University of Wollongong
Research Online

Faculty of Informatics - Papers (Archive)

Faculty of Engineering and Information Sciences

2006

Inequivalence of Nega-cyclic ±1 Matrices

R. Ang
University of Wollongong

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

T. A. Wysocki
University of Wollongong, wysocki@uow.edu.au

Publication Details

This article was originally published as Ang, R, Seberry, J and Wysocki, TA, Inequivalence of Nega-cyclic ±1 Matrices, Journal of Combinatorial Mathematics and Combinatorial Computing 56, 2006, 17-32.

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

Inequivalence of Nega-cyclic ±1 Matrices

Abstract

We study nega-cyclic ±1 matrices. We obtain preliminary results which are then used to decrease the search space. We find that there are 2, 4, 9, 23, 63, and 187 ip-equivalence classes for lengths 3, 5, 7, 9, 11, and 13 respectively. The matrices we find are used in a variant given here of the Goethals-Seidel array to form Hadamard matrices, the aim being to later check them for suitability for CDMA schemes.

Keywords

Hadamard matrix, nega-cyclic, ip-equivalence classes, Goethals-Seidel array, variant Goethals-Seidel array, AMS Subject Classification: Primary 05B20, Secondary 62K05, 62K10

Disciplines

Physical Sciences and Mathematics

Publication Details

This article was originally published as Ang, R, Seberry, J and Wysocki, TA, Inequivalence of Nega-cyclic ±1 Matrices, Journal of Combinatorial Mathematics and Combinatorial Computing 56, 2006, 17-32.

This journal article is available at Research Online: http://ro.uow.edu.au/infopapers/354

Inequivalence of Nega-cyclic ± 1 Matrices

Russell Ang[1], Jennifer Seberry[1] and Tadeusz Wysocki[2]
1. Centre for Computer Security Research School of IT and Computer Science
and
2. School of Electrical, Computer and Telecommunications Engineering
University of Wollongong
NSW 2522
Australia

Abstract

We study nega-cyclic ± 1 matrices. We obtain preliminary results which are then used to decrease the search space. We find that there are 2, 4, 9, 23, 63, and 187 ip-equivalence classes for lengths 3, 5, 7, 9, 11, and 13 respectively. The matrices we find are used in a variant given here of the Goethals-Seidel array to form Hadamard matrices, the aim being to later check them for suitability for CDMA schemes.

Key words and phrases: Hadamard matrix, nega-cyclic, ip-equivalence classes, Goethals-Seidel array, variant Goethals-Seidel array
AMS Subject Classification: Primary 05B20, Secondary 62K05, 62K10

1 Introduction

An *Hadamard matrix* H of order n is a square $(1, -1)$ matrix having inner product of distinct rows zero. Hence $HH^T = nI_n$. We note that $n = 1, 2$ or $n \equiv 0 \pmod 4$.
Circulant matrices of order n are polynomials in the shift matrix

$$T = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & & 1 \\ 1 & 0 & 0 & & 0 \end{pmatrix}.$$

Nega-cyclic matrices of order n are polynomials in the nega-shift matrix

$$N = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & & 1 \\ -1 & 0 & 0 & & 0 \end{pmatrix}.$$

If A is a circulant matrix of odd order, then XAX, where $X = \mathrm{diag}(1, -1, 1, -1, \ldots, 1)$, will be a *nega-cyclic matrix.*

The *back-diagonal matrix* R of order n is the matrix whose elements r_{ij} are given by

$$r_{ij} = \begin{cases} 1 & \text{if } i + j = n + 1, \\ 0 & \text{otherwise} \end{cases}$$

where $i, j = 1, \ldots, n$.

We note some properties of the nega-cyclic matrix N given above:

Lemma 1

$$(N^i)^T = -N^{n-i} \quad \text{and} \quad N^i R = -RN^{n-i}.$$

Hence we have

Lemma 2 $N^i(N^j R)^T = (N^j R)(N^i)^T$.

