UDC 004.438

A REVIEW AND NEW SYMMETRIC CONFERENCE MATRICES

N. A. Balonin[a], *Dr. Sc., Tech., Professor, korbendfs@mail.ru*
Jennifer Seberry[b], *PhD, Foundation Professor, jennifer_seberry@uow.edu.au*
[a]*Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation*
[b]*Centre for Computer Security Research, EIS, University of Wollongong, NSW, 2522, Australia*

Purpose: *The paper deals with symmetric conference matrices which were first highlighted by Vitold Belevitch, who showed that such matrices mapped to lossless telephone connections. The goal of this paper is developing a theory of conference matrices using the preliminary research results.* ***Methods:*** *Extreme (by determinant) solutions were obtained by minimization of the maximum of matrix elements absolute values, followed by their subsequent classification.* ***Results:*** *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. We give two symmetric conference matrices of order 46 which are inequivalent to those given by Rudi Mathon and show they lead to two new families of symmetric conference matrices of order* $5 \times 9^{2t+1} + 1$, $t \geq 0$ *is an integer.* ***Practical relevance:*** *Web addresses are given for other illustrations and other matrices with similar properties. Algorithms of building symmetric conference matrices have been used for developing research software.*

Keywords *— Conference Matrices, Hadamard Matrices, Weighing Matrices, Symmetric Balanced Incomplete Block Designs (SBIBD), Circulant Difference Sets, Symmetric Difference Sets, Relative Difference Sets, Constructions, Telephony.*

AMS Subject Classification: *05B20; 20B20.*

Introduction

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

$$\mathbf{C}^{\mathrm{T}}\mathbf{C} = \mathbf{C}\mathbf{C}^{\mathrm{T}} = (n-1)\mathbf{I}_n,$$

where "T" – denotes the matrix transpose and $\mathbf{I}_n$ is the identity matrix of order n. We say that a conference matrix is an *orthogonal matrix* (after the column-normalization).

In this paper we use – for –1 which corresponds to the usual Hadamard or weighing matrix notation [1–20].

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

Properties of Symmetric Conference Matrices

We note the following properties of a conference matrix:

— the order of a conference matrix must be ≡ 2 (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;

— $\mathbf{C}_n^{\mathrm{T}} = (n-1)\mathbf{C}_n^{-1}$.

Known Conference Matrix Orders

Conference matrices are known [see Appendix] 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	$5 \times 9^{2t+1} + 1$	$t \geq 0$ is an integer	[15]
c5	$(n-1)^s + 1$	$s \geq 2$ is an integer, n — the order of a conference matrix	[17, 14]
c6	$(h-1)^{2s} + 1$	$s \geq 1$ is an integer, h — the order of a skew-Hadamard matrix	[17, 14]
c7	4 circulant matrices with two borders	Example below	
c8	Certain relative difference sets with two borders		[1]

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, all rows are 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 of several different types of cells. Such notation allows us to describe special matrix structures for different C_{46}.

Rich Structures and Families of Mathon Structure

The Mathon C_{46} [10] has as its core the usual block-circulant matrix, every block has 9 little 3×3-cells. We write it as

$$\mathbf{W} = \mathrm{circ}(\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{C}^T, \mathbf{B}^T),$$

where all cells of type 0 are situated inside of $\mathbf{C}$.

The Basic Mathon C_{46} has cells only of types 0 and 1

Cells (Fig. 1) have

1) type 1: inside of $\mathbf{A} = \mathrm{circ}(\mathbf{a}, \mathbf{b}, \mathbf{b}^T)$;

2) type 1: inside of $\mathbf{B} = \mathrm{backcirc}(\mathbf{c}, \mathbf{d}, \mathbf{c}^T)$;

3) type 0: inside of $\mathbf{C} = \mathrm{crosscirc}(\mathbf{e})$.

