axioms

MDPI

Article

On the Existence of Optimal $(k(k-1)s+2,k,1)$ Binary Cyclically Permutable Constant Weight Codes

Tsonka Baicheva [1,2,*], Tsvetyana Yoveva [1] and Svetlana Topalova [1]

[1] Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria; ts.yoveva@pmgkn.com (T.Y.); svetlana@math.bas.bg (S.T.)
[2] Centre of Excellence in Informatics and Information and Communication Technologies, 1113 Sofia, Bulgaria
* Correspondence: tsonka@math.bas.bg

Abstract

We derive necessary conditions for the existence of optimal $(k(k-1)s+2,k,1)$ binary cyclically permutable constant weight codes with length divisible by 2^n, where $n \geq 2$. This is achieved by counting in different ways the pairs of points in the corresponding partial cyclic design whose incidence matrix is equivalent to a matrix containing circulants of order $\frac{v}{2^m}$ for $0 \leq m < n$. Using a computer we check if these conditions hold for $3 \leq k \leq 200$ and $1 \leq s \leq 10$. We generalize the computer results by proving analytically that optimal $(3k(k-1)+2,k,1)$ binary cyclically permutable constant weight codes do not exist for $k = 16u+6$.

Keywords: coding theory; binary cyclically permutable constant weight code; optical orthogonal code; cyclic design

MSC: 94B60; 05B05; 05B30

1. Introduction

1.1. The Content of the Paper

Necessary conditions for the existence of $(v,k,1)$ binary cyclically permutable constant weight (CPCW) codes with even v are presented in the paper of Buratti and Stinson [1], namely in Theorem 4.3, which is proved by counting even and odd differences in such codes. Using this theorem the nonexistence of several infinite families of optimal CPCW codes is established in [1], Section 4. The nonexistence of an optimal $(92,6,1)$ CPCW code does not follow from these results. In our recent paper on $(v,5,1)$ and $(v,6,1)$ binary cyclically permutable constant weight (CPCW) codes [2] it is proved that a $(92,6,1)$ CPCW code does not exist. The proof is based on some necessary conditions for the existence of such a code which we obtain by counting in different ways the pairs of points in the corresponding partial cyclic design. In the present paper in Theorem 2 we generalize these necessary conditions for optimal $(k(k-1)s+2,k,1)$ CPCW codes with length divisible by 2^n, where $n \geq 2$; namely we derive a system of linear equations which has at least one solution if a code with the chosen parameters exists. For each $0 \leq m < n$ this linear system contains equations reflecting the divisibility of v by 2^m. For $m > 0$ these equations depend on the solutions of the equations for $m-1$.

Our method for deriving these necessary conditions is different from the one used in [1], but for $(k(k-1)s+2,k,1)$ CPCW codes the requirements of [1], Theorem 4.3, can be presented by the equations of Theorem 2 for $m = 0$ (divisibility by 2). The here-proved

Check for updates

Academic Editor: Hashem Bordbar

Received: 24 July 2026
Revised: 3 September 2026
Accepted: 9 September 2026
Published: 11 September 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

Theorem 2 adds new restrictions for the cases when the code length v is not only even, but also divisible by a higher power of 2.

By a computer search we check if Theorem 2 holds for some small values of k and s, namely for $k = 3, 4, \ldots, 200$, and $s = 1, 2, \ldots, 10$. We establish that for this parameter range in most of the cases in which the necessary conditions do not hold there is no solution of the equations for $m = 0$, and therefore, these nonexistence results follow from the considerations in [1]. There is, however, a series of optimal $(3k(k-1)+2, k, 1)$ CPCW codes with $k = 6 + 16u$ whose nonexistence does not follow from the necessary conditions for even v considered in [1]. In these cases there exist solutions of the equations for $m = 0$, but there are no solutions of the equations for $m = 1$. By a computer search we establish this for small k. Then we prove the nonexistence of the infinite family of optimal CPCW codes with these parameters.

1.2. Definitions and Notations

Since we want to use some of the assertions that are proven in [2], we will only repeat very briefly the definitions given there. Readers who are not familiar with the subject can find more explanations and examples in [2]. Almost all notations we use are the same as in [2].

A $(v, k, 1)$ *binary cyclically permutable constant weight* (CPCW) code of size s can be defined as a collection $\mathcal{C} = \{C_1, \ldots, C_s\}$ of k-subsets of $\mathbb{Z}_v$ (codewords), such that any two distinct translates of a codeword share at most one element, and any two translates of two distinct codewords also share at most one element:

$$|C_i \cap (C_i + t)| \leq 1, \ \ 1 \leq i \leq s, \ \ 1 \leq t \leq v-1 \tag{1}$$

$$|C_i \cap (C_j + t)| \leq 1, \ \ 1 \leq i < j \leq s, \ \ 0 \leq t \leq v-1 \tag{2}$$

Condition (1) is called the auto-correlation property and (2) the cross-correlation property. The number of the codewords (the *size*) of $\mathcal{C}$, is denoted by s.

Consider a codeword $C = \{c_0, c_1, \ldots, c_{k-1}\}$. Denote by $\triangle C = \{c_i - c_j |\ i, j = 0, 1, \ldots, k-1; i \neq j\}$ the multiset of differences of C. The auto-correlation property means that all the differences of a codeword of a $(v, k, 1)$ CPCW code are different, and the cross-correlation property means that $\triangle C_1 \bigcap \triangle C_2 = \emptyset$ for two codewords C_1 and C_2. Since $|\triangle C| = k(k-1)$, the size of a $(v, k, 1)$ CPCW code cannot exceed

$$\left\lfloor \frac{v-1}{k(k-1)} \right\rfloor.$$

CPCW codes which reach this bound are called *optimal* [3,4]. If the code size is exactly $(v-1)/k(k-1)$, the optimal $(v, k, 1)$ CPCW code is *perfect*; that is, all nonzero differences are covered. In that case $v = k(k-1)s + 1$, while the case we consider is $v = k(k-1)s + 2$, namely, codes which are very near to perfection as they do not cover only one difference.

A $(v, k, 1)$ CPCW code is equivalent to a $(v, k, 1)$ optical orthogonal code (OOC) [3,5] and the application in optical communication systems is one of the main reasons for the great interest in these codes [3]. All the results for $(v, k, 1)$ CPCW codes which are obtained in the present paper hold for $(v, k, 1)$ OOCs too.

CPCW codes are related to other combinatorial structures too. Optimal $(v, k, 1)$ CPCW codes correspond to $(v, k; \lfloor (v-1)/k(k-1) \rfloor)$ difference packings, and perfect $(v, k, 1)$ CPCW codes are equivalent to $(v, k, 1)$ cyclic difference families. More information on these relations can be found in [1,6]. Here we consider in detail the equivalence of CPCW codes to partial cyclic designs, because it is used to prove the theorems in Section 3.

Let $V = \{P_i\}_{i=1}^{v}$ be a finite set of *points*, and $\mathcal{B} = \{B_j\}_{j=1}^{b}$ a finite collection of k-element subsets of V, called *blocks*. $D = (V, \mathcal{B})$ is a *design (partial design)* with parameters 2-(v,k,1) if any 2-subset of V is contained in exactly (at most) one block of $\mathcal{B}$. A 2-(v,k,1) design is equivalent to a Steiner system $S(2, k, v)$. Partial designs are sometimes called *packings* or *packing designs* [7–9].

An *automorphism* of a partial 2-$(v, k, 1)$ design is a permutation of its points which preserves the collection of its blocks. A 2-(v,k,1) design (partial design) is *cyclic* if it is invariant under a cyclic automorphism group of order v, and it is *strictly cyclic* if each block orbit under this group is of length v (no short orbits). A cyclic partial design with the maximum possible number of blocks is *optimal*.

A circulant matrix (circulant) of order v is a (0,1) square matrix $M = (m_{i,j})_{v \times v}$ with v rows and v columns, such that $m_{i+1,j+1} = m_{i,j}$, where $i, j \in \mathbb{Z}_v$.

Perfect $(v, k, 1)$ CPCW codes are equivalent to strictly cyclic 2-$(v, k, 1)$ designs. Optimal $(v, k, 1)$ CPCW codes are equivalent to optimal 2-$(v, k, 1)$ strictly cyclic partial designs.