Proof. $N^i(N^j R)^T = N^i R(N^j)^T = -N^i R N^{n-j} = N^i N^j R = N^j N^i R = -N^j R N^{n-i} = -N^j R(N^i)^T = (N^j R)(N^i)^T$. □

Furthermore

Theorem 1 *Let R_i, R_j be two rows of a nega-cyclic matrix of dimension n, where $1 < i < j \leq n$. Then $R_i R_j^T = R_1 R_{1+j-i}^T$.*

Proof. Let $i = 1+s$ and $j = 1+s+t$. If we write $R_1 = (x_1, \ldots, x_n)$, we have

$$\begin{aligned} R_{1+s} &= (-x_{n-s+1}, \ldots, -x_n, x_1, \ldots, x_{n-s}) \\ R_{1+t} &= (-x_{n-t+1}, \ldots, -x_n, x_1, \ldots, x_{n-t}) \\ R_{1+s+t} &= (-x_{n-s-t+1}, \ldots, -x_n, x_1, \ldots, x_{n-s-t}) \end{aligned}$$

We note that

$$R_{1+s} = (\overbrace{-x_{n-s+1}, \ldots, -x_n}^{s}, \overbrace{x_1, \ldots, x_t}^{t}, x_{t+1}, \ldots, x_{n-s})$$

$$R_{1+s+t} = (\underbrace{-x_{n-s-t+1}, \ldots, -x_{n-t}}_{s}, \underbrace{-x_{n-t+1}, \ldots, -x_n}_{t}, x_1, \ldots, x_{n-s-t})$$

Then

$$\begin{aligned}
R_i R_j^T &= R_{1+s} R_{1+s+t}^T \\
&= x_{n-s+1}x_{n-s-t+1} + \cdots + x_n x_{n-t} - x_1 x_{n-t+1} - \cdots - x_t x_n \\
&\quad + x_{t+1}x_1 + \cdots + x_{n-s}x_{n-s-t} \\
&= -x_1 x_{n-t+1} - \cdots - x_t x_n + x_{t+1}x_1 + \cdots + x_{n-s}x_{n-s-t} \\
&\quad + x_{n-s+1}x_{n-s-t+1} + \cdots + x_n x_{n-t} \\
&= -x_1 x_{n-t+1} - \cdots - x_t x_n + x_{t+1}x_1 + \cdots + x_n x_{n-t} \\
&= R_1 R_{1+t}^T \\
&= R_1 R_{1+j-i}^T.
\end{aligned}$$

□

Theorem 2 *Let R_1 be the first row of a nega-cyclic matrix of dimension n. Let R_ℓ be other rows of the $2n \times n$ matrix obtained by taking all the $2n-1$ nega-cyclic shifts of R_1. Then the inner products, k_ℓ, of R_1 and R_ℓ, $1 \le \ell \le 2n$ are $\pm k_2, \pm k_3, \ldots, \pm k_{\frac{n-1}{2}}, \pm n$. Specifically, the sequence of inner products of the nega-cyclic shifts is of the form*

$$k_2, k_3, \cdots, k_{\frac{n-1}{2}}, -k_{\frac{n-1}{2}}, \cdots, -k_3, -k_2, -n, -k_2, -k_3, \\ \cdots, -k_{\frac{n-1}{2}}, k_{\frac{n-1}{2}}, \cdots, k_3, k_2.$$

Proof. Considering that

$$R_{1+n} = (-x_1, -x_2, \ldots, -x_n) = -R_1$$

we have the inner products

$$\begin{aligned}
R_1 \cdot R_{1+n} &= -n, \\
R_1 \cdot R_{1+n+\ell} &= -R_1 \cdot R_{1+\ell}^T, \ \ell = 0, \ldots, n-1.
\end{aligned}$$

We note that

$$R_{1+\frac{n-3}{2}} = (\overbrace{-x_{\frac{n-3}{2}+1}, \ldots, -x_n}^{\frac{n+1}{2}}, \overbrace{x_1, \ldots, x_{\frac{n-1}{2}}}^{\frac{n-1}{2}})$$

and

$$R_{1+\frac{n-1}{2}} = (\underbrace{-x_{\frac{n+1}{2}+1}, \ldots, -x_n}_{\frac{n-1}{2}}, \underbrace{x_1, \ldots, x_{\frac{n+1}{2}}}_{\frac{n+1}{2}}).$$