The $\mathbf{C}$ = crosscirc($\mathbf{e}$) consists of $m = 3$ columns (m — size of $\mathbf{e}$), every column has $m = 3$ rows — circulant shifted cell of type 0. We will call it a *cross-shifted matrix* (or cross-matrix, for short).

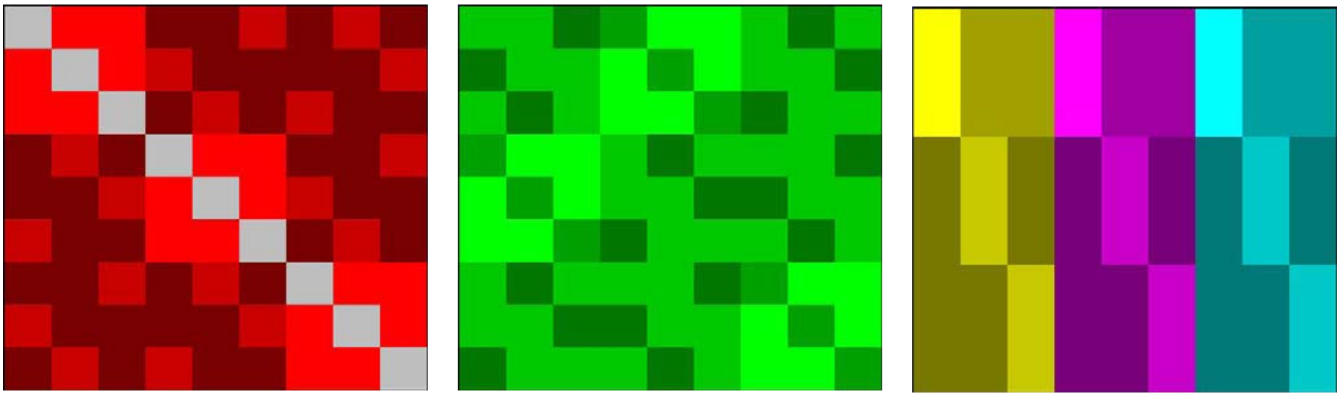
The new Balonin — Seberry C_{46} is based on cells of all types 0, 1 and 2 (that is there are richer cells)

The different structures that appear have cells (Fig. 2) with

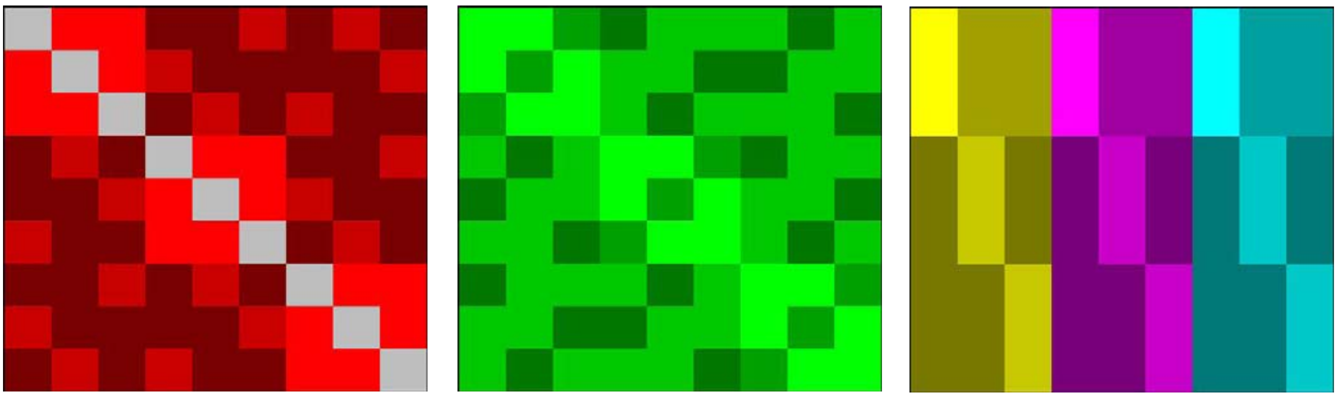
1) type 1: inside of $\mathbf{A} = \mathrm{circ}(\mathbf{a}, \mathbf{b}, \mathbf{b}^T)$;

