Designs, Codes and Cryptography, 3, 283–313 (1993)

The Last Packing Number of Quadruples, and Cyclic SQS

SARA BITAN AND TUVI ETZION*
Computer Science Department, Technion—Israel Institute of Technology, Haifa 32000, Israel

Communicated by D. Jungnickel
Received February 28, 1993; Revised February 24, 1993.

Abstract. The packing number of quadruples without common triples of an n-set, or the maximum number of codewords of a code of length n, constant weight 4, and minimum Hamming distance 4, is an old problem. The only unsolved case is $n \equiv 5 \pmod 6$. For 246 values of the form $n \equiv 5 \pmod 6$, we present constant weight codes with these parameters, of size $[(n-1)(n^2-3n-4)]/24$, which is greater by $(4n - 20/24)$ from the previous lower bound and leaves a gap of $\lfloor (n-5)/12 \rfloor$ to the known upper bound. For infinitely many values $n \equiv 5 \pmod 6$ we give enough evidence to believe that such codes exist. The constructed codes are optimal extended cyclic codes with these parameters. The construction of the code is done by a new approach of analyzing the Köhler orbit graph. We also use this analysis to construct new S-cyclic Steiner Quadruple Systems. Another important application of the analysis is in the design of optical orthogonal codes.

1. Introduction

The problem of determining the maximum number of quadruples from Z_n with no common triples has received a lot of attention from the point of view of combinatorics and coding theory. This number is denoted by the packing number, $d(3, 4, n)$, and by $A(n, 4, 4)$, where $A(n, d, w)$ is the maximum number of codewords in a code of length n, constant weight w, and minimum Hamming distance d.

Hanani [1] showed that $A(n, 4, 4) = n(n-1)(n-2)/24$, for $n \equiv 2$ or $4 \pmod 6$ by constructing a Steiner Quadruple System (SQS). An SQS of order n ($SQS(n)$) is a set of quadruples from Z_n such that each triple from Z_n is contained in exactly one quadruple. Combining Hanani result, the known values of $A(n, 4, 3)$[2] and the Johnson bound [3]

$$A(n, d, w) \leq \left\lfloor \frac{n}{w} A(n-1, d, w-1) \right\rfloor$$

we have that $A(n, 4, 4) = n(n-1)(n-3)/24$, for $n \equiv 1$ or $3 \pmod 6$. For $n \equiv 0 \pmod 6$ Kalbfleisch and Stanton [4] showed that for $n = 6 \cdot 2^k$, $k \geq 0$, $A(n, 4, 4) = n(n^2 - 3n - 6)/24$. By using the result of Mills [5], Brouwer [6] showed that $A(n, 4, 4) = n(n^2 - 3n - 6)/24$ for all $n \equiv 0 \pmod 6$. Thus, $A(n, 4, 4)$ attains the Johnson bound, for $n \not\equiv 5 \pmod 6$[6].

*This research was supported in part by the Technion V.P.R. Fund.

The most difficult case is $n \equiv 5 \pmod 6$ for which not many results are known [7, p. 395]. Best [8] (see also [9]) showed 11 different codes which meet the value $A(11, 4, 4) = 35$. Brouwer et al. [10] showed that $A(17, 4, 4) \geq 156$ (while from the Johnson bound $A(17, 4, 4) \leq 157$). All the other lower bounds are either obtained by the second Johnson bound

$$A(n, d, w) \leq \left\lfloor \frac{n}{n - w} A(n - 1, d, w) \right\rfloor$$

which in this case becomes $A(n, 4, 4) \geq (n - 3)(n^2 - n - 8)/24$, or by the partitioning method [10]–[12] for quadruples, which improves this bound by one or two for some values of n. Finally as mentioned by Brouwer [6] there is some information on the structure of a code which meets the Johnson bound. This information can be obtained from the structure of the optimal codes of length $n - 1$, weight 3, and minimum Hamming distance 4 [2], embedded in this code.

In this article we obtain new lower bounds on $A(n, 4, 4)$ for 246 values of the form $n \equiv 5 \pmod 6$. We describe a method that implies $A(n, 4, 4) \geq (n - 1)(n^2 - 3n - 4)/24$ for these values. For infinitely many values $n \equiv 5 \pmod 6$ we give enough evidence to believe that such codes exist. The method is applied for some $n = 2p + 1 \equiv 23 \pmod{48}$, p prime. It was also applied on $n = 29$. For example we have $A(23, 4, 4) \geq 418$ which improves the bound given in the tables of Brouwer et al. [10]. This lower bound is greater by $(4n - 20/24)$ from the previous lower bound. The gap between this bound and the upper bound is $\lfloor (n - 5)/12 \rfloor$.

Each of our codes has an automorphism which consists of a fixed point and a cycle. Such codes are called in [10] extended cyclic or cyclic with a fixed point. The code of length 17, weight 4, and minimum Hamming distance 4, presented in [10] is extended cyclic. Another 11 constant weight codes with $w \geq 7$ and $d \geq 8$ presented in [10] are extended cyclic. The block designs associated with extended cyclic codes are called 1-rotational. Phelps [13] proved that 1-rotational SQSs exist for order 2^k, $k \geq 2$, and if they exist for order $a + 1$ and order $b + 1$, where a and b are relatively primes then they exist for order $ab + 1$. Hartman and Phelps [14] mentioned that Carmichal $SQS(p + 1)$, $p \equiv 7 \pmod{12}$, for prime p is 1-rotational.

From the results obtained in this article it is natural to conjecture that for $n \equiv 5 \pmod 6$, $n \geq 17$ there exist an extended cyclic code of length n, weight 4, minimum Hamming distance 4 with $(n - 1)(n^2 - 3n - 4)/24$ codewords. It is easy to verify that this bound is tight for extended cyclic codes with these parameters.

Our codes are obtained by a new approach of analyzing Köhler orbit graph [15]. This graph was constructed for the purpose of generating cyclic SQS. A cyclic $SQS(n)$ is an SQS of order n, with an automorphism which consists of cycles of length n, $n/2$ or $n/4$. If each orbit of the automorphism contains for each quadruple $\{x, y, z, w\}$ its symmetric quadruple $\{n - x, n - y, n - z, n - w\}$, then the SQS is called S-cyclic, or symmetric. The method that we are using makes it possible to construct S-cyclic $SQS(4p)$ for all primes $p \equiv 5 \pmod{12}$, if a certain number theoretic conjecture is true. It was verified that the conjecture is true for $p \equiv 5 \pmod 6$ such that $p < 1500000$. A necessary condition for the existence of S-cyclic $SQS(n)$, is that whenever $2p$ divides n, there exists an S-cyclic $SQS(2p)$. Thus all odd prime factors must be congruent to 1 or 5 (mod 12) [14]. The works

of Köhler [15] and Siemon [16]–[19] show that S-cyclic $SQS(2p^{\alpha})$, $\alpha \geq 1$, exists when $p \equiv 5 \pmod{12}$ if a certain number theoretic conjecture is true. No other large family of S-cyclic SQS is known.

Our codes are closely related to another important family of constant weight codes, *Optical Orthogonal Codes*, which were introduced in [20]. Using the same techniques developed for the construction of our codes, we found some new optimal optical orthogonal codes.

