UDC 519.142 DOI 10.17223/20710410/52/3

ON THE NONEXISTENCE OF CERTAIN ORTHOGONAL ARRAYS OF STRENGTH FOUR[1]

R. Kiss*, G. P. Nagy**

*,** *Bolyai Institute, University of Szeged, Szeged, Hungary*
** *Department of Algebra, Budapest University of Technology and Economics, Budapest, Hungary*

E-mail: Kiss.Rebeka@stud.u-szeged.hu, nagyg@math.bme.hu

We show that no orthogonal arrays $OA(16\lambda, 11, 2, 4)$ exist with $\lambda = 6$ and 7. This solves an open problem of the NSUCRYPTO Olympiad 2018. Our result allows to determine the minimum weights of certain higher order correlation-immune Boolean functions.

Keywords: *orthogonal array, NSUCRYPTO.*

Introduction

In the Fifth International Students' Olympiad in Cryptography NSUCRYPTO'2018 [1, 2] the following problem was stated. Given three positive integers n, t, and λ such that $t < n$, we call a $\lambda 2^t \times n$ binary array (i.e., matrix over the two-element field) a $t-(2, n, \lambda)$ orthogonal array if in every subset of t columns of the array, every (binary) t-tuple appears in exactly λ rows; t is called the strength of this orthogonal array. Find a $4-(2, 11, \lambda)$ orthogonal array with minimal value of λ. So far, the best known answer to this question is $\lambda = 8$. Delsarte's Linear Programming Bound [3, Theorem 4.15 and Table 4.19] implies $\lambda \geqslant 6$.

In this short note, we use the terminology of the monograph [3] and we denote a $t-(2, n, \lambda)$ orthogonal array by $OA(2^t\lambda, n, 2, t)$. The integers $N = 2^t\lambda$ and n are called the number of runs and the number of factors of the array. In an orthogonal array, the same row can occur multiple times. The orthogonal array is *simple,* if each row occurs exactly once.

Our solution to the problem is stated in the following theorem.

Theorem 1. No orthogonal arrays $OA(16\lambda, 11, 2, 4)$ exist with $\lambda = 6$ and 7.

A Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is *correlation-immune* of some order $t < n$ (in brief, t-CI) if fixing at most t of the n input variables $x_1, \ldots, x_n$ does not change the output distribution of the function, whatever are the positions chosen for the fixed variables and the values chosen for them. Equivalently, the support of the function must be a simple binary orthogonal array of strength t [4, 5]. The weight of a Boolean function is the size of its support. Low weight t-CI Boolean functions have practical importance in cryptography, since they resist the Siegenthaler attack. Furthermore, t-CI Boolean functions allow reducing the overhead while keeping the same resistance to side channel attacks; see [5] and the references therein.

[1]Support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme, within the SETIT Project 2018-1.2.1-NKP-2018-00004. Partially supported by NKFIH-OTKA Grants 119687, 115288 and SNN 132625.

Theorem 1 allows us to determine the minimum weights of t^{th}-order correlation-immune Boolean functions in n variables,

$$n \in \{11, 12, 13\}, \quad t \in \{4, 5\}.$$

These values were marked as unknown in [4, Table 2] and [5, Table 2].

We would like to thank Claude Carlet (Paris, France and Bergen, Norway) for his detailed comments on the previous version of this paper.

1. Proof of the theorem

Our proof uses the results [6 – 9]. D. A. Bulutoglu and F. Margot [6] used integer linear programming (ILP) methods, while the algorithms [7, 8] are based on the systematic study of the extensions of orthogonal arrays by new columns. Moreover, both approaches must deal with the isomorphism problem of orthogonal arrays.

***Proof of the Theorem* 1.** From [6, Table 1], [7, Table III] and also [9] we can see that no $OA(96, 8, 2, 4)$ and no $OA(112, 7, 2, 4)$ exist. We explain the relevant rows of the two tables. In [6, Table 1] there are 4 columns with the following meanings (see Table 1):

— OA gives the parameters of the classified orthogonal array;
— m' is the number of linearly independent equality constraints of the generated ILP problem;
— $p_{\max}$ is an upper bound on the maximum number of times a run can appear in an $OA(2^t\lambda, n, 2, t)$;
— h is the number of non-isomorphic orthogonal arrays with the given parameters.

Table 1

OA	m'	$p_{\max}$	h
$OA(96, 8, 2, 4)$	163	2	0
$OA(112, 7, 2, 4)$	99	3	0

From this table we can see that if $\lambda = 6$ then no orthogonal array exists with $n = 8$, which implies that no OA exists with $n \geqslant 8$. Similarly if $\lambda = 7$ then no orthogonal array exists with $n = 7$, thus no OA exists with $n \geqslant 7$.

In [7, Table III] (see also Table 2) orthogonal arrays with strength 4 are included, where

— N gives the run-size of the classified orthogonal array;
— the notation 2^a for the factor set means a binary array with a factors;
— $a_{\max}$ is the maximum number a, such that there exists an OA with N runs and a factors;
— the numbers m_a, $a \in \{t+1, \ldots, a_{\max}\}$, in the last column denote the number of isomorphism classes of arrays with N runs and a factors.

