}$$

$$= \sum_{\substack{0\le 2m<n-1\\ m\not\equiv n \pmod 4}} \frac{n!}{(n-2m)!\,m!}2^{n-2m}. \qquad \square$$

Theorem 5.20. *If $f \in \mathscr{B}_{\mathscr{S}}$ satisfies the SAC of order $(n - 3)$, then f is exactly second-order correlation immune if and only if either*

(i) *there are exactly three pairs (x, y) with $\bar{f}(\{x, y\}) = 1$ and $F(x) = -F(y)$ or*
(ii) *f belongs to $C(n, m, r, t, q)$ and $2m = n - 1$ and $q \equiv 1 \pmod 4$.*

Corollary 5.21. *The number of functions satisfying the SAC of order $(n - 3)$ which are exactly second-order correlation immune is*

$$\begin{cases} T(n) + \dfrac{2n!}{((n-1)/2)!} & \textit{if} \quad n \equiv 1 \quad (\text{mod } 4), \\[2ex] T(n) & \textit{otherwise}, \end{cases}$$

where, here,

$$T(n) = \sum_{6 \leq 2m \leq n} \frac{n!}{3(n-2m)!\,(m-3)!} 2^{n-2m}.$$

Proof. By Lemma 2.3.8, the number of functions satisfying condition (i) of Theorem 5.20 is

$$\sum_{6 \leq 2m \leq n} \frac{n!}{(n-2m)!\,m!} 2^{n-2m+1} \binom{m}{3} = \sum_{6 \leq 2m \leq n} \frac{n!}{3(n-2m)!\,(m-3)!} 2^{n-2m}.$$

By Lemma 2.3.7, if $n = 2m + 1$, then the number of functions satisfying condition (ii) of Theorem 5.20 is

$$\sum_{0 \leq r \leq m} \sum_{\substack{0 \leq t \leq 1 \\ q \equiv 1 \ (\text{mod } 4)}} \frac{2(2m+1)!}{m!\,2^m} \binom{m}{r} \binom{1}{t}.$$

In this case, $q = 2r + 2t - m - 1$, so if $m \equiv 1 \pmod 2$, then $q \not\equiv 1 \pmod 4$, while if $m \equiv 0 \pmod 2$, then $q \equiv 1 \pmod 4$ if and only if $t \equiv \frac{1}{2}(2 + m - 2r) \pmod 2$. So the number of functions satisfying (ii) is

$$\begin{cases} 0 & \text{if} \quad m \equiv 1 \ (\text{mod } 2), \\[2ex] \dfrac{2(2m+1)!}{m!} & \text{if} \quad m \equiv 0 \ (\text{mod } 2). \end{cases}$$

□

Theorem 5.22. *If $f \in \mathscr{B}_{\mathscr{S}}$ satisfies the SAC of order $(n - 3)$, then f is exactly third-order correlation immune if and only if either*

(i) *there are exactly four pairs (x, y) with $\bar{f}(\{x, y\}) = 1$ and $F(x) = -F(y)$ or*
(ii) *f belongs to $C(n, m, r, t, q)$ and $2m = n$ and $q \equiv 1 \pmod 4$.*

Corollary 5.23. *The number of functions satisfying the SAC of order $(n - 3)$ which are exactly third-order correlation immune is*

$$\begin{cases} T(n) + \dfrac{(2m)!}{m!} & \textit{if} \quad n \equiv 2 \quad (\text{mod } 4), \\[2ex] T(n) & \textit{otherwise}, \end{cases}$$

where, here,

$$T(n) = \sum_{8 \le 2m \le n} \frac{n!}{3(n-2m)!\,(m-4)!} 2^{n-2m-2}.$$

Proof. By Lemma 2.3.8, the number of functions satisfying condition (i) of Theorem 5.22 is

$$\sum_{8 \le 2m \le n} \frac{n!}{(n-2m)!\, m!} 2^{n-2m+1} \binom{m}{4} = \sum_{8 \le 2m \le n} \frac{n!}{3(n-2m)!\,(m-4)!} 2^{n-2m-2}.$$

