How to Deal with non-Hamming Distances. *

International Meeting on Coding Theory and Cryptology

Edgar Martínez-Moro † F. Javier Galán-Simón ‡

Medina. September 8,1999

Abstract:

This report surveys a group theoretical approach to non-Haming distances. Combinatorial tools such association schemes and cycle indexes are the basic tools to deal with them. Groups actions and isometry classes play a central role in the report too. In this paper we show some techniques and computer algebra tools for dealing with the Bose-Mensner algebra (defined by the metric)[11]. We study some natural extensions of this method for arithmetic metric and for two dimensional modulo metrics using 2-orbit association schemes[15, 10, 12]. Cycle representation of the orbits involved in the group action of unit steps is the main tool for working out the properties of the schemes defined as well as for computing isometry classes of codes defined over these metrics[12]. Association schemes defined in the report are weakly metric schemes as defined by P. Solè[15] which allow us derive some nice properties from them. Some directions of research point towards finding all perfect codes among some classes of these metrics and study the possible application of techniques of arithmetic codes in codes for two dimensional modulo metrics. We also consider the study of partitions associated to the schemes defined. For these aims it is of great importance the study of the varieties $\mathcal{F}$ derived from the adjacency algebra of the scheme[11]. Further investigations points towards the classification of perfect codes over these metrics which must fulfill the constrains and equalities on the eigenvalues [14, 15] and on the Lloyd polynomials. Some basic references are included.

References

[1] **E. Bannai, T. Ito** *Algebraic combinatorics I: Association Schemes* Benjamin Cummimgs Publishers (1983)

[2] **N. Biggs**, *Algebraic Graph theory*, 2nd. edition, Cambridge University Press (1993).

*This work was partially supported by Digicyt PB97-0471 and by Junta de Castilla y León project "Construcciones criptográficas basadas en códigos correctores".

†Dpto. Matemática Aplicada F. ,Universidad de Valladolid, Valladolid, Spain,edgar.martinez@ieee.org .

‡Dpto. de Organización y Gestión de Empresas, Universidad de Valladolid, Valladolid, Spain, javi@tita.emp.uva.es

[3] **P. Camion**, *Codes and Association Schemes: Basic Properties of Association Schemes Relevant to Coding*, in " Handbook of Coding Theory vol 2", pp. 1441–1566, Ed. V.S. Pless, W.C. Huffman, North-Holland 1999

[4] **K. Huber**, *Codes over Gaussian integers.*, IEEE Trans. on Inf. Theory, 40 (1), 207-216 (1994).

[5] **K. Huber**, *The Mac Williams Theorem for Two-dimensional modulo metrics.*, AAECC, 8 (1), 41-48 (1997).

[6] **P. Delsarte**, *An algebraic approach to the association schemes of coding theory.*, Technical report, Philips Research Laboratory, 1973

[7] **P. Delsarte,V.I. Levenshtein**, *Association schemes and coding theory.*, IEEE Trans. on Inf. Theory, vol. 44, 6, pp.2477–2504. October 1998

[8] **H. Lehmann**, *Ein vereinheitlichender Ansatz für die Redfield-Polya-de Bruijnsche Abzähltheory.*, PhD. Thesis Universität Giessen, 1976

[9] **E. Martínez, F.J. Galán**: *Combinatorial structure of arithmetic codes.*, Winter School on Coding and Information Theory 1998 (Ebeltoft, Denmark)

[10] **E. Martínez,M.A. Borges, M. Borges** : *Combinatorial structure of rings of complex integers with Mannheim metric.*, 1st. Workshop on Combinatorics, Geometry, Coding Theory and related areas. CIMAF'99 La Habana, Cuba, March 1999.

[11] **E. Martínez**: *Computations on character tables of association schemes.*, Computer Algebra in Scientific Computing 99, pp. 293–307, Springer-Verlag, 1999.

[12] **E. Martínez, F.J. Galán, M.A. Borges, M. Borges**: *Combinatorial Structure of Finite Fields with Two Dimensional Modulo Metrics.*, 7th. IMA Conference on Cryptography and Coding , To appear in LNCS Springer-Verlag, 1999.

[13] **H. Tarnanen** , *On Abelian Schemes*, TUCKS Technical Report no. 88. Turku Centre for Computer Science 1996

[14] **P.Solé**, *On the parameters of codes for the Lee and modular distance.*, Discrete Mathematics 89 (1991), pp. 185–194.

[15] **P.Solé**, *A Lloyd theorem in weakly metric association schemes.*, Europ. J. of Combinatorics. **10** 189–196 (1989)