BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **18**, No 5
Special Thematic Issue on Optimal Codes and Related Topics
Sofia • 2018 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2018-0023

On the Classification of Splitting (v, $u\times c$, λ) BIBDs

Stela Zhelezova

Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria
E-mail: stela@math.bas.bg

Abstract: *The (v, $u\times c$, λ)-splitting balanced incomplete block designs correspond to c-splitting authentication codes. We classify splitting balanced incomplete block designs with definite parameters.*

Keywords: *Splitting balanced incomplete block design, splitting authentication code.*

1. Introduction

Authentication codes were invented by G i l b e r t, M a c W i l l i a m s and S l o a n e [9] for protecting the integrity of information. The authentication codes involve three active parties: A transmitter T, a receiver R, and an opponent O as a model of S i m m o n s [15]. The transmitter sends a message to the receiver using an insecure communication channel. The opponent has access to the channel and can interfere with the contents of the message transmitted via this channel.

The transmitter and the receiver share a common key e. It is chosen from some key space E. Given a source state s from some source state space S, the transmitter T computes a message $m = e(s) \in M$, where M is the message space, and sends $m \in M$ to the receiver. The receiver accepts or rejects the transmitted message $m \in M$ based on the same key e. It is possible that more than one message can be used to communicate a particular source state $s \in S$, so this is called splitting. If splitting occurs, then the transmitter and the receiver need to choose a splitting strategy to determine $m \in M$, given $s \in S$ and $e \in E$. For any $e \in E$, $e(s_1) \cap e(s_2) = 0$ if $s_1 \neq s_2$ otherwise decoding would be impossible.

O g a t a et al. [13] introduced a special type of a Balanced Incomplete Block Design (BIBD) in connection with authentication codes – a splitting BIBD. They established an equivalence between splitting BIBDs and splitting authentication codes. Recently this kind of combinatorial design has been studied intensively mainly with respect to the existence problem.

In this paper we classify splitting designs for some small parameters. We do this by a computer-aided method which differs from those used in the papers cited above. It is based on a construction method for resolvable balanced incomplete block designs

[18]. The method is explained in Section 3 and the obtained results are presented in Section 4.

2. Basic definitions and notations

An authentication code with splitting is a triple (S, M, E), together with probability distributions $\{p_S(s)\}_{s\in S}$, $\{p_E(e)\}_{e\in E}$, and $\{\{p(m|e, s)\}_{m\in M} : e\in E, s\in S\}$, such that:

- S is a finite set of u source states;
- M is a finite set of v messages;
- E is a finite set of b encoding rules associating to a source state $s\in S$ one or more messages in M.

A splitting authentication code is c-splitting if $|e(s)| = c$ for any $e\in E$, $s\in S$.

The family of encoding rules of an authentication code is described usually by an $b\times u$ encoding matrix with entries in M. Its rows are indexed by the elements of E, the columns are indexed by the elements of S, and the entry (e, s) of the matrix is the set $e(s)$ (Fig. 3).

For the basic concepts and notations concerning combinatorial designs refer, for instance, to [4, 5].

Let $V = \{P_i\}_{i=1}^{v}$ be a finite set of *points*, and $\mathcal{B} = \{B_j\}_{j=1}^{m}$ a finite collection of k-element subsets of V, called *blocks*. We say that $D = (V, \mathcal{B})$ is a *design* (BIBD) with parameters 2-(v, k, λ), if any 2-element subset of V is contained in exactly λ blocks of $\mathcal{B}$.

Each point of D is incident with R blocks and the number of the blocks of the design m is

$$R = \frac{\lambda(v-1)}{(k-1)},\ m = \frac{\lambda v(v-1)}{k(k-1)}.$$

An incidence matrix of the design is a matrix of v rows and m columns which contains a 1 in the i-th row and j-th column iff the i-th point is contained in the j-th block, and 0 if not. The design is completely determined by its incidence matrix.

Two designs are *isomorphic* if there exists an one-to-one correspondence between the point and block sets of the first design and respectively, the point and block sets of the second design, and if this one-to-one correspondence does not change the incidence. An *automorphism* of the design is a permutation of the points that transforms the blocks into blocks.

A *parallel class* is a partition of the point set by blocks. A near parallel class is a partial parallel class missing a single point. A (*near*) *resolution* is a partition of the blocks collection into (near) parallel classes. The design is (*near*) *resolvable* if it has at least one (near) resolution. The parameters of near resolvable designs are $(v, k, k–1)$ and for such a design, every point is absent from exactly one class.