The rest of this article is organized as follows. In Section 2 we introduce the basic concepts of difference quadruples and difference triples, used for generation of cyclic SQS. We also describe the structure of our extended cyclic codes. In Section 3 we describe a graph whose vertices are the difference triples and edges are the difference quadruples. In Section 4 we describe an automorphism of this graph. In Section 5 we describe Köhler orbit graph and its 1-factorization. In Section 6 we construct our codes and in Section 7 we present the possible extended cyclic codes for other lengths congruent to 5 modulo 6. In Section 8 we present the construction of the S-cyclic $SQS(4p)$. In Section 9 we present the application to optical orthogonal codes.

2. Basic Definitions and the Code Structure

A difference triple (DT) $<x, y, z>$, $x, y, z \in Z_v - \{0\}$, with $x + y + z = v$ is an equivalence class of ordered triples under the equivalence relation $<x, y, z> \sim <z, x, y>$. A difference quadruple (DQ) $<x, y, z, w>$, $x, y, z, w \in Z_v - \{0\}$, with $x + y + z + w = v$ is an equivalence class of ordered quadruples under the equivalence relation $<x, y, z, w> \sim <w, x, y, z>$. We will represent extended cyclic constant weight code with weight 4 by a set of DTs and DQs. A DT $<x, y, z>$ represents all the cyclic shifts of the first $v = n - 1$ bits of the word $(0, x, x + y, v)$. The indices indicate the places of the bits which are ONEs in the word. $<x, y, z>$ is the *base DT* of the set of words $X = \{(i, x + i, x + y + i, v) : i \in Z_v\}$ (throughout this article all operations in words, DTs, DQs, and pairs are taken modulo v, unless it is understood otherwise from the context). X is the *set of words induced by* the DT $<x, y, z>$. Given a codeword (t, l, m, v), $0 \leq t < l < m < v$ the DT that induces it is $<l - t, m - l, t - m>$. A DT $<x, y, z>$ contains three difference pairs $<x + y, z>$, $<x, y + z>$ and $<y, z + x>$, each pair corresponds to two out of the three first ONEs in the word.

In a similar way, a DQ $<x, y, z, w>$ induces all the cyclic shifts of the first v bits of the word $(0, x, x + y, x + y + z)$. $<x, y, z, w>$ is the base DQ of all the words in $\{(i, x + i, x + y + i, x + y + z + i) : i \in Z_v\}$. Given a codeword (t, l, m, k), $0 \leq t < l < m < k < v$, the DQ that induces it is $<l - t, m - l, k - m, t - k>$. A DQ $<x, y, z, w>$ contains the DTs $<x + y, z, w>$, $<x, y + z, w>$, $<x, y, z + w>$ and $<y, z, w + x>$. Each triple corresponds to three out of the four ONEs in the word. An extended cyclic code C has minimum Hamming distance 4 if and only if the set of base DTs and base DQs that induce the words in the code meets the following two conditions, which are a generalization of the condition in [21] for the purpose of constructing cyclic SQS.

(a1) each DT is contained at most once in the set of base difference tuples (either as one of the four DTs contained in a base DQ, or as a base DT).
(a2) any two base DTs, have no difference pair in common.

In this article we present a construction for extended cyclic codes of size $[(n-1)(n^2-3n-4)]/24$, for some $n \equiv 23 \pmod{48}$, such that $n = 2p+1$ where p is prime. By Dirichlet Theorem [22, p. 217] any arithmetic progression $a, a+b, a+2b, a+3b, \ldots$ contains infinitely many primes if the integers $a, b > 0$, are relatively primes. Hence, there are infinitely many primes of the form $p \equiv 11 \pmod{24}$, and only for 244 of them explicit construction is given.

The code C contains three sets of words, $C = C_0 \cup C_1 \cup C_2$. C_0 contains all the words induced by base DQs of the form $<i, i, j, j>$, and therefore $|C_o| = [(n-3)(n-1)]/4$. C_1 contains the words of an optimal cyclic code of length $n-1$, weight 3 and minimum Hamming distance 4, followed by a ONE, and therefore $|C_1| = [(n-1)(n-5)]/6$. C_2 contains words induced by base DQs of the form $<x, y, x, z>$, $y \neq z$. These DQs contain all the DTs of the form $<x, y, z>$ such that neither $<x, y, z>$ nor $<x, z, y>$ appear in any of the previous sets, and we found that $|C_2| = [(n-1)(n^2-13n+34)]/24$. Our construction builds a base set $B = B_0 \cup B_1 \cup B_2$. B_0, B_1 and B_2 contain the base DTs and the base DQs that induce the words of C_0, C_1 and C_2 respectively.

To construct B_1 and B_2 we build a graph whose vertices are all the DTs that don't participate in the DQs of B_0 (these are all the DTs $<x, y, z>$ such that x, y, z are different, and each one of them is not equal $v/2$). The edges of the graph correspond to DQs of the form $<x, y, x, z>$. This graph has been analyzed for the purpose of constructing cyclic SQSs. Based on this graph Köhler [15] defined the automorphism orbit graph which was studied by Siemon [16]–[19].

The DTs in B_1 correspond to an independent set taken out from the graph, such that no two vertices contain the same difference pair. The independent set is chosen in a way such that by removing it and its incident edges, the rest of the graph contains a 1-factor (a vertex set of disjoint edges that covers all the vertices). The edges of this 1-factor correspond to the base DQs in B_2.

3. A Graph for the DTs and DQs

As said before, $B = B_0 \cup B_1 \cup B_2$, where B_0 contains all the base DQs of the form $<i, i, j, j>$. These DQs contain all the DTs of the form $<i, i, 2j>$, $<j, j, 2i>$, $<i, j, v/2>$ and $<i, v/2, j>$. Let

$$T_v = \{\{x, y, z\} : x + y + z = v, \frac{v}{2} \notin \{x, y, z\}, |\{x, y, z\}| = 3\}$$

As we already said before, a DQ in B_2 has the form $<x, y, x, z>$, $y \neq z$. Such a DQ contains the DTs $\{<x+y, x, z>, <x, x+y, z>, <x+z, x, y>, <x+z, y, x>\}$. The second DT is the symmetric DT of the first, and the fourth is the symmetric DT of

the third. Hence, all the DTs formed from $\{x, y, z\} \in T_v$ appear in the same DQ of B_2. An element $\{x, y, z\} \in T_v$ will be called a $\overline{\text{DT}}$. For each $\overline{\text{DT}}$ $\{x, y, z\}$, there exist three $\overline{\text{DT}}$s, for which each one can be used to construct a DQ of the form $<a, b, a, c>$ together with $\{x, y, z\}$. We call those $\overline{\text{DT}}$s, the *derivatives* of $\{x, y, z\}$. The derivatives of a $\overline{\text{DT}}$ $\{x, y, z\}$ were defined in [16]. Our definition is slightly different from the definition of derivatives given in [16]. This definition will make the work of finding 1-factors in the graph simpler.

The derivatives of $\{x, y, z\}$ are defined as follows:

$$\begin{array}{lll} \text{First derivative} & \{x, y, z\}' & = \{x, -y, y - x\} = \{x, x + z, y - x\} \\ \text{Second derivative} & \{x, y\, z\}'' & = \{x, z - x, -z\} = \{x, z - x, x + y\} \\ \text{Third derivative} & \{x, y, z\}''' & = \{z - y, y, -z\} = \{z - y, y, x + y\} \end{array}$$

In this definition we gave an artificial order to the triple. Note that if we use another order of x, y, z in the $\overline{\text{DT}}$, to represent the same set of $\overline{\text{DT}}$s, the derivatives remain the same, but their order is changed.

