

Hadamard Matrices on Error Detection and Correction: Useful Links to BIBD



Carla Francisco, Teresa A. Oliveira, Amílcar Oliveira,
and Francisco Carvalho

Abstract In the areas of Computer Science and Telecommunications there is a huge amount of applications in which error control, error detection and error correction are crucial tools to enable reliable delivery of digital data over unreliable communication, thus providing quality of service. Hadamard matrices can almost directly be used as an error-correcting code using an Hadamard code, generalized in Reed-Muller codes. Advances in algebraic design theory by using deep connections with algebra, finite geometry, number theory, combinatorics and optimization provided a substantial progress on exploring Hadamard matrices. Their construction and its use on combinatorics are crucial nowadays in diverse fields such as: quantum information, communications, networking, cryptography, biometry and security. Hadamard matrices give rise to a class of block designs named Hadamard configurations and different applications of it based on new technologies and codes of figures such as QR Codes are present almost everywhere. Some connections to Balanced Incomplete Block Designs are very well known as a tool to solve emerging problems in these areas. We will explore the use of Hadamard matrices on QR Codes error detection and correction. Some examples will be provided.

Keywords BIBD · Error-correcting code · Hadamard matrices · QR Codes

C. Francisco (✉)

Département des Sciences du Bois et de la Forêt, Université Laval, Québec, QC, Canada
e-mail: carla.francisco.1@ulaval.ca

T. A. Oliveira · A. Oliveira

Departamento de Ciências e Tecnologia, Universidade Aberta, Portugal and Centro de Estatística e Aplicações, Universidade de Lisboa, Lisboa, Portugal

F. Carvalho

Unidade Departamental de Matemática e Física, Instituto Politécnico de Tomar and CMA – Centro de Matemática e Aplicações, Faculdade de Ciências e Tecnologia, Universidade Nova de Lisboa, Caparica, Portugal

1 Hadamard Matrices

An Hadamard¹ matrix is a square matrix \mathbf{H}_n of order n with entries ± 1 and whose rows (or columns vice versa) are mutually orthogonal, see Seberry [24]. If \mathbf{H}_n is Hadamard matrix, then $\mathbf{H}_n \mathbf{H}_n^T = n \mathbf{I}_n$. An Hadamard matrix remains so when any row or column is multiplied by -1 . Having this into consideration, one can always write an Hadamard matrix with its first row and first column having only $+1$'s, that it is the normal form of an Hadamard matrix, see Sylvester [26].

If \mathbf{H}_n exists for $n = 1$, then \mathbf{H}_2 can be written like the one below:

$$\mathbf{H}_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

More examples of Hadamard matrices:

$$\mathbf{H}_4 = \left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array} \right]; \mathbf{H}_8 = \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array} \right]$$

4×4 Hadamard matrix
 8×8 Hadamard matrix

The necessary condition for the existence of an Hadamard matrix \mathbf{H}_n , $n > 2$ is that $n \equiv 0(mod4)$; more about this can be found on Hall [8]. Hadamard matrices for all permissible values of $n \leq 100$, with the exception of $n = 92$ can be found on Plackett and Burman [18]. Only later on Baumert et al. [1] presented an Hadamard matrix of order 92.

According to Hedayat and Wallis [9] and to Sawade [23] Hadamard matrices have their existence confirmed for all permissible values of $n \leq 424$.

If \mathbf{H}_m and \mathbf{H}_n are Hadamard matrices of orders m and n , respectively, then their tensor product $\mathbf{H}_m \otimes \mathbf{H}_n$ is an Hadamard matrix of order mn , where \otimes denotes the Kronecker matrix product. So, in particular, an Hadamard matrix \mathbf{H}_n of order n where $n = 2s$ and $s \geq 2$ is an integer can be built by taking the s -fold tensor product

¹Jacques Hadamard (1865–1963).

of \mathbf{H}_2 with itself, as it is given below:

$$\mathbf{H}_{2^s} = \underbrace{\mathbf{H}_2 \otimes \mathbf{H}_2 \otimes \cdots \otimes \mathbf{H}_2}_{s \text{ times}}.$$