Two (near) resolutions are isomorphic if there exists an automorphism of the design mapping each (near) parallel class of the first (near) resolution into a (near) parallel class of the second one.

Let $\mathcal{R} = \mathcal{R}_i, \ldots, \mathcal{R}_R$ and $T = T_i, \ldots, T_R$ be both (near) resolutions of one and the same design. These two resolutions are orthogonal if $|\mathcal{R}_i \cap T_j| \leq 1$, $1 \leq i, j \leq R$. When a design has two orthogonal (near) resolutions it is doubly (near) resolvable [1]. Orthogonal (near) resolutions may or may not be isomorphic to each other.

A $(v, u\times c, \lambda_s)$-*splitting* BIBD [13] is a pair $(V, \mathcal{B})$ such that the following properties are satisfied, where $B_j \in \mathcal{B}$ is called a *super-block*.

- $|V| = v$ is a finite set of *points* p_i, $1 \leq i \leq v$, $|\mathcal{B}| = b$ is a finite family of super-blocks;
- Every $B_j \in \mathcal{B}$ is expressed as a disjoint union $B_j = B_{j,1} \cup \ldots \cup B_{j,u}$, where $B_{j,n} \subseteq V$, $1 \leq n \leq u$ and $|B_{j,1}| = \ldots = |B_{j,u}| = c$;
- For each $x, y \in V$ $(x \neq y)$, there exist *exactly* λ_s super-blocks B_j such that $x \in B_{j,n_1}$, $y \in B_{j,n_2}$, $n_1 \neq n_2$.

Each point of V is contained in exactly:

$$r = \frac{\lambda_s(v-1)}{c(u-1)},$$

super-blocks and the number of super-blocks is

$$b = \frac{\lambda_s v(v-1)}{c^2 u(u-1)}.$$

Therefore the necessary conditions for the existence of a $(v, u\times c, \lambda_s)$-splitting BIBD are [13]:

$$v \geq u.c,$$
$$\lambda_s(v-1) \equiv 0 \bmod (c(u-1)),$$
$$\lambda_s v(v-1) \equiv 0 \bmod (c^2 u(u-1)).$$

Two splitting BIBDs are *equivalent* if there exists a permutation of the points which transforms each super-block of the first splitting design to a super-block of the second one.

There are already quite a lot of works on the existence of $(v, u\times c, \lambda_s)$-splitting BIBDs with definite parameters, see for instance [6-8, 16, 17, 19]. O g a t a et al. [13] show that the existence of a (v, c, λ_s) u-external difference family over an Abelian group $(X, +)$ implies the existence of a $(v, u\times c, \lambda_s)$-splitting BIBD.

Up to now all construction methods involve some types of combinatorial designs. G e, M i a o and W a n g [8] show that splitting BIBDs are a special kind of balanced graph designs and establish the existence of $(v, u\times c, 1)$-splitting BIBDs for $u = \{3, 4\}$, $c = 2$ and for $u\times c = 2\times c$, c even or 3. In [7] group-divisible designs are used to set the existence of $(v, 2\times 3, \lambda_s)$-splitting BIBDs and in [16] to resolve the existence question for $(v, 3\times 3, \lambda_s)$-splitting BIBDs, λ between 2 and 9. W a n g [19] also use group-divisible designs to obtain a new infinite class of optimal 3-splitting authentication codes ($(v, 3\times 3, 1)$-splitting BIBDs).

In [6] and [7] perfect Mendelsohn designs, nested balanced incomplete block designs and a direct cyclic construction lead to the establishment of the existence of $(v, 2\times 2, \lambda_s)$-splitting, $(v, 2\times 3, \lambda_s)$-splitting and $(v, 3\times 2, \lambda_s)$-splitting BIBDs for

particular values of λ. A summary of the known results on the existence of splitting designs was recently published in [17, Theorem 1.2 - 4], where the authors also settle the existence problem of (v, 3×3, λ_s)-splitting and (v, 3×4, 1)-splitting designs.

From combinatorial point of view after the existence problem the question about the number of the splitting designs with definite parameters arises. A constructive classification might be very useful for application purposes because designs with some additional properties can be chosen for any particular application. The aim of the present work is the classi cation of splitting BIBDs with certain parameters.