1.3. Known Results and the Contribution of the Present Paper

Optimal $(v, k, 1)$ CPCW codes and the combinatorial structures corresponding to them are widely studied. Presently the existence problem has been completely solved only for $(v, 3, 1)$ and $(v, 4, 1)$ CPCW codes. It was proven in [10] that an optimal $(v, 3, 1)$ CPCW code exists for all v except for $v = 6t + 2$ and $t \equiv 2$ or 3 $\pmod 4$. Direct constructions with explicit codewords are presented in [11] to show the existence of an optimal $(v, 4, 1)$ CPCW code (OOC) for any positive integer $v \neq 25$. For optimal $(v, k, 1)$ CPCW codes with $k \geq 5$ there are many different constructions [6,8,12–25], and many nonexistence results are presented in [1]. A summary about $(v, 5, 1)$ and $(v, 6, 1)$ CPCW codes is given in [2].

Computer-aided classification results are known too [26–30]. They are only for relatively small parameters, but they often reveal important properties of these objects. It can be seen from them that a great deal of the cases in which no optimal codes exist are for $v = k(k-1)s + 2$. On the other hand, CPCW codes with these parameters are of particular importance because they are very close to the perfect codes since they do not cover only one difference, while perfect codes cover all differences. This motivated us to consider such codes in [2] and in the present paper.

The nonexistence of several infinite families of optimal $(k(k-1)s + 2, k, 1)$ CPCW codes has been proven in [1] as a consequence of Theorem 4.3 [1].

Namely, by [1], Theorem 4.6, there do not exist optimal $(k(k-1)s + 2, k, 1)$ CPCW codes if

- $k = 8u + 3$ and $s = 4w + 3$;
- $k = 8u + 3$ and $s = 4w + 2$;
- $k = 8u + 5$ and $s = 2w + 1$;
- $k = 8u + 7$ and $s = 4w + 1$;
- $k = 8u + 7$ and $s = 4w + 2$.

By [1], Theorem 4.12, there are infinitely many even integers k such that an optimal $(2k(k-1) + 2, k, 1)$ CPCW code does not exist.

By [1], Theorem 4.13, optimal $(3k(k-1) + 2, k, 1)$ CPCW codes do not exist if

- $k = (4^{a+1}(24c + 7) + 2)/3$ with $a, c \geq 0$, or
- $k = 4^{a+1}(8c + 5)$ with $a, c \geq 0$.

This theorem considers $s = 3$ and is therefore most closely connected to the nonexistence results in Sections 4 and 5.

In the present paper we use the approach from [2] to obtain new existence requirements for $(k(k-1)s+2, k, 1)$ CPCW codes, and corresponding nonexistence results which do not follow from the considerations in [1].

1.4. Structure of the Present Paper

The present paper consists of six sections. Section 2 presents the main ideas of the method for obtaining the existence requirements in [2], and Section 3 deals with deriving necessary conditions for the existence of $(v, k, 1)$ CPCW codes with $v = sk(k-1)+2$ if v is divisible by 2^n, where $n \geq 2$. This leads to Theorem 2, which is the first theoretical contribution in the present paper. Its requirements are implemented in our software, which checks if they hold for definite s and k. The principal way in which this software works and the obtained computer-aided nonexistence results are described in Section 4. The proof of the nonexistence of optimal $(v, k, 1)$ CPCW codes with $v = 3k(k-1)+2$ and $k = 16u+6$ is the subject of Section 5, where Proposition 1 is the second main contribution in the paper. Finally, Section 6 contains some general remarks and open problems.

2. Optimal $(v, k, 1)$ CPCW Codes with $v = sk(k-1)+2$

We shall briefly describe the most important properties of these codes and the way in which existence requirements are formulated in [2], where more details and proofs can be found. A similar approach and the presented examples are used in the next section, in which additional necessary conditions for the existence of such codes are formulated in the case when v is divisible by 4 or higher powers of 2. The example in Figure 1 illustrates the method by which the existence conditions are obtained. It presents the smallest example of a $(k(k-1)s+2, k, 1)$ CPCW code with v divisible by 2^n, where $n > 1$.

A strictly cyclic 2-$(v, k, 1)$ partial design corresponding to a $(v, k, 1)$ CPCW code of size s has an incidence matrix of v rows (corresponding to its v points) and $b = sv$ columns (corresponding to its sv blocks). This incidence matrix contains s submatrices which are circulant matrices of order v. The v columns of each such circulant matrix correspond to the translates of one of the codewords of the optimal $(v, k, 1)$ CPCW code. This is illustrated in Figure 1a,b.

The set of differences of the codewords of an optimal CPCW code of length $k(k-1)s+2$ does not contain the difference $v/2$, and contains all the other possible differences. For example, the set of differences of the optimal $(8, 3, 1)$ CPCW code from Figure 1a contains all possible differences, but not the difference 4. For the corresponding optimal partial cyclic 2-$(k(k-1)s+2, k, 1)$ design this means that the $\frac{v}{2}$ pairs of points $\{a, a+\frac{v}{2}\}$ are not contained in its blocks, while each of the remaining $\frac{v(v-2)}{2}$ pairs of points is in exactly one block of this partial design.

Denote the rows/columns of a circulant M of an even order v by the numbers $0, 1, 2, \ldots v-1 \in \mathbb{Z}_v$, and let ϕ_v be a pair (φ, ψ) of two permutations of the rows and columns of M respectively, where φ and ψ permute row (column) b as $b \to 2b$ if $b < \frac{v}{2}$ and $b \to 2b+1$ if $b \geq \frac{v}{2}$. After applying ϕ_v the rows/columns follow each other as $0, 2, 4 \ldots v-2, 1, 3, 5, \ldots v-1$. Our further considerations substantially use the fact that the application of ϕ_v to M results in a matrix made of 4 circulants of order $\frac{v}{2}$ [2]. We can apply ϕ_v to all the s circulants of order v of the incidence matrix of an optimal partial cyclic 2-$(k(k-1)s+2, k, 1)$ design (Figure 1c).

Consider the two rows of $2s$ circulants of order $\frac{v}{2}$ of the permuted by ϕ_v incidence matrix of the partial cyclic 2-$(k(k-1)s+2, k, 1)$ design. If $\frac{v}{2}$ is even the two points of the pair $(a, a+\frac{v}{2})$ are either both odd, or both even. If $\frac{v}{2}$ is odd one of the two points of the pair $(a, a+\frac{v}{2})$ is odd, and the other even. The even points are in the first row of circulants, and the odd ones in the second. That is why if $\frac{v}{2}$ is even both points of the pair $(a, a+\frac{v}{2})$ are in

the same circulant (of order $\frac{v}{2}$) row, and if $\frac{v}{2}$ is odd the two points of the pair $(a, a+\frac{v}{2})$ are in different circulant rows.

(**a**) Optimal (8,3,1) CPCW code has one codeword

$\mathcal{C}$	$\triangle C$
{0, 1, 3}	{1, 2, 3, 5, 6, 7}

Uncovered difference: 4

(**b**) Related optimal partial cyclic 2-(8,3,1) design

	01234567
0	**1**0000**1**0**1**
1	**1**1000**1**0
2	0**1**100000**1**
3	**1**0**11**0000
4	0**1**0**11**000
5	00**1**0**11**00
6	000**1**0**11**0
7	0000**1**0**11**

Number of ones in a row/column of the circulant of order 8: 3

(**c**) All even rows/columns of the upper circulant precede the odd rows/columns

	0246	1357
0	**1**000	00**11**
2	0**1**00	**1**00**1**
4	00**1**0	**11**00
6	000**1**	0**11**0
1	**1**00**1**	**1**000
3	**11**00	0**1**00
5	0**11**0	00**1**0
7	00**11**	000**1**

Number of ones in a row/column of the circulants of order 4

$$\begin{matrix} 1\,2 \\ 2\,1 \end{matrix} \longrightarrow A_{3,1} \qquad \begin{matrix} a_{3,0}=0, \\ a_{3,1}=1 \end{matrix}$$

(**d**) All even rows/columns of the upper circulants precede the odd rows/columns

	04	26	15	37
0	**1**0	00	0**1**	0**1**
4	0**1**	00	**1**0	**1**0
2	00	**1**0	**1**0	0**1**
6	00	0**1**	0**1**	**1**0
1	**1**0	0**1**	**1**0	00
5	0**1**	**1**0	0**1**	00
3	**1**0	**1**0	00	**1**0
7	0**1**	0**1**	00	0**1**

Number of ones in a row/column of the circulants of order 2

$$\begin{matrix} 1\,0 & 1\,1 \\ 0\,1 & 1\,1 \end{matrix} \longrightarrow A'_{1,0}\ A'_{2,1} \qquad \begin{matrix} a'_{2,1}=1, \\ a'_{1,0}=1 \end{matrix}$$

$$\begin{matrix} 1\,1 & 1\,0 \\ 1\,1 & 0\,1 \end{matrix}$$

Figure 1. Optimal partial cyclic 2-(8,3,1) design.

