Numerical and Algorithmic Aspects of Orthogonal Sequences in Combinatorial Design Theory

Dimitris E. Simos[a], and Christos Koukouvinos[a]

[a]Department of Mathematics, National Technical University of Athens,

Zografou 15773, Athens, Greece

ckoukouv@math.ntua.gr,dsimos@math.ntua.gr

Key words: Orthogonal designs, sequences, algorithm, complexity analysis, software.

Combinatorial Design Theory studies questions about arrangements of elements of a finite set into subsets so that certain properties are satisfied. Combinatorial Design Theory has applications in cryptography, coding theory, numerical analysis, telecommunications and other areas.

Orthogonal designs constitute a special class of combinatorial designs that preserves orthogonality in the sense of mutual Euclidean product, and problems related to their existence and construction are directly amenable to algebraic formulations that enable the application of powerful combinatorial tools and computational methods. Orthogonal designs boil down to their numerical counterparts, Hadamard and weighing matrices, upon suitable substitution of their variables with integer values or integer matrices. Prolific methods for constructing the later designs often involve the use of orthogonal sequences in suitable arrays.

For a sequence $A = [a_1, a_2, \ldots, a_n]$ of length n the periodic autocorrelation function, PAF, $P_A(s)$ and the non-periodic autocorrelation function, NPAF, $N_A(s)$ are defined as

$$P_A(s) = \sum_{i=1}^{n} a_i a_{i+s} \, , s = 0, 1, \ldots, n-1 \quad N_A(s) = \sum_{i=1}^{n-s} a_i a_{i+s} \, , s = 0, 1, \ldots, n-1.$$

where in PAF we consider (i+s) modulo n. Sequences of previous kind are referred to as orthogonal, in the sense that the sum of their autocorrelations is zero. Periodic and non-periodic (sometimes are also called aperiodic) ternary complementary pairs are used to construct sequences with desirable properties for radar applications and cryptographic systems. Moreover, these sequences intervene in coded aperture imaging and higher-dimensional signal processing applications. The structure and the number of steps encountered for an interpretation of these methods in terms of a computer implementation, has shown in the past that it is an ideal case for meta-meta programming.

Recently, we established new formalisms on PAF and NPAF of orthogonal sequences suitable for efficient computation of their autocorrelation, by using signed difference sets. A complexity analysis of the proposed combinatorial algorithms for the check of the autocorrelation has revealed that for sequences of small weight our formalism is optimal, and we cannot expect asymptotically better algorithms. These formalisms, allows further consideration of meta-programming techniques and the development of numerical software aided by high-performance computing, for the deployment of several combinatorial design databases.