Table 2

N	Factor set	$a_{\max}$	Isomorphism classes
96	2^a	7	$4, 9, 4$
112	2^a	6	$4, 3$

This means that with run-size 96 the maximum number a such that an $OA(96, a, 2, 4)$ exists is 7, and with run-size 112 the maximum number a with an existing $OA(112, a, 2, 4)$ is 6. ■

Remark 1. According to [8], the number of isomorphism classes of binary orthogonal arrays with run-size $N = 128$, factor-size $n = 11$, and strength $t = 4$ is 477. The papers [6, 7] claim to achieve the above results within a few seconds. Using SageMath [10], the GLPK package [11] and the integer linear programming solver SCIP [12], a straightforward implementation of the formulas of [6] used 51 630 s and 481 s CPU time for the nonexistence of $OA(96, 8, 2, 4)$ and $OA(112, 7, 2, 4)$, respectively.

2. Minimum weight of correlation-immune Boolean functions

Using the notation of [3], we denote by $F(n, 2, t)$ the minimal number of runs N in any $OA(N, n, 2, t)$ for given values n and t. Theorem 1 says that $F(11, 2, 4) \geqslant 128$, and in fact, equality holds. Let $\omega_{n,t}$ denote the minimum weight of t-CI Boolean functions in n variables. Equivalently, $\omega_{n,t}$ is the minimum number of runs in a *simple* orthogonal array with number of factors n and strength t. Hence,

$$F(n, 2, t) \leqslant \omega_{n,t}. \tag{1}$$

Suppose A is an $OA(N, n, s, t)$. As in [3, p. 5], one can construct an $OA(N/s, n-1, s, t-1)$, say A'. Clearly, if A is simple then A' is simple too. This implies

$$F(n-1, 2, t-1) \leqslant \frac{1}{2}F(n, 2, t),$$
$$\omega_{n-1,t-1} \leqslant \frac{1}{2}\omega_{n,t}. \tag{2}$$

We are now able to fill some unknown values of [4, Table 2] and [5, Table 2].

Proposition 1. For the minimum weight of t-CI Boolean functions in n variables, we have

$$\omega_{11,4} = \omega_{12,4} = \omega_{13,4} = \omega_{14,4} = \omega_{15,4} = 128; \tag{3}$$
$$\omega_{11,5} = \omega_{12,5} = \omega_{13,5} = \omega_{14,5} = \omega_{15,5} = \omega_{16,5} = 256. \tag{4}$$

Proof. The Nordstrom — Robinson code and also Sloane gives a simple $OA(256, 16, 2, 5)$, see [1, 13, 14]. Straightforward computation shows that deleting the last 5 columns of it, the resulting orthogonal array is simple. Hence, $\omega_{n,5} \leqslant 256$ for $n \in \{11, \ldots, 16\}$. By (2), $\omega_{n,4} \leqslant 128$ for $n \in \{10, \ldots, 15\}$. Theorem 1 implies $F(n, 2, 4) \geqslant 128$ for $n \geqslant 11$. From (1) and (2) follow (3) and (4). ■

REFERENCES

1. *Gorodilova A., Agievich S., Carlet C., et al.* The Fifth International Students' Olympiad in cryptography — NSUCRYPTO: Problems and their solutions. Cryptologia, 2020, vol. 44, no. 3, pp. 223–256.
2. `www.nsucrypto.nsu.ru/unsolved-problems/` — NSUCRYPTO Unsolved problems, 2020.
3. *Hedayat A. S., Sloane N. J. A., and Stufken J.* Orthogonal Arrays: Theory and Applications. N.Y., Springer Verlag, 1999.
4. *Carlet C. and Chen X.* Constructing low-weight dth-order correlation-immune Boolean functions through the Fourier — Hadamard transform. IEEE Trans. Inform. Theory, 2018, vol. 64, no. 4, pp. 2969–2978.
5. *Carlet C. and Guilley S.* Correlation-immune Boolean functions for easing counter measures to side-channel attacks (Ch. 3). H. Niederreiter, A. Ostafe, D. Panario, A. Winterhof (eds.). Algebraic Curves and Finite Fields Cryptography and Other Applications, Radon Series on Computational and Applied Mathematics, vol. 16, Berlin, De Gruyter, 2014, pp. 41–70.
6. *Bulutoglu D. A. and Margot F.* Classification of orthogonal arrays by integer programming. J. Statistical Planning Inference, 2008, vol. 138, no. 3, pp. 654–666.

7. *Schoen E. D., Eendebak P. T., and Nguyen M. V. M.* Complete enumeration of pure-level and mixed-level orthogonal arrays. J. Combinat. Designs, 2009, vol. 18, no. 2, pp. 123–140.
8. *Schoen E. D., Eendebak P. T., and Nguyen M. V. M.* Correction to: Complete enumeration of pure-level and mixed-level orthogonal arrays. J. Combinat. Designs, 2010, vol. 18, no. 6, pp. 488–488.
9. *Eendebak P.* Complete series of non-isomorphic orthogonal arrays. `www.pietereendebak.nl/oapackage/series.html`. 2020.
10. `www.sagemath.org` — The Sage Developers. SageMath, the Sage Mathematics Software System (Version 9.1), 2020.
11. *Makhorin A.* Gnu linear programming kit. `www.gnu.org/software/glpk/`. 2020.
12. *Gamrath G., Anderson D., Bestuzheva K., et al.* The SCIP Optimization Suite 7.0. `www.optimization-online.org/DB_HTML/2020/03/7705.html`. 2020.
13. *Bierbrauer J.* Nordstrom — Robinson code and A_7-geometry. Finite Fields and Their Appl., 2007, vol. 13, no. 1, pp. 158–170.
14. *Sloane N. J. A.* A Library of Orthogonal Arrays. `www.neilsloane.com/oadir/`. 2020.