Consider a circulant matrix M of order v which has i ones in a row/column, and is transformed by ϕ_v to the 4 circulants C, D, E, and F of order $\frac{v}{2}$, namely $\phi_v M = \begin{pmatrix} C & D \\ E & F \end{pmatrix}$. The *weight matrix* of M is an integer square matrix of dimension 2×2, the elements of which are the number of ones c, d, e and f in a row/column of C, D, E, and F respectively. Note that $c = f$, and $d = e$. We further denote the weight matrix $\begin{pmatrix} j & i-j \\ i-j & j \end{pmatrix}$ by $A_{i,j}$, where $j \leq \frac{i}{2}$. The matrices $A_{i,j}$ for $i = 3, 4$ and 5 follow.

Example 1. *$A_{i,j}$ for $i = 3, 4$ and 5*

$A_{3,0}$	$A_{3,1}$
0 3	1 2
3 0	2 1

$A_{4,0}$	$A_{4,1}$	$A_{4,2}$
0 4	1 3	2 2
4 0	3 1	2 2

$A_{5,0}$	$A_{5,1}$	$A_{5,2}$
0 5	1 4	2 3
5 0	4 1	3 2

Consider the s circulants of order v in the incidence matrix of an optimal partial cyclic 2-$(k(k-1)s+2, k, 1)$ design. We denote by $a_{i,j}$ the number of circulants with weight

matrices $A_{i,j}$. In Figure 1c $s = 1$ and the weight matrix of the circulant is $A_{3,1}$. That is why $a_{3,1} = 1$ and $a_{3,0} = 0$.

The necessary conditions which we use further are obtained by counting in different ways the pairs of points in which the two points are from different rows of circulants of order $\frac{v}{2}$. A circulant of order v with weight matrix $A_{k,j}$ adds $j(k-j)v$ such pairs of points. On the other hand the whole number of these pairs is $\frac{v^2}{4}$ if $\frac{v}{2}$ is even, and $\frac{v^2}{4} - \frac{v}{2}$ if $\frac{v}{2}$ is odd, because in that case the non-covered $\frac{v}{2}$ pairs are among them. Therefore we obtain that $\sum_{j=1}^{\lfloor \frac{k}{2} \rfloor} j(k-j)a_{k,j} = \frac{v-2}{4}$ if $\frac{v}{2}$ is odd, and $\sum_{j=1}^{\lfloor \frac{k}{2} \rfloor} j(k-j)a_{k,j} = \frac{v}{4}$ if $\frac{v}{2}$ is even. Taking into account that there are s circulants of order k, $\lfloor \frac{v}{4} \rfloor = \frac{v}{4}$ if $\frac{v}{2}$ is even, and if $\frac{v}{2}$ is odd $\lfloor \frac{v}{4} \rfloor = \lfloor \frac{\frac{v}{2}}{2} \rfloor = \frac{\frac{v}{2}-1}{2} = \frac{v-2}{4}$, we obtain

$$\sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} a_{k,j} = s \tag{3}$$

$$\sum_{j=1}^{\lfloor \frac{k}{2} \rfloor} j(k-j)a_{k,j} = \left\lfloor \frac{v}{4} \right\rfloor \tag{4}$$

This result was derived in [2], Theorems 1 and 2, by the above illustrated approach. It did not directly lead to new nonexistence results, however, because it turns out that Equations (3) and (4) can be derived from Theorem 4.3 of [1]. That is why additional restrictions were used in [2] to prove the nonexistence of an optimal $(92, 6, 1)$ CPCW code. In the next section we generalize them in order to consider codes with v divisible by 2^n, where $n \geq 2$.

3. Optimal $(v, k, 1)$ CPCW Codes with $v = k(k-1)s + 2$ and v Divisible by 2^n, Where $n \geq 2$

If v is divisible by 4, after ϕ_v we can apply the permutation $\phi_{\frac{v}{2}}$ on the circulants of order $\frac{v}{2}$, and this way a matrix made of 4 rows of circulants of order $\frac{v}{4}$ will be obtained. An example is presented in Figure 1d. We denote by $A'_{i,j}$ the weight matrices of circulants of order $\frac{v}{2}$.

Consider the first row of circulants of order $\frac{v}{2}$, which was formed by the application of ϕ_v (the second row is isomorphic to it, so we do not deal with it). We denote by $a'_{i,j}$ the number of circulants of order $\frac{v}{2}$ with weight matrices $A'_{i,j}$.

You can see from Figure 1d that the weight matrices of the first row of circulants of order 4 (Figure 1c) are $A'_{1,0}$ and $A'_{2,1}$, and respectively $a'_{1,0} = 1$ and $a'_{2,1} = 1$.

Theorem 1. *For an optimal $(v, k, 1)$ CPCW code with $v = sk(k-1) + 2$ and v divisible by 4 the following equations hold:*

$$\sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} a_{k,j} = s \tag{5}$$

$$\sum_{j=1}^{\lfloor \frac{k}{2} \rfloor} j(k-j)a_{k,j} = \frac{v}{4} \tag{6}$$

$$\sum_{j=0}^{\lfloor \frac{i}{2} \rfloor} a'_{i,j} = \begin{cases} a_{k,i} & \text{if } i < \left\lfloor \frac{k}{2} \right\rfloor \\ a_{k,k-i} & \text{if } i > \left\lfloor \frac{k}{2} \right\rfloor \\ 2a_{k,\frac{k}{2}} & \text{if } k \text{ is even and } i = \frac{k}{2} \end{cases} \tag{7}$$

$$\sum_{i=2}^{k} \sum_{j=1}^{\lfloor \frac{i}{2} \rfloor} j(i-j)a'_{i,j} = \left\lfloor \frac{v}{8} \right\rfloor \tag{8}$$

Proof. The first two equations are Equations (3) and (4) from the previous section. They follow from [1], Theorem 4.3, or from [2], Theorem 2.

Let there be at least one solution of the system of linear equations, Equations (5) and (6). By such a solution we know the values of $a_{k,j}$ for $j = 0, 1, \ldots, \left\lfloor \frac{k}{2} \right\rfloor$. According to one of the solutions the first row of circulants of order $\frac{v}{2}$ obtained by ϕ_v contains $a_{k,i}$ circulants with i ones in a row/column, and $a_{k,i}$ circulants with $k-i$ ones in a row/column, $i = 0, 1, \ldots, \left\lfloor \frac{k}{2} \right\rfloor$. That is why if $i < \left\lfloor \frac{k}{2} \right\rfloor$ the number of circulants of order $\frac{v}{2}$ with i ones in a row/column is $a_{k,i}$ (the first equation in (7)), and if $i > \left\lfloor \frac{k}{2} \right\rfloor$, it is $a_{k,k-i}$ (the second equation in (7)). If k is even and $i = \frac{k}{2}$, then $k - i = \frac{k}{2}$ too and the third equation in (7) follows.

This is illustrated in Figure 1c where $a_{3,0} = 0$ and $a_{3,1} = 1$, and the first row of circulants of order $\frac{v}{2}$ has one circulant with 1 one in a row/column, and one circulant with 2 ones in a row/column. That is why it must hold that $a'_{2,0} + a'_{2,1} = 1$ and $a'_{1,0} = 1$.

Consider the first row of circulants of order $\frac{v}{2}$. It contains the points of the partial cyclic design with numbers divisible by 2. When $\phi_{\frac{v}{2}}$ is applied, it is transformed into two rows of circulants of order $\frac{v}{4}$. The first of these rows contains points with numbers divisible by 4, and the second points with even numbers not divisible by 4. That is why if $\frac{v}{2}$ is divisible by 4, the pairs of points $(a, a + \frac{v}{2})$ are in the same row of circulants of order $\frac{v}{4}$, and if $\frac{v}{2}$ is not divisible by 4, the points a and $a + \frac{v}{2}$ are in different rows of circulants of order $\frac{v}{4}$.

