1-1-2014

A review and new symmetric conference matrices

N. A. Balonin
Saint-Petersburg State University Of Aerospace Instrumentation, korbendfs@mail.ru

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

A review and new symmetric conference matrices

Abstract

We consider symmetric conference matrices which were first highlighted by Vitold Belevitch, who showed that such matrices mapped to lossless telephone connections. We give the known properties of symmetric conference matrices, known orders and illustrations for some elementary and some interesting cases. We restrict our attention in this note to symmetric conference matrices. Web addresess are given for other illustrations.

Keywords

matrices, conference, symmetric, review

Disciplines

Engineering | Science and Technology Studies

Publication Details

Balonin, N. A.. & Seberry, J. (2014). A review and new symmetric conference matrices. Informatsionno-upravliaiushchie sistemy, 71 (4), 2-7.

A Review and New Symmetric Conference Matrices

N. A. Balonin *and Jennifer Seberry †
Email: [korbendfs@mail.ru] and [jennifer_seberry]@uow.edu.au

Abstract

We consider symmetric conference matrices which were first highlighted by Vitold Belevitch, who showed that such matrices mapped to lossless telephone connections. We give the known properties of symmetric conference matrices, known orders and illustrations for some elementary and some interesting cases. We restrict our attention in this note to *symmetric conference* matrices. Web addresess are given for other illustrations.

Key Words and Phrases: Conference matrices, Hadamard matrices, symmetric balanced incomplete block designs (SBIBD), circulant difference sets, symmetric difference sets, constructions, telephony.

AMS Subject Classification: 05B20; 20B20.

1 Introduction

Symmetric Conference matrices are a particularly important class of $\{0, \pm 1\}$ matrices. Usually written as, C, they are $n \times n$ matrices with elements 0, $+1$ or -1 which satisfy

$$CC^\top = C^\top C = nI_n,$$

where " $^\top$" denotes the matrix transpose and I_n is the identity matrix of order n. We say that a conference matrix is an *orthogonal matrix*.

In this paper we use $-$ for -1 which corresponds to the usual Hadamard or weighing matrix notation.

A *circulant matrix* $C = (c_{ij})$ of order n satisfies $c_{ij} = c_{1,j-i+1(\text{mod n})}$.

2 Properties of Symmetric Conference Matrices.

We note the following properties of a conference matrix

- the order of a conference matrix must be $\equiv 2(\text{mod } 4)$;
- $n - 1$, where n is the order of a conference matrix, must be the sum of two squares;
- if there is a conference matrix of order n then there is a symmetric conference matrix of order n with zero diagonal. The two forms are equivalent as one can be transformed into the other by (i) interchanging rows (columns) or (ii) multiplying rows (columns) by -1;
- a conference matrix is said to be normalized if it has first row and column all plus ones.
- $C^{-1} = nC^\top$.

*Saint Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, St. Petersburg, Russian Federation
†Centre for Computer Security Research, EIS, University of Wollongong, NSW, 2522, Australia

3 Known Conference Matrix Orders

Conference matrices are known for the following orders

Key	Method	Explanation	References
c1	$p^r + 1$	$p^r \equiv 1 (\mathrm{mod}\ 4)$ is a prime power	[11, 6]
c2	$q^2(q+2)+1$	$q \equiv 3 (\mathrm{mod}\ 4)$ is a prime power $q+2$ is a prime power	[10]
c3	46		[10]
c4	$5 \times 9^{2t+1} + 1$	$t \geq 0$ an integer	[14]
c5	$(n-1)^s + 1$	$s \geq 2$ is an integer n the order of a conference matrix	[16, 13]
c6	$(h-1)^{2s} + 1$	$s \geq 1$ is an integer, h the order of a skew-Hadamard matrix	[16, 13]

We now describe the examples of the C(46) which differ from that of Mathon. We will observe and use three types of cells.

1. **type 0:** 0-circulant (zero shift, every row is equal to each-other);
2. **type 1:** circulant (circulant shift every new row right);
3. **type 2:** back-circulant (circulant shift every new row left).

