Asymptotic enumeration of correlation-immune boolean functions

E. Rodney Canfield[*]

Department of Computer Science
University of Georgia
Athens, GA 30602, USA

erc@cs.uga.edu

Zhicheng Gao

School of Mathematics and Statistics
Carleton University, Ottawa, Canada

zgao@math.carleton.ca

Catherine Greenhill

School of Mathematics and Statistics
University of New South Wales
Sydney, Australia 2052

csg@unsw.edu.au

Brendan D. McKay[†]

School of Computer Science
Australian National University
Canberra, ACT Australia

bdm@cs.anu.edu.au

Robert W. Robinson

Department of Computer Science
University of Georgia
Athens, GA 30602, USA

rwr@cs.uga.edu

[*] Research supported by the NSA Mathematical Sciences Program

[†] Research supported by the Australian Research Council

Abstract

A boolean function of n boolean variables is *correlation-immune* of order k if the function value is uncorrelated with the values of any k of the arguments. Such functions are of considerable interest due to their cryptographic properties, and are also related to the orthogonal arrays of statistics and the balanced hypercube colourings of combinatorics. The *weight* of a boolean function is the number of argument values that produce a function value of 1. If this is exactly half the argument values, that is, 2^{n-1} values, a correlation-immune function is called *resilient*.

An asymptotic estimate of the number $N(n,k)$ of n-variable correlation-immune boolean functions of order k was obtained in 1992 by Denisov for constant k. Denisov repudiated that estimate in 2000, but we will show that the repudiation was a mistake.

The main contribution of this paper is an asymptotic estimate of $N(n,k)$ which holds if k increases with n within generous limits and specialises to functions with a given weight, including the resilient functions. In the case of $k=1$, our estimates are valid for all weights.

1 Introduction

Let n, k, q be integers satisfying $1 \leq k \leq n$ and $0 \leq 2^k q \leq 2^n$, and define $\lambda = 2^k q / 2^n$. A *correlation-immune boolean function* of n variables, order k and weight $2^k q$ is a boolean-valued function of n boolean variables with this property: if any k arguments are given arbitrary values, exactly the fraction λ of the 2^{n-k} possible assignments to the remaining arguments give a function value of 1. (See for example [9, 13, 15] and [5, Chapter 4].) Let $N(n,k,q)$ denote the number of such functions. An important special case is the *resilient functions*, which have $\lambda = \frac{1}{2}$. Correlation-immune functions, and in particular the resilient functions, have desirable cryptographic properties: see for example [2, 13]. In this paper we will derive an asymptotic estimate of $N(n,k,q)$ for a wide range of k and q values, and deduce an asymptotic formula for the sum $N(n,k) = \sum_q N(n,k,q)$, which is the number of correlation-immune boolean functions of n variables and order k.

An n-variable boolean function can be represented as a matrix of n columns over $\{0,1\}$ whose rows consist of those argument lists which give the function value 1. A correlation-immune boolean function of n variables, order k and weight $2^k q$ gives rise to a matrix with $2^k q$ distinct rows and n columns, such that in any set of k columns each of the 2^k possible 0-1 patterns appears exactly q times. In statistics, such a matrix is called an *orthogonal array* of 2 levels, n variables, $2^k q$ runs, and strength k; see [8] for a detailed exposition. Since the $2^k q$ rows are by definition distinct, and permuting the rows does not change the associated function, there is an uninteresting ratio of $(2^k q)!$ between the number of matrices and the number of functions. We will work with functions rather than matrices.

The special case $k = 1$ has also been studied under the name of *balanced colourings of a hypercube.* These are placements of equal weights on some of the vertices of a hypercube such that the centroid is at the center of the hypercube. Exact enumerations have been found in this case [11, 21], but they do not appear suitable for asymptotics.

Early papers on the number of correlation-immune functions focussed on the case $k = 1$. Upper and lower bounds for $N(n, 1)$ were given in [9, 10, 12, 20] but these do not appear as sharp as the bounds given by Bach [1].

The case of general k was first considered by Schneider [15], who gave upper bounds for $N(n, k, q)$ as well as for $N(n, k)$. For large k an improved upper bound is given by Carlet and Klapper [4], both for $N(n, k)$ and for the resilient functions of order k. Carlet and Gouget [3] gave an upper bound for the number of resilient functions of order k, which improves upon Schneider's bound for $k > n/2 - 1$ and which partially improves upon the upper bound of [4]. Tarannikov [16] proved that when c is a fixed positive integer, the function $N(n, n - c)$ is bounded above by a polynomial in n. Exact expressions for $N(n, n - c)$ when $c = 1, 2, 3$ are also given in [16, Theorem 3]. (See also [17].)

The first asymptotic enumeration of correlation-immune functions was achieved by Denisov. Define

$$M = \sum_{j=0}^{k} \binom{n}{j} \quad \text{and} \quad Q = \sum_{j=1}^{k} j \binom{n}{j}.$$

Theorem 1.1 (Denisov [6])**.** *If $k \geq 1$ is a constant integer then, as $n \to \infty$,*

$$N(n, k) \sim 2^{2^n + Q - k} (2^{n-1} \pi)^{-(M-1)/2}. \quad \square$$

Denisov's formula for $N(n, 1)$ was refined by Bach [1], who showed that an asymptotic expansion for $N(n, 1)$ exists and calculated the first few terms of it.

In a later paper [7], Denisov repudiated Theorem 1.1 and proposed a different value. However, we will show that Denisov's repudiation was a mistake, and Theorem 1.1 is correct. More discussion of [7] is given in Section 8.

We now state our results. Define

$$A = \lambda(1 - \lambda).$$

In addition to common asymptotic notations like $O(\cdot)$, we use $\omega(f(n))$ to represent any function $g(n)$ such that $g(n)/f(n) \to \infty$ as $n \to \infty$.

Theorem 1.2. *Consider a sequence of triples (n,k,q) of positive integers such that $n \to \infty$ and*

$$\omega\bigl(2^{5k}n^{6k+3}M^3\bigr) \le q \le 2^{n-k} - \omega\bigl(2^{5k}n^{6k+3}M^3\bigr). \tag{1.1}$$

Then

$$N(n,k,q) = 2^Q \left(\lambda^\lambda(1-\lambda)^{1-\lambda}\right)^{-2^n} \left(\pi A\, 2^{n+1}\right)^{-M/2} \bigl(1 + O(\eta(n,k,q))\bigr), \tag{1.2}$$

where $\eta(n,k,q) = 2^{-n/2+3k}n^{3k+3/2}M^{3/2}\lambda^{-1/2}(1-\lambda)^{-1/2} = o(1)$.