We define a relation R on T_v by $R = \{(t_1, t_2) : t_2 = t_1'$ or $t_2 = t_1''$ or $t_2 = t_1''' \}$, and a graph $Q(v)$ whose vertices are the elements of T_v and the edges are the elements of R.

LEMMA 1. *An edge e in $Q(v)$ uniquely defines a DQ of the form $<x, y, x, z>$.*

Proof. The quadruple defined by the edge $e_1 = (\{x, y, z\}, \{x, y, z\}') = (\{x, y, z\}, \{x, x + z, y - x\})$ is $<x, y - x, x, z>$. The DQ defined by the edge $e_2 = (\{x, y, z\}, \{x, y, z\}'') = (\{x, y, z\}, \{x, z - x, x + y\})$ is $<x, z - x, x, y>$. The quadruple defined by the edge $e_3 = (\{x, y, z\}, \{x, y, z\}''') = (\{x, y, z\}, \{z - y, y, x + y\})$ is $<y, z - y, y, x>$. A simple calculation shows that the four $\overline{\text{DT}}$s of the DQ defined by e_i are represented by the vertices incident to e_i. □

4. Automorphisms of $Q(v)$

In this section we will define an automorphism group $U_v \subseteq Aut(Q(v))$ [15], [16], and use this automorphism group to define Köhler orbit graph, whose vertices are representative of orbits of T_v under U_v. Then, we analyze this orbit graph, and use it to understand the structure of $Q(v)$.

Let $E(v)$ be the multiplicative group of the residues modulo v, $v = 2p \equiv 22 \pmod{48}$, between 1 and $v - 1$, which are relatively prime to v. For $\{x, y, z\} \in T_v$, and $m \in E(v)$, we define $m\{x, y, z\}$ [16] as follows:

$$m\{x, y, z\} = \begin{cases} \{mx, my, mz\} & \text{if } mx + my + mz = v. \\ \{-mx, -my, -mz\} & \text{if } mx + my + mz = 2v. \end{cases} \tag{1}$$

where mx, my and mz are taken modulo v. It is easy to verify that

$$\tilde{m} : \{x, y, z\} \to m\{x, y, z\}$$

is an automorphism of $Q(v)$, by noting that the set of derivatives of $m\{x, y, z\}$ is the set which contains $m\{a, b, c\}$, for each $\{a, b, c\}$ which is a derivative of $\{x, y, z\}$. The set of all such automorphisms will be called U_v.

LEMMA 2 [16]. *$\sigma : m \to \tilde{m}$ is an homomorphism from $E(v)$ to the group of all automorphisms defined in* (1) *with kernel* $\{1, -1\}$, *and* $E(v)/\{1, -1\} \cong U_v \subseteq Aut(Q(v))$.

U_v is a subgroup of $Aut(Q(v))$. It is well known [22, p. 79] that the group $E(v)$, for $v = 2p$, p odd prime, has a generator, and since $\phi(v) = p - 1 = 2\delta$, where $\phi(.)$ is the Euler function, it follows that in $E(v)$ there are elements of order δ and 2δ. Elements of order δ are quadratic residues modulo v, and since -1 is not a quadratic residue modulo v for $p \equiv 11 \pmod{24}$, we can view all the elements of $E(v)$ which are quadratic residues as *positive* elements, and all the other elements as *negative*. Hence, $U_v = \{\tilde{m} : m \in E(v)$ and m is a quadratic residue modulo $v\}$, and if g is a generator of $E(v)$, and $w = g^2$, then $\tilde{w}$ is a generator of U_v. The orbit of $\{x, y, z\} \in T_v$ under U_v is defined by

$$\{x, y, z\}U_v = \{\tilde{m}(\{x, y, z\}) : \tilde{m} \in U_v\}$$

LEMMA 3. *All the orbits of U_v are of equal length δ.*

Proof. From the previous discussion $|U_v| = |E(v)|/2 = \phi(v)/2 = \delta$. Let $\tilde{w}$ be a generator of U_v, then $\{x, y, z\}U_v$, the orbit of $\{x, y, z\} \in T_v$ under U_v is $\{x, y, z\}U_v = \{\tilde{w}^i(\{x, y, z\}) : 0 \le i \le \delta - 1\}$. Since the order of $\tilde{w}$ is δ, $\tilde{w}^i$, $0 \le i \le \delta - 1$, are all different. If $w^i\{x, y, z\} = w^{i+r}\{x, y, z\}$, $1 \le r \le \delta - 1$, we set $x' = w^i x$, $y' = w^i y$ and $z' = w^i z$, and then $\{x', y', z'\} = w^r\{x', y', z'\}$, or $\{x', y', z'\} = w^r\{-x', -y', -z'\}$. This implies w.l.o.g. that $w^r x' = y'$, $w^r y' = z'$, $w^r z' = x'$ (or $w^r x' = -y'$, $w^r y' = -z'$, $w^r z' = -x'$). Hence, $w^{3r}x' = x'$ (or $w^{3r}x' = -x'$). The first case implies that δ is divisible by 3, contradiction. The second case is impossible since w is a quadratic residue, and -1 is not. Hence, all the elements $\tilde{w}^i(\{x, y, z\})$, $0 \le i \le \delta - 1$, are different. □

5. Factorization of $Q(v)$

As Siemon [16] we decompose $Q(v)$ into two subgraphs $Q_1(v)$, and $Q_2(v)$. $Q_1(v)$ consists of all the vertices $\{x, y, z\}$ such that two of x, y, z are odd. $Q_2(v)$ consists of all the vertices $\{x, y, z\}$ such that x, y, z are even. Note that in $Q(v)$ there is no edge connecting a vertex from $Q_1(v)$ with a vertex from $Q_2(v)$.

5.1. *Factorization of $Q_1(v)$*

Given a vertex $u \in Q_1(v)$, we represent $u = \{x, y, z\}$ by $[i, j, k]$ where k is even. Therefore, only two of the six permutations of $\{x, y, z\}$ can be used to represent a vertex $<x, y, z>$ in $Q_1(v)$. As proved in Lemma 3, the orbit of a vertex $[x, y, z]$ is

$$\begin{aligned}[x, y, z]U_v &= \{\tilde{m}([x, y, z]) : \tilde{m} \in U_v\} \\ &= \{w^i[x, y, z] : 0 \le i \le \delta - 1,\ w \in E(v) \text{ and } o(w) = \delta\},\end{aligned}$$

where $o(w)$ stands for the order of w. In the following lemmas we try to identify a group of representatives from the orbits of U_v on $Q_1(v)$, i.e., to select one vertex from each orbit.

LEMMA 4. *The representatives of the orbits of U_v on $Q_1(v)$ can be given by* $[1, w^i, -(1 + w^i)]$ *and* $[1 - w^i, -(1 - w^i)]$, *where* $i = 1, 2, \ldots, \delta - 1/2$, $w \in E(v)$, *and* $o(w) = \delta$.