We will say that a matrix has a *rich structure*, if it consists several different types of cells. Such notation allows us to describe special matrix structures for different C(46).

3.1 Rich Structures and Families of Mathon Structure

The Mathon C(46) [10] has as its core the usual symmetry block-circulant matrices, where every block has 9 little 3x3-cells. We write

$$W = circ(A, B, C, C^\top, B^\top)$$

where all cells of type 0 are situated inside of C.

3.1.1 The Basic Mathon C(46) has cells only of types 0 and 1

Cells have type 1 inside of $A = circ(a, b, b^\top)$, cells have type 1 inside of $B = backcirc(c, d, c^\top)$, cells have type 0 inside of $C = crosscirc(e)$.

The C=crosscirc(e) consists of m=3 columns (m – size of e), every column has m=3 rows – circulant shifted cell of type 0. We will call it as cross-shifted matrix (or cross-matrix, in short).

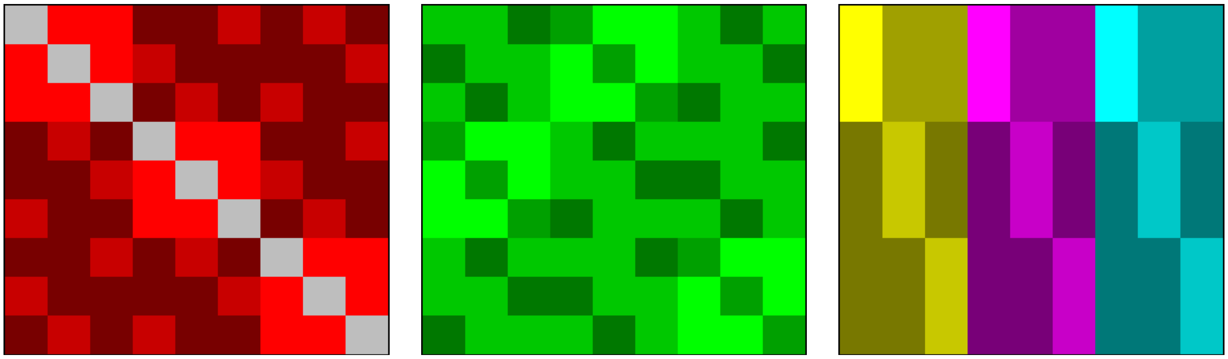

Figure 1: Matrices A, B, C of old cell-structure

3.1.2 The new Balonin-Seberry C(46) is based on cells of all types 0, 1 and 2 (that is there are richer cells)

The different structures that appear have cells with

1. type 1: $A = circ(a, b, b^\top)$,
2. type 2: $B = circ(c, d, d^*)$,
3. type 0: $C = crosscirc(e)$.

Now let $d = [d_1 d_2 d_3]$ then cell $d^* = [d_3 d_1 d_2]$ is used instead of $d^\top$ with back-circulant cells.

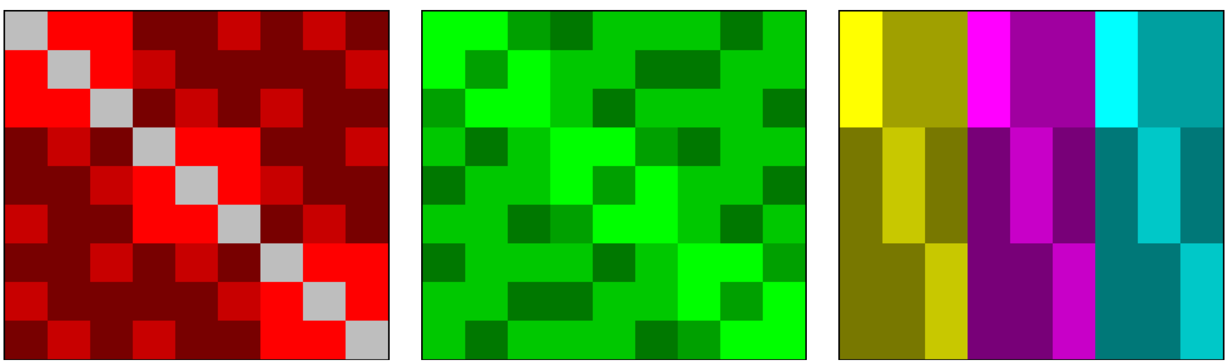

Figure 2: Matrices A, B, C of new cell-structure

This the most compact description of Mathon's matrix based on the term: "rich structure".

