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

Teresa A. Oliveira[1] **and** **Carla Francisco**[2] **and Amílcar Oliveira**[1]

[1]*Departamento de Ciências e Tecnologia, Universidade Aberta, Portugal*
Centro de Estatística e Aplicações, Universidade de Lisboa, Portugal
[2]*Departamento de Ciências e Tecnologia, Universidade Aberta, Portugal*

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 channels, thus providing quality of service. Hadamard matrices can almost directly be used as an error-correcting code using a 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, Block Designs, Hadamard Matrices, QR Codes, Reed-Muller codes

Acknowledgments: The authors were partially sponsored by Fundação para a Ciência e a Tecnologia, Portugal, through the project UID/MAT/00006/2013.

References

[1] Baumert, L. D., Golomb, S. W. and Hall Jr., M.: Discovery of an Hadamard matrix of order 92. *Bull. Amer. Math. Soc.* 68 (3) 237-238 (1962).

[2] Caliński, T. and Kageyama, S.: Block Designs: A Randomization Approach. Vol. I: Analysis. *Lecture Notes in Statistics*, Springer, 150 (2000).

[3] Caliński, T. and Kageyama, S.: Block Designs: A Randomization Approach. Vol. II: Design. *Lecture Notes in Statistics*, Springer, 170 (2003).

[4] Francisco, C. and Oliveira, T., Risk of Data Loss on QR Codes: Hadamard Matrices and links to Block Designs, International Conference on Risk Analysis ICRA 6 / RISK 2015, Editors: Eds GuillÃ©n, M., Juan, A., Ramalhinho, H., Serra, I., Serrat, C., Editor:Cuadernos de la FundaciÃ³n. Ã rea de Seguro y PrevisiÃ³n Social, FundaciÃ³n MAPFRE, p.311-318. Barcelona, Spain,(2015).

[5] Francisco, C.: Experimental Design in Incomplete Blocks: Particular Case Studies. Master Thesis. Open University, Lisbon. Portugal (2014)

[6] Hall Jr, M.: Combinatorial Theory, 2nd edition. New York, Wiley (1986).

[7] Ogata, W. , Kurosawa, K., Stinson, D. , Saido H.: New combinatorial designs and their applications to authentication codes and secret sharing schemes. Discrete mathematics, vol 279, pp. 383-405, (2004).

[8] Plackett, R. L. and Burman, J. P.: The design of optimum multifactorial experiments. *Biometrika* 33 (4), 305-325 (1946)

[9] Raghvarao, D.: Constructions and Combinatorial Problems in Design of Experiments. New York: Wiley (1971).

[10] Reed, I. S. and Solomon, G.: Polynomial Codes Over Certain Finite Fields. Journal of the Society for Industrial and Applied Mathematics Vol. 8, No. 2 , pp. 300-304 (Jun., 1960).

[11] Georgiou, S., Koukouvinos, C. and Seberry, J. , Hadamard matrices, orthogonal designs and construction algorithms, in Designs 2002: Further Combinatorial and Constructive Design Theory, *(W.D.Wallis, ed.)*, Kluwer Academic Publishers, Norwell, Ma, 133-205 (2002).