Theoretical Computer Science 407 (2008) 274–277

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

Heuristic algorithms for Hadamard matrices with two circulant cores

M. Chiarandini [a], I.S. Kotsireas [b,*], C. Koukouvinos [c], L. Paquete [d]

[a] *Department of Mathematics and Computer Science, University of Southern Denmark, Campusvej 55 DK-5230 Odense M, Denmark*
[b] *Wilfrid Laurier University, Department of Physics and Computer Science, 75 University Avenue West, Waterloo, Ontario N2L 3C5, Canada*
[c] *Department of Mathematics, National Technical University of Athens, Zografou 15773, Athens, Greece*
[d] *CISUC, Department of Informatics Engineering, University of Coimbra, Polo II, 3030-290 Coimbra, Portugal*

ARTICLE INFO

Article history:
Received 3 October 2007
Accepted 5 June 2008
Communicated by V. Pan

Keywords:
Hadamard matrices
Heuristic algorithms

ABSTRACT

We design heuristic algorithms to construct Hadamard matrices with two circulant cores. This hard combinatorial problem can be formulated in terms of objective functions of several binary variables, so that heuristic methodologies can be used. Our algorithms are based on local and tabu search and they use information on the geometry of the objective function landscapes. In addition, we use the supplementary difference sets formalism to detect when solutions of a special structure exist. Using these algorithms we have computed at least one Hadamard matrix with two circulant cores of the sixteen orders 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116. In particular, the Hadamard matrix with two circulant cores of order 116 is constructed here for the first time, indeed it was accidentally reported as known in an earlier paper.

1. Introduction

Hadamard matrices with two circulant cores can be defined in terms of the periodic autocorrelation function of the two binary sequences that generate the two circulant cores. The periodic autocorrelation function of a sequence is a measure of how much the given sequence differs from its translates.

Let ℓ be a positive integer and A be a (finite) sequence of ℓ real numbers $\{a_0, a_1, \ldots, a_{\ell-1}\}$. The *periodic autocorrelation function* $P_A(s)$ is defined by

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

where $i + s$ is taken modulo ℓ.

The following *symmetry property* will be helpful later on, in reducing the size of the objective functions involved. Suppose that ℓ is odd. Then we have that

$$P_A(s) = P_A(\ell - s), \quad s = 1, \ldots, \frac{\ell - 1}{2}. \tag{2}$$

Two $\{-1, +1\}$ sequences A and B both of length ℓ such that their corresponding PAF terms (except the first one) sum to -2

$$P_A(s) + P_B(s) = -2, \quad s = 1, \ldots, \ell - 1 \tag{3}$$

can be used as the first rows of circulant matrices C_A and C_B respectively, so that the matrix

* Corresponding author. Tel.: +1 519 884 0710.
E-mail address: ikotsire@wlu.ca (I.S. Kotsireas).

0304-3975/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2008.06.002

$$
H_{2\ell+2} = \left(\begin{array}{cc|cc}
- & - & + \cdots + & + \cdots + \\
- & + & + \cdots + & - \cdots - \\
\hline
+ & + & & \\
\vdots & \vdots & C_A & C_B \\
+ & + & & \\
\hline
+ & - & & \\
\vdots & \vdots & C_B^{\mathrm{T}} & -C_A^{\mathrm{T}} \\
+ & - & &
\end{array}\right) \tag{4}
$$

is a Hadamard matrix of order $2\ell + 2$ with two circulant cores. The superscript T denotes matrix transposition.

A Hadamard matrix of order n is an $n \times n$ matrix H which has ± 1 elements such that $HH^{\mathrm{T}} = H^{\mathrm{T}}H = nI_n$, where I_n is the identity matrix of order n.

Hadamard matrices with two circulant cores (also called generalized Legendre pairs) have been studied in [3] using discrete Fourier transform, decimation and power spectral density techniques, in [7] using computational algebra techniques and in [6] using simple genetic algorithm.

Sometimes it may happen that the two sequences A and B that have property (3) are equal. A sufficient condition for when this can happen, can be expressed conveniently via supplementary difference sets. See [9] and [10] for the definition and properties of supplementary difference sets.

The following theorem is taken from [2].

Theorem 1. (1) *If P, Q are supplementary difference sets $2 - \{\ell;\ k_1,\ k_2;\ \lambda\}$ and A, B are the corresponding $(-1, 1)$ incidence matrices, then*

$$AA^{\mathrm{T}} + BB^{\mathrm{T}} = 4(k_1 + k_2 - \lambda)I_\ell + 2(\ell - 2(k_1 + k_2 - \lambda))J_\ell. \tag{5}$$

(2) *Given two $\ell \times \ell$ circulant matrices A, B satisfying (5), then the corresponding sets P, Q are supplementary difference sets $2 - \{\ell;\ k_1,\ k_2;\ \lambda\}$, where k_1, k_2 is the number of -1's in each row of A, B respectively.*

In [4] it is pointed out that a sufficient condition for the existence of two $\{-1, +1\}$ sequences A and B that satisfy property (3) is the existence of an SDS $2 - \{\ell;\ \frac{\ell+1}{2},\ \frac{\ell+1}{2};\ \frac{\ell+1}{2}\}$.

