Genetic Algorithms for Hadamard matrices of Williamson type

I. Kotsireas* and C. Koukouvinos**

* Wilfrid Laurier University, Department of Physics and Computer Science, 75 University Avenue West, Waterloo, Ontario N2L 3C5, Canada. Supported in part by a grant from NSERC.
e-mail: ikotsire@wlu.ca
** Department of Mathematics, National Technical University of Athens, Zografou 15773, Athens, Greece. e-mail: ckoukouv@math.ntua.gr

Abstract

Introduction

Hadamard matrices arise in Statistics and Combinatorics and have many applications in Engineering, Optical Communications, Cryptography and other areas. The book [2] is a very readable and self-contained introduction to Hadamard matrices.
There are several well-known constructions for Hadamard matrices. Some constructions are better suited for various purposes than others. A construction which is advantageous to use as far as Genetic Algorithms are concerned is the Williamson construction. Hadamard matrices of Williamson type are typically made up of four square matrices satisfying certain algebraic conditions. By exploiting an analogy between Williamson's construction for four matrices and a real matrix representation of the algebra of quaternions, we were able to extend Williamson's construction to eight matrices, based on left and right representations of the algebra of octonions. The reason why we need to consider left and right representations of octonions, is that this algebra is not associative, but its right and left actions are associative. There are theoretical restrictions that prohibit the existence of an array with sixteen Williamson matrices.
Using our Computational Algebra formalism we are able to apply Genetic Algorithms in the search for Hadamard matrices of Williamson type and discover solutions to quite large systems of polynomial equations, which do not seem to be solvable with other methods. One advantage of Williamson's constructions with four and eight matrices is that they provide the vehicle for computing with large order Hadamard matrices, without using too many equations and too many variables, in striking contrast with other constructions. Another advantage of Williamson's constructions with four and eight matrices is that the cardinalities of the associated zero-dimensional algebraic varieties grow exponentially with respect to the order of the block matrix and this makes them ideal candidates for applying Genetic Algorithms.
Genetic Algorithms are a powerful metaheuristic that mimicks processes from the Theory of Evolution to establish search algorithms by defining algorithmic analogues of biological concepts such as reproduction crossover and mutation. The book [3] is a very readable and self-contained introduction to Genetic Algorithms.

Hadamard matrices of Williamson type

The classical Williamson construction for Hadamard matrices is based on the 4×4 matrix

$$W = \begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}$$

which has the property

$$WW^T = (A^2 + B^2 + C^2 + D^2) \otimes I_4.$$

(here A, B, C, D are square matrices of order n and the symbol $\otimes$ denotes the Kronecker product) When A, B, C, D are square circulant and symmetric $(1, -1)$ matrices of order n, then W turns out to be a Hadamard matrix of order $4n$, i.e. we have $WW^T = 4nI_{4n}$. See [4] for all the details.

The matrix W appears in the context of quaternions. See [1, 7] for general background on quaternions. The next number system in the hierarchy of hypercomplex numbers is given by octonions. See [1, 6] for general background on octonions.

The real quaternion division algebra $\mathbb{H}$ is algebraically isomorphic to a four dimensional real matrix algebra given by the matrix W. This striking similarity raises the question whether it is possible to use similar isomorphisms of the real octonion division algebra $\mathbb{O}$ to construct Hadamard matrices via a Williamson array with 8 matrices. In this paper we show that this is indeed possible.
Consider the 8×8 matrices

$$W_L = \begin{pmatrix} A & -B & -C & -D & -E & -F & -G & -H \\ B & A & -D & C & -F & E & H & -G \\ C & D & A & -B & -G & -H & E & F \\ D & -C & B & A & -H & G & -F & E \\ E & F & G & H & A & -B & -C & -D \\ F & -E & H & -G & B & A & D & -C \\ G & -H & -E & F & C & -D & A & B \\ H & G & -F & -E & D & C & -B & A \end{pmatrix}$$

and

$$W_R = \begin{pmatrix} A & -B & -C & -D & -E & -F & -G & -H \\ B & A & D & -C & F & -E & -H & G \\ C & -D & A & B & G & H & -E & -F \\ D & C & -B & A & H & -G & F & -E \\ E & -F & -G & -H & A & B & C & D \\ F & E & -H & G & -B & A & -D & C \\ G & H & E & -F & -C & D & A & -B \\ H & -G & F & E & -D & -C & B & A \end{pmatrix}$$

which specify the left and right matrix representations of an octonion $\alpha \in \mathbb{O}$ over the set of real numbers. See [5] for complete descriptions of the derivation of these matrices. These two matrices satisfy the property:

$$W_L W_L^T = W_R W_R^T = (A^2 + B^2 + C^2 + D^2 + E^2 + F^2 + G^2 + H^2) \otimes I_8.$$

(here A, B, C, D, E, F,G, H are square matrices of order n and the symbol $\otimes$ denotes the Kronecker product) When A, B, C, D, E, F,G, H are square circulant and symmetric $(1, -1)$ matrices of order n, then W_L and W_T turn out to be Hadamard matrices of order $8n$, i.e. we have $W_L W_L^T = W_R W_R^T = 8nI_{8n}$.

The Williamson constructions with four and eight matrices, lead to polynomial systems of equations that are not easily solvable with conventional techniques. The four and eight Williamson arrays are in essence orthogonal designs as described in [2].

Results obtained with Genetic Algorithms

In this section we mention a summary of some results obtained by applying SGA (Simple Genetic Algorithm, see [3]) to the problem of constructing Hadamard matrices of Williamson type from 4 and 8 submatrices. SGA was implemented in C by Jason Cousineau. In the solutions of polynomial systems presented below, we follow the standard notation for Hadamard matrices, i.e. 1 stands for $+1$ and $-$ stands for -1.