Let us now count in different ways the pairs of points in which the two points are from different rows of circulants of order $\frac{v}{4}$. A circulant of order $\frac{v}{2}$ with weight matrix $A_{i,j}$ adds $j(i-j)\frac{v}{2}$ such pairs of points. The whole number of these pairs is $\frac{v^2}{16}$ if $\frac{v}{4}$ is even, and $\frac{v^2}{16} - \frac{v}{4}$ if $\frac{v}{4}$ is odd, because in that case the non-covered $\frac{v}{4}$ pairs are among them. This way Equation (8) is obtained. □

We next generalize this result in order to consider codes with v divisible by 2^n, where $n \geq 2$. If v is divisible by $2^n > 4$ after ϕ_v on the circulants of order v and $\phi_{\frac{v}{2}}$ on the circulants of order $\frac{v}{2}$, we can go on applying $\phi_{\frac{v}{4}}$ on the circulants of order $\frac{v}{4}$, then $\phi_{\frac{v}{8}}$ on the circulants of order $\frac{v}{8}, \ldots,$ and finally $\phi_{\frac{v}{2^{n-1}}}$ on the circulants of order $\frac{v}{2^{n-1}}$.

In this case we will use more complex notations. We denote by $A_{m,i,j}$ the weight matrix $\begin{pmatrix} j & i-j \\ i-j & j \end{pmatrix}$ of a circulant of order $\frac{v}{2^m}$. When we consider a row of circulants of order $\frac{v}{2^m}$ we denote by $a_{m,i,j}$ the number of circulants with weight matrices $A_{m,i,j}$ in the row. Then the next theorem follows.

Theorem 2. *The following equations hold for an optimal $(v, k, 1)$ CPCW code with $v = k(k-1)s + 2$ and v divisible by 2^n:*

$$\sum_{j=0}^{\left\lfloor \frac{k}{2} \right\rfloor} a_{0,k,j} = s, \qquad a_{0,i,j} = 0 \ \ for \ \ i \neq k \tag{9}$$

$$\sum_{j=0}^{\left\lfloor \frac{i}{2} \right\rfloor} a_{m,i,j} = \begin{cases} \sum_{h=2i}^{k} a_{m-1,h,i} + \sum_{h=i}^{2i} a_{m-1,h,h-i} & if \ \ i \leq \left\lfloor \frac{k}{2} \right\rfloor \\ \sum_{h=i}^{2i} a_{m-1,h,h-i} & if \ \ i > \left\lfloor \frac{k}{2} \right\rfloor \end{cases} \quad \begin{matrix} i = 1, 2, \ldots, k \\ m = 1, 2, \ldots, n-1 \end{matrix} \tag{10}$$

$$\sum_{i=2}^{k} \sum_{j=1}^{\left\lfloor \frac{i}{2} \right\rfloor} j(i-j) a_{m,i,j} = \left\lfloor \frac{v}{2^{m+2}} \right\rfloor, \quad m = 0, 1, \ldots, n-1 \quad if \quad 2^{m+2} \leq v \tag{11}$$

Proof. The incidence matrix of the considered partial cyclic design consists of s circulants of order v with k ones in a row/column. This fact is presented by Equation (9).

Consider $m \geq 1$. It does not make sense to consider solutions for $a_{m,i,j}$ if there are no solutions for $a_{m-1,i,j}$. If there are solutions for $a_{m-1,i,j}$, then each solution for $a_{m,i,j}$ depends on one of the solutions for $a_{m-1,i,j}$, because from the solutions for $a_{m-1,i,j}$ we know the number of ones in the circulants from one row of circulants of order $\frac{v}{2^m}$, namely the application of $\phi_{\frac{v}{2^{m-1}}}$ to the circulants of order $\frac{v}{2^{m-1}}$ which have h ones in a row/column leads to $a_{m-1,h,i}$ circulants of order $\frac{v}{2^m}$ with i ones in a row/column, and $a_{m-1,h,i}$ circulants of order $\frac{v}{2^m}$ with $h-i$ ones in a row/column, $i \leq \frac{h}{2}$. The number h of the ones in a row/column might be different for the different circulants of order $\frac{v}{2^{m-1}}$ from which circulants of order $\frac{v}{2^m}$ with i ones in a row/column are obtained by $\phi_{\frac{v}{2^{m-1}}}$. That is why we need a sum over all possible h. There are two cases. By definition, $i \leq \frac{h}{2}$ for $a_{m-1,h,i}$ and therefore $a_{m-1,h,i}$ should not be considered if $i > \frac{k}{2}$. We obtain that $\sum_{j=0}^{\lfloor \frac{i}{2} \rfloor} a_{m,i,j} = \sum_{h=i}^{2i} a_{m-1,h,h-i}$ (Equation (10) for $i > \frac{k}{2}$), where the range of values of h follows from the requirement that $0 \leq h-i \leq \frac{h}{2}$. For $i \leq \frac{k}{2}$ both $a_{m-1,h,i}$ and $a_{m-1,h,h-i}$ have to be considered because both $i \leq \frac{h}{2}$ and $i > \frac{h}{2}$ are possible. If $i = \frac{h}{2}$ then $h-i = \frac{h}{2}$ too. That is why $h = 2i$ is included in the range of values of h for both sums in the right part of Equation (10) for $i \leq \frac{h}{2}$.

Equation (11) refers to the requirements for the first row of circulants of order $\frac{v}{2^m}$. It contains the points of the partial cyclic design with numbers divisible by 2^{m+1}. When $\phi_{\frac{v}{2^m}}$ is applied, it is transformed into two rows of circulants of order $\frac{v}{2^{m+1}}$. The first of these rows contains points with numbers divisible by 2^{m+1}, and the second points with even numbers not divisible by 2^{m+1}. That is why if $\frac{v}{2}$ is divisible by 2^{m+1}, the pairs of points $(a, a+\frac{v}{2})$ are in the same row of circulants of order $\frac{v}{2^{m+1}}$, and if $\frac{v}{2}$ is not divisible by 2^{m+1}, the points a and $a+\frac{v}{2}$ are in different rows of circulants of order $\frac{v}{2^{m+1}}$. Note that the latter might only happen when $m = n-1$. If $m < n-1$ there are exactly $\frac{v}{2^{m+2}}$ missing pairs of points in a row of circulants of order $\frac{v}{2^{m+1}}$.

We count the pairs of points from different rows of circulants of order $\frac{v}{2^{m+1}}$. A circulant of order $\frac{v}{2^m}$ with weight matrix $A_{m,i,j}$ adds $j(i-j)\frac{v}{2^m}$ such pairs of points. The whole number of these pairs is $\frac{v^2}{2^{2(m+1)}}$ if $\frac{v}{2^{m+1}}$ is even, and $\frac{v^2}{2^{2(m+1)}} - \frac{v}{2^{m+1}}$ if $\frac{v}{2^{m+1}}$ is odd, because in that case the non-covered $\frac{v}{2^{m+1}}$ pairs are among them. This way Equation (11) is obtained. The requirement $2^{m+2} \leq v$ comes from the right side of this equation and affects only cases in which $m = n-1$ is not considered because $v = 2^n$. In that case if $m = n-2$ we consider two rows of circulants of order $\frac{v}{2^{m+1}} = \frac{2^n}{2^{n-1}} = 2$. The application of ϕ_2 to a circulant of order 2 preserves the circulant and does not lead to additional requirements. That is why $m = n-1$ is not possible. If $v = 2^n g$, then $m = n-1$ is possible, because the application of ϕ_{2g} to a circulant of order $2g$ results in rows of circulants of order g. An example for $v = 32$ is presented in the next section. □

The power of Theorem 2 comes from the fact that by Equation (10) the restrictions for $a_{m+1,i,j}$ depend on the solution for $a_{m,i,j}$.

4. Computer-Aided Results

To see if the requirements of Theorem 2 hold for definite parameters s and k we first have to find a solution for $a_{0,k,j}$, and then for $a_{1,i,j}$, $a_{2,i,j}$, etc. We do this using our own software written in $C++$ which checks if the theorem holds for optimal $(sk(k-1)+2, k, 1)$ CPCW codes with relatively small parameters. The recursive function `bool TotalSolution(int v, int m, int A[k+1])` is an important part of this software. Its work is briefly illustrated in Figure 2.

The function `TotalSolution` has three parameters: v is the order of the circulants, m is as formulated in Theorem 2, and A is an integer array such that $A[i]$ is the number of circulants of order $\frac{v}{2^m}$ with i ones in a row/column. Using these parameters and Theorem 2, the program constructs the equations for $a_{m,i,j}$, and calls the function `NextSolution` to look

for integer solutions of this system of linear equations. Successive calls to `NextSolution(m)` will save the next found solution in an array, or it will return false if there are no more solutions. If there are no more solutions `TotalSolution` returns false. Otherwise if $2^{m+3} \leq v$, `TotalSolution(v, m+1, B)` is recursively called with each solution for $a_{m,i,j}$ and its corresponding array B, and if it returns true, the requirements of Theorem 2 hold. If $2^{m+3} > v$ or $\frac{v}{2^m}$ is odd, the requirement (11) (Theorem 2) does not hold for $m+1$ and `TotalSolution` returns `true` instead of calling `TotalSolution(v, m+1, B)`.