Hence, straightforwardly, the inner product

$$R_1 \cdot R_{\frac{n-1}{2}} = -R_1 \cdot R_{\frac{n+1}{2}}.$$

Similarly

$$R_1 \cdot R_{\frac{n-1}{2}-\ell} = -R_1 \cdot R_{\frac{n+1}{2}+\ell}, \ \ell = 0, \ldots, \ \frac{n-5}{2}.$$

□

Remark 1 In other words we observe that

1. the $n+1$st nega-cyclic shift of the first row is the negative of the first row.
2. the inner product of the ith row with the first, $i = 1, 2, \cdots, \frac{n-1}{2}$ is minus the inner product of the $n+2-i$th row with the first.
3. the sequence of inner products of the nega-cyclic shifts is of the form

   $k_2, k_3, \cdots, k_t, -k_t, \cdots, -k_3, -k_2, -n, -k_2, -k_3,$
   $\cdots, -k_t, k_t, \cdots, k_3, k_2$ where $t = \frac{n-1}{2}$.

□

Lemma 3 *Suppose A, B are polynomial in T or N then $A(BR)^T = (BR)A^T$.*

Proof. The result for T, circulant, can be found in Seberry Wallis [6]. For N, nega-cyclic, we note A and B are polynomials in N so by repeated applications of lemma 2 we have the result. □

We note from Seberry Wallis and Whiteman [7] that circulant can be replaced by group-type or type 1 in abelian groups so that all results that follow for circulant also follow for group-type or type 1. Similarly we observe that group-type or type 1 nega-cyclic can be used instead of nega-cyclic and the corresponding results hold. So we have, modifying Goethals-Seidel construction [6]:

Theorem 3 *Suppose there exist four nega-cyclic* $(1,-1)$ *matrices* A, B, C, D *of order* n. *Further, suppose*

$$AA^T + BB^T + CC^T + DD^T = 4nI_n. \tag{1}$$

Then

$$S = \begin{bmatrix} A & BR & CR & DR \\ -BR & A & D^TR & -C^TR \\ -CR & -D^TR & A & B^TR \\ -DR & C^TR & -B^TR & A \end{bmatrix} \tag{2}$$

is an Hadamard matrix of order $4n$ *of* S type. *(Here* R *is the back diagonal matrix.) If* A *is skew-type, then* S *is skew-Hadamard.*

A later section will be devoted to Hadamard matrices constructed using this theorem.

2 Desired Characteristics of CDMA Spreading Codes

This section motivates our search strategy by highlighting the desirable characteristics of spreading codes.

For bipolar (that is two value or ± 1) spreading codes $\{s_n^{(i)}\}$ and $\{s_n^{(l)}\}$ of length N, the normalized discrete aperiodic correlation function is defined as [1]:

$$c_{i,l}(\tau) = \begin{cases} \frac{1}{N}\sum_{n=0}^{N-1-\tau} s_n^{(i)} s_{n+\tau}^{(l)}, & 0 \le \tau \le N-1 \\ \frac{1}{N}\sum_{n=0}^{N-1+\tau} s_{n-\tau}^{(i)} s_n^{(l)}, & 1-N \le \tau < 0 \\ 0, & |\tau| \ge N \end{cases}$$

When $\{s_n^{(i)}\}$ equals $\{s_n^{(l)}\}$, the above equation defines the normalized discrete aperiodic auto-correlation function.

In order to evaluate the performance of a whole set of M spreading codes, the average mean square value of cross-correlation for all codes in the set, denoted by R_{cc}, was introduced by Oppermann and Vucetic [3] as a measure of the set cross-correlation performance:

$$R_{CC} = \frac{1}{M(M-1)} \sum_{i=1}^{M} \sum_{\substack{k=1 \\ k \neq i}}^{M} \sum_{\tau=1-N}^{N-1} |c_{i,k}(\tau)|^2$$

A similar measure, denoted by R_{AC} was introduced there for comparing the auto-correlation performance:

$$R_{AC} = \frac{1}{M} \sum_{i=1}^{M} \sum_{\substack{\tau=1-N \\ \tau \neq 0}}^{N-1} |c_{i,j}(\tau)|^2$$

The R_{AC} allows for comparison of the auto-correlation properties of the set of spreading codes on the same basis as their cross-correlation properties.