3. Construction method

We can rearrange an incidence matrix of a resolvable BIBD with respect to the parallel classes (an example is given in Fig. 1). The first m/R matrix columns are a partition of the point set and hence one parallel class, the second m/R columns are the next parallel class and so on. Vertical lines separate the different parallel classes in Fig. 1.

$$\left(\begin{array}{cc|cc|cc|cc|cc|cc|cc|cc|cc} 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0\\ 1&0&1&0&1&0&1&0&0&1&0&1&0&1&0&1&0&1\\ 1&0&0&1&0&1&0&1&1&0&1&0&1&0&0&1&0&1&0&1\\ 0&1&1&0&0&1&0&1&1&0&0&1&0&1&1&0&1&0&0&1\\ 0&1&0&1&1&0&0&1&0&1&1&0&0&1&1&0&0&1&1&0\\ 0&1&0&1&0&1&1&0&0&1&0&1&1&0&0&1&1&0&1&0 \end{array}\right)$$

Fig. 1. The incidence matrix of a resolvable (6, 3, 4) BIBD

Usually a splitting BIBD is presented by a list of it's super-blocks as in [6, 7, 13] or by a family of arrays as in [8, 16, 17, 19]. Here we use a different representation of a splitting BIBD as super-matrix. In this way we reduce the size of the objects and we succeed to classify splitting BIBDs for some parameters.

Let's define an *incidence matrix A* of a (v, u×c, λ_s)-splitting BIBD in a similar way as for BIBD: $A = (a_{i,(j-1)u+n})_{v\times ub}$, where $a_{i,(j-1)u+n} = 1$ if $p_i \in B_{j,n}$ and $a_{i,(j-1)u+n} = 0$ if $p_i \notin B_{j,n}$ (i = 1, 2, …, v, j = 1, 2,…, b, and n = 1, 2, …, u). Note that here B_j is a super-block and it is split into u blocks. Each point p_i, $1 \le i \le v$, is incident with r super-blocks and each block is incident with c points. It is obvious that there are $v - uc$ missing points in each super-block.

As an example let us consider an incidence matrix of a (7, 2×3, 3)-splitting design (Fig. 2). Here v = 7 points (rows of the matrix) and ub = 14 blocks (columns), b = 7 super-blocks, where each of them consists of u = 2 blocks. Each block is incident with c = 3 points and each point is incident with r = 6 super-blocks. The first u = 2 matrix columns are in a super-block, the next two in another and so on. A point is absent from each super-block ($v - uc$ = 1).

For a splitting BIBD a super-block is not a partition of the point set as a parallel class is for a BIBD, but each point is at most once in a super-block.

$$\left(\begin{array}{cc|cc|cc|cc|cc|cc|cc}
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1
\end{array}\right)$$

Fig. 2. Incidence matrix of a (7, 2×3, 3)-splitting design

One popular approach for constructing a resolvable BIBD is to generate not the resolution itself, but the corresponding equidistant code. There is a one-to-one correspondence [14] between the resolutions of 2-(qk, k, λ) designs and the (R, qk, $R - \lambda$)$_q$ equidistant codes, $q > 1$. An equidistant (R, v, H_d)$_q$ code is a set of v words of length R over an alphabet with q elements, such that the Hamming distance between any two distinct codewords is exactly H_d. The equidistant code given in Fig. 3 corresponds to the resolution of the design from Fig. 1.

$$\begin{array}{cccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 \\
1 & 2 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 2 \\
2 & 1 & 2 & 2 & 1 & 2 & 2 & 1 & 1 & 2 \\
2 & 2 & 1 & 2 & 2 & 1 & 2 & 1 & 2 & 1 \\
2 & 2 & 2 & 1 & 2 & 2 & 1 & 2 & 1 & 1
\end{array}$$

Fig. 3. An equidistant (10, 6, 6)$_2$ code

Each parallel class is replaced by a q-ary column, $q = \frac{v}{k}$ such that symbol n is assigned to a row with one in the n-th position. So we define in the same manner the incidence super-matrix G of a splitting BIBD: $G = (g_{i,j})_{v \times b}$, where $g_{i,j} = n$ if $p_i \in B_{j,n}$ and $g_{i,j} = 0$ if $p_i \notin B_j$ ($i = 1, 2, \ldots, v$, $j = 1, 2, \ldots, b$, and $n = 1, 2, \ldots, u$). In this case the alphabet is with $q = \frac{v}{c} + 1 = u + 1$ elements, because we use one more element to denote the super-block missing points. The number of zeroes in each column is the number of absent points from each super-block. In this way we deal with a $v \times b$ matrix (Fig. 4) instead of a $v \times ub$ one (Fig. 2).