Remark 1.1. *Given a function g in the class counted by $N(n,k,q)$, we can form another, namely $1-g$, counted by $N(n,k,2^{n-k}-q)$. This complementation operation is a bijection which exchanges q with $2^{n-k}-q$ and λ with $1-\lambda$. This means, for example, that we can assume $\lambda \le \frac{1}{2}$ in our proof when it is convenient.*

Remark 1.2. *By Stirling's formula, $\log M = o(n)$ whenever $k = O(n/\log n)$. From this it follows that (1.1) is non-vacuous whenever*

$$1 \le k \le \left(\frac{\log 2}{6} - \varepsilon\right)\frac{n}{\log n} \tag{1.3}$$

for some $\varepsilon > 0$.

Corollary 1.1. *If $k = k(n)$ satisfies (1.3) then, as $n \to \infty$, the number of k-resilient boolean functions of n variables is*

$$2^{2^n+Q}(2^{n-1}\pi)^{-M/2}\bigl(1 + O(2^{-n/2+3k}n^{3k+3/2}M^{3/2})\bigr) \sim 2^{2^n+Q}(2^{n-1}\pi)^{-M/2}.$$

Corollary 1.2. *If $k = k(n)$ satisfies (1.3) then, as $n \to \infty$, the number of order k correlation-immune boolean functions of n variables is*

$$\begin{aligned} N(n,k) &= 2^{2^n+Q-k}(2^{n-1}\pi)^{-(M-1)/2}\bigl(1 + O(2^{-n/2+3k}n^{3k+3/2}M^{3/2})\bigr) \qquad (1.4)\\ &\sim 2^{2^n+Q-k}(2^{n-1}\pi)^{-(M-1)/2}. \end{aligned}$$

Corollary 1.2 shows that Denisov's result Theorem 1.1 is true, despite his later retraction.

In Section 2, we write $N(n,k,q)$ as an integral in many complex dimensions. In Section 3 we identify the points where the integrand has maximum magnitude and define a region $\mathcal{R}+\mathcal{C}$ consisting of a small hypercuboid surrounding each of those points. The integral is then bounded outside $\mathcal{R}+\mathcal{C}$ in Section 4 and estimated inside $\mathcal{R}+\mathcal{C}$ in Section 5. The proof of Theorem 1.2 is completed in Section 6 where we also prove Corollaries 1.1 and 1.2. In the final sections we consider some additional topics including a closer look at the case $k = 1$ and a connection with Hadamard matrices.

2 The desired quantity as a complex integral

Define $[n] = \{1, 2, \ldots, n\}$ and $\mathcal{I}_k = \{S \in 2^{[n]} : |S| \le k\}$. We will identify $N(n, k, q)$ as the constant term in a generating function over the M variables $\{x_S : S \in \mathcal{I}_k\}$. Let $\boldsymbol{x}$ denote a vector of all these variables, in arbitrary order. For $D = \lambda/(1-\lambda)$, define the rational function $F(\boldsymbol{x})$ by

$$F(\boldsymbol{x}) = \prod_{\alpha \in \{\pm 1\}^n} \biggl(1 + D \prod_{S \in \mathcal{I}_k} x_S^{\alpha_S}\biggr),$$

where

$$\alpha_S = \prod_{j \in S} \alpha_j$$

for each S (including the case $\alpha_\emptyset = 1$). The value of D is determined by a saddle point condition, as will become apparent in Section 5.

Lemma 2.1. *$N(n, k, q)$ is the constant term of $(Dx_\emptyset)^{-2^k q} F(\boldsymbol{x})$.*

Proof. For a boolean function $g(y_1, \ldots, y_n)$, the *Walsh transform* of g is the real-valued function $\hat{g}$ over $\{0, 1\}^n$ defined by

$$\hat{g}(w_1, \ldots, w_n) = \sum_{(y_1, \ldots, y_n) \in \{0,1\}^n} g(y_1, \ldots, y_n)\, (-1)^{w_1 y_1 + \cdots + w_n y_n}.$$

Given $\alpha \in \{\pm 1\}^n$, form $\bar{\alpha} \in \{0, 1\}^n$ from α by changing each 1 entry into 0 and each -1 entry into 1.

For $S \in \mathcal{I}_k$, let $w_S \in \{0, 1\}^n$ be the characteristic vector of S. Then, given a vector $\alpha \in \{\pm 1\}^n$ and any $S \in \mathcal{I}_k$, we have

$$\alpha_S = (-1)^{\bar{\alpha} \cdot w_S}.$$

We can view $F(\boldsymbol{x})$ as the sum of 2^{2^n} terms, with one term for each boolean function g of n variables. Specifically, the term corresponding to a boolean function $g : \{0, 1\}^n \to \{0, 1\}$ is exactly

$$\prod_{\substack{\alpha \in \{\pm 1\}^n \\ g(\bar{\alpha}) = 1}} \biggl(D \prod_{S \in \mathcal{I}_k} x_S^{\alpha_S}\biggr) = D^{\hat{g}(w_\emptyset)} \prod_{S \in \mathcal{I}_k} x_S^{\hat{g}(w_S)}.$$

By the spectral characterisation of correlation-immune functions [14, 19], the boolean function g is correlation-immune of order k if and only if $\hat{g}(w_S) = 0$ for all $S \in \mathcal{I}_k \setminus \{\emptyset\}$. Moreover, the functions counted by $N(n, k, q)$ have $\hat{g}(w_\emptyset) = 2^k q$. Therefore the coefficient of the monomial $x_\emptyset^{2^k q}$ in $F(\boldsymbol{x})$ is exactly $D^{2^k q}\, N(n, k, q)$. □