Hadamard matrices are very well known because of the wide range of applications, not only in several areas of mathematics, but also in other sciences and mainly those connected with new technological advances, like cryptography Ogata et al. [15], image analysis, signal processing, coding theory and algorithm design, see e.g. Francisco [6]. In Statistics, Combinatorial Designs and Experimental design the Hadamard matrices play a key role in the block design construction. We refer to Din and Mavron [5] and to Koukouvinos [11] where one can see how these matrices are useful for the construction of BIBD (balanced incomplete block design)—see Sect. 2—, and for designs and secret sharing schemes, respectively.

2 Relationship Between Hadamard Matrices and BIBD

Consider now an Hadamard matrix \mathbf{H}_{4u} , which without loss of generality is assumed to be in its normal form. Delete from \mathbf{H}_{4u} , its first row and first column of all ones, thus obtaining a matrix \mathbf{A} of order $(4u - 1) \times (4u - 1)$.

Taking \mathbf{A} we can define $\mathbf{N} = \frac{1}{2}(\mathbf{A} + \mathbf{J}_{4u-1})$, where $\mathbf{J}_u = \mathbf{1}_u \mathbf{1}_u^\top$.

This means that \mathbf{N} is obtained from \mathbf{A} , by replacing the -1 's in \mathbf{A} by zero and keeping $+1$'s unaltered. Then, it is easy to see that \mathbf{N} is the incidence matrix of a balanced incomplete block design (BIBD) with parameters:

$$v = 4u - 1 = b ; r = 2u - 1 = k ; \lambda = u - 1 \quad (1)$$

as presented by Yates, see [28], in his agriculture experiments, where these parameters would stand for v varieties in b blocks of size k , so that each variety occurs exactly r times along the blocks and every pair of varieties concurs in exactly λ blocks, see Raghvarao [19].

Conversely, if \mathbf{N} is the incidence matrix of a BIBD with parameters given by (1), then by replacing the 0's in \mathbf{N} by -1 and bordering the resultant matrix by a row and column of all ones, one gets an Hadamard matrix of order $4u$.

We thus have the following theorem

Theorem 1 *The existence of an Hadamard matrix of order $4u$ is equivalent to the existence of a BIBD with parameters given by (1).*

Example 1 Consider an Hadamard matrix \mathbf{H}_{16} which can be obtained by forming the tensor product $\mathbf{H}_4 \otimes \mathbf{H}_4$, where \mathbf{H}_4 is as below:

$$\mathbf{H}_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Following the construction method described above, we get a solution of a BIBD with parameters $v = 15 = b, r = 7 = k, \lambda = 3$.

A review of several construction methods to synthesize these matrices was presented by Oliveira [16, 17], namely Paley Matrices, Sylvester Matrices and Kronecker recursive product. We also refer to Stinson [25] and Cameron [4], as well as to the webpage

<http://mathworld.wolfram.com/HadamardMatrix.html>

for more examples of such matrices.

Now consider the BIBD (7,7,3,3,1) and the BIBD(13,13,4,4,1). If we add a row and a column of 1's, and if we replace all the null entrances in the matrix by (1), we obtain the following Hadamard matrices:

$$\mathbf{H}_7 = \begin{bmatrix} 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\ -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\mathbf{H}_{13} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \end{bmatrix}$$

Fig. 1 BIBD (7,7,3,3,1)

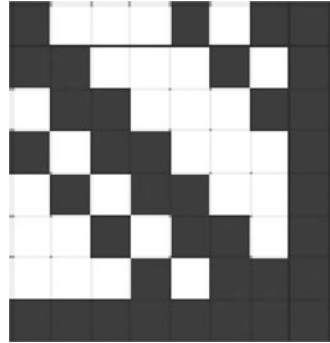
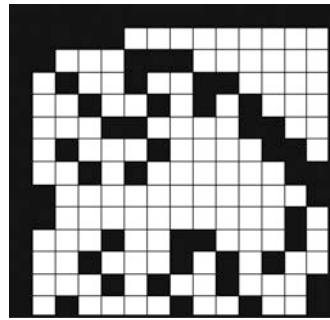


Fig. 2 BIBD (13,13,4,4,1)



Sometimes in the literature Hadamard matrices are represented by a square in black and white, as we can have for our examples. Using this form, in figures, see Figs. 1 and 2, we present Hadamard matrices corresponding to the BIBD(7,7,3,3,1) and BIBD (13,13,4,4,1), from [16, 17].