If in addition we are looking for such sequences, with the additional constraint that $A = B$, then the sufficient condition is the existence of an $(\ell, \frac{\ell+1}{2}, \frac{\ell+1}{4})$ difference set. In particular, this implies that $\ell \equiv 3 \pmod 4$. See [1] for the definition and properties of difference sets.

When $\ell \equiv 3 \pmod 4$ is a *prime*, then the quadratic residues form an $(\ell, \frac{\ell+1}{2}, \frac{\ell+1}{4})$ difference set, so the condition is necessary and sufficient.

2. Objective functions

The objective functions that we used in our algorithms are given by:

$$OF_1 = |2 + P_A(1) + P_B(1)| + \cdots + |2 + P_A(\ell - 1) + P_B(\ell - 1)|$$

and

$$OF_2 = (2 + P_A(1) + P_B(1))^2 + \cdots + (2 + P_A(\ell - 1) + P_B(\ell - 1))^2.$$

Note that OF_1 and OF_2 can be described succinctly in terms of the 1-norm and the 2-norm of the PAF vector $v = [P_A(1), \ldots, P_A(\ell - 1)]$ as follows:

$$OF_1 = \|v\|_1, \quad OF_2 = \|v\|_2^2.$$

We note that OF_2 is a smooth and continuous function, but which attains larger values (has a bigger range) than OF_1, in general. We also occasionally supplemented OF_1 and OF_2 with linear equations of the form

$$a_0 + \cdots + a_{\ell-1} = 1, \qquad b_0 + \cdots + b_{\ell-1} = 1, \tag{6}$$

without loss of generality, due to the Diophantine constraint

$$(a_0 + \cdots + a_{\ell-1})^2 + (b_0 + \cdots + b_{\ell-1})^2 = 2.$$

See [7], for instance, for a derivation of the Diophantine constraint above.

Note that the symmetry property (2) of the PAF vector can be used to reduce the size of the objective functions OF_1 and OF_2 by half, as we only need to consider its first $\frac{\ell-1}{2}$ elements. Specifically, setting $m = \frac{\ell-1}{2}$, we may define the objective functions by:

$$OF_1 = \sum_{i=1}^{m} |2 + P_A(i) + P_B(i)| \quad \text{and} \quad OF_2 = \sum_{i=1}^{m} (2 + P_A(i) + P_B(i))^2.$$

The heuristic algorithms described in this paper attempt to find values of the binary variables a_i, b_i that make the (non-negative) objective functions OF_1 and OF_2 equal to zero, i.e. minimize them.

To illustrate the difficulty of minimizing these objective functions we mention that the size of the discrete search space $\{-1, +1\}^{2\ell}$ (often called the boolean cube) is equal to $2^{2\ell}$. A probabilistic analysis regarding the size of the subspace defined by Eq. (6) is given in [6] where the following lemma is proved.

Lemma 1. *The size of the subspace of the boolean cube $\{-1, +1\}^{2\ell}$ defined by the equations $a_0 + \cdots + a_{\ell-1} = 1$ and $b_1 + \cdots + b_{\ell-1} = 1$ is approximately $\left[\frac{\pi\ell}{2}\right]$ times smaller than the size of the entire boolean cube.*

3. Heuristic approach

The heuristic algorithms developed for the minimization of the objective functions OF_1 and OF_2 are based on the tabu search method, see [5], which has been shown to be very effective for similar hard problems with quadratic objective functions, see for instance [8] for the Quadratic Assignment Problem. Tabu search is essentially a local search that selects the best solution from a neighborhood opportunely restricted in order to avoid cycling.

In our implementation, we considered two different neighborhoods. The first ($\mathcal{N}_1$) consists of all feasible solutions that are obtained from another feasible solution by exchanging the sign between a_i (b_i) and a_j (b_j) with $a_i \neq a_j$ ($b_i \neq b_j$) and $0 \leq i < j \leq \ell - 1$. The second neighborhood ($\mathcal{N}_2$) explores the cases in which A may be equal to B, that is, when $\ell \equiv 3 \pmod 4$ and ℓ is a prime. For this neighborhood, a sign exchange between a_i and a_j implies a sign exchange between b_i and b_j.

Both neighborhoods are of size $\mathcal{O}(\ell^2)$ and it takes $\mathcal{O}(\ell^4)$ time to choose the best neighboring solution. However, a faster computation of the objective function can be obtained by computing the contribution $U_A(s)$ to $P_A(s)$ of the terms that changed. This value can be computed as follows.

$$U_A(s) = -2 \cdot \begin{cases} a_j a_{\phi(j+s)} + a_{\phi(i-s)} a_i & s = j - i \\ a_i a_{\phi(j+s)} + a_{\phi(i-s)} a_j & s = \ell - j + i \\ a_i a_{\phi(i+s)} + a_i a_{\phi(i-s)} + a_j a_{\phi(j+s)} + a_j a_{\phi(j-s)} & \text{otherwise} \end{cases}$$

where $\phi(x)$ is defined as a modulus function $\phi(x) = x - \ell\lfloor \frac{x}{\ell} \rfloor$. The contribution of $U_B(s)$ to $P_B(s)$ is computed similarly with the necessary changes. Hence, the best solution in the neighborhood can be found in $\mathcal{O}(\ell^3)$ time.