The parameter n is the order of the submatrices. For each solution found, we give the number of generations evolved, until the algorithm converged to a solution. The populations used in the runs, were typically of the order of $6 \cdot 10^5$ chromosomes (binary vectors).

Results obtained from 4 Williamson arrays

• $n = 21$
The polynomial system being solved is:

2+a0 a1+a1 a2+a2 a3+a3 a4+a4 a5+a5 a6+a6 a7+a7 a8+a8 a9+a9 a10 + bterms + cterms + dterms = 0

2+a0 a2+a1 a3+a2 a4+a3 a5+a4 a6+a5 a7+a6 a8+a7 a9+a8 a10+a9 a10 + bterms + cterms + dterms = 0

2+a0 a3+a1 a2+a1 a4+a2 a5+a3 a6+a4 a7+a5 a8+a6 a9+a7 a10+a8 a10 + bterms + cterms + dterms = 0

2+a0 a4+a1 a3+a1 a5+a2 a6+a3 a7+a4 a8+a5 a9+a6 a10+a7 a10+a8 a9 + bterms + cterms + dterms = 0

2+a0 a5+a1 a4+a1 a6+a2 a3+a2 a7+a3 a8+a4 a9+a5 a10+a6 a10+a7 a9 + bterms + cterms + dterms = 0

2+a0 a6+a1 a5+a1 a7+a2 a4+a2 a8+a3 a9+a4 a10+a5 a10+a6 a9+a7 a8 + bterms + cterms + dterms = 0

2+a0 a7+a1 a6+a1 a8+a2 a5+a2 a9+a3 a4+a3 a10+a4 a10+a5 a9+a6 a8 + bterms + cterms + dterms = 0

2+a0 a8+a1 a7+a1 a9+a2 a6+a2 a10+a3 a5+a3 a10+a4 a9+a5 a8+a6 a7 + bterms + cterms + dterms = 0

2+a0 a9+a1 a8+a1 a10+a2 a7+a2 a10+a3 a6+a3 a9+a4 a5+a4 a8+a5 a7 + bterms + cterms + dterms = 0

2+a0 a10+a1 a9+a1 a10+a2 a8+a2 a9+a3 a7+a3 a8+a4 a6+a4 a7+a5 a6 + bterms + cterms + dterms = 0

where the 44 variables a0, ... a10, b0, ... b10, c0, ... c10, d0, ... d10 take ± 1 values only and the symbols bterms, cterms, dterms denote sums of quadratic monomials following the same pattern as the sum of the quadratic monomials in the a variables as given in each equation separately. A solution found with SGA is: (format a0 ... a10 b0 ... b10 c0 ... c10 d0 ... d10)

$$1-1111-11---1-1--11---1-1111-11--11-1--11---$$

SGA evolved 1166 generations before converging to this solution, which gives rise to a Hadamard matrix of order $4 \times 21 = 84$.
• $n = 27$

$$1111---11--1-1-1-1--1---11--111-1-1-------111--1--11-1---$$

Number of Generations: 47873. This solution gives rise to a Hadamard matrix of order $4 \times 27 = 108$.

Results obtained from 8 Williamson arrays

• $n = 19$

$$-11-11----1--1-111--1-1-1--1----1-11111-$$
$$--11----111---1--11-1-11-1-1111---111-11$$

Number of Generations: 949. This solution gives rise to a Hadamard matrix of order $8 \times 19 = 152$.
• $n = 21$

$$11-1-1111--1-111--1-1-11-1-------1---11-1--1-$$

$$111-1---1---1-111--11-111--11--111111-11-1--$$

Number of Generations: 5358. This solution gives rise to a Hadamard matrix of order $8 \times 21 = 168$.

Acknowledgments

We thank Jason Cousineau for implementing SGA in C. All the results in the paper were obtained by running C programs at *Centre de calcul formel MEDICIS, École Polytechnique, Paris, France*, *Computer Algebra Research Group, Wilfrid Laurier University, Waterloo, Ontario, Canada*, *SHARCnet high performance computing clusters, University of Western Ontario, London, ON, Canada* and *WestGrid high performance computing clusters, University of British Columbia, Simon Fraser University, Vancouver, BC, Canada*.

Conclusion

In this work we used SGA to find solutions to many challenging systems of polynomial equations arising from the 4 and 8 Williamson arrays for Hadamard matrices. Details on SGA and the complete results are deferred to the full paper.

References :

References

[1] Dixon, G. M. *Division algebras: octonions, quaternions, complex numbers and the algebraic design of physics*, Mathematics and its Applications, 290, Kluwer Academic Publishers Group, Dordrecht, 1994.

[2] Geramita, A. V. and Seberry, J. *Orthogonal designs: Quadratic forms and Hadamard matrices*, Marcel Dekker, 1979

[3] Goldberg, D. E. *Genetic algorithms in search, optimization, and machine learning*, Addison-Wesley, 1989

[4] M. Hall, Jr. *Combinatorial theory*, Reprint of the 1986 second edition, Wiley Classics Library, 1998. Wiley, New York.

[5] Tian, Y. Adv. Appl. Clifford Algebras **10** (2000), no. 1, pp. 61–90.

[6] Springer, T. A.; Veldkamp, F. D. *Octonions, Jordan algebras and exceptional groups*, Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.

[7] Ward, J. P. *Quaternions and Cayley numbers. Algebra and applications*, Mathematics and its Applications, 403. Kluwer Academic Publishers Group, Dordrecht, 1997.