Proof. Let $\tilde{w}$ be a generator of U_v and $[x, y, z] \in Q_1(v)$. Since $x \neq v/2$, x is odd, and $v = 2p$, where p is prime, it follows that $x \in E(v)$. Therefore, there exists $u \in E(v)$ such that $u = x^{-1}$, and there also exists j, $0 \leq j \leq \delta - 1$ such that either $x = w^j$ or $x = -w^j$, hence $[x, y, z] \in [1, yu, zu]U_v$. Note that by similar reasons, there exists $t \in E(v)$ such that $t = y^{-1}$, and there exists k, $0 \leq k \leq \delta - 1$ such that $y = \pm w^k$ and hence $[x, y, z] \in [tx, 1, tz]U_v$.

We now claim that $[1, l, -(1 + l)]$ and $[1, l^{-1}, -(1 + l^{-1})]$ are the only vertices that contain 1 in $[1, l, -(1 + l)]U_v$. Assume the contrary, i.e., that there exists a vertex $[1, s, -(1 + s)]$ in the orbit of $[1, l, -(1 + l)]$, $s \neq l$. Hence, there exists j, $1 \leq j \leq \delta - 1$, such that $[1, s, -(1 + s)] = w^j[1, l, -(1 + l)]$. Since $-(1 + s)$ and $-(1 + l)$ are even, this is possible only if $s = l^{-1}$.

One can easily see that for $1 \leq i < j \leq (\delta - 1)/2$, we have $\pm w^i \neq \pm w^j$, and also $\pm w^i \neq \pm (w^j)^{-1}$. Also note that $w^i[1, 1, -2]$ and $w^i[1, v/2, -(1 + v/2)]$ are not vertices in $Q(v)$. Hence, the representatives of the orbits of U_v on $Q_1(v)$ can be given by $[1, w^i, -(1 + w^i)]$, and $[1, -w^i, -(1 - w^i)]$, where $i = 1, 2, \ldots, (\delta - 1)/2$. □

COROLLARY 1. *$Q_1(v)$ has $\delta - 1$ orbits.*

COROLLARY 2. *The number of vertices in $Q_1(v)$, $v = n - 1$ and $n \equiv 23 \pmod{48}$* is $(n - 3)(n - 7)/16$.

Proof. By Lemma 3 and Corollary 1, $Q_1(v)$ has $\delta - 1$ orbits of length δ, where $\delta = (n - 3)/4$. Therefore, the number of vertices in $Q_1(v)$ is $\delta(\delta - 1) = (n - 3)(n - 7)/16$. □

In the sequel we will represent the orbit of $[1, w^i, -(1 + w^i)]$ by $[w^i]$ or $[w^{-i}]$. After we found a set of representatives to the orbits of U_v on $Q_1(v)$, we define $Q_1(v)$'s orbits graph $OQ_1(v)$. The vertices of $OQ_1(v)$ are the orbits representative of $Q_1(v)$, orbits O_1 and O_2 form an edge (O_1, O_2) iff there exist $\Delta_1 \in O_1$, $\Delta_2 \in O_2$ such that $(\Delta_1, \Delta_2) \in R$.

LEMMA 5. *A vertex $[x] \in OQ_1(v)$, is incident to at most three edges,* $([x], [-x])$, $([x], [-(x + 2)])$, and $([x], [-(x^{-1} + 2)])$, *which correspond to the first, second, and third derivative, respectively.*

Proof. Let $\tilde{w}$ be a generator for U_v. Consider $\Delta = [x, y, z] \in Q_1(v)$. Assume $\Delta \in [w^i]$, i.e., $\Delta = w^j[1, w^i, -(1 + w^i)]$ for some j. The three derivatives are

$$\begin{aligned}
\Delta' &= w^j[1, -w^i, -(1 - w^i)] \\
\Delta'' &= w^j[1, -(2 + w^i), 1 + w^i] \\
\Delta''' &= w^j[-(1 + 2w^i), w^i, 1 + w^i] = w^{i+j}[-(w^{-i} + 2), 1, w^{-i} + 1].
\end{aligned}$$

Therefore, if $\Delta \in [x]$ then $\Delta' \in [-x]$, $\Delta'' \in [-(x+2)]$ and $\Delta''' \in [-(x^{-1}+2)]$. □

COROLLARY 3. *The graph $OQ_1(v)$ has 1-factor given by the edges* $([x], [-x])$.

Note that the selection of orbit representative affects the derivatives, i.e., selecting $[x^{-1}]$ instead of $[x]$ exchanges the second and third derivative. An immediate result of the selection of the above representative set is the 1-factor composed of the first derivative edges. We will now define a different set of representatives; this new set will give us a 1-factor composed of the second derivative edges, and a 1-factor short of one edge composed of the third derivative edges. Together they form a Hamiltonian path in $OQ_1(v)$.

Let $\{x_i\}$, $0 \le i < 2\delta$ be the sequence defined as follows

$$x_i = \begin{cases} 1 & \text{if } i = 0 \\ -(x_{i-1}+2) & \text{if } i \text{ is odd} \\ x_{i-1}^{-1} & \text{if } i \neq 0 \text{ and } i \text{ is even} \end{cases}$$

where the computation is done modulo v.

LEMMA 6. *The sequence x_i has the following properties:*

(1) *All the x_is are odd.*
(2) *For* $0 \le j \le (\delta - 3)/2$,

$$x_{4j+1} = -\frac{3+4j}{1+4j};\ x_{4j+2} = -\frac{1+4j}{3+4j};\ x_{4j+3} = -\frac{5+4j}{3+4j};\ x_{4j+4} = -\frac{3+4j}{5+4j} \quad (2)$$

(3) $x_{2\delta-1} = v/2$.
(4) *All the x_i's are distinct.*
(5) *For odd i, $i \ge 3$, x_i is the second derivative of x_{i-1}, x_i is the third derivative of x_{i-2}, and $[x_i]$ and $[x_{i+1}]$ represent the same vertex in $OQ_1(v)$.*

Proof.

(1) is a simple observation from the definition.
(2) First note that $x_1 = -3$. Now simple induction proves that (2) is correct. We only have to show that no x_i for odd $i < 2\delta - 1$ is equal to $v/2 = 2\delta + 1$, since $v/2$ has no inverse. We really show that no $x_i = v/2$ for $i < 2\delta - 1$. Again, this is a simple observation from the fact that $x_{4k+r} = -a/b$, $0 \le k \le (\delta - 3)/2$, $1 \le r \le 4$, and $a \neq v/2$.
(3) $x_{2\delta-1} = x_{4(\delta-1)/2+1} = -(x_{4(\delta-3)/2+4} + 2) = (2\delta + 1)/(2\delta - 1) = v/2$
Since $2\delta + 1 = v/2$, and $v/2i$, for odd $i < v$, $i \neq v/2$, is equal $v/2$ modulo v.
(4) Assume the contrary; let i be the smallest integer such that $x_i = x_j$, and $0 \le j < i \le 2\delta - 1$. From (2) it is easy to verify that for x_{4k+r} $-a/b$, $0 \le k \le (\delta - 3)/2$, $1 \le r \le 4$, $a \not\equiv b \pmod v$ and $a \not\equiv -b \pmod v$ and hence $x_i \notin \{1, -1\}$. Now

note that $x_{2k} = x_{2k-1}^{-1}$ for $1 \le k \le \delta - 1$. Hence, i should be odd, i.e., $x_i = -(x_{i-1} + 2)$. Obviously if j is odd then $x_j = -(x_{j-1} + 2)$ implying $x_{i-1} = x_{j-1}$ with contradiction to our assumption. Therefore, j should be even. We distinguish between two cases. If $j = i - 1$ then $x_j = x_i = -(x_j + 2)$ and hence $x_j = -1$, contradiction. If $j < i - 1$ then since $x_i = x_j$, $x_{j+1} = -(x_j + 2)$, and $x_i = -(x_{i-1} + 2)$, it follows that $x_{j+1} = x_{i-1}$, contradicting our assumption.