By Cauchy's integral formula, it follows from Lemma 2.1 that

$$N(n,k,q) = \frac{1}{(2\pi i)^M D^{2^k q}} \oint \cdots \oint \frac{F(\boldsymbol{x})}{x_\emptyset^{2^k q} \prod_{S\in\mathcal{I}_k} x_S}\, d\boldsymbol{x},$$

where each x_S is integrated anticlockwise around a circle of radius 1 centred at the origin. Now introduce variables θ_S ($S \in \mathcal{I}_k$) and the M-dimensional vector $\boldsymbol{\theta}$ of the θ_S variables in arbitrary order. Change variables from $\boldsymbol{x}$ to $\boldsymbol{\theta}$ using $x_S = e^{i\theta_S}$ for each S. Then

$$N(n,k,q) = \frac{(1+D)^{2^n}}{(2\pi)^M D^{2^k q}}\, I(n,k,q), \tag{2.1}$$

where

$$I(n,k,q) = \int_{-\pi}^{\pi} \cdots \int_{-\pi}^{\pi} G(\boldsymbol{\theta})\, d\boldsymbol{\theta},$$

$$G(\boldsymbol{\theta}) = e^{-i2^k q\theta_\emptyset} \prod_{\alpha\in\{\pm1\}^n} \frac{1+De^{if_\alpha(\boldsymbol{\theta})}}{1+D}, \tag{2.2}$$

and

$$f_\alpha(\boldsymbol{\theta}) = \sum_{S\in\mathcal{I}_k} \alpha_S\theta_S. \tag{2.3}$$

The elements of $\boldsymbol{\theta}$ belong to the set $\mathbb{R}_{2\pi}$ of real numbers modulo 2π. In this set, addition, and multiplication by integers, have their usual meanings. We use $\equiv$ to indicate equality in $\mathbb{R}_{2\pi}$. For example, $\theta \equiv 0$ means that θ is the element of $\mathbb{R}_{2\pi}$ corresponding to the real number $2\pi t$ for any integer t. Also let

$$z : \mathbb{R}_{2\pi} \longrightarrow (-\pi, \pi]$$

be the standard mapping of $\mathbb{R}_{2\pi}$ onto the real interval $(-\pi,\pi]$ and define the absolute value $d(\theta) = |z(\theta)|$ for any $\theta \in \mathbb{R}_{2\pi}$. Clearly $d(\cdot)$ satisfies the triangle inequality. $d(\theta+\theta') \le d(\theta) + d(\theta')$.

3 Analysis of the domain of integration

The integrand $G(\boldsymbol{\theta})$ defined in (2.2) has modulus at most 1. We will later show that the value of the integral $I(n,k,q)$ comes mostly from the near vicinity of those points where equality occurs, so our next task will be to identify those points. Define

$$\mathcal{C} = \bigl\{\, \boldsymbol{\theta} \in \mathbb{R}_{2\pi}^M \,:\, |G(\boldsymbol{\theta})| = 1 \,\bigr\}.$$

Lemma 3.1.
$$\mathcal{C} = \Big\{ \boldsymbol{\theta} \in \mathbb{R}_{2\pi}^M \,:\, 2^{|S|} \sum_{T\in\mathcal{I}_k, T\supseteq S} \theta_T \equiv 0 \ \textit{for each } S \in \mathcal{I}_k \Big\}, \tag{3.1}$$
and moreover $|\mathcal{C}| = 2^Q$.

Proof. Throughout the proof we work in $\mathbb{R}_{2\pi}$. For $1 \le j \le n$, define the linear difference operator δ_j by

$$\delta_j f_{(\alpha_1,\ldots,\alpha_j,\ldots,\alpha_n)} = f_{(\alpha_1,\ldots,\alpha_j,\ldots,\alpha_n)} - f_{(\alpha_1,\ldots,\alpha_{j-1},-\alpha_j,\alpha_{j+1},\ldots,\alpha_n)}.$$

For $S \in \mathcal{I}_k$, define $\delta_S = \prod_{j\in S} \delta_j$, noting that the product is commutative. From the definition of $f_\alpha(\boldsymbol{\theta})$ we can easily prove by induction on $|S|$ that

$$\delta_S f_\alpha(\boldsymbol{\theta}) = 2^{|S|} \sum_{T\in\mathcal{I}_k, T\supseteq S} \alpha_T \theta_T. \tag{3.2}$$

Since
$$\left| \frac{1+De^{ix}}{1+D} \right| = \frac{\sqrt{1+2D\cos(x)+D^2}}{1+D} \le 1,$$
a necessary and sufficient condition for $\boldsymbol{\theta} \in \mathcal{C}$ is that $f_\alpha(\boldsymbol{\theta}) \equiv 0$ for all $\alpha \in \{\pm 1\}^n$.

Suppose that $\boldsymbol{\theta} \in \mathcal{C}$. Then, since $f_\alpha(\boldsymbol{\theta}) \equiv 0$ for all α, the difference $\delta_S f_{\alpha_0}(\boldsymbol{\theta})$ satisfies $\delta_S f_{\alpha_0}(\boldsymbol{\theta}) \equiv 0$ for all $S \in \mathcal{I}_k$, where $\alpha_0 = (1,1,\ldots,1)$. By (3.2) we conclude that $\boldsymbol{\theta}$ lies in the set $\mathcal{C}^*$ given by the right hand side of (3.1), and hence $\mathcal{C} \subseteq \mathcal{C}^*$. Conversely, if $\boldsymbol{\theta} \in \mathcal{C}^*$ then every $f_\alpha(\boldsymbol{\theta}) \equiv 0$ since

$$f_\alpha(\boldsymbol{\theta}) \equiv \Big(\prod_{\{j:\alpha_j=-1\}} (1-\delta_j) \Big) f_{\alpha_0}(\boldsymbol{\theta}).$$

Therefore, $\mathcal{C} = \mathcal{C}^*$.

Since the set of equations in (3.1) is triangular, we can find all solutions by choosing each θ_S in order of decreasing $|S|$. There are exactly $2^{|S|}$ choices for θ_S, so the total number of solutions is $|\mathcal{C}| = 2^Q$. □

As noted in Remark 1.1, we will assume that $\lambda \le \frac{1}{2}$ without losing generality. Let Δ be the positive number defined by

$$\Delta = 2^{-n/2+k+3} \lambda^{-1/2} n^{k+1/2} M^{1/2}.$$

The left side of (1.1) is equivalent to

$$\Delta = o\big(2^{-2k} n^{-2k-1} M^{-1}\big). \tag{3.3}$$

Let $\mathcal{R}$ be the subset of $\mathbb{R}_{2\pi}^M$ defined by

$$\mathcal{R} = \big\{ \boldsymbol{\theta} \in \mathbb{R}_{2\pi}^M \,:\, d(\theta_S) \le \Delta (2n)^{-|S|} \ \text{ for all } \ S \in \mathcal{I}_k \big\}.$$

This is a hypercuboid centred at the origin. Denote the union of 2^Q copies of $\mathcal{R}$ centred at the points in $\mathcal{C}$ by

$$\mathcal{R}{+}\mathcal{C} = \bigcup_{\boldsymbol{\theta}^* \in \mathcal{C}} \{\mathcal{R} + \boldsymbol{\theta}^*\} \subseteq \mathbb{R}^M_{2\pi}.$$

Since all the elements of vectors in $\mathcal{C}$ are integer multiples of $2\pi/2^k$, it follows from (3.3) that these copies are disjoint. The region $\mathcal{R}{+}\mathcal{C}$ includes all the points where $|G(\boldsymbol{\theta})|$ is maximal; we will prove in the following sections that in fact it includes all the points which contribute substantially to $I(n,k,q)$.