2) type 2: inside of $\mathbf{B} = \mathrm{circ}(\mathbf{c}, \mathbf{d}, \mathbf{d}^*)$;

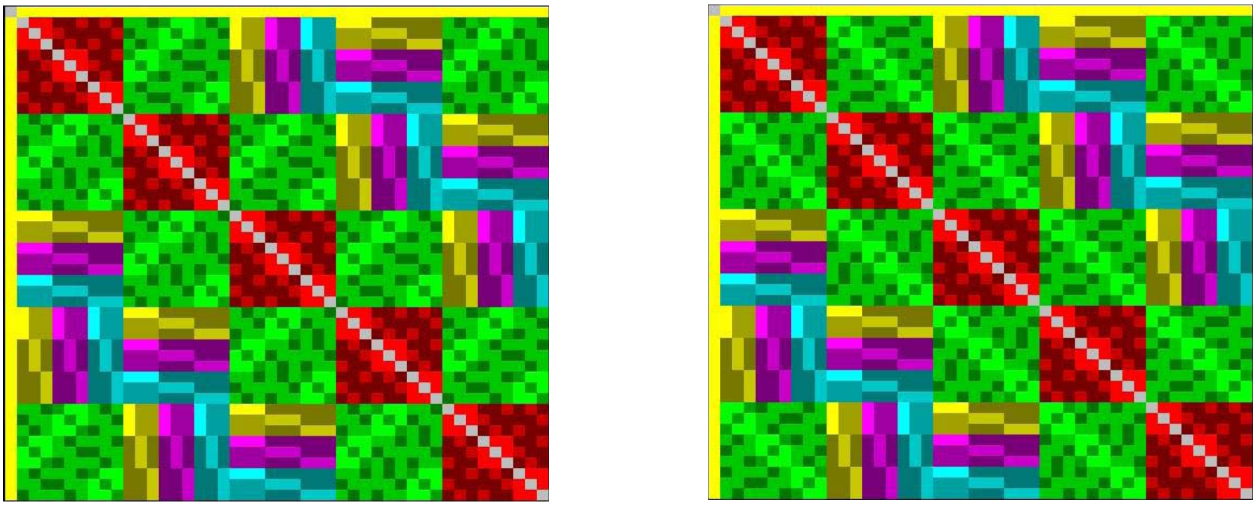
3) type 0: inside of $\mathbf{C} = \mathrm{crosscirc}(\mathbf{e})$.



■ ***Fig. 1.*** Matrices **A**, **B**, **C** of original cell-structure



■ ***Fig. 2.*** Matrices **A**, **B**, **C** of new cell-structure



■ ***Fig. 3.*** Matrices $\mathbf{C}_{46}$ of original (poor) and new (rich) cell-structures

Now let $\mathbf{d} = [\mathbf{d}_1\ \mathbf{d}_2\ \mathbf{d}_3]$ then cell $\mathbf{d}^* = [\mathbf{d}_3\ \mathbf{d}_1\ \mathbf{d}_2]$ is used instead of $\mathbf{d}^{\mathrm{T}}$ with back-circulant cells.

This the most compact description of Mathon's matrix based on the term: "rich structure" (Fig. 3).

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 important *structural invariant*: the common quantity of types (cells and matrices) is equal to 5.

To show the inequivalence of these $\mathbf{C}_{46}$ we would start by using permutations of size 5 to try to transform the blocks from the second matrix into the form of the first. This is carried out for both the row blocks and column blocks. However, when we look at the resulting structure we see it is not symmetric. To force it to be symmetric we have to reverse the operations we have just carried out. Hence we can not permute one structure into the other. About the inequivalence of rich and poor structures, we can say the following: there are "inequivalence by structure" (ornamental inequivalence) and "inequivalence by permutations". Among Hadamard matrices (for example) there are well known Sylvester and Walsh constructions, they have the first type of difference: ornamental inequivalence.