(5) By definition of the sequence when i is odd $x_i = -(x_{i-1} + 2) = -(x_{i-2}^{-1} - 2)$. Since $x_{i+1} = x_i^{-1}$ when i is odd, $[x_i]$ and $[x_{i+1}]$ represent the same vertex in $OQ_1(v)$. □

Since $\{x_i\}_{i=1}^{2\delta-2}$ contains all the odd elements excluding 1, -1 and $v/2$, and by Lemma 6 (5), $[x_i]$ and $[x_{i+1}]$, i odd, represent the same vertex in $OQ_1(v)$ it follows by Lemma 6 (2) that $S = \{[-(1 + 4j)/(3 + 4j)], [-(5 + 4j)/(3 + 4j)] : j = 0, 1, \ldots, (\delta - 1)/2 - 1\}$ is a set of representatives of the orbits of U_v on $Q_1(v)$.

COROLLARY 4. (1) *The vertices* $[-1/3]$ *and* $[-(2\delta - 1)/(2\delta - 3)]$ *have degree* 2.

(2) $OQ_1(v)$ *has a* 1*-factor defined by the second derivative edges*

$$\left\{\left(\left[-\frac{1 + 4j}{3 + 4j}\right], \left[-\frac{5 + 4j}{3 + 4j}\right]\right) : 0 \le j < \frac{\delta - 1}{2}\right\}.$$

(3) $OQ_1(v) - \{[-1/3], [-(2\delta - 1)/(2\delta - 3)]\}$ *has a 1-factor defined by the third derivative edges*

$$\left\{\left(\left[-\frac{5 + 4j}{3 + 4j}\right], \left[-\frac{1 + 4(j + 1)}{3 + 4(j + 1)}\right]\right) : 0 \le j < \frac{\delta - 3}{2}\right\}.$$

(4) *The path*

$$\mathbf{Oh} \triangleq [x_2] - [x_3] - [x_6] - [x_7] - \ldots - [x_{2\delta-4}] - [x_{2\delta-3}] =$$

$$\left[-\frac{1}{3}\right] - \left[-\frac{5}{3}\right] - \left[-\frac{5}{7}\right] - \left[-\frac{9}{7}\right] - \ldots - \left[-\frac{2\delta - 5}{2\delta - 3}\right] - \left[-\frac{2\delta - 1}{2\delta - 3}\right]$$

is a Hamiltonian path in $OQ_1(v)$.

Proof.

(1) This is an immediate result from the facts that $[-1/3]''' = [-((-1/3)^{-1} + 2)] = [1]$, $[-(2\delta - 1)/(2\delta + 1)]''' = [(-(-(2\delta - 1)/(2\delta - 3))^{-1} + 2)] = [-(2\delta + 1)/(2\delta - 1)] = [v/2]$, and none of the orbits is $[1]$ or $[v/2]$ (these orbit correspond to vertices of the form $[i, i, j]$ and $[i, j, v/2]$ not included in T_v).

(2) and (3) are immediate consequences from the fact that S is a set of representatives for the orbits, and from Lemma 6 (5).

(4) is a consequence of (1), (2) and (3). □

We now define the following set $\{h_i\}_{i=0}^{\delta-1}$ of isomorphic paths in $Q_1(v)$. Each path h_i contains one vertex from each orbit of $Q_1(v)$ and the order between the vertices in each path h_i is identical to the order between the orbits in **Oh**.

$$h_0 = [-3, 1, 2] - [3, -5, 2] - \ldots - [-(2\delta - 3), 2\delta - 5, 2] - [2\delta - 3, -(2\delta - 1), 2]$$

and $h_i = w^i h_0$, $0 \leq i \leq \delta - 1$, where w is an element of order δ in $E(v)$. Since **Oh** is a Hamiltonian path in $OQ_1(v)$ we infer that

THEOREM 1. *$Q_1(v)$, $v = 2p$, $p \equiv 11$ (mod 24) can be factored into δ paths of length $\delta - 1$.*

In the sequel we will use the number theory results on the Legendre symbol, $\left(\frac{a}{p}\right)$ [22] for an odd prime p.

LEMMA 7 [22]. *If $a \equiv b$ (mod p) then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

LEMMA 8 [22]. $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

LEMMA 9 [22]. (*The Gaussian reciprocity law*): *If p and q are distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{((p-1)/2)((q-1)/2)}$$

LEMMA 10. *$OQ_1(v)$ can be factored into disjoint cycles of even length.*

Proof. By Corollaries 3 and 4, $OQ_1(v)$ has two 1-factors. If these two 1-factors share an edge, then for some x, $-x^{-1} = -(x + 2)$. This implies that $x^2 + 2x - 1 = 0$, and the solutions are $-1 \pm \sqrt{2}$ (mod p). Thus, 2 should be a quadratic residue modulo p. By Lemma 8

$$\left(\frac{2}{p}\right) = \left(\frac{2}{11 + 24k}\right) = (-1)^{(p^2-1)/8} = (-1)^{72k^2+66k+15}$$

and hence for $p = 11 + 24k$, 2 is not a quadratic residue. Therefore, the 1-factors are disjoint, and $OQ_1(v)$ can be factored into disjoint cycles of even length. □

From Lemma 10, and from the properties of the automorphism, it follows that $Q_1(v)$ can also be factored to disjoint cycles of even length. If a cycle in $OQ_1(v)$ is $[o_1] - [o_2] - [o_3] - \ldots - [o_l]$, then in $Q_1(v)$ there are a few corresponding cycles of the form $v_0^1 - v_0^2 - \ldots - v_0^l - v_1^1 - v_1^2 - \ldots - v_1^l - \ldots v_{r-1}^1 - v_{r-1}^2 - \ldots v_{r-1}^k$, where all the $v_i^j \in [o_j]$, for some $r, 1 \leq r \leq \delta - 1$, $0 \leq i \leq r - 1$, $1 \leq j \leq l$. All these cycles have even length since l is even by Lemma 10.

5.2. Factorization of $Q_2(v)$

Given a vertex $u \in Q_2(v)$, we represent $u = \{x, y, z\}$, where $2x' = x$, $2y' = y$, and $2z' = z$, by $[x', y', z']$. Since $x' + y' + z' = p$, in this subsection, all operations will be done modulo p. We must also change the representation of the automorphisms in U_v, and hence the new group of automorphisms is defined by

$$U_v' \triangleq \{\tilde{m} : m \in Z_p \text{ and } (m \in U_v \text{ or } m + p \in U_v)\}.$$

It is easily verified that $U_v' = \{\tilde{m} : m \in Z_p$ and m is a quadratic residue modulo $p\}$. Since for $m \in E(v)$ the order of m modulo p is equal to the order of m modulo $v = 2p$, it follows that w is a generator of U_v' iff w or $w + p$ is a generator of U_v. Also, for $[x, y, z] \in Q_2(v)$, $\{2x, 2y, 2z\}U_v \cong [x, y, z]U_v'$, where a vertex $[x', y', z'] \in [x, y, z]U_v'$ is isomorphic to the vertex $\{2x', 2y', 2z'\} \in \{2x, 2y, 2z\}U_v$. To denote the orbit of a vertex $[1, x, y] \in Q_2(v)$ we will use the same notation used for the orbits of $Q_1(v)$. Thus, the orbit of a vertex $[1, x, y]$ is denoted by $[x]$ or $[y]$. Note that since we changed the vertices representation, the derivatives definition should also be changed. Similarly to $OQ_1(v)$ we define $OQ_2(v)$ and Lemma 5 holds also for $OQ_2(v)$.