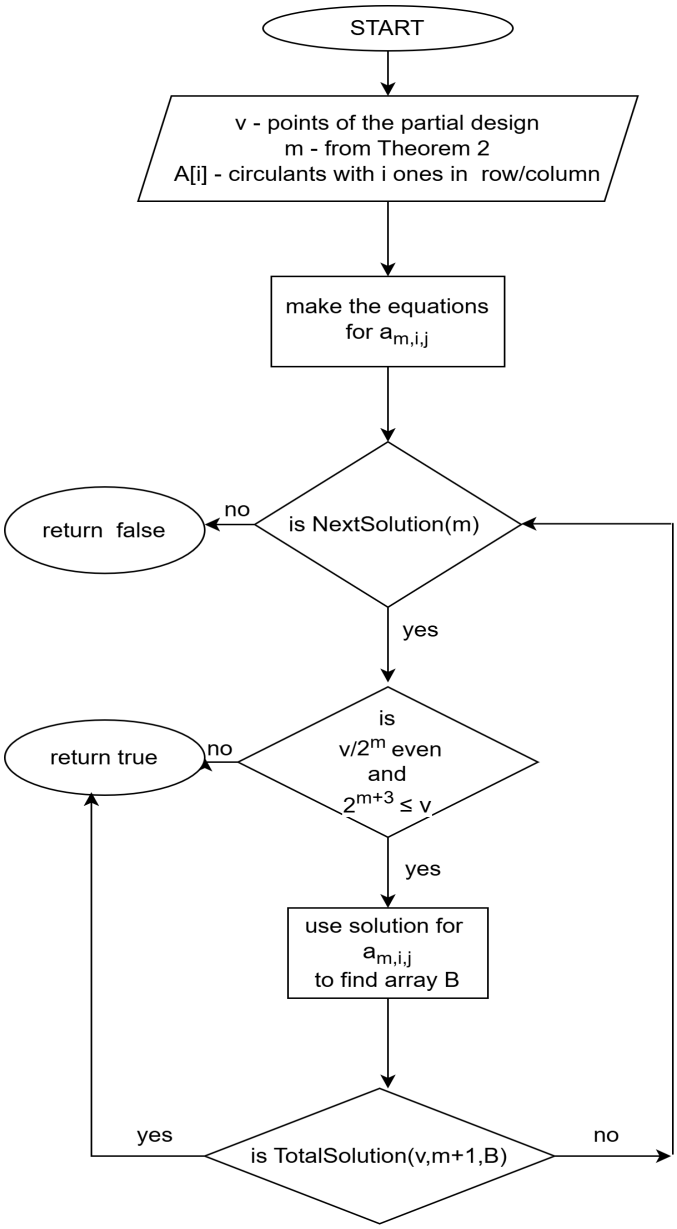


Figure 2. The function `bool TotalSolution(int` v`, int` m`, int` $A[k+1]$`)`.

The main program calls `TotalSolution(v, 0, A)` where $A[k] = s$ and $A[i] = 0$ for $i = 0, 1, \ldots k-1$. If the function returns true, the requirements of Theorem 2 hold. If it returns false, an optimal CPCW code with these parameters cannot exist.

We shall illustrate this by the next two examples. Note that we do not consider $a_{m,0,0}$ because they do not take part in (11).

Example 2. *Consider an optimal* $(v, k, 1)$ *CPCW code with* $k = 3$ *and* $v = 5k(k-1)+2 = 32$. *We call* `TotalSolution(32, 0, A)`. *It starts with making the equations for* $a_{0,i,j}$*; namely,*

From the array A: $a_{0,3,0} + a_{0,3,1} = 5$;

From (11): $2a_{0,3,1} = 8$.

`NextSolution(0)` *finds the first solution of this system:* $a_{0,3,0} = 1, a_{0,3,1} = 4$. *From (10):* $a_{1,1,0} = 4$, $a_{1,2,0} + a_{1,2,1} = 4$, $a_{1,3,0} + a_{1,3,1} = 1$. *We use this to assign values to the elements of array B, namely* $B[1] = 4, B[2] = 4, B[3] = 1$. *Then* `TotalSolution(32, 1, B)` *is called. It starts with making the equations for* $a_{1,i,j}$; *namely,*

From B: $a_{1,1,0} = 4$, $a_{1,2,0} + a_{1,2,1} = 4$, $a_{1,3,0} + a_{1,3,1} = 1$

From (11): $a_{1,2,1} + 2a_{1,3,1} = 4$.

`NextSolution(1)` *finds the first solution of this system with nonzero elements:* $a_{1,0,0} = 1$, $a_{1,1,0} = 4, a_{1,2,1} = 4, a_{1,3,0} = 1$. *In a similar way solutions are next found for* $m = 2$ *and* 3. *When* `NextSolution(3)` *finds a solution the condition* $2^{m+3} \leq v$ *is false because* $2^6 = 64 > 32$. *That is why* `TotalSolution(32, 3, B)` *returns true, and so do* `TotalSolution(32, 2, B)`, `TotalSolution(32, 1, B)` *and* `TotalSolution(32, 0, A)`. *This means that the requirements of Theorem 2 hold for these parameters.*

Example 3. *Consider an optimal* $(v, k, 1)$ *CPCW code with* $k = 22$ *and* $v = 3k(k-1)+2 = 1388$. *We call* `TotalSolution(1388, 0, A)`. *It starts with making the equations for* $a_{0,i,j}$; *namely,*

From the array A: $a_{0,22,0} + a_{0,22,1} + a_{0,22,2} + a_{0,22,3} + a_{0,22,4} + a_{0,22,5} + a_{0,22,6} + a_{0,22,7} + a_{0,22,8} + a_{0,22,9} + a_{0,22,10} + a_{0,22,11} = 3$.

From (11): $21a_{0,22,1} + 40a_{0,22,2} + 57a_{0,22,3} + 72a_{0,22,4} + 85a_{0,22,5} + 96a_{0,22,6} + +105a_{0,22,7} + 112a_{0,22,8} + 117a_{0,22,9} + 120a_{0,22,10} + 121a_{0,22,11} = 347$.

`NextSolution(0)` *finds the first solution of this system. Its nonzero elements are* $a_{0,22,7} = 1$ *and* $a_{0,22,11} = 2$. *Then the nonzero elements of the array B are* $B[7] = 1$, $B[11] = 4$, *and* $B[15] = 1$. `TotalSolution(1388, 1, B)` *is called and it starts with making the equations for* $a_{1,i,j}$:

From B: $a_{1,7,0} + a_{1,7,1} + a_{1,7,2} + a_{1,7,3} = 1$,

$a_{1,11,0} + a_{1,11,1} + a_{1,11,2} + a_{1,11,3} + a_{1,11,4} + a_{1,11,5} = 4$,

$a_{1,15,0} + a_{1,15,1} + a_{1,15,2} + a_{1,15,3} + a_{1,15,4} + a_{1,15,5} + a_{1,15,6} + a_{1,15,7} = 1$.

From (11): $6a_{1,7,1} + 10a_{1,7,2} + 12a_{1,7,3} + 10a_{1,11,1} + 18a_{1,11,2} + 24a_{1,11,3} + 28a_{1,11,4} + 30a_{1,11,5} + 14a_{1,15,1} + 26a_{1,15,2} + 36a_{1,15,3} + 44a_{1,15,4} + 50a_{1,15,5} + 54a_{1,15,6} + 56a_{1,15,7} = 173$.

This linear system of equations has no integer solutions. `NextSolution(1)` *returns false and so does* `TotalSolution(1388, 1, B)`, *which was called from* `TotalSolution(1388, 0, B)`. *The latter calls* `NextSolution(0)`, *which returns false because there are no more solutions for* $a_{0,i,j}$ *and thus* `TotalSolution(1388, 0, B)` *returns false. This means that the necessary conditions from Theorem 2 do not hold for these parameters, and therefore an optimal* $(1388, 22, 1)$ *CPCW code does not exist.*

The function `NextSolution` is the main part of the computation. It finds a solution of the linear system for a fixed m. We have to find only integer solutions for $a_{m,i,j}$, $i, j = 0, 1, \ldots k$. That is why we do not use the standard approach to solving linear systems by considering the equations as the rows of a matrix, and finding a triangular form of this matrix. Instead of that we first assign 0 to all unknowns and then start the backtrack search for giving non-negative integer values to them.