4 The integral outside the critical region

Lemma 4.1. *If the conditions of Theorem 1.2 are satisfied and* $\lambda \le \frac{1}{2}$ *then*

$$\int_{(\mathcal{R}+\mathcal{C})^c} |G(\boldsymbol{\theta})|\, d\boldsymbol{\theta} < (2\pi)^M \exp\bigl(-\tfrac{4}{5}nM\bigr),$$

where $(\mathcal{R}{+}\mathcal{C})^c = \mathbb{R}^M_{2\pi} \setminus (\mathcal{R}{+}\mathcal{C})$.

Proof. Fix $\boldsymbol{\theta} \in (\mathcal{R}{+}\mathcal{C})^c$. First we show that there exists some set $S_0 = S_0(\boldsymbol{\theta}) \in \mathcal{I}_k$ such that

$$d(\delta_{S_0} f_\alpha(\boldsymbol{\theta})) > (2 - e^{1/2})\Delta n^{-|S_0|} \tag{4.1}$$

for all $\alpha \in \{\pm 1\}^n$. Define $\boldsymbol{\theta}^* = \boldsymbol{\theta}^*(\boldsymbol{\theta}) \in \mathcal{C}$ recursively, as follows: starting with sets $S \in \mathcal{I}_k$ with $|S| = k$, and then proceeding to smaller k, choose $\theta^*_S \in \mathbb{R}_{2\pi}$ such that $2^{|S|} \sum_{T \in \mathcal{I}_k, T \supseteq S} \theta^*_T \equiv 0$ and $d(\theta_S - \theta^*_S)$ is minimal over all such choices of θ^*_S. (Break ties arbitrarily.) Since $\boldsymbol{\theta} \notin \mathcal{R}{+}\mathcal{C}$, there is a set $S_0 \in \mathcal{I}_k$ of maximum cardinality such that

$$d(\theta_{S_0} - \theta^*_{S_0}) > (2n)^{-|S_0|}\Delta. \tag{4.2}$$

By the maximality of S_0 we have

$$\begin{aligned}
\sum_{T \in \mathcal{I}_k, T \supset S_0} d(\theta_T - \theta^*_T) &\le \sum_{j \ge 1} \binom{n}{j} \Delta (2n)^{-|S_0| - j} \\
&\le \Delta (2n)^{-|S_0|} \sum_{j \ge 1} \frac{2^{-j}}{j!} \\
&= (e^{1/2} - 1)\Delta(2n)^{-|S_0|}.
\end{aligned} \tag{4.3}$$

Now take any $\alpha \in \{\pm 1\}^n$ and write, using (3.2),

$$\delta_{S_0} f_\alpha(\boldsymbol{\theta}) \equiv 2^{|S_0|} \sum_{T \in \mathcal{I}_k, T \supseteq S_0} \alpha_T \theta_T \equiv \Sigma_1 + \Sigma_2 + U$$

where

$$\begin{aligned}\Sigma_1 &\equiv 2^{|S_0|} \sum_{T\in\mathcal{I}_k, T\supseteq S_0} \alpha_T \theta^*_T,\\ \Sigma_2 &\equiv 2^{|S_0|} \sum_{T\in\mathcal{I}_k, T\supset S_0} \alpha_T (\theta_T - \theta^*_T),\\ U &\equiv 2^{|S_0|} \alpha_{S_0}(\theta_{S_0} - \theta^*_{S_0}).\end{aligned}$$

Since $\boldsymbol{\theta}^* \in \mathcal{C}$, (3.1) implies that $\Sigma_1 \equiv 0$. Next, since $d(\alpha_T\theta_T) = d(\theta_T)$, (4.3) implies that

$$d(\Sigma_2) \le (e^{1/2} - 1)\Delta n^{-|S_0|}.$$

Finally,

$$d(U) > \Delta n^{-|S_0|},$$

by (4.2) and the fact that $d(\theta_{S_0} - \theta^*_{S_0}) < 2^{-|S_0|}\pi$. Therefore, using the triangle inequality,

$$d(\delta_{S_0} f_\alpha(\boldsymbol{\theta})) = d(U + \Sigma_2) \ge d(U) - d(\Sigma_2) > (2 - e^{1/2})\Delta n^{-|S_0|}.$$

Since $\alpha \in \{\pm 1\}^n$ was arbitrary, this establishes the existence of the desired set S_0.

Next, partition the set $\{\pm 1\}^n$ into $2^{n-|S_0|}$ parts, each of size $2^{|S_0|}$, such that two vectors α, α' belong to the same part if and only if they agree in every coordinate $j \notin S_0$. Let P be an arbitrary part of the partition. For any $\alpha \in P$, the difference $\delta_{S_0} f_\alpha(\boldsymbol{\theta})$ is a linear combination, with coefficients ± 1, of the elements of the set $\{f_{\alpha'}(\boldsymbol{\theta}) : \alpha' \in P\}$. Therefore, by (4.1) and using the triangle inequality,

$$(2 - e^{1/2})\Delta n^{-|S_0|} < d(\delta_{S_0} f_\alpha(\boldsymbol{\theta})) \le \sum_{\alpha' \in P} d(f_{\alpha'}(\boldsymbol{\theta})). \tag{4.4}$$