Let $u = [x, y, z]$, and let $\tilde{w}$ be a generator of U_v'. Since p is prime, there exist k, such that $k = x^{-1}$, and there exist i, $0 < i \leq \delta - 1$, such that $x = \pm w^i$. It follows that the vertex $u = [x, y, z] \in [1, yx^{-1}, zx^{-1}]U_v'$. Let $\gamma = yx^{-1}$, then $u \in [1, \gamma, -(1 + \gamma)]U_v'$, $u \in [1, 1/\gamma, -(1 + 1/\gamma)]U_v'$, and $u \in [1, -1/(1 + \gamma), -\gamma/(1 + \gamma)]U_v'$. These are the only vertices that contain 1 in the orbit of u, i.e., $u \in [\gamma] = [\gamma^{-1}] = [-(1 + \gamma)] = [-1/(1 + \gamma)] = [-(1 + 1/\gamma)] = [-\gamma/(\gamma + 1)]$. The only case when some of the numbers are equal is for the orbit $[1] = [(p - 1)/2] = [p - 2]$. This orbit corresponds to vertices of the form $[i, i, p - 2i]$, which are not included in T_v. Each orbit can be represented by three pairs $[x]$, $[x^{-1}]$, where $x, x^{-1} \in Z_p - \{0, 1, (p - 1)/2, p - 2, p - 1\}$, and therefore similarly to the proof in [15], [18],

LEMMA 11. *$Q_2(v)$ has $(\delta - 2)/3$ orbits.*

LEMMA 12. *The number of the vertices in $Q_2(v)$ is $[(n - 3)(n - 11)]/48$.*

Proof. By Lemma 3 and Lemma 11, $Q_2(v)$ has $(\delta - 2)/3$ orbits of length δ. Therefore, the number of vertices in $Q_2(v)$ is $\delta(\delta - 2)/3 = [(n - 3)(n - 11)]/48$. □

For $1 \leq x \leq p - 2$, let $x^* = \min\{x, p - 1 - x\}$, $\kappa(x) = \{x^*, (x^{-1})^*, -(1 + x)^{-1}*\}$. Note that $[x]$ and $[p - 1 - x]$ represent the same orbit in $OQ_2(v)$, and that $\kappa(x)$ contains the three representative of the orbit $[x]$ in $OQ_2(v)$ which are less than $(p - 1)/2$. We partition the vertices in $OQ_2(v)$ into two sets. The first set contains all the orbits $[y]$, such that there exists $x \in \kappa(y)$ with $\kappa(y) = \{x, -(x + 1)/x, -x/(x + 1)\}$. The second set contains all the orbits $[y]$, such that there exists $x \in \kappa(y)$ with $\kappa(y) = \{x, -1/(x + 1), -(x + 1)/x\}$. We will call the vertices in the first set *blue* vertices, and the vertices in the second set *red* vertices.

A vertex $[x]$ of $OQ_2(v)$ has degree 3, for its three derivatives with exceptions in the following three cases:

Case 1. One of the derivatives of $[x]$ is $[y]$, where $y \in \{0, 1, (p-1)/2, p-2, p-1\}$. In this case $[x] = [2] = [(p-2)/3] = [(p-3)/2] = [p-3] = [(2p-1)/3] = [(p+1)/2]$. The other two derivatives of $[x]$ are $[3]$ and $[(p-5)/2]$. Hence, the vertex $[2]$ has degree 2.

Case 2. One of the derivatives of $[x]$ is $[x]$. As in Siemon [19], we have to solve the equations $x^{-1} = x$ and $-x = -(1+x)^{-1}$. The solutions of the first equation are $\pm\sqrt{1}$, but -1 is not a quadratic residue for $p \equiv 11 \pmod{24}$. The solutions of the second equation are $(-1 \pm \sqrt{5})/2$ which corresponds to one orbit $[(1+\sqrt{5})/2]$. The only derivative of $[(1+\sqrt{5})/2]$ which is different from $[(1+\sqrt{5})/2]$ is $[(3+\sqrt{5})/2]$, and hence the degree of $[(1+\sqrt{5})/2]$ is 1. To complete this case we have to find when 5 is a quadratic residue modulo $p = 11 + 24k$. Since 5 and $11 + 24k$ are primes, we can use Lemmas 7 and 9 and obtain:

$$\left(\frac{5}{11+24k}\right) = \left(\frac{11+24k}{5}\right) = \left(\frac{1+4k}{5}\right)$$

Since

$$\left(\frac{1}{5}\right) = 1; \left(\frac{2}{5}\right) = -1; \left(\frac{3}{5}\right) = -1; \left(\frac{4}{5}\right) = 1;$$

it follows that 5 is a quadratic residue modulo $p = 11 + 24k$ iff $k \equiv 0$ or $2 \pmod 5$.

Case 3. Some of the derivatives of $[x]$ are equal, for $[x] \neq [(1+\sqrt{5})/2]$. Again, as in Siemon [19], this is possible only when $-x = -(x^{-1}+2)$ and the solutions are $1 \pm \sqrt{2}$. But, this is impossible since in the proof of Lemma 10 we showed that 2 is not a quadratic residue modulo $p \equiv 11 \pmod{24}$.

Thus, we have the following

LEMMA 13. *Consider the graph $OQ_2(v)$, where $v = 2p$ and $p = 11 + 24k$.*

- *If $k \equiv 1, 3$ or $4 \pmod 5$ then the degree of the vertex $[2]$ is two. The degree of all the other vertices is three.*
- *If $k \equiv 0$ or $2 \pmod 5$ then the degree of the vertex $[2]$ is two, the degree of the vertex $[(1+\sqrt{5})/2]$ is one, and the degree of all the other vertices is three.*

LEMMA 14 [18]. *The vertices $[x]$, $[y]$ are connected by an edge iff there exist $u \in \kappa(x)$, and $v \in \kappa(y)$ such that $|v-u| = 1$. Furthermore, if $([x], [y])$ is an edge in $OQ_2(v)$, then there exist $u_1, u_2 \in \kappa(x)$ and $v_1, v_2 \in \kappa(y)$ such that $u_1 \neq u_2$, $v_1 \neq v_2$, $|v_1 - u_1| = 1$, and $|v_2 - u_2| = 1$. If there exist three different pairs $|v_1 - u_1| = |v_2 - u_2| = |v_3 - u_3| = 1$, such that $v_1, v_2, v_3 \in \kappa(y)$, $u_1, u_2, u_3 \in \kappa(x)$ then the degree of $[x]$ and $[y]$ is less than three.*

Lemma 14 implies that for a vertex t, such that $\kappa(t) = \{x, y, z\}$ and the degree of $[t]$ is 3, all the six numbers, $x-1, x+1, y-1, y+1, z-1, z+1$, appear in the vertices

adjacent to $[t]$. Siemon [19] observed, that from each vertex $[t]$, where $\kappa(t) = \{x, y, z\}$, there are edges to the vertices $[x - 1]$, $[x + 1]$, $[y - 1]$, $[y + 1]$, $[z - 1]$, $[z + 1]$, if these vertices exist. By using this property one can easily prove,