It is highly desirable to have both R_{CC} and R_{AC} as low as possible, as the higher value of R_{CC} results in stronger multi-access interference (MAI), and an increase in the value of R_{AC} impedes the code acquisition process. Unfortunately, decreasing the value of R_{CC} causes increase in the value of R_{AC}, and vice versa.

Both R_{CC} and R_{AC} are very useful for large code sets and large number of active users, when the constellation of interferers (i.e. relative delays among the active users and the spreading codes used) changes randomly for every transmitted information symbol. However, for a more static situation, when the constellation of interferers stays constant for the duration of many information symbols, it is also important to consider the worst-case scenarios. This can be accounted for by analyzing the maximum value of peaks in the aperiodic cross-correlation functions over the whole set of sequences and in the aperiodic autocorrelation function for $\tau \neq 0$. Hence, one needs to consider two additional measures to compare the spreading sequence sets:

Maximum value of the aperiodic cross-correlation functions C_{max}:

$$c_{max}(\tau) = \max_{\substack{i=1\cdots M \\ k=1\cdots M \\ i\neq k}} |c_{i,k}(\tau)|; \quad \tau=(-N+1)\cdots(N-1)$$

Maximum value of the off-peak aperiodic autocorrelation functions A_{max}

$$a_{max}(\tau) = \max_{k=1\cdots M} |c_{k,k}(\tau)|;$$

$$A_{max} = \max_{\tau\neq 0}\{a_{max}(\tau)\}$$

The known relationships between C_{max} and A_{max} are due to Welch [8] and Levenshtein [2].

The Welch bound and states that for any set of M bipolar sequences of length N

$$max\{C_{max}, A_{max}\} \geq \sqrt{\frac{M-1}{2NM-M-1}}$$

A tighter Levenshtein bound is expressed by:

$$max\{C_{max}, A_{max}\} \geq \sqrt{\frac{(2N^2+1)M-3N^2}{3N^2(MN-1)}}$$

It must be noted here that both Welch and Levenshtein bounds are derived for sets of bipolar sequences where the condition of orthogonality for perfect synchronization is not imposed. Hence, one can expect that by introducing the orthogonality condition, the lower bound for the aperiodic cross-correlation and aperiodic out-of-phase auto-correlation magnitudes must be significantly lifted. This is further discussed in [4].

3 Ip-equivalence and Nega-cyclic Matrices

We define two *nega-cyclic* ± 1 matrices as *ip-equivalent* if they yield the same ordered set of inner products between their first rows and the nega-cyclic shifts of the first row.

Example 1 Consider the eight possible first rows of a nega-cyclic matrix ± 1 of row length 3 and create their nega-cyclic shifts. We have

- - -	- - 1	- 1 -	- 1 1	1 - -	1 - 1	1 1 -	1 1 1
1 - -	- - -	1 - 1	- - 1	1 1 -	- 1 -	1 1 1	- 1 1
1 1 -	1 - -	- 1 -	- - -	1 1 1	1 - 1	- 1 1	- - 1
1 1 1	1 1 -	1 - 1	1 - -	- 1 1	- 1 -	- - 1	- - -
- 1 1	1 1 1	- 1 -	1 1 -	- - 1	1 - 1	- - -	1 - -
- - 1	- 1 1	1 - 1	1 1 1	- - -	- 1 -	1 - -	1 1 -

Table 1: List of first rows and their negacyclic shifts, for length 3

If we examine the inner product of the first row with the second, third, and so on rows, we find that the ordered set of inner products are either:

$$\{+1, -1, -3, -1, +1\}, \text{ or } \{-3, +3, -3, +3, -3\}.$$

Hence we can group these matrices into two sets of *ip-equivalent* nega-cyclic matrices, according to their ordered set of inner products. We say there are two *ip-equivalence classes* for length 3. □

Observing the matrices in Example 1, we note that many matrices are simply a "shifted" version of other matrices. That is, cycling the bottom rows onto the top of the matrix, we can generate one matrix from another.