3 BIBD and R Project for Statistical Computing

As stated before, a BIBD is an arrangement of v treatments (varieties) in b blocks, each of size $k (< v)$, where each variety occurs exactly r times and every pair of varieties concurs in exactly λ blocks. The necessary, but not sufficient conditions for the existence of a BIBD are:

$$\begin{cases} v < b \\ vr = bk \\ \lambda(v - 1) = r(k - 1) \end{cases}$$

In order to generate BIBD with the aid of the computational statistical program ‘R’, we can use the extra ‘package’, ‘crossdes’. This ‘package’ includes several functions that assist in building balanced designs. Each BIBD produced with the aid

of this ‘package’ has five parameters described above. To install the ‘package’ the command ‘install.packages (“crossdes”)’ is used. To load the ‘package’ in order to be able to use the functions contained herein, the command ‘library (“crossdes”)’ is used. The ‘find.BIB’ function is used to generate a block design with a specific number of treatments, blocks (which correspond to the lines of the generated design) and elements per block (corresponding to the columns of the generated design). It is also possible to use another function to test if the generated design meets the conditions to be a BIBD. For instance, to create a design with five treatments in four blocks of three elements the function is as follows (Fig. 3):

```
> find.BIB(5, 4, 3)
```

The corresponding ‘R’ output is:

The resulting structure is not a BIBD because the treatments are not all repeated the same number of times. This observation can be confirmed by using the ‘isGYD’ function as follows: ‘isGYD (find.BIB (5, 4, 3))’. The result of executing this function in ‘R’ is (Fig. 4):

Consider now another example, this time with seven treatments and seven blocks of three elements (Fig. 5):

It is confirmed through the use of the ‘isGYD’ function that this experimental design is indeed a BIBD:

Another useful ‘package’ to generate outlines designs for BIBDs is the ‘dae’. As the one above, this package has several different functions targeted to aid in

	[,1]	[,2]	[,3]
[1,]	2	3	5
[2,]	1	2	4
[3,]	3	4	5
[4,]	1	3	5

Fig. 3 Output of instruction find.BIB(5,4,3)

```
> isGYD (find.BIB (5, 4, 3))
```

```
[1] The design is neither balanced w. r. t. rows nor w. r. t. columns.
```

Fig. 4 Output of instruction isGYD(find.BIB(5,4,3))

```
> outro . plano = find. BIB (7, 7, 3)
> outro . plano
```

	[,1]	[,2]	[,3]
[1,]	1	2	6
[2,]	3	5	6
[3,]	4	6	7
[4,]	2	3	7
[5,]	1	3	4
[6,]	2	4	5
[7,]	1	5	7

Fig. 5 Output of instruction find.BIB(7,7,3)

```
> isGYD (find.BIB (7,7,3) )
```

[1] The design is a balanced incomplete block design w. r. t. rows.