By Lemma 2.3.7, if $n = 2m$, then the number of functions satisfying condition (ii) of Theorem 5.22 is

$$\sum_{\substack{0 \le r \le m \\ q \equiv 1 \pmod 4}} \frac{2(2m)!}{m!\,2^m} \binom{m}{r}.$$

In this case, $q = 2r - m$, so if $m \equiv 0 \pmod 2$, then $q \not\equiv 1 \pmod 4$, while if $m \equiv 1 \pmod 2$, then $q \equiv 1 \pmod 4$ if and only if $r \equiv \frac{1}{2}(1 + m) \pmod 2$. So the number of functions satisfying (ii) is

$$\begin{cases} 0 & \text{if } m \equiv 0 \pmod 2, \\ \dfrac{(2m)!}{m!} & \text{if } m \equiv 1 \pmod 2. \end{cases}$$

□

Theorem 5.24. *If $f \in \mathscr{B}_{\mathscr{S}}$ satisfies the SAC of order $(n-3)$, then f is* p*th-order correlation immune* $(p > 3)$ *if and only if there are exactly* $(p + 1)$ *pairs* (x, y) *with* $\bar{f}(\{x, y\}) = 1$ *and* $F(x) = -F(y)$.

Corollary 5.25. *The number of functions satisfying the SAC of order $(n-3)$ which are exactly* p*th-order correlation immune* $(p > 3)$ *is*

$$\sum_{2p \le 2m \le n} \frac{n!}{(n-2m)!\, m!} 2^{n-2m+1} \binom{m}{p}.$$

Proof. Immediate from Lemma 2.3.8 and Theorem 5.24. □

6. Balance and Correlation Immunity

Theorem 6.1. *If $f \in \mathscr{B}_{\mathscr{S}}$ satisfies the SAC of order $(n-3)$, then f is both balanced and correlation immune if and only if either*

(i) *there exist at least two pairs (x, y) such that $\bar{f}(\{x, y\}) = 1$ and $F(x) = -F(y)$ or*
(ii) *f belongs to $C(n, m, r, t, q)$ and $n = 2m$ and $q \equiv 3 \pmod 4$.*

Theorem 6.2. *The number of functions satisfying the SAC of order $(n-3)$ which* *are also balanced and correlation immune is*

$$\begin{cases} \displaystyle\sum_{0 \le 2m \le n} \frac{n!}{(n-2m)!\,m!} 2^{n-2m+1}(2^m - 1 - m) + \frac{n!}{(n/2)!} & \textit{if} \quad n \equiv 2 \pmod 4, \\ \displaystyle\sum_{0 \le 2m \le n} \frac{n!}{(n-2m)!\,m!} 2^{n-2m+1}(2^m - 1 - m) & \textit{otherwise.} \end{cases}$$

Proof. By Lemma 2.3.8, the number of functions satisfying condition (i) of Theorem 6.1 is

$$\sum_{4 \le 2p \le n} \sum_{2p \le 2m \le n} \frac{n!}{(n-2m)!\,m!} 2^{n-2m+1} \binom{m}{p}$$

$$= \sum_{4 \le 2m \le n} \sum_{2 \le p \le m} \frac{n!}{(n-2m)!\,m!} 2^{n-2m+1} \binom{m}{p}$$

$$= \sum_{4 \le 2m \le n} \frac{n!}{(n-2m)!\,m!} 2^{n-2m+1}(2^m - 1 - m)$$

$$= \sum_{0 \le 2m \le n} \frac{n!}{(n-2m)!\,m!} 2^{n-2m+1}(2^m - 1 - m).$$

By Lemma 2.3.7, if $n = 2m$, then the number of functions satisfying condition (ii) of Theorem 6.1 is

$$\sum_{\substack{0 \le r \le m \\ q \equiv 3 \pmod 4}} \frac{2(2m)!}{m!\,2^m} \binom{m}{r}.$$