Lemma 4 *If A and B are nega-cyclic matrices of row length n sharing a common row, then B can be generated from A using nega-cyclic shifts on all rows of A.*

Proof. Firstly, we note that given a row of length n, after enough nega-cyclic shifts, it will repeat itself. (At most $2n$ shifts are required until a repeat occurs, but it can occur earlier). In other words, the sequence of rows produced by nega-cyclic shifts of a given row, is finite and fixed.

Let A and B be nega-cyclic matrices sharing a common row R. Let a_1 and b_1 be the first rows of A and B respectively. Since A and B have a common row R, R must be within the sequence of rows produced by both a_1 and b_1 through nega-cyclic shifts. Further

more, this implies that a_1 and b_1 are in the same sequence, and hence a_1 can be generated by b_1 and vice versa.

Finally, we note that nega-cyclic matrices remain nega-cyclic if we perform a nega-cyclic shift on every row of the matrix. Hence, we conclude that we can construct B from A, by performing nega-cyclic shifts on A until $a_1 = b_1$. The result is a nega-cyclic matrix with first row equal to the first row of B. □

Lemma 5 *If A and B are nega-cyclic matrices sharing a common row, then A and B have the same ordered set of inner products between the first and second row, first and third row, and so on.*

Proof. Proof follows from observing that given any two rows, if we perform a nega-cyclic shift on both rows, the dot product between the two rows is the same. Hence given matrices A and B which share a common row, perform nega-cyclic shifts on B until it is equal to A. Hence A must have the same ordered set of inner products as B. □

These two lemmas allow us to generate the sets of ip-equivalent matrices without having to examine each first row explicitly. Once one matrix is examined, we in fact discover a set of matrices which are ip-equivalent.

Example 2 As an illustration, observe the sets of matrices generated for a row of size three in Example 1. Notice how performing a nega-cyclic shift on all rows of the first matrix results in the fifth matrix being generated. Also notice how matrices 1, 2, 4, 5, 7, and 8 have the same inner product sequence, and 3 and 6 have the same inner product sequence. □

We note that if we treat $-$ as 0, each row has a unique binary number representation. Performing a nega-cyclic shift on the row, we observe that if the row is:

1. An odd row (where the rightmost element is a 1), it results in a division by two (rightshift) to that binary number.

2. An even row (where the rightmost element is a $-$), it results in a division by two, and an addition of 2^{n-1}, where n is the row length.

We also note that each nega-cyclic matrix has both odd and even rows. (Examine the generator: if it only contains 1, the next row will have a 0 upon a negacyclic shift, which will then travel rightwards until it is the rightmost element, and hence the matrix contains an even number, hence becoming even. The same idea applies for odd.)

Hence all local (and hence the global) minima occur on an even number, and all local (and hence global) maxima occur on an odd number. Since each nega-cyclic matrix contains both even and odd binary numbers we know that the minimum binary number (row) in each matrix is even. □

Summarizing, we have:

Lemma 6 *To search the space of all nega-cyclic* ± 1 *matrices we only need to consider those rows, which when the row is written in binary (by replacing* -1 *as* 0*) the binary number is even.*

Now,

Lemma 7 *There are* 4 *ip-equivalence classes for nega-cyclic* ± 1 *matrices of length* 5*. They have first rows listed in Table 2*

Binary ip-equivalent	First Row	Inner Product Sequence
0	- - - - -	{3, 1, -1, -3, -5, -3, -1, 1,3}
2	- - - 1 -	{-1, 1, -1, 1, -5, 1, -1, 1, -1}
4	- - 1 - -	{-1, -3, 3, 1, -5, 1, 3, -3, -1}
10	- 1 - 1 -	{-5, 5, -5, 5, -5, 5, -5, 5, -5}

Table 2: Lowest generators for rows of length 3

We know that if two matrices share a common row, then they share the same ordered set of dot products. However, the reverse is not true. This can be observed for matrices of row size 7.