As $1 - \cos x \le 2x^2/\pi^2$ for $-\pi \le x \le \pi$, we find that for all $x \in \mathbb{R}$,

$$\begin{aligned}\left|\frac{1 + De^{ix}}{1 + D}\right|^2 &= 1 - \frac{2D(1 - \cos x)}{(1 + D)^2}\\ &\le \exp\Bigl(-\frac{4D\, d(x)^2}{(1 + D)^2\pi^2}\Bigr)\\ &= \exp\Bigl(-\frac{4\lambda(1 - \lambda)}{\pi^2}\, d(x)^2\Bigr)\\ &\le \exp\Bigl(-\frac{2\lambda}{\pi^2}\, d(x)^2\Bigr)\end{aligned}$$

using the assumption $\lambda \le \frac{1}{2}$ for the last inequality. Thus, using the Cauchy-Schwarz inequality and (4.4),

$$\begin{aligned}\prod_{\alpha\in P}\left|\frac{1+De^{if_\alpha(\boldsymbol{\theta})}}{1+D}\right| &\le \exp\Bigl(-\frac{\lambda}{\pi^2}\sum_{\alpha\in P} d(f_\alpha(\boldsymbol{\theta}))^2\Bigr)\\ &\le \exp\Bigl(-\frac{\lambda}{\pi^2|P|}\Bigl(\sum_{\alpha\in P} d(f_\alpha(\boldsymbol{\theta}))\Bigr)^2\Bigr)\\ &\le \exp\Bigl(-\frac{\lambda}{\pi^2}\,2^{-|S_0|}\,((2-e^{1/2})\Delta n^{-|S_0|})^2\Bigr).\end{aligned}$$

Since there are $2^{n-|S_0|}$ parts in the partition, taking the product over all parts and applying the definition of Δ gives

$$\begin{aligned}|G(\boldsymbol{\theta})| &\le \exp\bigl(-(2-e^{1/2})^2\pi^{-2}2^{2k-2|S_0|+6}n^{2k-2|S_0|+1}M\bigr)\\ &\le \exp\bigl(-2^6\,(2-e^{1/2})^2\pi^{-2}nM\bigr),\end{aligned}$$

as $|S_0|\le k$. Finally we note that $2^6\,(2-e^{1/2})^2\,\pi^{-2} > \frac{4}{5}$, so we have

$$|G(\boldsymbol{\theta})| < \exp\bigl(-\tfrac{4}{5}nM\bigr).$$

As this inequality holds for any $\boldsymbol{\theta}\notin\mathcal{R}+\mathcal{C}$ and the volume of $(\mathcal{R}+\mathcal{C})^c$ is at most $(2\pi)^M$, the proof is complete. □

5 The integral inside the critical region

Lemma 5.1. *If the conditions of Theorem 1.2 are satisfied and* $\lambda\le\frac{1}{2}$ *then*

$$\int_{\mathcal{R}} G(\boldsymbol{\theta})\,d\boldsymbol{\theta} = \Bigl(\frac{2\pi}{\lambda(1-\lambda)2^n}\Bigr)^{M/2}\bigl(1+O(2^{5k/2}n^{3k+3/2}M^{3/2}q^{-1/2})\bigr).$$

Proof. Let $\boldsymbol{\theta}=(\theta_S)_{S\in\mathcal{I}_k}\in\mathcal{R}$. In this section we perform expansions that are valid in $\mathbb{R}$ rather than $\mathbb{R}_{2\pi}$, so we identify $\boldsymbol{\theta}$ with $\bigl(z(\theta_S)\bigr)_{S\in\mathcal{I}_k}$. Since

$$\exp\Bigl(i\sum_{S\in\mathcal{I}_k}\alpha_S\theta_S\Bigr) = \exp\Bigl(i\sum_{S\in\mathcal{I}_k}\alpha_S z(\theta_S)\Bigr),$$

this identification has no effect on $G(\boldsymbol{\theta})$. Also note that

$$|f_\alpha(\boldsymbol{\theta})| = \Bigl|\sum_{S\in\mathcal{I}_k}\alpha_S z(\theta_S)\Bigr| \le \Delta\sum_{j=0}^{k}\binom{n}{j}(2n)^{-j}\le e^{1/2}\Delta. \qquad (5.1)$$

Define

$$h(x) = \log\Bigl(\frac{1+De^{ix}}{1+D}\Bigr).$$

By Taylor's Theorem with the integral form of the remainder (which also holds for complex-valued functions),

$$h(f_\alpha(\boldsymbol{\theta})) = i\,\frac{D}{1+D}\,f_\alpha(\boldsymbol{\theta}) - \tfrac{1}{2}\frac{D}{(1+D)^2}\,f_\alpha(\boldsymbol{\theta})^2 + R(f_\alpha(\boldsymbol{\theta}))$$

where

$$R(f_\alpha(\boldsymbol{\theta})) = \int_0^{f_\alpha(\boldsymbol{\theta})} \tfrac{1}{2}h'''(t)(f_\alpha(\boldsymbol{\theta}) - t)^2 dt. \tag{5.2}$$

Now $\cos(\cdot)$ is unimodal on $[-e^{1/2}\Delta, e^{1/2}\Delta]$ by (3.3). Therefore for $|t| \le e^{1/2}\Delta$ we have

$$|h'''(t)| = \frac{D\sqrt{1-2D\cos(t)+D^2}}{(1+2D\cos(t)+D^2)^{3/2}} \le\; D \le 2\lambda$$

using the assumption that $\lambda \le \frac{1}{2}$. Hence by (5.1) and (5.2),

$$|R(f_\alpha(\boldsymbol{\theta}))| \le \frac{\lambda\, e^{3/2}\Delta^3}{3} \le 2\lambda\Delta^3.$$

Then

$$\begin{aligned} G(\boldsymbol{\theta}) &= \exp\biggl(-i2^k q\theta_\emptyset + \sum_{\alpha\in\{\pm1\}^n}\biggl(i\frac{D}{1+D}f_\alpha(\boldsymbol{\theta}) - \tfrac{1}{2}\frac{D}{(1+D)^2}f_\alpha(\boldsymbol{\theta})^2 + R(f_\alpha(\boldsymbol{\theta}))\biggr)\biggr) \\ &= \exp\biggl(\sum_{\alpha\in\{\pm1\}^n}\biggl(-\tfrac{1}{2}\frac{D}{(1+D)^2}f_\alpha(\boldsymbol{\theta})^2 + R(f_\alpha(\boldsymbol{\theta}))\biggr)\biggr) \\ &= \exp(a(\boldsymbol{\theta}))\,\exp\biggl(-\tfrac{1}{2}\,A\sum_{\alpha\in\{\pm1\}^n} f_\alpha(\boldsymbol{\theta})^2\biggr) \end{aligned}$$

where

$$a(\boldsymbol{\theta}) = \sum_{\alpha\in\{\pm1\}^n} R(f_\alpha(\boldsymbol{\theta})).$$