LEMMA 15 [15]. *$OQ_2(v)$ is connected.*

We now define two types of edges in $OQ_2(v)$. Consider two orbits $[x]$, $[y] \in OQ_2(v)$, such that there exist $x_1, x_2 \in \kappa(x)$ $y_1, y_2 \in \kappa(y)$, and $|y_1 - x_1| = |y_2 - x_2| = 1$. An edge $([x], [y])$ is a *blue* edge if $y_1 - x_1 = y_2 - x_2 \in \{-1, 1\}$. An edge $([x], [y])$ with $y_1 - x_1 = -1$ and $y_2 - x_2 = 1$, is a *red* edge. Consider a vertex $[x]$, $\kappa(x) = \{x, y, z\}$, $2 < x, y, z < (p - 1)/2$. Since $[x]$ is adjacent to $[x - 1]$, $[x + 1]$, $[y - 1]$, $[y + 1]$, $[z - 1]$, $[z + 1]$, it follows that each vertex in $OQ_2(v)$ (except [2]) has either two blue edges, and one red edge, or three red edges (some of the edges can be self loops, as in the case of $[(1 + \sqrt{5})/2]$) while [2] has only two blue edges. Note that the blue edges form disjoint cycles in $OQ_2(v)$.

LEMMA 16. *A blue vertex $[x] \neq [2]$ is adjacent to two blue edges and one red edge. A red vertex, is adjacent to three red edges.*

Proof. Consider the derivatives of both types of edges.

blue vertex: By definition, if $[x]$ is a blue vertex then $\kappa(x) = \{x, -(x + 1)/x, -x/(x + 1)\}$.

$$[x]' = [-x] = [x - 1] = \left[-\frac{1}{x}\right] = \left[-\frac{x+1}{x}+1\right]$$

$$[x]'' = [-(x + 2)] = [x + 1] = \left[\frac{1}{x+1}\right] = \left[-\frac{x}{x+1}+1\right]$$

$$[x]''' = \left[-\left(\frac{1}{x}+2\right)\right] = \left[-\frac{2x+1}{x}\right] = \left[-\frac{x+1}{x}-1\right] = \left[-\frac{2x+1}{x+1}\right] = \left[-\frac{x}{x+1}-1\right]$$

Thus, the edge $([x], [x]')$ is a red edge, and the edges $([x], [x]'')$ $([x], [x]''')$ are blue.

red vertex: By definition, if $[x]$ is a red vertex then $\kappa(x) = \{x, -1/(x + 1), -(x + 1)/x\}$.

$$[x]' = [-x] = [x - 1] = \left[-\frac{1}{x}\right] = \left[-\frac{x+1}{x}+1\right]$$

$$[x]'' = [-(x + 2)] = [x + 1] = \left[-\frac{x+2}{x+1}\right] = \left[-\frac{1}{x+1}-1\right]$$

$$[x]''' = \left[-\left(\frac{1}{x}+2\right)\right] = \left[-\frac{2x+1}{x}\right] = \left[-\frac{x+1}{x}-1\right] = \left[\frac{x}{x+1}\right] = \left[-\frac{1}{x+1}+1\right]$$

Thus, all three edges are red. □

COROLLARY 5.

(1) *If* $([x], [y])$ *is a red edge, then there exists* $u \in \kappa(x)$ *and* $v \in \kappa(y)$ *such that* $uv = -1$.
(2) *If* $[x]$ *is a blue vertex, and* $([x], [y])$ *is its red edge, then* $\kappa(x) = \{x_1, x_2, x_3\}$, *where* $x_1x_2 = 1$ *and* $-x_3^{-1} \in \kappa(y)$.

Before preceding to the next theorem, we define the term of an unsigned inverse. Let $x \in GF(p)$, then $\tilde{x}^{-1}$, *the unsigned inverse* (modulo p) of x is defined as follows

$$\tilde{x}^{-1} = \begin{cases} x^{-1} \pmod p & \text{if } x^{-1} \leq \dfrac{p-1}{2} \\ -x^{-1} \pmod p & \text{otherwise} \end{cases}$$

An edge e of a connected undirected graph G is called a *bridge* if its deletion destroys the connectivity of G. In [19] Siemon showed that bridgelessness of $OQ_2(v)$ can be reduced to a number theoretic claim that he called "the complete interval conjecture." We found another necessary and sufficient condition to the existence of a bridge in $OQ_2(v)$.

THEOREM 2. *An edge* $([a-1], [a]) \in OQ_2(v)$ *is a bridge iff* $(p - 1 - a^{-1}) \in \kappa(a)$ *and the set* $I = \{a+1, \ldots, p-1-a^{-1}\}$ *is closed under unsigned inverse.*

The condition of Theorem 2 is easier to check with computer than the complete interval condition. We do not give a proof of Theorem 2 since it is long and there exists another condition which has a proof and can be also checked by computer. Using a computer program, we have verified that for all the primes $p \equiv 5 \pmod 6$, $p < 1500000$, there is no $a \neq (1+\sqrt{5})/2$, $2 < a$, $p - 1 - a^{-1} < (p-3)/2$, such that $(p - 1 - a^{-1} \in \kappa(a))$ and the set $\{a+1, \ldots, p-1-a^{-1}\}$ is closed under unsigned inverse.

In the following proof we use a generalization of Petersen's theorem,

THEOREM 3 [23, pp. 160–162]. *If* G *is a connected cubic bridgeless graph then* G *has a 1-factor. Furthermore, for each edge* e *in* G *there is a 1-factor which includes* e, *and there is a 1-factor which doesn't include* e.

In the following discussion we will use the notation $I_p \triangleq [2, \ldots, (p-3)/2]$.

THEOREM 4. *If* $p \equiv 11$ *or* $59 \pmod{120}$, $\alpha = (1+\sqrt{5})/2$, *and the set* I_p *does not contain any proper subset closed under unsigned inverse besides* $\{\alpha - 1, \alpha\}$ *then the graph* $OQ_2^-(v) \triangleq OQ_2(v) - \{[\alpha]\}$ *contains a 1-factor.*

Proof. By Theorem 2 if I_p does not contain any proper subset closed under unsigned inverse besides $\{\alpha - 1, \alpha\}$ then $OQ_2^-(v)$ is bridgeless.