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*, this is c1a below, or *a conference matrix constructed from two circulant matrices*, this is c1b below, the latter matrices will not be normalized. The type described as c7, for which we give an example, but not an infinite class may also be useful.

Key	Method	Explanation	References
c1a	$p+1$	$p \equiv 1 \pmod 4$ is a prime	[11, 6]
c1b	$p+1$	$p \equiv 1 \pmod 4$ is a prime	[5]
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[1] given here is of the type c7.

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

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

Families of Conference Matrices

Seberry and Whiteman [15] showed how to extend the symmetric conference matrix $\mathbf{C}_{46}$ of Mathon to an infinite familiy of symmetric conference matrices of order $5\times 9^{2t+1}+1$, $t \ge 0$ is an integer. That paper carefully calculated all the interactions between the basic blocks of the 9×9 original blocks.

Since this calculation is arithmetical and not instructive we do not copy it here. However exactly the same techniques can be used to find new, inequivalent families, c4bswa and c4bswb from our two new $\mathbf{C}_{46}$. This technique is also similar to that in Seberry [13].

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

$$\left(\begin{array}{c|c} \mathbf{0} & \mathbf{e} \\ \hline \mathbf{e}^{\mathrm{T}} & \mathbf{A} \end{array}\right) \text{ and } \left(\begin{array}{c|c} \mathbf{A} & \mathbf{B} \\ \hline \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{array}\right).$$

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.

$$\left[\begin{array}{c|ccccc} 0 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & - & - & 1 \\ 1 & 1 & 0 & 1 & - & - \\ 1 & - & 1 & 0 & 1 & - \\ 1 & - & - & 1 & 0 & 1 \\ 1 & 1 & - & - & 1 & 0 \end{array}\right] \text{ and } \left[\begin{array}{ccc|ccc} 0 & 1 & 1 & - & 1 & 1 \\ 1 & 0 & 1 & 1 & - & 1 \\ 1 & 1 & 0 & 1 & 1 & - \\ \hline - & 1 & 1 & 0 & - & - \\ 1 & - & 1 & - & 0 & - \\ 1 & 1 & - & - & - & 0 \end{array}\right].$$

In this example the two matrices are in fact equivalent [13, 15].

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 they 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.

Useful URLs and Webpages Related to 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/
4) http://mathscinet.ru/catalogue/belevitch3646/
5) http://www.indiana.edu/~maxdet/
6) http://www.math.ntua.gr/~ckoukouv/
7) http://www.uow.edu.au/~jennie/Hadamard.html/
8) http://tomas.rokicki.com/newrec.html

We also note a very useful package for Latin to Cyrillic conversion: *package*[*utf* 8]*inputenc*

Acknowledgements

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

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, 19]; versions $n = 5 \times 9 \times 9 \times 9 + 1$ and in general $n = 5 \times 9^{2t+1}$ is class c4 [15]: c4bswa and c4bswb, given above, are also this type. 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 $\mathbf{C}_{46}$ reflects phases "shift right"–"0-shift"–"shift-left"–"shift-left"–"0-shift".