The vanishing of the linear terms explains our choice of D. Note that $a(\boldsymbol{\theta})$ is a complex number which is bounded in modulus by

$$|a(\boldsymbol{\theta})| \le \lambda\, 2^{n+1}\Delta^3. \tag{5.3}$$

Next, note that the reflection $\boldsymbol{\theta} \mapsto -\boldsymbol{\theta}$ preserves the region $\mathcal{R}$ and maps $G(\boldsymbol{\theta})$ to its complex conjugate. It follows that

$$\int_{\mathcal{R}} G(\boldsymbol{\theta})\, d\boldsymbol{\theta}$$

is real, and therefore is equal to the integral of the real part of its integrand. Hence

$$\begin{aligned}\int_{\mathcal{R}} G(\boldsymbol{\theta})\,d\boldsymbol{\theta} &= \int_{\mathcal{R}} \operatorname{Re}(\exp(a(\boldsymbol{\theta})))\,\exp\Bigl(-\tfrac{1}{2}\,A \sum_{\alpha\in\{\pm1\}^n} f_\alpha(\boldsymbol{\theta})^2\Bigr)\,d\boldsymbol{\theta}\\ &= \operatorname{Re}(\exp(a(\boldsymbol{\theta}_0)))\int_{\mathcal{R}} \exp\Bigl(-\tfrac{1}{2}\,A \sum_{\alpha\in\{\pm1\}^n} f_\alpha(\boldsymbol{\theta})^2\Bigr)\,d\boldsymbol{\theta}\end{aligned}$$

for some $\boldsymbol{\theta}_0 \in \mathcal{R}$, using the Intermediate Value Theorem.

Since $\lambda 2^n\Delta^3 = o(1)$ using (1.1), it follows from (5.3) that $|a(\boldsymbol{\theta}_0)| \le 1$ when n is sufficiently large. It is routine to check that for any complex number z with $|z| \le 1$,

$$\exp(-|z|) \le \operatorname{Re}(\exp(z)) \le \exp(|z|).$$

By (5.3) we can apply this with $z = a(\boldsymbol{\theta}_0)$ to find that

$$\int_{\mathcal{R}} G(\boldsymbol{\theta})\,d\boldsymbol{\theta} = \exp\bigl(O(\lambda\,2^n\Delta^3)\bigr)\int_{\mathcal{R}} \exp\Bigl(-\tfrac{1}{2}\,A \sum_{\alpha\in\{\pm1\}^n} f_\alpha(\boldsymbol{\theta})^2\Bigr)\,d\boldsymbol{\theta}. \tag{5.4}$$

Now we calculate that

$$\sum_{\alpha\in\{\pm1\}^n} f_\alpha(\boldsymbol{\theta})^2 = 2^n \sum_{S\in\mathcal{I}_k} \theta_S^2.$$

Since this quantity is real and $\lambda 2^n\Delta^3 = o(1)$, we have that

$$\int_{\mathcal{R}} G(\boldsymbol{\theta})\,d\boldsymbol{\theta} = \bigl(1 + O(\lambda 2^n\Delta^3)\bigr)\prod_{S\in\mathcal{I}_k}\int_{-\Delta(2n)^{-|S|}}^{\Delta(2n)^{-|S|}} \exp\bigl(-\tfrac{1}{2}\lambda(1-\lambda)2^n\theta_S^2\bigr)\,d\theta_S.$$

Next we apply the well-known estimate

$$\int_{-x\sigma}^{x\sigma} e^{-u^2/(2\sigma^2)}\,du = \sigma\sqrt{2\pi}\,\bigl(1 + o(e^{-x^2/2})\bigr) \quad \text{for } x\to\infty,$$

with $\sigma = \bigl(\lambda(1-\lambda)2^n\bigr)^{-1/2}$ and $x = \Delta(2n)^{-|S|}\sigma^{-1} > \sqrt{32nM} \to \infty$. This gives

$$\int_{\mathcal{R}} G(\boldsymbol{\theta})\,d\boldsymbol{\theta} = \Bigl(\frac{2\pi}{\lambda(1-\lambda)2^n}\Bigr)^{M/2}\bigl(1 + O(\lambda 2^n\Delta^3) + O(Me^{-16nM})\bigr).$$

The lemma follows on noting that the second error term is subsumed by the first. □

6 Proofs of Theorem 1.2 and its corollaries

The theory we have developed over the preceding sections allows us to complete the proofs of our main results.

Proof of Theorem 1.2. By (2.1) we have that

$$N(n,k,q) = \frac{(1+D)^{2^n}}{(2\pi)^M D^{2^k q}} \biggl(\int_{\mathcal{R}+\mathcal{C}} G(\boldsymbol{\theta})\, d\boldsymbol{\theta} + \int_{(\mathcal{R}+\mathcal{C})^c} G(\boldsymbol{\theta})\, d\boldsymbol{\theta} \biggr).$$

First suppose that $\lambda \le \frac{1}{2}$. Then the first integral is $2^Q \int_{\mathcal{R}} G$, where $\int_{\mathcal{R}} G$ has been evaluated in Lemma 5.1, while the second integral is bounded in absolute value by Lemma 4.1 and hence is covered by the error term of Lemma 5.1. This completes the proof when $\lambda \le \frac{1}{2}$, and the result follows for $\lambda > \frac{1}{2}$ by Remark 1.1. □

Corollary 1.1 follows from Theorem 1.2 by setting $\lambda = \frac{1}{2}$. Corollary 1.2 requires a little more effort.

Proof of Corollary 1.2. We divide the interval of summation into five ranges. Define

$$q_1 = \lceil 2^{n-k-1} n^{-1} \rceil, \quad q_2 = \lceil 2^{n-k-1} - 2^{n/2-k} n \rceil, \quad q_3 = 2^{n-k} - q_2, \quad q_4 = 2^{n-k} - q_1.$$

Also define

$$W(\lambda) = W(\lambda, k, n) = 2^Q \bigl(\pi A 2^{n+1}\bigr)^{-M/2} \bigl(\lambda^\lambda (1-\lambda)^{1-\lambda}\bigr)^{-2^n},$$

which is the right side of (1.2) apart from the error term.