Fig. 6 Output of instruction isGYD(find.BIB(7,7,3))

```
> BIBD.unit<-list(Blocks=4, Plots=3)
> BIBD.nest<-list(Plots="Blocks")
> Treats<-factor(c(1,2,3, 1,2,4, 1,3,4, 2,3,4), labels=c("A","B","C","D"))
> BIBD.lay<-fac.layout(unrandomized=BIBD.unit, nested.factors=BIBD.nest, randomized=Treats, seed=987)
> BIBD.lay
```

	Units	Permutation	Blocks	Plots	Treats
1	1	2	1	1	C
2	2	3	1	2	A
3	3	1	1	3	B
4	4	10	2	1	B
5	5	12	2	2	C
6	6	11	2	3	D
7	7	9	3	1	C
8	8	7	3	2	D
9	9	8	3	3	A
10	10	4	4	1	A
11	11	5	4	2	D
12	12	6	4	3	B

Fig. 7 Randomized factors BIBD with 3 treatments and 4 blocks

obtaining experimental designs. The following example illustrates the use of one of the features of “dae”, the “fac.layout” to generate an experiment of BIBD consisting of randomized factors (Fig. 6):

A page from CRAN—The Comprehensive R Archive Network—aggregates all the existing information about the various ‘packages’ related to experimental design with the aid of the ‘R’. This page can be found at the url: <http://cran.r-project.org/web/views/ExperimentalDesign.html>.

This page presents first the general-purpose packages and proceeds with those that perform more specific tasks such as the ones used in the design of experiments for agriculture, industry and clinical trials among others (Fig. 7).

4 Application of Hadamard Matrices to Error Correction

Reed–Muller codes, see Reed [20] and Muller [14], are a family of linear error-correcting codes that were first used in communications.

Special cases of Reed–Muller codes include the Hadamard code, the Walsh–Hadamard code and the Reed–Solomon code, see Wicker and Bhargava [27].

The Hadamard code is an error-correcting code that is used for error detection and correction when transmitting messages over very noisy or unreliable channels. A famous application of the Hadamard code was the NASA space probe Mariner 9 in 1971, where the code was used to transmit photos of Mars.

Generalized Hadamard codes are obtained from an $n \times n$ Hadamard matrix \mathbf{H} . In particular, the $2n$ codewords of the code are the rows of \mathbf{H} and the rows of \mathbf{H} . To obtain a code over the alphabet $\{0, 1\}$, the mapping $1 \mapsto 1, 1 \mapsto 0$, or, equivalently, $x \mapsto (1+x)/2$, is applied to the matrix elements. That the minimum distance of the code is $n/2$ follows from the defining property of Hadamard matrices, namely that their rows are mutually orthogonal.

To get the punctured Hadamard code with $n = 2^{k-1}$ the chosen Hadamard matrix \mathbf{H} has to be of Sylvester type, see [13], which gives rise to a message length of $\log_2(2n) = k$.

Quick response codes (QR-Codes) contain codewords that are 8 bits long and use the Reed–Solomon error correction algorithm with four different error correction levels. It is well known that higher the error correction level, the less the available storage capacity there is.

The Reed–Solomon algorithm was created by Irving Reed and Gustave Solomon, both engineers at MIT's Lincoln Labs, and their work, see Reed and Solomon [21], led to the extent of and later on used with the creation of the QR code in 1994 for the Japanese automotive industry by Denso Wave, a subsidiary that produces automatic identification products.

Since its debut a long way was overcome and the amount of information that a QR code may store is massive. The four levels of security, that include redundant information, may go up to 30%, allowing the retrieval of information even when the QR code is damaged and thus giving space for error correction.

Below some examples of the relation between QR codes and information capacity (Figs. 8, 9 and 10).

Crossing the level of information redundant and the number of characters, Version 1, will allow 41 characters at his lowest and 17 on its highest level. Version 40 allows 7089 numerical characters.

Fig. 8 Version 1, 21×21 blocks

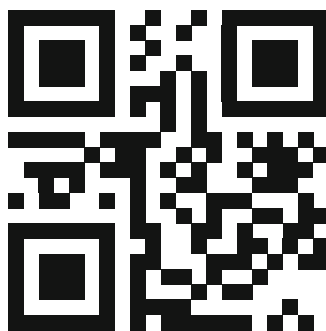


Fig. 9 Version 1, 25×25 blocks

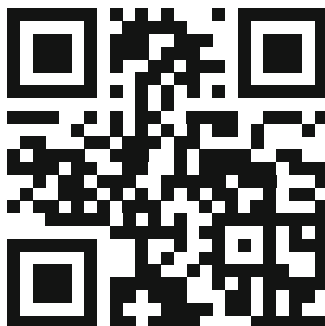
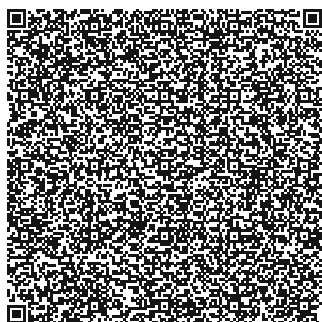