References

1. Arasu K. T., Chen Yu. Q., Pott A. Hadamard and Conference Matrices. *Journal Algebraic Combinatorics*, 2001, no. 14, pp. 103–117.
2. Belevitch V. Conference Networks and Hadamard Matrices. *Ann. Soc. Scientifique Bruxelles*, 1968, no. 82, pp. 13–32.
3. Belevitch V. Theorem of 2n-terminal Networks with Application to Conference Telephony. *Electrical Communication*, 1950, no. 26, pp. 231–244.
4. Balonin N. A., Sergeev M. B. Local Maximum Determinant Matrices. *Informatsionno-upravliaiushchie sistemy*, 2014, no. 1(68), pp. 2–15 (In Russian).
5. Delsarte P., Goethals J.-M., Seidel J. J. Orthogonal Matrices with Zero Diagonal. II. *Canadian Journal of Mathematics*, 1971, no. 23, pp. 816–832.
6. Geramita A. V., Seberry J. *Orthogonal Designs: Quadratic forms and Hadamard matri-ces*. New York — Basel, Marcel Dekker, 1979. 460 p.
7. Goethals J.-M., Seidel J. J. Orthogonal Matrices with Zero Diagonal. *Canadian Journal of Mathematics*, 1967, no. 19, pp. 1001–1010.
8. Horton J., Koukouvinos C., Seberry Jennifer. A Search for Hadamard Matrices Constructed from Williamson Matrices. *Bull. Inst. Combin. Appl.* 2002, no. 35, pp. 75–88.
9. Koukouvinos C., Seberry J. New Weighing Matrices Constructed Using Two Se-quences with Zero Autocorrelation Function — a Review. *Journal Stat. Planning and Inf.*, 1999, no. 81, pp. 153–182.
10. Mathon R. Symmetric Conference Matrices of Order $pq^2 + 1$. *Canadian Journal of Mathematics*, 1978, no. 30, pp. 321–331.
11. Paley R. E. A. C. On Orthogonal Matrices. *J. Math. Phys.*, 1933, no. 12, pp. 311–320.
12. Neil J. A. Sloane. *Online Encyclopedia of Integer Sequences ®, OEIS ®*. Available at: http://oeis.org (accessed 5 Juny 2014).
13. Seberry J. New Families of Amicable Hadamard Matrices. *J Statistical Theory and Practice*, in memory of Jagdish N Srivastava, 2013, iss. 4, no. 7, pp. 650–657.
14. Seberry J. W. *Combinatorial Matrices*, PhD Thesis, La Trobe University, 1971.
15. Seberry J., Whiteman A. L. New Hadamard Matrices and Conference Matrices Obtained via Mathon's Construction. *Graphs Combin.*, 1988, no. 4, pp. 355–377.
16. Turyn R. J. An Infinite Class of Williamson Matrices. *Journal Combin. Theory. Ser. A*, 1972, no. 12, pp. 391–321.
17. Turyn R. J. On *C*-matrices of Arbitrary Powers. *Bull. Canad. Math. Soc.*, 1971, no. 23, pp. 531–535.
18. Van Lint J. H., Seidel J. J. Equilateral Point Sets in Elliptic Geometry. *Indagationes Mathematicae*, 1966, no. 28, pp. 335–348.
19. Scarpis U. Sui Determinanti di Valore Massimo. *Rendiconti della R. Istituto Lombardo di Scienze e Lettere*, 1898, 31, pp. 1441–1446 (In Italian).
20. Wallis W. D., Street A. P., Seberry J. W. *Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices*. Lecture Notes in Mathematics. Vol. 292. Berlin–Heidelberg–New York, Springer–Verlag, 1972. 508 p.

Appendix

■ Known Conference Matrix Orders Less than 1000

Order	Exist?	Type	Order	Exist?	Type	Order	Exist?	Type	Order	Exist?	Type
6	√	c1, c1a	254	NE		506	?		758	√	c1, c1a
10	√	c1a, c6	258	√	c1, c1a	510	√	c1, c1a	762	√	c1, c1a
14	√	c1, c1a	262	?		514	NE		766	?	
18	√	c1, c1a	266	?		518	NE		770	√	c1, c1a
22	NE		270	√	c1, c1a	522	√	c1, c1a	774	√	c1, c1a
26	√	c1	274	NE		526	NE		778	NE	
30	√	c1, c1a	278	√	c1, c1a	530	√	c1, c6	782	NE	
34	NE		282	√	c1, c1a	534	?		786	?	
38	√	c1, c1a	286	NE		538	NE		790	NE	
42	√	c1, c1a	290	√	c1	542	√	c1, c1a	794	?	
46	√	c2, c3, c4	294	√	c1, c1a	546	?		798	√	c1, c1a
50	√	c1, c6	298	NE		550	?		802	?	
54	√	c1, c1a	302	NE		554	NE		806	NE	
58	NE		306	?		558	√	c1, c1a	810	√	c1, c1a
62	√	c1, c1a	310	NE		562	NE		814	NE	
66	?		314	√	c1, c1a	566	?		818	NE	