Lemma 8 *There are* 9 *ip-equivalence classes for nega-cyclic* ± 1 *matrices of length* 7*. They have first rows listed in Table 3.*

Remark 2 In Lemma 8 note that two disjoint sets of nega-cyclic rows (identified by the least binary ip-equivalent numbers 4 and 6) share the same ordered set of inner products. □

Binary ip-equivalent	First Row	Inner Product Sequence
0	- - - - - - -	{5,3,1,-1,-3,-5,-7,-5,-3,-1,1,3,5}
2	- - - - - 1 -	{1,3,1,-1,-3,-1,-7,-1,-3,-1,1,3,1}
4 and 6	- - - - 1 - -	{1,-1,1,-1,1,-1,-7,-1,1,-1,1,-1,1}
	- - - - 1 1 -	{1,-1,1,-1,1,-1,-7,-1,1,-1,1,-1,1}
8	- - - 1 - - -	{1,-1,-3,3,1,-1,-7,-1,1,3,-3,-1,1}
10	- - - 1 - 1 -	{-3,3,-3,3,-3,3,-7,3,-3,3,-3,3,-3}
12	- - - 1 1 - -	{1,-5,-3,3,5,-1,-7,-1,5,3,-3,-5,1}
18	- - 1 - - 1 -	{-3,-1,5,-5,1,3,-7,3,1,-5,5,-1,-3}
20	- - 1 - 1 - -	{-3,-1,1,-1,1,3,-7,3,1,-1,1,-1,-3}
42	- 1 - 1 - 1 -	{-7}

Table 3: Lowest generators for rows of length 5

The motive behind grouping matrices according to their ordered set of dot products, is that it then makes it very easy for use in generating Hadamard Matrices using the construction of theorem 3. This results in a huge explosion of possible number of generated Hadamard matrices, as n increases.

4 Construction of Hadamard Matrices

Construction of Hadamard matrices using our variant in theorem 3 of the Goethals-Seidel array is simplified by grouping matrices according to their inner product of the first rows with the corresponding rows.

Let A, B, C, and D be four square nega-cyclic matrices. If the sum of the inner products of all distinct rows of A, B, C, and D is 0, then these matrices satisfy:

$$AA^T + BB^T + CC^T + DD^T = 4nI_n.$$

Because of our grouping of matrices according to their ordered set of dot products, we now have a efficient method of producing Hadamard matrices. That is, take one matrix from each ip-equivalence class of matrices A, B, C, and D, where the ordered set of dot products for A, B, C, and D satisfy the above condition. If a, b, c, and d are the number of matrices in the sets A, B, C, and D, then we have $a * b * c * d$ possible Hadamard matrices.

Example 3 For rows of length three, there are two ip-equivalence classes, which have lowest generators 0 $(---)$ and 2 $(-1-)$. These ip-equivalence classes have the inner product sequence {+1,-1,-3,-1,+1} and {-3,+3,-3,+3,-3} respectively. Because we are working with rows of length 3, it is only necessary to sum the first two elements of the inner product sequence. Upon observation, it is found that a combination of 3 matrices from the first class, and 1 matrix from the second class will satisfy Equation 1. Hence, we can use $(---, ---, ---,$ and $-1-)$ as the first rows of A, B, C, and D in order to generate a Hadamard matrix.

Example 4 As another example, consider nega-cyclic matrices of row size 5 given in Lemma 7. If we let A, B, C, and D be the nega-cyclic matrices identified by first rows (binary ip-equivalent) 0, 2, 2, and 4 respectively, then the ordered sum of the dot products for A, B, C, and D will equal 0, and hence A, B, C, and D will satisfy:

$$AA^T + BB^T + CC^T + DD^T = 4nI_n.$$

Because A, B, C, and D belong to ip-equivalence classes consisting of 10 matrices each, each matrix can be interchanged with an ip-equivalent matrix from it's ip-equivalence class. Hence, we have 10^4 possible Hadamard matrices which can be constructed using our variant, in Theorem 3 of the Goethals-Seidel construction. Further more, it is possible to permute the order of A, B, C, and D, producing even more matrices.

In a separate paper we will discuss how altering the orders of A, B, C, and D can give significantly different results in CDMA codes constructed using these methods. □

It turns out that this combination of matrices are the only ones which satisfy the above condition for size 5. However, for larger n, the number of possible matrices generated in this fashion grows rapidly.

For example, for nega-cyclic matrices of row size 7, there are not 1 but 6 combinations of numbers which satisfy the above condition. These are listed in Table 4.