We start with the range $q \in [q_2, q_3]$, for which $\lambda = \frac{1}{2} + O(2^{-n/2} n)$. By Taylor expansion, we have for $x = O(2^{-n/2} n)$ that

$$W\bigl(\tfrac{1}{2} + x\bigr) = W\bigl(\tfrac{1}{2}\bigr) \exp\bigl(-(2^{n+1} - 2M)x^2 + O(2^{-n} n^4)\bigr). \tag{6.1}$$

The error term in (6.1) is smaller than $2^{-n/2+3k} n^{3k+3/2} M^{3/2}$ for any λ in this range so, by Theorem 1.2,

$$\sum_{q=q_2}^{q_3} N(n,k,q) = \bigl(1 + O(2^{-n/2+3k} n^{3k+3/2} M^{3/2})\bigr) W\bigl(\tfrac{1}{2}\bigr) \sum_{q=q_2}^{q_3} h(q),$$

where $h(q) = \exp\bigl(-2^{-2n+2k+1}(2^n - M)(q - 2^{n-k-1})^2\bigr)$. By Euler-Maclaurin summation (see for example [18, p. 36]),

$$\begin{aligned} \sum_{q=q_2}^{q_3} h(q) &= O(e^{-n^2}) + \bigl(1 + O(2^{-n})\bigr) \int_{q_2}^{q_3} h(q)\, dq \\ &= \bigl(1 + O(2^{-n})\bigr) \pi^{1/2} 2^{n-k-1/2} (2^n - M)^{-1/2} \\ &= \bigl(1 + O(2^{-n} M)\bigr) \pi^{1/2} 2^{n/2-k-1/2}. \end{aligned}$$

This proves that $\sum_{q=q_2}^{q_3} N(n,k,q)$ is given by an expression of the same form as the right side of (1.4).

Next consider the range $q \in [q_1, q_2)$, which is the mirror image of the range $q \in (q_3, q_4]$. Then

$$\begin{aligned}\frac{d\log W(\lambda)}{d\lambda} &= a_1(\lambda)2^n + a_2(\lambda)\bigl(\lambda(1{-}\lambda)2^n - M\bigr), \quad \text{where}\\ a_1(\lambda) &= \log(\lambda^{-1} - 1) + \lambda - \tfrac{1}{2} \;\text{ and }\; a_2(\lambda) = \frac{1-2\lambda}{2\lambda(1{-}\lambda)}.\end{aligned}$$

For $\frac{1}{2n} \le \lambda \le 1 - \frac{1}{2n}$ we find that $\lambda(1{-}\lambda)2^n > M$, while $a_1(\lambda)$ and $a_2(\lambda)$ have the same sign as $\frac{1}{2} - \lambda$. Therefore $W(\lambda)$ is unimodal in this range. Since $\eta(n,k,q) = o(1)$, we have

$$\begin{aligned}\sum_{q=q_1}^{q_2-1} N(n,k,q) &= O(2^n) W\bigl(\tfrac{1}{2} - 2^{-n/2}n\bigr)\\ &= O(2^n)\,\exp\bigl(-(2-o(1))n^2\bigr)\,W\bigl(\tfrac{1}{2}\bigr)\\ &= e^{-O(n^2)}\,W\bigl(\tfrac{1}{2}\bigr)\end{aligned}$$

using (6.1). This shows that the sum over $[q_1, q_2)$ is covered by the error term of the Corollary. By Remark 1.1 the same conclusion holds for the summation from $q_3 + 1$ to q_4.

Finally consider the range $q \in [0, q_1)$, which is the mirror image of the range $q \in (q_4, 2^{n-k}]$. Here we use the trivial bound

$$\sum_{q=0}^{q_1-1} N(n,k,q) < \bigl(2^n\bigr)^{2^k q_1} = 2^{2^{n-1}+O(n2^k)}$$

which also fits into the error term of the corollary. By Remark 1.1, the same conclusion holds for the summation from $q_4 + 1$ to 2^{n-k}, which completes the proof. □

7 More on the case $k = 1$

In the case of $k = 1$, which corresponds to the "balanced colourings" enumerated by Palmer, Read and Robinson [11], it is possible to fill in the range of very small or very large values of q excluded by (1.1).

Lemma 7.1. *If* $0 \le q = o(2^{n/2})$ *then*

$$(2q)!\,N(n,1,q) = \binom{2q}{q}^n \bigl(1 + O(q^2/2^n)\bigr).$$

Proof. Generate a $2q \times n$ matrix by a random process: for each column independently, randomly insert 0 in q rows and 1 in the other q. This matrix is one of those counted by $(2q)!\,N(n,1,q)$ provided all the rows are different. (Recall that $N(n,1,q)$ counts matrices up to row order.)

The probability that a specified pair of rows are equal is

$$2^n\left(\binom{2q-2}{q}\Big/\binom{2q}{q}\right)^n = \left(\frac{q-1}{2q-1}\right)^n < 2^{-n},$$

so, by the Bonferroni inequality, the probability that no two rows are equal is $1-O(q^2/2^n)$. This completes the proof. □

Theorem 7.1. *Uniformly for* $0 \le q \le 2^{n-1}$,

$$N(n,1,q) = \binom{2^n}{2q}\left(\frac{\binom{2^{n-1}}{q}^2}{\binom{2^n}{2q}}\right)^n \bigl(1 + o(n^5 2^{-n/5})\bigr).$$

Proof. We begin by motivating the given formula. Choose, uniformly at random, a set of $2q$ distinct elements of $\{0,1\}^n$. The event that exactly q of these elements have 1 in some specified position has probability

$$\binom{2^{n-1}}{q}^2\Big/\binom{2^n}{2q}.$$

Therefore, the theorem is stating that these n events are very close to being independent in some sense.

We can derive the theorem from Theorem 1.2 and Lemma 7.1. First consider the case that $2^{2n/5}n^{12/5} \le q \le 2^{n-2}$. Then, by Stirling's formula,

$$\left(\binom{2^{n-1}}{q}^2\Big/\binom{2^n}{2q}\right)^n = \bigl(\pi A 2^{n-1}\bigr)^{-n/2}\bigl(1 + O(n/q)\bigr)$$

and

$$\binom{2^n}{2q} = (\pi A 2^{n+1})^{-1/2}\left(\lambda^\lambda(1-\lambda)^{1-\lambda}\right)^{-2^n}(1 + O(1/q))$$

and the theorem follows from Theorem 1.2.

In the case that $0 \le q \le 2^{2n/5}n^{12/5}$, we calculate that

$$\binom{2^{n-1}}{q}^2\Big/\binom{2^n}{2q} = \binom{2q}{q}\binom{2^n-2q}{2^{n-1}-q}\Big/\binom{2^n}{2^{n-1}} = \binom{2q}{q}2^{-2q}\bigl(1 + O(q/2^n)\bigr),$$

so the theorem follows from Lemma 7.1.