Fig. 10 Version 40, 117×117 blocks



Reed-Solomon codes are of the same family of error correcting codes as the Hadamard codes. The rows of a $k \times v$ generating matrix, for a generalized Reed-Solomon code $GR_k(c, 1)$, where $c = (1, c, \dots, c^{v-1})$ for some $c \in GF(q)$, of order v , are rows of a cocyclic matrix. For $v = p$, an odd prime number, the resulting Reed-Solomon codes are cocyclic Hadamard codes. So Reed-Solomon codes are closely related to Hadamard matrices as well.

5 Biometry

In information technology, biometrics refers technologies to identify human body characteristics, such as fingerprints and iris, see Jain et al. [10]. However, there is a tremendous amount of research that demonstrates biometrics can be easily faked. There are several examples on the Internet on how to make false fingerprints or forge iris images, big companies like Facebook are making efforts to develop both hardware tokens and software-based authentication for their social network. Software code generation like QR Codes seem to offer a preferable solution, rather than biometric recognition, thanks to their mathematical properties, see Gonçalves [7].

Gregg Stefancik, a Facebook engineer has stated in an interview that he would like his company to eventually move away from using passwords, but opposes

Fig. 11 Damaged QR code

the use of biometrics. However biometrics security can be leveraged with a two-factor authentication solution, ensuring that alphanumeric passwords or generated codes enter the authentication steps, see Anongporn [22]. A combination of voice recognition based, for example, on a phrase, along with a generated QR Code is an extremely strong authentication solution, see Lakshmanaswamy et al. [12].

Lumidigm, an ATM manufacturer, is already using this principle on their machines. Their ATMs use biometrics and QR Codes for secure cash withdrawals.

6 Considerations and Remarks

The QR Codes are 2-dimensional bar codes that can be easily read by a device capable of image capture, as is the case of most existing mobile phones. These codes can represent text, an address for a web site (URL), a phone number, a geo-referenced location, an email, a contact or an SMS.

QR codes have, as the base of their error correcting structure, Hadamard matrices. The mathematical properties jointly with the new technological advances allow simple figures to contain and transmit a huge amount of information. The mathematical properties that are intrinsic to these structures will allow great advances for error detection and correction, in huge amounts of information. Potential developments using well-studied properties of randomized block designs, namely with Orthogonal Block Designs, see, e.g., Calinski and Kageyama [2] and Calinski and Kageyama [3], will create a vast spectrum of research (Fig. 11).

Acknowledgements This research was partially sponsored by national funds through the FCT—Fundação para a Ciência e Tecnologia, Portugal—FCT under the project PEST-OE/MAT/UI0006/2013 (CEAUL).