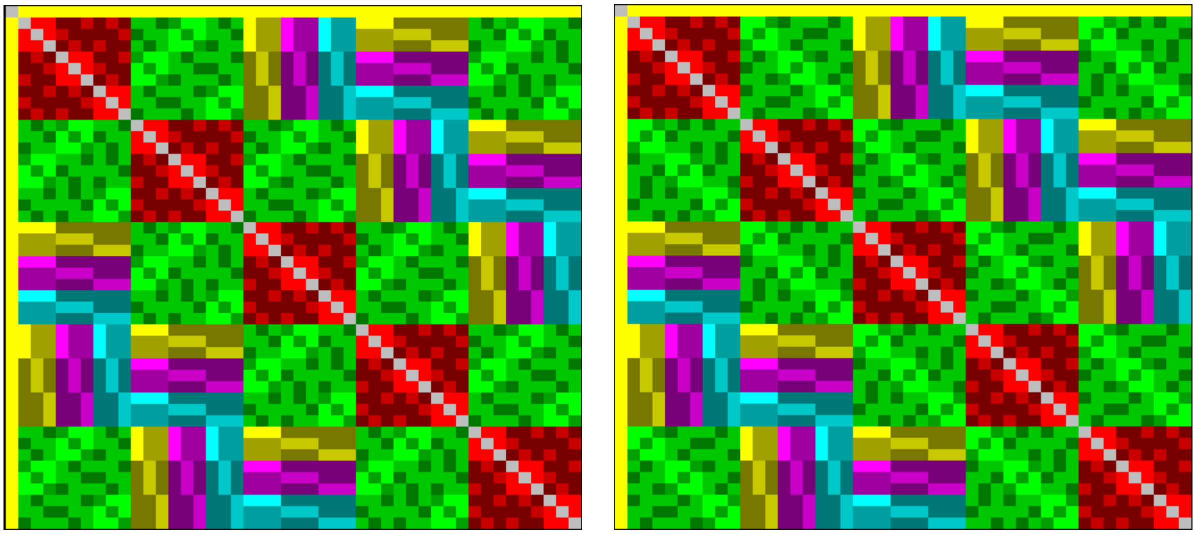

Figure 3: Matrice C46 of old (poor) and new (rich) cell-structures

The old structure has 2 types of cells and 3 types of matrices A, B, C. The new structure has 3 types of cells and 2 types of matrices. There is an imortant structural invaruant: the common quantity of types (cells and matrices) is equal to 5.

3.2 Easy to use Conference Matrix Forms

When used in real world mechanical applications it may be useful to have them in one of a few main forms: a *conference matrix with circulant core* or a *conference matrix constructed from two circulant matrices* the latter matrices will not be normalized.

Key	Method	Explanation	References
c1a	$p+1$	$p \equiv 1(\text{mod } 4)$ is a prime	[11, 6]
c1b	$p+1$	$p \equiv 1(\text{mod } 4)$ is a prime (power?)	[]
c7	4 circulant matrices with two borders.		