Finally, for $2^{n-2} \le q \le 2^{n-1}$, take the complement as in Remark 1.1, noting that the binomial coefficients in the statement of the theorem are symmetric around $q = 2^{n-2}$. □

8 Final remarks

As mentioned in the Introduction, Denisov in [7] incorrectly repudiated the result from [6] that we quoted as Theorem 1.1. Denisov's mistake was due to the incorrect computation of the matrix inverse A^{-1} on page 95 of [7]. In fact the I, J element of A^{-1} is $(-1)^{|J|-|I|}2^{|I|}$ for $I \subseteq J$ and 0 otherwise. Correcting the mistake shows that the critical value $\bar{z}^T Q^{-1} \bar{z}$ on page 97 equals 2^{2k-n+2} and not the value stated. Except for this error, Denisov would have extended Theorem 1.1 to $k = o(n^{1/2})$ and in fact would have matched Theorem 1.2 (with a different vanishing error term) for $k = o(n^{1/2})$ and

$$|q - 2^{n-k-1}| < \rho\, 2^{n/2-k}\, n^{1/2}$$

for any positive constant $\rho < \sqrt{\frac{\log 2}{2}}$. Note that our coverage of both k and q is considerably wider than that.

Finally we mention a connection between correlation-immune boolean function and Hadamard matrices. Recall that a *Hadamard matrix of order n* is an $n \times n$ matrix over ± 1 whose columns are pairwise orthogonal. Such matrices are known to exist for $n = 1$, $n = 2$, and for infinitely many other n. If $n > 2$ then $n \equiv 0 \mod 4$ is a necessary condition for the existence of a Hadamard matrix of order n. It is a long-standing open problem to show that this necessary condition is also sufficient. Let H_n be the number of Hadamard matrices of order n. By a simple normalization, it can be seen that H_n equals 2^n times the number of Hadamard matrices whose leftmost column equals all $+1$'s. If such a column is removed, and each -1 changed to 0, there remains an $n \times (n-1)$ matrix of the sort counted (up to row permutation) by $N(n-1, 2, n/4)$. Hence, $H_n = 2^n n!\, N(n-1, 2, n/4)$ for $n > 2$. This connection raises the possibility of proving the Hadamard conjecture by asymptotic methods. Unfortunately, the coverage of Theorem 1.2 is inadequate for that purpose.

References

[1] E. Bach, Improved asymptotic formulas for counting correlation-immune Boolean functions, Technical Report 1616, Computer Sciences Dept., University of Wisconsin, 2007.

[2] C. Carlet, Boolean functions for cryptography and error correcting codes, Preprint. To appear as a chapter of *Boolean Functions: Theory, Algorithms and Applications* (Y. Crama and P. Hammer, eds.), Cambridge University Press.

[3] C. Carlet and A. Gouget, An upper bound on the number of m-resilient Boolean functions, ASIACRYPT 2002, *Lecture Notes in Comput. Sci.* **2501** (2002) 484–496.

[4] C. Carlet and A. Klapper, Upper bounds on the number of resilient functions and of bent functions, Springer-Verlag, Lecture Notes dedicated to Philippe Delsarte (to appear). A shorter version has appeared in the Proceedings of the 23rd Symposium on Information Theory in the Benelux, Louvain-La-Neuve, Belgian, 2002.

[5] T. W. Cusick and P. Stanica, Cryptographic Boolean Functions and Applications, Elsevier, 2009.

[6] O. V. Denisov, An asymptotic formula for the number of correlation-immune of order q boolean functions, *Discrete Math. Appl.*, **2** (1992) 279–288. originally published in *Diskretnaya Matematika* **3** (1990) 25–46 (in Russian). Translated by A.V. Kolchin.

[7] O. V. Denisov, A local limit theorem for the distribution of a part of the spectrum of a random binary function, *Discrete Math. Appl.*, **10** (2000) 87–101. originally published in *Diskretnaya Matematika*, **12**,1 (2000) (in Russian). Translated by the author.

[8] A. S. Heydayat, N. J. A. Sloane, J. Stufken, Orthogonal arrays : theory and applications, Springer-Verlag, 1999.

[9] S. Maitra and P. Sarkar, Enumeration of correlation immune boolean functions, ACSIP'99, *Lecture Notes in Comput. Sci.*, **1587** (1999) 12–25.

[10] C. Mitchell, Enumerating Boolean functions of cryptographic significance, *J. Cryptology*, **2** (1990), 155-170.

[11] E. M. Palmer, R. C. Read and R. W. Robinson, Balancing the n-cube: a census of colorings, *J. Algebraic Combin.*, **1** (1992) 257–273.

[12] S. M. Park, S. J. Lee, S. H. Sung and K. J. Kim, Improving bounds for the number of correlation immune Boolean functions, *Inform. Process. Lett.*, **61** (1997), 209–212.

[13] N. Roy, A brief outline of research on correlation immune functions, ACISP 2002, *Lecture Notes in Comput. Sci.*, **2384** (2002) 379–394.

[14] P. Sarkar, A note on the spectral characterization of correlation immune Boolean functions, *Inform. Process. Lett.*, **74** (2000) 191–195.

[15] M. Schneider, A note on the construction and upper bounds of correlation-immune functions, *Lecture Notes in Comput. Sci.*, **1355** (1997) 295–306.

[16] Y. Tarannikov, On the structure and numbers of higher order correlation-immune functions, in Proceedings of IEEE International Symposium on Information Theory, 2000, 185.

[17] Y. Tarannikov and D. Kirienko, Spectral analysis of high order correlation immune functions, Proceedings of 2001 IEEE International Symposium on Information Theory, 2001, 69.

[18] R. Wong, *Asymptotic approximations of integrals*, Academic Press, Boston, 1989.

[19] G-Z. Xiao and J. L. Massey, A spectral characterization of correlation-immune combining functions. *IEEE Trans. Inform. Theory*, **34** (1988) 569–571.

[20] Y. X. Yang and B. Guo, Further enumerating Boolean functions of cryptographic significance, *J. Cryptology*, **8** (1995), 115–122.

[21] J-Z. Zhang, Z-S. You and Z-L. Li, Enumeration of binary orthogonal arrays of strength 1, *Discrete Math.*, **239** (2001) 191–198.