References

1. Baumert, L. D., Golomb, S. W., & Hall, Jr., M. (1962). Discovery of an Hadamard matrix of order 92. *Bulletin of the American Mathematical Society*, 68(3), 237–238.
2. Caliński, T., & Kageyama, S. (2000). *Block designs: A randomization approach. Vol. I: Analysis*. Lecture Notes in Statistics (p. 150). Berlin: Springer.
3. Caliński, T., & Kageyama, S. (2003). *Block designs: A randomization approach. Vol. II: Design*. Lecture Notes in Statistics (p. 170). Berlin: Springer.
4. Cameron, P. J. (2006). Hadamard matrices in *The Encyclopaedia of Design Theory* at <http://www.maths.qmul.ac.uk/~leonard/designtheory.org/library/encycl/>.
5. Din S. U., & Mavron V. C. (1984). On designs constructed from Hadamard matrices. *Proceedings of the London Mathematical Society*, 49, 274–288.
6. Francisco, C. (2014). Experimental Design in Incomplete Blocks: Particular Case Studies. Master Thesis. Open University. Lisbon. Portugal.
7. Gonçalves, R. M. P. (2015). Handwritten signature authentication using motion detection and QRcodes. Master Thesis on Computers Sciences. Porto University.
8. Hall, Jr, M. (1986). *Combinatorial theory*, 2nd edn. New York: Wiley.
9. Hedayat, A., & Wallis, W. D. (1978). Hadamard matrices and their applications. *Annals of Statistics*, 6(6), 1184–1238.
10. Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM*, 43(2), 91–98. <https://doi.org/10.1145/328236.328110>
11. Koukouvinos C., Simos, D. E., & Varbanov, Z. (2011). Hadamard matrices, designs and the secret-sharing schemes. *CAIII Proceedings of the forth International Conference on Algebraic Informatics*, 216–229.
12. Lakshmanaswamy, K., Das Gupta, D., Toppo N. S., & Senapati, B. (2014). Multi-layered security by embedding biometrics in quick response (QR) codes. *International Journal of Engineering Research & Technology*, 3(4). e-ISSN: 2278-0181.
13. Mitrouli, M. (2014). Sylvester Hadamard matrices revisited. *Special Matrices*, 2, 120–124.
14. Muller, D. E. (1954). Application of boolean algebra to switching circuit design and to error detection. *IRE Transactions on Electronic Computers*, 3, 6–12.
15. Ogata, W., Kurosawa, K., Stinson, D., & Saido H. (2004). New combinatorial designs and their applications to authentication codes and secret sharing schemes. *Discrete Mathematics*, 279, 383–405
16. Oliveira, T. A. (2010). Planos em Blocos Incompletos Equilibrados e Parcialmente Equilibrados (BIB e PBIB Designs): Na fronteira entre a Estatística e a Matemática, Actas da ENSPM 2010, 8–10 Julho de 2010, Escola Superior de Tecnologia e Gestão, Instituto Politécnico de Leiria.
17. Oliveira, T. A. (2011). Exploring the links between the BIBD and PBIBD and mathematics. In D. Hampel, J. Hartmann & J. Michálek (Eds.) *Biometric Methods and Models in Current Science and Research. Proceedings of XIXth. Summer School of Biometrics 6-10.9.2010*. Faculty of Horticulture of Mendel University, Lednice, República Checa (pp. 183–194) Brno: Central Institute of Supervising and Testing in Agriculture.
18. Plackett, R. L., & Burman, J. P. (1946). The design of optimum multifactorial experiments. *Biometrika*, 33(4), 305–325.
19. Raghvarao, D. (1971). *Constructions and combinatorial problems in design of experiments*. New York: Wiley.
20. Reed, I. S. (1954). A class of multiple-error-correcting codes and the decoding scheme. *Transactions of the IRE Professional Group on Information Theory*, 4, 38–49.
21. Reed, I. S., & Solomon, G. (1960). Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2), 300–304.
22. Salaiwarakul, A. (2010). *Verification of secure biometric authentication protocols*. Ph.D. thesis. Birmingham: University of Birmingham.
23. Sawade, K. (1985). A Hadamard matrix of order-268. *Graphs Combinatorics*, 1, 185–187.

24. Seberry, J. (2012). *Hadamard matrices*. University of Wollongong.
25. Stinson, D. R. (2004). *Combinatorial designs – constructions and analysis*. Berlin: Springer.
26. Sylvester, J. J. (1867). Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. *Philosophical Magazine*, 34, 461–475.
27. Wicker, S. B., Bhargava, V. K. (1999). *Reed-Solomon codes and their applications*. Hoboken: Wiley-IEEE Press. ISBN: 978-0-7803-5391-6.
28. Yates, F. (1936). Incomplete randomized blocks. *Annals of Eugenics*, 7, 121–140.