0	1	1	1	2	2	2
1	1	2	2	0	1	2
1	2	1	2	1	2	0
1	2	2	1	2	0	1
2	0	1	2	2	1	1
2	1	2	0	1	2	1
2	2	0	1	1	1	2

Fig. 4. Incidence super-matrix of a (7, 2×3, 3)-splitting design

In the case $v \equiv 1 \pmod{c}$, i.e., $v = uc + 1$ (v, $u \times c$; λ_s)-splitting BIBD corresponds to a (v, c, $c - 1$) doubly near resolvable design. The columns of a super-matrix form the near parallel classes of the first near resolution while its rows – the near parallel classes of the second one. In [10, Theorem 2] authors introduce the correspondence between near resolutions of (v, k, λ_s) BIBDs and special kind of codes. They are defined in the same manner as above. There the absent point is denoted by a special symbol while we use the zero symbol. Also in [2, Theorem 1] the correspondence between near resolvable BIBDs and constant-weight codes meeting the Johnson's bound is presented. Both papers consider only this particular case. Near resolvable designs were generalized in [3] to m-nearly resolvable BIBDs under additional restrictions. There are no correspondence between splitting BIBDs with more than one missing point and m-nearly resolvable BIBDs.

In our example (Fig. 4) looking at the incidence super-matrix of the considered splitting BIBD if we choose 1's for the source state s_1, 2's for s_2 and if each column i corresponds to a key rule e_i a 3-splitting authentication code is obtained (Fig. 5).

e_i	s_1	s_2
e_1	{2, 3, 4}	{5, 6, 7}
e_2	{1, 2, 6}	{3, 4, 7}
e_3	{1, 3, 5}	{2, 4, 6}
e_4	{1, 4, 7}	{2, 3, 5}
e_5	{3, 6, 7}	{1, 4, 5}
e_6	{2, 5, 7}	{1, 3, 6}
e_7	{4, 5, 6}	{1, 2, 7}

Fig. 5. A 3-splitting authentication code from the (7, 2×3, 3)-splitting design

By permuting the points, the super-blocks and the blocks within a super-block, a splitting design can be transformed in a splitting design with the following properties:

- The first super-block is fixed and its blocks are:

$\{v - cu + 1, v - cu + 2, \ldots, v - c(u - 1)\}$,

$\{v - c(u - 1) + 1, \ldots, v - c(u - 2)\}, \ldots, \{v - c + 1, v - c + 2, \ldots, v\}$.

- The rows of the incidence super-matrix are in ascending lexicographic order.
- The columns of the incidence super-matrix are in ascending lexicographic order.

Regarding the defined incidence super-matrix (Fig. 4) this means that the first column is $(0, \ldots, 0, 1, 1, \ldots, 1, \ldots, u, u, \ldots, u)^T$ and the rows and the columns are in lexicographic order.

Let us consider part of the design points and their incidence with the design blocks. We shall call the structure obtained in this manner *partial solution*.

We generate by backtrack search row by row the incidence super-matrix that corresponds to a splitting BIBD with definite parameters. An equivalence test is applied on the partial solutions after each added row (point). This equivalence test checks if some permutation of the constructed rows can transform the current solution into a lexicographically smaller one which has already been considered. If this happens, the partial solution is not extended and the next possibility for the current row is considered. The details of such a technique are well described, for instance, in [11].

4. Results

This way we succeed to classify up to equivalence splitting designs with some small parameters. The results are summarized in Table 1. In the last column the number of nonisomorphic splitting BIBDs is given.

In [12] all $(2k + 1, k, k – 1)$ near resolvable BIBDs for $3 \le k \le 13$ are enumerated. There are only one nonisomorphic such near resolvable BIBD for $k \le 11$. Writing them in terms of super-matrix defined above shows that they also are doubly resolvable. This concerns (5, 2×2, 2)-splitting, (7, 2×3, 3)-splitting and (11, 2×5, 5)-splitting designs. They correspond to (5, 2, 1), (7, 3, 2) and (11, 5, 4) doubly near resolvable BIBDs.