The last entry in Table 4 especially notable, as the three sets which are repeated actually consist of two different generators which

Lowest Generators	Number of Matrices
{0, 8, 20, 20}	38416
{0, 10, 12, 18}	38416
{2, 2, 12, 20}	38416
{2, 4/6, 8, 20}	76832
{2, 8, 8, 18}	38416
{4/6, 4/6, 4/6, 10}	307328

Table 4: Ip-equivalence sets which satisfy modified GS condition

produce disjoint sets of rows, and hence the last entry produces an extremely large number of matrices.

This is to be investigated [5]with regard to the significance to in CDMA codes constructed using these methods.

5 Table of Results

Given below are some of the results obtained for various row lengths. These include the ip-equivalence classes of matrices, as well as the combinations of ip-equivalence classes can produce Hadamard Matrices using the Goethals-Seidel variant construction.

For rows of length 9, 23 ip-equivalence classes were found. These sets are listed in Table 5, identified by the lowest binary number which can generate the class. In cases where multiple binary numbers are generators for the ip-equivalence class, these are included as well. For example, 4 and 6 produce the same dot product sequence, but generate disjoint sets of rows. Hence both are noted in the same row.

Using the above table, a list of combinations of classes which satisfy Equation 1 was generated. This list can be found in Table 6

For rows of length 11, 63 ip-equivalence classes were found. In Table 7 the generators of these ip-equivalence classes are given. Where multiple generators produce disjoint sets of rows, one generator from each set is given. The combinations of classes found to satisfy Equation 1 were also calculated. There were found to be 240 combinations.

For larger row lengths, the number of sets of ip-equivalent matrices, as well as the combinations of sets which produce Hadamard matrices grows rapidly, and it becomes impractical to list them all here. However, we provide a summary of the results for larger row

Num	Generators	Dot product sequence
1	0	7 5 3 1 -1 -3 -5 -7 -9 -7 -5 -3 -1 1 3 5 7
2	2	3 5 3 1 -1 -3 -5 -3 -9 -3 -5 -3 -1 1 3 5 3
3	4 6	3 1 3 1 -1 -3 -1 -3 -9 -3 -1 -3 -1 1 3 1 3
4	8 14	3 1 -1 1 -1 1 -1 -3 -9 -3 -1 1 -1 1 -1 1 3
5	10	-1 5 -1 1 -1 1 -5 1 -9 1 -5 1 -1 1 -1 5 -1
6	12	3 -3 -1 1 -1 1 3 -3 -9 -3 3 1 -1 1 -1 -3 3
7	16	3 1 -1 -3 3 1 -1 -3 -9 -3 -1 1 3 -3 -1 1 3
8	18 22	-1 1 3 -3 3 -3 -1 1 -9 1 -1 -3 3 -3 3 1 -1
9	20 26	-1 1 -1 -3 3 1 -1 1 -9 1 -1 1 3 -3 -1 1 -1
10	24 28	3 -3 -5 -3 3 5 3 -3 -9 -3 3 5 3 -3 -5 -3 3
11	34	-1 1 -1 5 -5 1 -1 1 -9 1 -1 1 -5 5 -1 1 -1
12	36 54	-1 -3 3 1 -1 -3 3 1 -9 1 3 -3 -1 1 3 -3 -1
13	38	-1 -3 3 5 -5 -3 3 1 -9 1 3 -3 -5 5 3 -3 -1
14	40	-1 1 -5 1 -1 5 -1 1 -9 1 -1 5 -1 1 -5 1 -1
15	42	-5 5 -5 5 -5 5 -5 5 -9 5 -5 5 -5 5 -5 5 -5
16	44 50	-1 -3 -1 1 -1 1 3 1 -9 1 3 1 -1 1 -1 -3 -1
17	52	-1 -3 -1 -3 3 1 3 1 -9 1 3 1 3 -3 -1 -3 -1
18	56	3 -3 -9 -3 3 9 3 -3 -9 -3 3 9 3 -3 -9 -3 3
19	74	-5 1 3 -3 3 -3 -1 5 -9 5 -1 -3 3 -3 3 1 -5
20	76	-1 -7 3 5 -5 -3 7 1 -9 1 7 -3 -5 5 3 -7 -1
21	82	-5 1 3 -7 7 -3 -1 5 -9 5 -1 -3 7 -7 3 1 -5
22	84	-5 1 -1 1 -1 1 -1 5 -9 5 -1 1 -1 1 -1 1 -5
23	170	-9 9 -9 9 -9 9 -9 9 -9 9 -9 9 -9 9 -9 9 -9

Table 5: List of ip-equivalence classes for rows of length 9

lengths.