The conference matrix (actually an $OD(13; 4, 9)$) found by D. Gregory of Queens University, Kingston, Canada [7] given here is of the type c7.

$$
\left[\begin{array}{cc|cccccccccccc}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & - & - & - & 1 & 1 & 1 & - & - & - \\
\hline
1 & 1 & 0 & - & - & 1 & - & - & 1 & 1 & - & 1 & 1 & - \\
1 & 1 & - & 0 & - & - & 1 & - & - & 1 & 1 & - & 1 & 1 \\
1 & 1 & - & - & 0 & - & - & 1 & 1 & - & 1 & 1 & - & 1 \\
1 & - & 1 & - & - & 0 & 1 & 1 & - & 1 & 1 & 1 & - & - \\
1 & - & - & 1 & - & 1 & 0 & 1 & 1 & - & 1 & - & 1 & - \\
1 & - & - & - & 1 & 1 & 1 & 0 & 1 & 1 & - & - & - & 1 \\
1 & 1 & 1 & - & 1 & - & 1 & 1 & 0 & - & - & - & 1 & - \\
1 & 1 & 1 & 1 & - & 1 & - & 1 & - & 0 & - & - & - & 1 \\
1 & 1 & - & 1 & 1 & 1 & 1 & - & - & - & 0 & 1 & - & - \\
1 & - & 1 & - & 1 & 1 & - & - & - & - & 1 & 0 & 1 & 1 \\
1 & - & 1 & 1 & - & - & 1 & - & 1 & - & - & 1 & 0 & 1 \\
1 & - & - & 1 & 1 & - & - & 1 & - & 1 & - & 1 & 1 & 0
\end{array}\right]
$$

4 Conference matrices with cores and from two block matrices.

We particularly identify conferences matrices, of order n, which are normalized and can be written in one of the two forms: conference matrices with core or conference matrices made from two blocks.

These two forms look like

$$
\begin{array}{c|c} 1 & e \\ \hline e^\top & B \end{array} \qquad \text{and} \qquad \begin{bmatrix} A & B \\ B^\top & -A^\top \end{bmatrix}
$$

It is not necessary for A or B in either case to be circulant. However, in the form written they must commute. A variation of the second matrix can be used if A and B are amicable.

Then we say we have a *conference matrix with circulant core* or a *conference matrix constructed from two circulant matrices* the latter matrices will not be normalized.

Example 1

$$
\begin{bmatrix}
0 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & - & - & 1 \\
1 & 1 & 0 & 1 & - & - \\
1 & - & 1 & 0 & 1 & - \\
1 & - & - & 1 & 0 & 1 \\
1 & 1 & - & - & 1 & 0
\end{bmatrix}
\qquad \textit{and} \qquad
\left[\begin{array}{ccc|ccc}
0 & 1 & 1 & - & 1 & 1 \\
1 & 0 & 1 & 1 & - & 1 \\
1 & 1 & 0 & 1 & 1 & - \\
- & 1 & 1 & 0 & - & - \\
1 & - & 1 & - & 0 & - \\
1 & 1 & - & - & - & 0
\end{array}\right]
$$

In this example the two matrices are in fact equivalent.

5 A Classification to Differentiate between Symmetric Conference Matrices

We classify these by whether they

1. have a circulant core;

2. are constructed from two circulant blocks;
3. have a core but it is not circulant;
4. are constructed from two blocks but thay are not circulant;
5. Mathon's type;
6. from skew Hadamard matrices;
7. are constructed from four blocks with two borders;
8. any other pattern we see;
9. ad hoc.

6 Useful URLs and Webpages for this Study

Some useful url's include:

1. `http://mathscinet.ru/catalogue/OD/`
2. `http://mathscinet.ru/catalogue/artifact22/`
3. `http://mathscinet.ru/catalogue/conference/blocks/`

7 Acknowledgements

The authors would like to acknowledge the great effort of Mr Max Norden (Wollongong), and Tamara Vladimirovna Balonina (Gerasimova), who greatly helped with the LaTex, design, layout and presentation of this paper

8 Conclusion and Future Work

Comment In order to consider other matrices with these kinds of cells we consider the condition $n = p^2(q+2)+1$ as this allows many more little cells.

Version $n = 9 \times 9 + 1$ is very well known and class c1 [11]; Versions $n = 5 \times 9 \times 9 \times 9 + 1$ and in general $n = 5 \times 9^{2t+1}$ is class c4 [14];

Version $n = 9 \times 9 \times 9 \times 9 + 1$ is very well known and class c1 [11]; To continue to look at the versions $mp^r + 1$ we would next have to consider version $n = 13 \times 9 \times 9 + 1$ and so on.