We begin with $a_{0,k,0}$. After choosing a value for $a_{m,i,j}$ we check if the left side of Equations (10) and (11) is smaller than the right side. If this is true, we set a value for $a_{m,i,j+1}$, or for $a_{m,i+1,0}$ if $j + 1 > \frac{i}{2}$. If the left side of one of Equations (10) and (11) is greater than the right side, we assign 0 to $a_{m,i,j}$ and increment by 1 the value of $a_{m,i,j-1}$, or $a_{m,i-1,\lfloor \frac{i}{2} \rfloor}$ if $j = 0$. We next compute the left side of Equations (10) and (11) and repeat the same procedure.

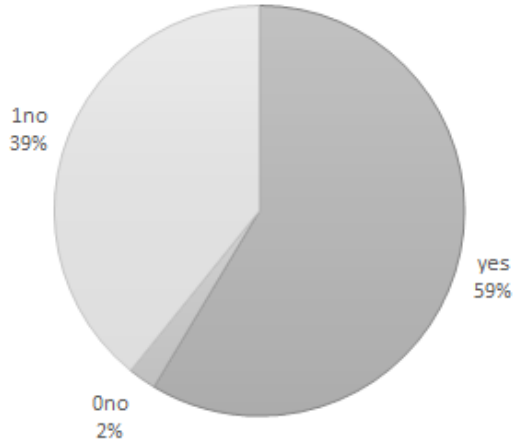
If the left side of Equations (10) and (11) is equal to the right side, a solution has been found. If a next solution is needed and the function is called again, it works in the same way, but instead of starting from $a_{m,i,j} = 0$ it starts from the last solution that was found by incrementing by 1 the last nonzero $a_{m,i,j}$ which was chosen.

To avoid errors the algorithm was independently implemented in C++ by the second and third authors. We obtain the same results (Table 1) by both implementations. Note that the above description only concerns the basic structure of our software and its most important functions `TotalSolution` and `NextSolution`. Each of the two implementations uses a lot of additional variables and function parameters. One of the implementations organizes the communication between `TotalSolution` and `NextSolution` in a slightly different way, namely after finding a solution `NextSolution` calls the function `MakeLevelArrays` which assigns values to the array B and other necessary variables, and when this has been done, `MakeLevelArrays` calls `TotalSolution` to look for a solution at the next level. We attach the C++ source of this implementation as Supplementary Material.

By this software we check if Theorem 2 holds for optimal $(sk(k-1)+2, k, 1)$ CPCW codes with $k \leq 200$ and $s \leq 10$. We obtain plenty of nonexistence results, but most of them are not new, because they follow from Equations (3) and (4) and have been described in [1].

The computer-aided results are presented in Table 1. It contains only the results for values of v which are divisible by 4, namely $k(k-1)s+2 = 4u$. This means that $k(k-1)s$ is not divisible by 4. Since $k(k-1)$ is divisible by 2, it follows that s is odd, and not all values of $k \leq 200$ are considered. We are interested in the nonexistence results for which there is at least one solution for $m = 0$, but no solution exists for $m = 1$. In the table they are denoted by **1 no**. As Supplementary Material we attach a file with the solutions for the considered parameters.

Table 1. Computer-aided check for the requirements of Theorem 2. yes—the requirements of Theorem 2 hold; 0 no—no integer solution for $a_{0,i,j}$ from Theorem 2; **1 no**—a solution for $a_{0,i,j}$ exists, but there is no integer solution for $a_{1,i,j}$ from Theorem 2.



k	s = 1	s = 3	s = 5	s = 7	s = 9
3	yes	0 no	yes	0 no	yes
6	yes	**1 no**	yes	yes	yes
7	0 no	yes	0 no	yes	0 no
10	0 no	0 no	yes	yes	yes
11	yes	0 no	yes	0 no	yes
14	0 no	yes	yes	yes	yes
15	0 no	yes	0 no	yes	0 no
18	yes	yes	yes	yes	yes
19	0 no	0 no	yes	0 no	yes
22	0 no	**1 no**	yes	yes	yes

Table 1. *Cont.*

k	s = 1	s = 3	s = 5	s = 7	s = 9
23	0 no	yes	0 no	yes	0 no
26	0 no	yes	yes	yes	yes
27	yes	0 no	yes	0 no	yes
30	0 no	yes	yes	yes	yes
31	0 no	yes	0 no	yes	0 no
34	0 no	yes	yes	yes	yes
35	0 no	0 no	yes	0 no	yes
38	yes	0 no	yes	yes	yes
39	0 no	yes	0 no	yes	0 no
42	0 no	0 no	yes	yes	yes
43	0 no	0 no	yes	0 no	yes
46	0 no	yes	yes	yes	yes
47	0 no	yes	0 no	yes	0 no
50	0 no	yes	yes	yes	yes
51	yes	0 no	yes	0 no	yes
54	0 no	**1 no**	yes	yes	yes
55	0 no	yes	0 no	yes	0 no
58	0 no	yes	yes	yes	yes
59	0 no	0 no	yes	0 no	yes
62	0 no	yes	yes	yes	yes
63	0 no	yes	0 no	yes	0 no
66	**1 no**	yes	yes	yes	yes
67	0 no	0 no	yes	0 no	yes
70	0 no	**1 no**	yes	yes	yes
71	0 no	yes	0 no	yes	0 no
74	0 no	0 no	yes	yes	yes
75	0 no	0 no	yes	0 no	yes
78	0 no	yes	yes	yes	yes
79	0 no	yes	0 no	yes	0 no
82	0 no	yes	yes	yes	yes
83	yes	0 no	yes	0 no	yes
86	0 no	**1 no**	yes	yes	yes
87	0 no	yes	0 no	yes	0 no
90	0 no	yes	yes	yes	yes
91	0 no	0 no	yes	0 no	yes
94	0 no	yes	yes	yes	yes
95	0 no	yes	0 no	yes	0 no
98	0 no	yes	yes	yes	yes
99	0 no	0 no	yes	0 no	yes
102	yes	**1 no**	yes	yes	yes
103	0 no	yes	0 no	yes	0 no
106	0 no	0 no	yes	yes	yes
107	0 no	0 no	yes	0 no	yes
110	0 no	yes	yes	yes	yes
111	0 no	yes	0 no	yes	0 no
114	0 no	yes	yes	yes	yes
115	0 no	0 no	yes	0 no	yes
118	0 no	**1 no**	yes	yes	yes
119	0 no	yes	0 no	yes	0 no
122	0 no	yes	yes	yes	yes
123	yes	0 no	yes	0 no	yes
126	0 no	yes	yes	yes	yes
127	0 no	yes	0 no	yes	0 no
130	0 no	yes	yes	yes	yes

Table 1. *Cont.*

k	s = 1	s = 3	s = 5	s = 7	s = 9
131	0 no	0 no	yes	0 no	yes
134	0 no	**1 no**	yes	yes	yes
135	0 no	yes	0 no	yes	0 no
138	0 no	0 no	yes	yes	yes
139	0 no	0 no	yes	0 no	yes
142	0 no	yes	yes	yes	yes
143	0 no	yes	0 no	yes	0 no
146	yes	yes	yes	yes	yes
147	0 no	0 no	yes	0 no	yes
150	0 no	0 no	yes	yes	yes
151	0 no	yes	0 no	yes	0 no
154	0 no	yes	yes	yes	yes
155	0 no	0 no	yes	0 no	yes
158	0 no	yes	yes	yes	yes
159	0 no	yes	0 no	yes	0 no
162	0 no	yes	yes	yes	yes
163	0 no	0 no	yes	0 no	yes
166	0 no	0 no	yes	yes	yes
167	0 no	yes	0 no	yes	0 no
170	0 no	0 no	yes	yes	yes
171	yes	0 no	yes	0 no	yes
174	0 no	yes	yes	yes	yes
175	0 no	yes	0 no	yes	0 no
178	0 no	yes	yes	yes	yes
179	0 no	0 no	yes	0 no	yes
182	0 no	**1 no**	yes	yes	yes
183	0 no	yes	0 no	yes	0 no
186	0 no	yes	yes	yes	yes
187	0 no	0 no	yes	0 no	yes
190	0 no	yes	yes	yes	yes
191	0 no	yes	0 no	yes	0 no
194	0 no	yes	yes	yes	yes
195	0 no	0 no	yes	0 no	yes
198	yes	**1 no**	yes	yes	yes
199	0 no	yes	0 no	yes	0 no

CPCW codes with one codeword are separately considered in [1] and restrictions which hold only for them are presented. By [1], Corollary 3.4, a $(k(k-1)+2, k, 1)$ CPCW code with $k = 8u+2$ exists if $8u$ is a perfect square and k is the sum of two squares. Since 66 cannot be written as a sum of two squares, the nonexistence for $k = 66$ and $s = 1$ is not a new result. The other cases in which there are solutions for $m = 0$ but no solution exists for $m = 1$ are for $s = 3$ and $k = 6 + 16u$, namely for $k = 22, 54, 70, 86, 102, 118, 134, 182$, and 198. Example 3 presents one of these cases. Note that there are three values of $k = 6 + 16u$ for which there is no solution for $m = 0$. These are $k = 38, 150$, and 166. Their nonexistence follows from [1], Theorem 4.13.