Order	Exist?	Type	Order	Exist?	Type	Order	Exist?	Type	Order	Exist?	Type
70	NE		318	√	c1, c1a	570	√	c1, c1a	822	√	c1, c1a
74	√	c1, c1a	322	NE		574	NE		826	NE	
78	NE		326	?		578	√	c1, c1a	830	√	c1, c1a
82	√	c1, c6	330	NE		582	NE		834	?	
86	?		334	?		586	?		838	NE	
90	√	c1, c1a	338	√	c1, c1a	590	NE		842	√	c1
94	NE		346	NE		594	√	c1, c1a	846	?	
98	√	c1, c1a	350	√	c1, c1a	598	NE		850	NE	
102	√	c1, c1a	354	√	c1, c1a	602	√	c1, c1a	854	√	c1, c1a
106	NE		358	NE		606	?		858	√	c1, c1a
110	√	c1, c1a	362	√	c1, c6	610	NE		862	NE	
114	√	c1, c1a	366	?		614	√	c1, c1a	866	?	
118	?		370	?		618	√	c1, c1a	870	NE	
122	√	c1, c6	374	√	c1, c1a	622	NE		874	?	
126	√	c1	378	?		626	√	c1	878	√	c1, c1a
130	NE		382	NE		630	?		882	√	c1, c1a
134	NE		386	NE		634	NE		886	NE	
138	√	c1, c1a	390	√	c1, c1a	638	?		890	NE	
142	NE		394	NE		642	√	c1, c1a	894	NE	
146	?		398	√	c1, c1a	646	NE		898	NE	
150	√	c1, c1a	402	√	c1, c1a	650	NE		902	?	
154	?		406	?		654	√	c1, c1a	906	?	
158	√	c1, c1a	410	√	c1, c1a	658	?		910	?	
162	NE		414	NE		662	√	c1, c1a	914	NE	
166	NE		418	NE		666	NE		918	NE	
170	√	c1	422	√	c1, c1a	670	NE		922	NE	
174	√	c1, c1a	426	?		674	√	c1, c1a	926	?	
178	NE		430	NE		682	NE		930	√	c1, c1a
182	√	c1, c1a	434	√	c1, c1a	686	?		934	NE	
186	?		438	NE		690	?		938	√	c1, c1a
190	NE		442	√	c2	694	NE		942	√	c1, c1a
194	√	c1, c1a	446	?		698	?		946	NE	
198	√	c1, c1a	450	√	c1, c1a	702	√	c1, c1a	950	?	
202	NE		454	NE		706	NE		954	√	c1, c1a
206	?		458	√	c1, c1a	710	√	c1, c1a	958	NE	
210	NE		462	√	c1, c1a	714	NE		962	√	c1, c6
214	NE		466	NE		718	NE		966	?	
218	NE		470	NE		722	NE		970	NE	
222	?		474	NE		726	?		974	NE	
226	?		478	?		730	√	c1, c6	978	√	c1, c1a
230	√	c1, c1a	482	?		734	√	c1, c1a	982	?	
234	√	c1, c1a	486	?		738	NE		986	?	
238	NE		490	NE		742	NE		990	NE	
242	√	c1, c1a	494	?		746	?		994	NE	
246	?		498	NE		750	NE		998	√	c1, c1a
250	NE		502	NE		754	NE		1002	?	