Henceforth we consider the Mathon matrix as **oscillations** motivated by the Fourier basis.

Then the new Balonin-Seberry C(46) reflects phases "shift right"-"0-shift"-"shift-left"-"shift-left"-"0-shift".

References

[1] V. Belevitch, Conference networks and Hadamard matrices, *Ann. Soc. Sci. Brux. T.* 82, (1968), 13-32.

[2] V. Belevitch, (1950), Theorem of 2n-terminal networks with application to conference telephony. *Electr. Commun.*, vol. 26, (1950), 231-244.

[3] N.A. Balonin, M.B. Sergeev, Matritsy lokal'nogo maksimuma determinanta, *Informatsionno-upravliaiushchie sistemy*, 1, 68, (2014), 215, (in Russian).

[4] P Delsarte,J.-M. Goethals, J.J. Seidel, Orthogonal matrices with zero diagonal. II. *Canad. J. Math.* 23, (1971), 816832.

[5] A.V.Geramita and Jennifer Seberry, *Orthogonal Designs: Quadratic forms and Hadamard matrices*, Marcel Dekker, New York - Basel, (1979), viii, 460 pages.

[6] J.-M. Goethals and J.J. Seidel, Orthogonal matrices with zero diagonal, *Canad, J, Math,* 19, (1967), 1001-1010.

[7] D. Gregory, private communication, 1973.

[8] J. Horton, C. Koukouvinos, Jennifer Seberry, A search for Hadamard matrices constructed from Williamson matrices. *Bull. Inst. Combin. Appl.* 35, (2002), 75-88.

[9] Christos Koukouvinos and Jennifer Seberry, New weighing matrices constructed using two sequences with zero autocorrelation function - a review, *J. Stat. Planning and Inf.*, 81, (1999), 153-182. ISSN 0378-3758/99.

[10] R. Mathon, Symmetric conference matrices of order pq^2+1, *Canad. J. Math.*, 30, (1978), 321-331.

[11] R.E.A.C. Paley, On orthogonal matrices, *J. Math. Phys.*, 12, (1933), 311-320.

[12] Neil J.A. Sloane, *Online Encyclopedia of Integer Sequences (R), OEIS (R)*, accessed 2014:2:5:30.

[13] Jennifer Seberry Wallis, *Combinatorial Matrices*, PhD Thesis, La Trobe University, 1971.

[14] Jennifer Seberry and A. L. Whiteman, New Hadamard matrices and conference matrices obtained via Mathon's construction, *Graphs Combin.* 4, (1988), 355-377.

[15] R.J. Turyn, An infinite class of Williamson matrices. *J. Combin. Theory Ser. A*, 12, (1972), 391-321.

[16] R. J. Turyn, On C-matrices of arbitrary powers, *Bull. Canad. Math. Soc.* 23, (1971), 531-535.

[17] J.H. van Lint and J.J. Seidel, Equilateral point sets in elliptic geometry. *Indagationes Mathematicae*, 28, (1966), 335-348.

[18] W.D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis, *Combinatorics : Room Squares, Sum-free Sets, Hadamard Matrices*, 292, Lecture Notes in Mathematics, Springer–Verlag, Berlin–Heidelberg–New York, (1972), 508 pages.