The complexity of a backtrack search algorithm is usually not discussed, because it is always exponential, namely the worst possible. In our case the possible values for $a_{m,i,j}$ are $0, 1, \ldots 2^m s$ and thus the search for a solution at level m is $O((2^m s)^{k^2})$, and the worst-case time complexity of the whole search is $O((2^{n!} s^n)^{k^2})$. Despite its awful time complexity, backtrack search is often used in combinatorial constructions for relatively small parameters when the mathematical properties of the constructed objects allow the rejection of some of the partial solutions [31]. The time which an exponential algorithm needs to complete

a definite job grows exponentially with the growth of the considered amount of data, or parameters, but in our case we do not always need to obtain all solutions for a definite level m, since obtaining one of them is enough when this solution is extendable to a solution for level $m+1$, $m+2$, etc. That is why the program sometimes needs a totally different amount of time for very similar parameters. For instance, on a 64.0 GB 3.2 GHz Intel-i9 PC several days are needed to find a solution for $k = 126$ and $s = 7$, and less than a minute is enough for $k = 126$ and $s = 9$ and for most of the other cases from Table 1. It can be seen from the file which we give as Supplementary Material that there are solutions for $m = 6$ or 7. They have been obtained very quickly too.

There are certainly possible ways to make the programs faster for some of the parameter ranges, but we have not done it, because we do not expect to obtain new nonexistence results which are not for $k = 6 + 16u$ and $s = 3$. Greater values of s and k lead to a big number of unknowns, and to more possible solutions. This makes new nonexistence results almost impossible. The known infinite families [1] for which no optimal CPCW codes exist have been obtained by the consideration of divisibility arguments for odd k, because in that case $i(k-i)$ is always even. To use a similar method in the next section is only possible because in that case all the considered circulants of order $\frac{v}{2}$ have an odd number of ones. We implemented the algorithm twice because we expected to find several isolated new nonexistence results for small s and k. For that purpose, not the speed but the correctness of the programs was important. The infinite class is far beyond our expectations. In the next section we prove that optimal $(3k(k-1)+2, k, 1)$ CPCW codes with $k = 6 + 16u$ do not exist.

5. Nonexistence of Optimal $(v, k, 1)$ CPCW Codes with $v = 3k(k-1)+2$ and $k = 16u+6$

The proof of the nonexistence of these codes uses divisibility considerations. That is why we need the following lemma.

Lemma 1. *The length v of an optimal $(3k(k-1)+2, k, 1)$ CPCW code with $k = 16u+6$ is divisible by 4 and not divisible by 8; namely, $v = 4(192u^2+132u+23)$.*

Proof. We will prove this by direct substitution:

$$v = 3k(k-1)+2 = 3(16u+6)(16u+5)+2 = 4(192u^2+132u+23) \quad \square$$

In Example 3, $v = 1388$ and $\frac{v}{4} = 347$.

The nonexistence of optimal $(3k(k-1)+2, k, 1)$ CPCW codes with $k = 16u+6$ follows from the fact that all circulants of order $\frac{v}{2}$, which are obtained by applying ϕ_v to the circulants of the partial design, have an odd number of ones in a row/column. This is the subject of the next lemma.

Lemma 2. *If Equations (5) and (6) (Theorem 1) hold for an optimal $(3k(k-1)+2, k, 1)$ CPCW code with $k = 16u+6$, and the nonzero elements of the solution are $a_{k,b}$, $a_{k,c}$, and $a_{k,d}$ (b, c and d are not necessarily different), then b, c and d are odd integers.*

Proof. From (6),

$$\begin{aligned} &b(k-b)+c(k-c)+d(k-d) = \tfrac{v}{4} \Rightarrow k(b+c+d)-(b^2+c^2+d^2) = \tfrac{v}{4} \Rightarrow \\ &\Rightarrow (16u+6)(b+c+d)-(b^2+c^2+d^2) = 192u^2+132u+23 \text{ (by Lemma 1)} \Rightarrow \\ &\Rightarrow 6(b+c+d)-(b^2+c^2+d^2)-3 = 192u^2+132u-16u(b+c+d)+20 \end{aligned}$$

Since the right side of this equation is divisible by 4, we can write

$$-6(b+c+d)+(b^2+c^2+d^2)+3=4x \Rightarrow$$
$$\Rightarrow b(b-6)+c(c-6)+d(d-6)+3=4x$$

The left side should be divisible by 4 too. That is why $b(b-6)+c(c-6)+d(d-6)$ is odd. Then either b, c and d are odd integers (what has to be proved), or two of them are even.

Suppose b and c are even. Then $b(b-6)$ and $c(c-6)$ are divisible by 4 and we can write

$$d(d-6)+3=4y$$

With respect to divisibility by 4 there are two possibilities for the odd number d:

$$d=4z+1, \text{or } d=4z+3.$$

In the first case

$$(4z+1)(4z-5)+3=4y \Rightarrow$$
$$\Rightarrow 16z^2-16z-2=4y.$$

This equation is impossible because its left side is not divisible by 4, while the right side is.

In the second case

$$(4z+3)(4z-3)+3=4y \Rightarrow$$
$$\Rightarrow 16z^2-6=4y$$

This is impossible too. The only possibility for b, c and d is that they are all odd. □

In Example 3, $a_{0,22,7}=1$ and $a_{0,22,11}=2$; namely, $b=7$, and $c=d=11$ are odd numbers.

Now we are ready to prove the main nonexistence result in the paper.

Proposition 1. *An optimal* $(3k(k-1)+2,k,1)$ *CPCW code with* $k=16u+6$ *does not exist.*

Proof. It follows from (7) (Theorem 1) and Lemma 2 that for these parameters the elements $a'_{i,j}$ can be nonzero if i is odd. This means that all the elements of the sum on the left side of Equation (8) (Theorem 1) are even, because $j(i-j)$ is even if i is odd. The right side is $\lfloor \frac{v}{8} \rfloor$. We know from Lemma 1 that

$v/4=192u^2+132u+23.$

Then

$\lfloor \frac{v}{8} \rfloor = 96u^2+66u+11.$

This means that $\lfloor \frac{v}{8} \rfloor$ is an odd integer. Therefore, for the considered parameters the left side of Equation (8) is even, and the right one odd. That is why a solution is not possible in this case. The requirements of Theorem 1 do not hold, and therefore an optimal $(3k(k-1)+2,k,1)$ CPCW code with $k=16u+6$ does not exist. □

In Example 3 the left side of (8) or (11) is even, while the right side is odd:

$$(11): \quad 6a_{1,7,1}+10a_{1,7,2}+12a_{1,7,3}+10a_{1,11,1}+18a_{1,11,2}+24a_{1,11,3}+$$
$$+28a_{1,11,4}+30a_{1,11,5}+14a_{1,15,1}+26a_{1,15,2}+36a_{1,15,3}+44a_{1,15,4}+$$
$$+50a_{1,15,5}+54a_{1,15,6}+56a_{1,15,7}=173$$

6. Discussion

In Theorem 2 of the present paper we derive new necessary conditions for the existence of optimal $(k(k-1)s+2, k, 1)$ CPCW codes of length divisible by 2^n, where $n \geq 2$. We apply a computer-aided search to establish if the requirements of Theorem 2 hold for some relatively small parameters, and this way we find several parameter sets for which $(k(k-1)s+2, k, 1)$ CPCW codes do not exist. Using the derived necessary conditions we also prove the nonexistence of optimal $(3k(k-1)+2, k, 1)$ CPCW codes with $k = 16u+6$.

The obtained results might be useful in several aspects:

The $(v, k, 1)$ CPCW codes have multiple applications in communications, cryptography, etc. The knowledge that a code with certain parameters does not exist can sometimes save serious unnecessary efforts to construct it.