Since $n = 2m$, we have $q = 2r - m$, so, for $q \equiv 3 \pmod 4$, we must have $m \equiv 1 \pmod 2$ and $r \equiv \frac{1}{2}(3 + m) \pmod 2$. So the number of functions satisfying (ii) is 0 if $m \equiv 0 \pmod 2$ and

$$\frac{2(2m)!}{m!\,2^m} \sum_{\substack{0 \le r \le m \\ q \equiv 3 \pmod 4}} \binom{m}{r} = \frac{2(2m)!}{m!\,2^m} 2^{m-1} = \frac{(2m)!}{m!}$$

if $m \equiv 1 \pmod 2$. □

7. Conclusions

In Table 1 we present some actual values of the numbers of functions derived above. All numbers in the table refer to functions satisfying the SAC of order $(n - 3)$, so, for example, the column labelled "Balanced" contains the numbers of functions which are balanced and satisfy the SAC of order $(n - 3)$. The final column shows the proportion of functions satisfying the SAC of order $(n - 3)$ which are both balanced and correlation immune, and we see that this proportion is increasing rapidly as n increases.

From the table we see that there is indeed a sufficient supply of suitable functions. We note that the proportion of functions satisfying the SAC of order $(n - 3)$ which

Table 1. Numbers of functions satisfying the SAC of order ($n - 3$) and other criteria.

n	Total number	Balanced	Correlation immune	Balanced and correlation immune	Proportion
3	64	32	20	0	0.0000000
4	320	216	96	24	0.0750000
5	1,664	1,192	392	240	0.1442310
6	9,728	7,560	3.184	2,520	0.2837170
7	59,392	49,856	24,992	20,160	0.3394400
8	391,168	343,392	205,184	171,360	0.4380730
9	2,682,880	2,424,032	1,566,944	1,407,168	0.5244990
10	19,447,808	18,061,920	12,563,584	11,803,680	0.6131610
11	146,210,816	138,492,928	102,036,288	98,588,160	0.6742880
12	1,148,125,184	1,101,919,104	861,577,728	843,511,680	0.7346860

are also balanced and correlation immune appears to tend to 1 as n tends to infinity, although we offer no proof of this observation. We conclude that, unlike the highest-order SAC, this order of SAC is compatible with balance and correlation immunity, which makes it more desirable cryptographically. We therefore recommend the use of the SAC of order ($n - 3$), rather than the highest-order SAC.

References

[1] Forré, R., The Strict Avalanche Criterion: Spectral properties of Boolean functions and an extended definition, *Advances in Cryptology, Proceedings Crypto '88*, Springer-Verlag, Berlin, 1986, pp. 450–468.

[2] Lloyd, S. A., Balance, uncorrelatedness and the Strict Avalanche Criterion, *Discrete Applied Mathematics*, to appear.

[3] Lloyd, S. A., Characterising and counting functions satisfying the Strict Avalanche Criterion of order ($n - 3$), *Proceedings of the Second IMA Conference on Cryptography and Coding*, 1989, Clarendon Press, Oxford, 1992, pp. 165–172.

[4] Siegenthaler, T., Correlation immunity of nonlinear combining functions for cryptographic applications, *IEEE Transactions on Information Theory*, vol. 30 (1984), pp. 776–780.

[5] Siegenthaler, T., Decrypting a class of stream ciphers using ciphertext only, *IEEE Transactions on Computers*, vol. 34 (1985), pp. 81–85.

[6] Xiao, G. Z., and Massey, J. L., A spectral characterization of correlation-immune combining functions, *IEEE Transactions on Information Theory*, vol. 34, no. 3 (1988), pp. 569–571.

[7] Webster, A. F., and Tavares, S. E., On the design of S-boxes, *Advances in Cryptology, Proceedings Crypto '85*, Springer-Verlag, Berlin, 1986, pp. 523–534.