Appendix

A Known Conference Matrix Orders Less than 1000

Order	Exist?	Type
6	√	c1, c1a
10	√	c1a, c6
14	√	c1, c1a
18	√	c1, c1a
22	NE	
26	√	c1
30	√	c1, c1a
34	NE	
38	√	c1, c1a
42	√	c1, c1a
46	√	c2, c3, c3
50	√	c1, c6
54	√	c1, c1a
58	NE	
62	√	c1, c1a
66	?	
70	NE	
74	√	c1, c1a
78	NE	
82	√	c1, c6
86	?	
90	√	c1, c1a
94	NE	
98	√	c1, c1a
102	√	c1, c1a
106	NE	
110	√	c1, c1a
114	√	c1, c1a
118	?	
122	√	c1, c6
126	√	c1
130	NE	
134	NE	
138	√	c1, c1a
142	NE	
146	?	
150	√	c1, c1a
154	?	
158	√	c1, c1a
162	NE	
166	NE	
170	√	c1
174	√	c1, c1a
178	NE	
182	√	c1, c1a
186	?	
190	NE	
194	√	c1, c1a
198	√	c1, c1a
202	NE	
206	?	
210	NE	
214	NE	
218	NE	
222	?	
226	?	
230	√	c1, c1a
234	√	c1, c1a
238	NE	
242	√	c1, c1a
246	?	
250	NE	
254	NE	
258	√	c1, c1a
262	?	
266	?	
270	√	c1, c1a
274	NE	
278	√	c1, c1a
282	√	c1, c1a
286	NE	
290	√	c1
294	√	c1, c1a
298	NE	
302	NE	
306	?	
310	NE	
314	√	c1, c1a
318	√	c1, c1a
322	NE	
326	?	
330	NE	
334	?	
338	√	c1, c1a
346	NE	
350	√	c1, c1a
354	√	c1, c1a
358	NE	
362	√	c1, c6
366	?	
370	?	
374	√	c1, c1a
378	?	
382	NE	
386	NE	
390	√	c1, c1a
394	NE	
398	√	c1, c1a
402	√	c1, c1a
406	?	
410	√	c1, c1a
414	NE	
418	NE	
422	√	c1, c1a
426	?	
430	NE	
434	√	c1, c1a
438	NE	
442	√	c2
446	?	
450	√	c1, c1a
454	NE	
458	√	c1, c1a
462	√	c1, c1a
466	NE	
470	NE	
474	NE	
478	?	
482	?	
486	?	
490	NE	
494	?	
498	NE	
502	NE	
506	?	
510	√	c1, c1a
514	NE	
518	NE	
522	√	c1, c1a
526	NE	
530	√	c1, c6
534	?	
538	NE	
542	√	c1, c1a
546	?	
550	?	
554	NE	
558	√	c1, c1a
562	NE	
566	?	
570	√	c1, c1a
574	NE	
578	√	c1, c1a
582	NE	
586	?	
590	NE	
594	√	c1, c1a
598	NE	
602	√	c1, c1a
606	?	
610	NE	
614	√	c1, c1a
618	√	c1, c1a
622	NE	
626	√	c1
630	?	
634	NE	
638	?	
642	√	c1, c1a
646	NE	
650	NE	
654	√	c1, c1a
658	?	
662	√	c1, c1a
666	NE	
670	NE	
674	√	c1, c1a
682	NE	
686	?	
690	?	
694	NE	
698	?	
702	√	c1, c1a
706	NE	
710	√	c1, c1a
714	NE	
718	NE	
722	NE	
726	?	
730	√	c1, c6
734	√	c1, c1a
738	NE	
742	NE	
746	?	
750	NE	
754	NE	
758	√	c1, c1a
762	√	c1, c1a
766	?	
770	√	c1, c1a
774	√	c1, c1a
778	NE	
782	NE	
786	?	
790	NE	
794	?	
798	√	c1, c1a
802	?	
806	NE	
810	√	c1, c1a
814	NE	
818	NE	
822	√	c1, c1a
826	NE	
830	√	c1, c1a
834	?	
838	NE	
842	√	c1
846	?	
850	NE	
854	√	c1, c1a
858	√	c1, c1a
862	NE	
866	?	
870	NE	
874	?	
878	√	c1, c1a
882	√	c1, c1a
886	NE	
890	NE	
894	NE	
898	NE	
902	?	
906	?	
910	?	
914	NE	
918	NE	
922	NE	
926	?	
930	√	c1, c1a
934	NE	
938	√	c1, c1a
942	√	c1, c1a
946	NE	
950	?	
954	√	c1, c1a
958	NE	
962	√	c1, c6
966	?	
970	NE	
974	NE	
978	√	c1, c1a
982	?	
986	?	
990	NE	
994	NE	
998	√	c1, c1a
1002	?	