The solutions of the equations from Theorems 1 and 2 can be helpful in further theoretical or computer-aided research on optimal $(k(k-1)s+2, k, 1)$ CPCW codes whose existence remains undecided. In our opinion the probability of finding new computer-aided nonexistence results by covering greater values of s and k is small, but not impossible.

The existence of solutions for $a_{m,i,j}$, $i, j = 0, 1, \ldots, k$ does not prove the existence of codes with the considered parameters, but the solutions give a better knowledge of the cyclic structure of the partial designs. This knowledge can be used to restrict the search space when algorithms for the construction of such partial designs are considered for relatively small parameters.

The general approach for proving Theorems 1 and 2 might be applicable to other partial cyclic designs whose number of points is divisible by four, and for which it is possible to follow where the points of the uncovered pairs are after the application of ϕ_v.

Supplementary Materials: The following supporting information can be downloaded at https://www.mdpi.com/article/10.3390/axioms15090679/s1. The computer-aided results and the C++ source code of the software implementation by the second author are available as supplementary material.

Author Contributions: Conceptualization, S.T. and T.B.; methodology, S.T. and T.B.; software, T.Y. and S.T.; validation, S.T., T.Y. and T.B.; investigation, T.Y., S.T. and T.B.; data curation, T.B.; writing—original draft preparation, S.T., T.Y. and T.B.; writing—review and editing, S.T., T.Y. and T.B. All authors have read and agreed to the published version of the manuscript.

Funding: The research of T. Baicheva was partially supported by the Centre of Excellence in Informatics and ICT under the Grant No BG16RFPR002-1.014-0018-C01, financed by the Research, Innovation and Digitalization for Smart Transformation Programme 2021–2027 and co-financed by the European Union. The research of S. Topalova was partially supported by the National Science Fund of Bulgaria under Contract No KP-06-H92/3-08.12.2025.

Data Availability Statement: All the new results are included in the paper and the Supplementary Materials.

Acknowledgments: The authors are grateful to the anonymous reviewers for their adequate remarks on the presentation of the material.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CPCW code	Binary Cyclically Permutable Constant Weight code
OOC	Optical Orthogonal Code

References

1. Buratti, M.; Stinson, D.R. New results on modular Golomb rulers, optical orthogonal codes and related structures. *Ars Math. Contemp.* **2020**, *20*, 1–27. [CrossRef]
2. Baicheva, T.; Topalova, S. On the existence of optimal (v, 5, 1) and (v, 6, 1) binary cyclically permutable constant weight codes. *Axioms* **2026**, *15*, 35. [CrossRef]
3. Chung, F.R.K.; Salehi, J.A.; Wei, V.K. Optical orthogonal codes: Design, analysis and applications. *IEEE Trans. Inf. Theory* **1989**, *35*, 595–604. [CrossRef]
4. Bitan, S.; Etzion, J. Constructions for optimal constant weight cyclically permutable codes and difference families. *IEEE Trans. Inf. Theory* **1992**, *41*, 77–87.
5. Colbourn, C.J.; Dinitz J.H.; Stinson D.R. Applications of Combinatorial Designs to Communications, Cryptography, and Networking. In *Surveys in Combinatorics*; Lamb, J.D., Preece, D.A., Eds.; London Mathematical Society Lecture Note Series; Cambridge University Press: Cambridge, UK, 1999; pp. 37–100.
6. Buratti, M.; Pasotti, A. Further progress on difference families with block size 4 or 5. *Des. Codes Cryptogr.* **2010**, *56*, 1–20. [CrossRef]
7. Stinson, D.R.; Wei, R.; Yin, J. Packings. In *The CRC Handbook of Combinatorial Designs*, 2nd ed.; Colbourn, C.J., Dinitz, J.H., Eds.; Chapman and Hall/CRC Press: Boca Raton, FL, USA, 2006; pp. 550–556.
8. Fuji-Hara, R.; Miao, Y. Optical orthogonal codes: Their bounds and new optimal constructions. *IEEE Trans. Inf. Theory* **2000**, *46*, 2396–2406. [CrossRef]
9. Chu, W.; Colbourn, C.J. Optimal (n, 4, 2)- OOC of small order. *Discret. Math.* **2004**, *279*, 163–172. [CrossRef]
10. Brickell, E.F.; Wei, V. K. Optical orthogonal codes and cyclic block designs. *Congr. Numer.* **1987**, *58*, 175–192.
11. Zhao, C.; Chang, Y.; Feng, F. The existence of optimal (v, 4, 1) optical orthogonal codes achieving the Johnson bound. *IEEE Trans. Inf. Theory* **2024**, *70*, 8746–8757. [CrossRef]
12. Hanani, H. Balanced incomplete block designs and related designs. *Discret. Math.* **1975**, *11*, 255–369. [CrossRef]
13. Nguyen, Q.A.; Gyöfri, L.; Massey, J.L. Constructions of binary constant weight cyclic codes and cyclically permutable codes. *IEEE Trans. Inf. Theory* **1992**, *38*, 940–949. [CrossRef]
14. Moreno, O.; Zhan, Z.; Kumar, P.V.; Zinoviev, V.A. New constructions of optimal cyclically permutable constant weight codes. *IEEE Trans. Inf. Theory* **1995**, *41*, 448–455. [CrossRef]
15. Chen, K.; Zhu, L. Existence of (q, 6, 1) difference families with q a prime power. *Des. Codes Cryptogr.* **1998**, *15*, 167–173. [CrossRef]
16. Yin, J. Some combinatorial constructions for optical orthogonal codes. *Discret. Math.* **1998**, *185*, 201–219. [CrossRef]
17. Chen, K.; Zhu, L. Existence of (q, k, 1) difference families with q a prime power and k = 4,5. *J. Comb. Des.* **1999**, *7*, 21–30. [CrossRef]
18. Chen, K.; Wei, R.; Zhu, L. Existence of (q, 7, 1) difference families with q a prime power. *J. Comb. Des.* **2002**, *10*, 126–138. [CrossRef]
19. Tang, Y.; Yin, J. Combinatorial constructions for a class of optimal OOCs. *Sci. China A* **2002**, *45*, 1268–1275. [CrossRef]
20. Chu, W.; Golomb, S.W. A new recursive construction for optical orthogonal codes. *IEEE Trans. Inf. Theory* **2003**, *49*, 3072–3076. [CrossRef]
21. Chang, Y.; Ji, L. Optimal $(4up, 5, 1)$ optical orthogonal codes. *J. Comb. Des.* **2004**, *12*, 346–361. [CrossRef]
22. Julian, R.; Abel, R.; Costa, S.; Finizio, N. Directed-ordered whist tournaments and (v,5,1) difference families: Existence results and some new classes of Z-cyclic solutions. *Discret. Appl. Math.* **2004**, *143*, 43–53. [CrossRef]
23. Ma, S.; Chang, Y. A new class of optimal optical orthogonal codes with weight five. *IEEE Trans. Inf. Theory* **2004**, *50*, 1848–1850. [CrossRef]
24. Ma, S.; Chang, Y. Constructions of optimal optical orthogonal codes with weight five. *J. Comb. Des.* **2005**, *13*, 54–69. [CrossRef]
25. Wang, S.; Wang, L.; Wang, J. A new class of optimal optical orthogonal codes with weight six. In Proceedings of the Seventh International Workshop of Signal Design and its Applications in Communications, Bengaluru, India, 14–18 September 2015.
26. Colbourn, M.J.; Mathon, R.A. On cyclic Steiner 2-designs. *Ann. Discret. Math.* **1980**, *7*, 215–253. [CrossRef]
27. Colbourn, C.J.; Colbourn, M.J. On cyclic Steiner systems S(2,6,91). *Abstr. Pap. Present. Am. Math. Soc.* **1982**, *5*, 463.
28. Janko, Z.; Tonchev, V.D. Cyclic 2-(91, 6, 1) designs with multiplier automorphisms. *Discret. Math.* **1991**, *97*, 265–268. [CrossRef]
29. Baicheva, T.; Topalova, S. Classification of optimal (v, k, 1) binary cyclically permutable constant weight codes with k = 5, 6 and 7 and small lengths. *Des. Codes Cryptogr.* **2019**, *87*, 365–374. [CrossRef]
30. Hetman, I.; Baicheva, T.; Topalova, S. Construction of (v,k,1) cyclic difference families with small parameters. *J. Algebra Comb. Discret. Struct. Appl.* **2025**, *13*, 111–119. [CrossRef]
31. Kaski, P.; Östergård, P. *Classification Algorithms for Codes and Designs*; Springer: Berlin/Heidelberg, Germany, 2006.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.