Our tabu search chooses at each iteration the best non-tabu or tabu but *aspired* solution from the neighborhood, improving over an initial feasible solution that is generated randomly. The tabu restriction works as follows: If a selected neighbor is obtained by a sign exchange between a_i (b_i) and a_j (b_j), the same exchange is forbidden in A (B) for the next *iter* iterations. For this reason, the indices i and j need to be maintained in an additional $\mathcal{O}(\ell^2)$-space data structure for each sequence. The tabu status of a neighboring solution is overruled if it improves over the best solution found so far (known as the *aspiration criterion*). If more than one neighboring solution yields the same value in the evaluation function, then one of those neighbors is selected in lexicographic order. We restrict the neighborhood to the sequence A or B, changing sequence at each iteration. Some preliminary experiments indicated that this tabu search may be less effective for larger ℓ. Therefore, if no improvement is obtained over the best solution found for a given number *riter* of iterations, the sequences are reinitialized. The parameters *iter* and *riter* were set experimentally.

The largest objective function that we were able to solve in this paper is the one corresponding to $\ell = 57$. This objective function contains 114 binary variables, so the size of the entire search space is 2^{114}. The solution was found within a set of 60 runs per each different tabu length parameter from the set $\{0.5\ell, 1\ell, 5\ell, 10\ell, 15\ell, 20\ell\}$, each run having a different random seed and consisting of 10^6 seconds with internal restart every 10 000 non improving iterations. The solution was found with a tabu length parameter equal to 0.5.

4. Results

The tabu search using neighborhood $\mathcal{N}_1$ was run for $\ell = 27, 29, 31, 33, 35, 37, 39, 41, 43, 45$, for 10 000 s. The parameter *iter* was set equal to ℓ and *riter* equal to 10000 iterations. The tabu search using neighborhood $\mathcal{N}_2$ was run for $\ell = 31$ and 43. The values for *riter* and *iter* were defined as above. Table 1 shows the number of unique solutions found by the tabu search using neighborhoods $\mathcal{N}_1$ and $\mathcal{N}_2$. Recently, we also found solutions for $\ell = 47, 49, 51, 53, 55, 57$. The solution for $\ell = 57$ is given here for the first time. Indeed, it was accidentally reported as known in [3].

An implementation of the tabu search algorithm and the results we obtained are available on-line at the web page http://www.cargo.wlu.ca/2cc. These solutions have been used to construct Hadamard matrices with two circulant cores of the sixteen orders 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116.

Table 1
Number of solutions found by tabu search using neighborhoods $\mathcal{N}_1$ and $\mathcal{N}_2$

ℓ	27	29	31	33	35	37	39	41	43	45	47	49	51	53	55	57
$\mathcal{N}_1$	26525	8121	2061	372	190	46	20	1	2	1	1	1	1	1	1	1
$\mathcal{N}_2$	–	–	1143	–	–	–	–	–	147	–	–	–	–	–	–	–

Acknowledgments

All computations in C have been performed remotely at *SHARCnet* high performance computing clusters.
The second author is supported by a grant from the Natural Sciences and Engineering Research Council of Canada.

References

[1] L.D. Baumert, Cyclic Difference Sets, in: Lecture Notes in Mathematics, vol. 182, Springer-Verlag, Berlin, 1971.
[2] Th. Chadjipantelis, S. Kounias, Supplementary difference sets and *D*-optimal designs for $n \equiv 2 \bmod 4$, Discrete Math. 57 (3) (1985) 211–216.
[3] R.J. Fletcher, M. Gysin, J. Seberry, Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices, Australas. J. Combin. 23 (2001) 75–86.
[4] S. Georgiou, C. Koukouvinos, On generalized Legendre pairs and multipliers of the corresponding supplementary difference sets, Util. Math. 61 (2002) 47–63.
[5] F. Glover, M. Laguna, Tabu Search, in: Handbook of Combinatorial Optimization, vol. 3, Kluwer Acad. Publ, Boston, MA, 1998, pp. 621–757.
[6] I.S. Kotsireas, C. Koukouvinos, Genetic algorithms for the construction of Hadamard matrices with two circulant cores, J. Discrete Math. Sci. Cryptogr. 8 (2) (2005) 241–250.
[7] I.S. Kotsireas, C. Koukouvinos, J. Seberry, Hadamard ideals and Hadamard matrices with two circulant cores, European J. Combin. 27 (5) (2006) 658–668.
[8] É.D. Taillard, Comparison of iterative searches for the quadratic assignment problem, Location Sci. 3 (1995) 87–105.
[9] J. Wallis, On supplementary difference sets, Aequationes Math. 8 (1972) 242–257.
[10] J. Wallis, A note on supplementary difference sets, Aequationes Math. 10 (1974) 46–49.