Table 1. Splitting BIBDs

v	$u \times c$	λ	r	b	Number
5	2×2	2	4	5	1
9	2×2	1	4	9	2
9	2×2	2	8	18	2,083
6	2×3	6	10	10	1
7	2×3	3	6	7	1
11	2×5	5	10	11	1
9	3×2	3	6	9	14,966

***Acknowledgements*:** This work is supported by the Bulgarian National Science Fund (Contract No DH 02/2, 13.12.2016).

References

1. A b e l, R. J. R., G. G e, J. Y i n. Resolvable and Near-Resolvable Designs. – In: C. J. Colbourn, J. H. Dinitz, Eds. Handbook of Combinatorial Designs. 2nd Edition. Boca Raton, FL. CRC Press, 2007, pp. 124-132.
2. B a s s a l y g o, L. A., V. A. Z i n o v i e v. Remark on Balanced Incomplete Block Designs, Near-Resolvable Block Designs, and *q*-ary Constant-Weight Codes. – Problems of Information Transmissions, Vol. **53**, 2017, No 3, pp. 51-54.
3. B a s s a l y g o, L. A., V. S. L e b e d e v, V. A. Z i n o v i e v. On m-Nearly Resolvable BIB Designs and *q*-ary Optimal Constant Weight Codes. – In: Proc. of 10th International Workshop on Coding and Cryptography, 18-22 September 2017, Saint-Petersburg, Russia.
4. B e t h, T., D. J u n g n i c k e l, H. L e n z. Design Theory. Cambridge University Press, 1993.
5. C. J. Colbourn, J. H. Dinitz, Eds. Handbook of Combinatorial Designs. 2nd Edition – Discrete Mathematics and Its Applications, K. Rosen, Eds. Boca Raton, FL., CRC Press, 2007.
6. D u, B. Splitting Balanced Incomplete Block Designs with Block Size 3×2. – J. Combin. Des., Vol. **12**, 2004, pp. 404-420.
7. D u, B. Splitting Balanced Incomplete Block Designs. – Australas. J. Comb., Vol. **31**, 2005, pp. 287-298.
8. G e, G., Y. M i a o, L. W a n g. Combinatorial Constructions for Optimal Splitting Authentication Codes. – SIAM J. Discrete Math., Vol. **18**, 2005, No 4, pp. 663-678.
9. G i l b e r t, E. N., F. J. M a c W i l l i a m s, N. J. A. S l o a n e. Codes which Detect Deception. – Bell. System Tech. J., Vol. **53**, 1974, pp. 405-424.
10. H a a n p ä ä, H., P. K a s k i. The Near Resolvable 2-(13, 4, 3) Designs and Thirteen-Player Whist Tournaments. – Des. Codes Cryptogr., Vol. **35**, 2005, No 3, pp. 271-285.
11. K a s k i, P., P. Ö s t e r g å r d. Classification Algorithms for Codes and Designs. Berlin, Springer, 2006.
12. M o r a l e s, L. B., R. S a n A g u s t i n, C. V e l a r d e. Enumeration of All $(2k + 1, k, k – 1)$-NRBIBDs for $3 \leq k \leq 13$, 2007.
    http://www.mcc.unam.mx/ lbm/JCMCC05.pdf
13. O g a t a, W., K. K u r o s a w a, D. R. S t i n s o n, H. S a i d o. New Combinatorial Designs and Their Applications to Authentication Codes and Secret Sharing Schemes. – Discrete Math., Vol. **279**, 2004, No 1-3, pp. 383-405.
14. S e m a k o v, N., V. Z i n o v i e v. Equidistant *q*-ary Codes with Maximal Distance and Resolvable Balanced Incomplete Block Designs. – Problems Inform. Transmission, Vol. **4**, 1968, No 2, pp. 3-10.
15. S i m m o n s, G. J. A Game Theory Model of Digital Message Authentication. – Congressus Numer., Vol. **34**, 1982, pp. 413-424.
16. S u, R., J. W a n g. On the Existence of $(v, 3\times3, \lambda)$-Splitting Balanced Incomplete Block Design with λ between 2 to 9. – Journal of Shanghai Jiaotong University (Science), Vol. **3**, 2008, No 4, pp. 482-486.
17. S u, R., J. W a n g. Further Results on the Existence of Splitting BIBDs and Application to Authentication Codes. – Acta Appl. Math., Vol. **109**, 2010, No 3, pp. 791-803.
18. T o p a l o v a, S., S. Z h e l e z o v a. Doubly Resolvable Designs with Small Parameters. – Ars Combin., Vol. **117**, 2014, pp. 289-302.
19. W a n g, J. A New Class of Optimal 3-Splitting Authentication Codes. – Des. Codes Cryptogr., Vol. **38**, 2006, pp. 373-381.

Received 30.09.2017; Second Version 05.12.2017; Accepted 28.12.2017