References

[1] A. W. Lam and S. Tantaratana. *Theory and applications of spread-spectrum systems.* IEEE/EAB Self-Study Course, IEEE Inc, Piscataway, 1994.

[2] V. I. Levenshtein. A new lower bound on aperiodic crosscorrelation of binary codes. *4th International Symp. On Communication Theory and Applications*, ISCTA '97:147–149, 1997.

[3] I. Oppermann and B. S. Vucetic. Complex spreading sequences with a wide range of correlation properties. *IEEE Trans. on Commun*, 45:365–375, 1997.

{1,16,17,22}	{2,6,17,22}	{2,9,16,16}	{2,10,12,22}	{2,11,17,17}
{2,12,14,17}	{2,13,18,19}	{3,4,17,22}	{3,5,16,17}	{3,6,9,22}
{3,6,14,19}	{3,7,16,22}	{3,8,14,16}	{3,9,11,17}	{3,9,12,14}
{3,10,11,19}	{4,4,16,19}	{4,5,12,17}	{4,6,8,22}	{4,6,11,21}
{4,7,12,22}	{4,8,11,17}	{4,8,12,14}	{4,9,9,13}	{5,6,6,19}
{5,6,8,16}	{5,6,9,12}	{5,7,9,20}	{5,7,12,16}	{5,7,13,17}
{5,8,10,13}	{6,7,11,19}	{6,8,9,11}	{7,7,13,22}	{7,8,11,16}
{7,8,13,14}	{7,9,11,12}			

Table 6: List of combinations of which satisfy Eqn 1 for length 9

{0 }	{2 }	{4 6 }	{8 14 }	{10 }
{12 }	{16 30 }	{18 22 }	{20 26 }	{24 28 }
{32 }	{34 46 }	{36 54 }	{38 }	{40 58 }
{42 }	{44 50 }	{48 60 }	{52 }	{56 }
{66 }	{68 110 }	{70 78 }	{72 118 }	{74 86 }
{76 102 }	{80 }	{82 90 }	{84 106 }	{88 114 }
{92 98 }	{100 108 }	{104 116 }	{112 }	{136 }
{138 }	{140 }	{146 182 }	{148 214 }	{150 }
{152 200 }	{154 166 }	{156 198 }	{162 }	{164 218 }
{168 }	{170 }	{172 202 }	{178 }	{180 210 }
{184 }	{204 }	{212 }	{216 }	{292 }
{298 }	{300 306 }	{308 }	{330 }	{332 }
{338 }	{340 }	{682 }		

Table 7: Sets of lowest unique first rows for ip-equivalence classes, row length 11

[4] B J Wysocki R Ang, J Seberry and T A Wysocki. Application of nega-cyclic matrices to generate spreading sequences. *International Symp. on Communication Theory and Applications*, ISCTA '2003, 2003.

[5] Jennifer Seberry Russell Ang and T. Wysocki. Application of nega-cyclic matrices to generate orthogonal speading sequences. *submitted*, pages –, 2003.

[6] J. S. Wallis. Hadamard matrices. In *Combinatorics: Room squares, sum-free sets and Hadamard matrices*, volume 292 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-Heidelberg-New York, 1972. Part IV of W. D. Wallis, Anne Penfold Street, and Jennifer Seberry Wallis.

Row length	Ip-equivalence classes	Num. Combinations
9	23	37
11	63	240
13	187	2963
15	572	46811
17	1964	> 300000

Table 8: Summary of results for larger row lengths

[7] Jennifer Seberry Wallis and A. L. Whiteman. Some classes of Hadamard matrices with constant diagonal. *Bull. Austral. Math. Soc.*, 7:233–249, 1972.

[8] L. R. Welch. Lower bounds on the maximum cross-correlation of signals. *IEEE Trans. Inform. Theory*, 20:397–399, 1974.