By Lemma 13, $OQ_2^-(v)$ has two vertices $[2]$ and $[(3+\sqrt{5})/2]$ with degree two and all the other vertices has degree three. By connecting $[2]$ and $[(3+\sqrt{5})/2]$ with an edge, we obtain a cubic graph $OQ_2^+(v)$. Since $OQ_2^-(v)$ is bridgeless, it follows that $OQ_2^+(v)$ is

bridgeless. By Theorem 3, $OQ_2^+(v)$ has a 1-factor, which doesn't contain the edge $([2], [(3 + \sqrt{5})/2])$ and therefore, this 1-factor is also a 1-factor of $OQ_2^-(v)$. □

Let $([x], [y])$ be an edge in the 1-factor of $OQ_2^-(v)$. From the definition of $OQ_2(v)$ it follows, that there are vertices $u \in [x]$ and $v \in [y]$, $u, v \in Q_2(v)$, such that (u, v) is an edge in $Q_2(v)$. Since all the orbits of U_v' are of length δ, it follows from the properties of the automorphism that the vertices in $[x]$ and $[y]$ can be matched in pairs, such that each pair is connected by an edge in $Q_2(v)$. Thus, from the fact that $OQ_2^-(v)$ contains a 1-factor we have

COROLLARY 6. *If* $v \equiv 22$ *or* $118 \pmod{240}$, $v = 2p$, *and the set* I_p *does not contain any proper subset closed under unsigned inverse then the graph* $Q_2(v) - [\alpha]$ *contains a 1-factor.*

It is clear that either $(1 + \sqrt{5})/2$ or $-(1 + \sqrt{5})/2$ is a quadratic residue modulo p. Let $\hat{\alpha}$ be this quadratic residue, and let $o(\hat{\alpha}) = s$. Let β be a primitive root modulo p, and $\gamma = \beta^2$. One can verify that $\{\gamma^{ir} : 0 \le i \le s - 1\} = \{\alpha^i : 0 \le i \le s - 1\}$, where $\delta = rs$.

LEMMA 17. *If* $p = 11 + 24k$, *and* $k \equiv 0$ *or* $2 \pmod 5$ *then the vertices of* $[(1 + \sqrt{5})/2]$, *in* $Q_2(v)$ *create* r *cycles* $v_0^t - v_1^t \ldots - v_{s-1}^t$, $0 \le t \le r - 1$, *and for* $0 \le i \le s - 1$, $v_i^t = \gamma^{ir+t}[1, (1 + \sqrt{5})/2, -(1 + (1 + \sqrt{5})/2)]$.

Proof. By the proof of Lemma 13 for $k \equiv 0$ or $2 \pmod 5$, 5 is a quadratic residue modulo p. Now, let $c_i = v_i^0$, $0 \le i \le s - 1$,

$$c_0''' = \left[1, \frac{1 + \sqrt{5}}{2}, -\frac{3 + \sqrt{5}}{2}\right]''' = \left[-(2 + \sqrt{5}), \frac{1 + \sqrt{5}}{2}, \frac{3 + \sqrt{5}}{2}\right] =$$

$$\frac{1 + \sqrt{5}}{2}\left[1, \frac{1 + \sqrt{5}}{2}, -\left(1 + \frac{1 + \sqrt{5}}{2}\right)\right] = \frac{1 + \sqrt{5}}{2} c_0 = c_1$$

From the properties of the automorphism it follows that

$$c_i''' = \left(\left(\frac{1 + \sqrt{5}}{2}\right)^i c_0\right)''' = \left(\frac{1 + \sqrt{5}}{2}\right)^i c_0''' = \left(\frac{1 + \sqrt{5}}{2}\right)^i c_1 = c_{i+1}.$$

Note that $-\{x, y, z\} = \{x, y, z\}$ for each $\overline{\mathrm{DT}}$ $\{x, y, z\}$ in T_v. This proves for $t = 0$ and the properties of the automorphism implies the proof for $1 \le t \le r - 1$. □

6. The Construction of the Code

For $t = \{x, y, z\}$ let D_t be the set of difference pairs induced by t, i.e., $D_t = \{<x, y + z>, <y, x + z>, <z, x + y>\} = \{<x, -x>, <y, -y>, <z, -z>\}$. Two DTs, t and m, are *disjoint* if $D_t \cap D_m = \phi$. A set $T \subset T_v$ has *property D* if all the DTs in T are disjoint in pairs. In a set of DTs with property D, there are no two DTs which share a common difference pair. Thus, a code that contains words induced by a set of base DTs

with property D has weight 3 and minimum Hamming distance 4. The code C_1 which was defined in section 2, has minimum Hamming distance 4, iff the set B_1 has property D. The maximal set with property D in T_v has size $(n-5)/6$. Since each DT from $Q_1(v)$ contains one even element, and two odd elements, and each DT from $Q_2(v)$ contains three even elements, a set of size $(n-5)/6$ with property D must contain $(n-7)/8 = (\delta-1)/2$ DTs from $Q_1(v)$ and $(n+1)/24 = (\delta+1)/6$ DTs from $Q_2(v)$.

In the next lemma we present sets with property D of size $r \cdot \lfloor s/3 \rfloor$ (r and s are as defined in Lemma 17) from $Q_2(v)$, in the case $v = 22 + 48k$, and $k \equiv 0$ or 2 (mod 5). In this case we proved that 5 is a quadratic residue modulo p (Lemma 13), and hence it is also a quadratic residue module v. The set with property D that we need is a subset of $[(1+\sqrt{5})/2]$.

LEMMA 18. *For $v = 22 + 48k$, where $k \equiv 0$ or 2 (mod 5), $\alpha = (1+\sqrt{5})/2$, and γ as in Lemma 17, the set*

$$W = \left\{ \gamma^t[\alpha^k, \alpha^{k+1}, -(\alpha^k + \alpha^{k+1})] : 0 \le t \le r-1, k = 3i, 0 \le i < \left\lfloor \frac{s}{3} \right\rfloor \right\},$$

of vertices from $Q_2(v)$, has property D.

Proof. As we mentioned before (Lemma 11), 1 appears exactly three times in each orbit of U_v' on $Q_2(v)$, from the automorphism properties it follows that each even number in $Z_v - \{0\}$ appears three times in the difference pairs induced by the DTs in each orbit. Since $\alpha^i = \alpha^{i-1} + \alpha^{i-2}$ and $\gamma^t \notin \{\alpha^i : 0 < i \le s-1\}$, it follows that the DT $\gamma^t[\alpha^i, \alpha^{i+1}, -(\alpha^i + \alpha^{i+1})]$ has a common difference pair with the following five DTs of $[\alpha]$,

$$\begin{aligned}
&\gamma^t[\alpha^{i-2}, \alpha^{i-1}, -(\alpha^{i-2} + \alpha^{i-1}) = -\alpha^i] \\
&\gamma^t[\alpha^{i-1}, \alpha^i, -(\alpha^{i-1} + \alpha^i) = -\alpha^{i+1}] \\
&\gamma^t[\alpha^i, \alpha^{i+1}, -(\alpha^i + \alpha^{i+1}) = -\alpha^{i+2}] \\
&\gamma^t[\alpha^{i+1}, \alpha^{i+2}, -(\alpha^{i+1} + \alpha^{i+2}) = -\alpha^{i+3}] \\
&\gamma^t[\alpha^{i+2}, \alpha^{i+3}, -(\alpha^{i+2} + \alpha^{i+3}) = -\alpha^{i+4}].
\end{aligned}$$

Since the set $\{\gamma^t[\alpha^i, \alpha^{i+1}, -(\alpha^i + \alpha^{i+1})] : 0 \le i \le s-1\}$, contains s vertices, where $s \not\equiv 0 \pmod 3$, we can take from each such set at most $\lfloor s/3 \rfloor$ DTs, without violating property D. It follows that the set W has property D. □

Now we want to show that $Q(v)$ has sets of $(n-5)/6$ vertices with property D. Since these sets include vertices from $Q_1(v)$ and from $Q_2(v)$ we will represent a vertex $[x, y, z] \in Q_2(v)$ by the original notation $\{2x, 2y, 2z\}$ in order that all the integers in all the vertices will be residues modulo v.

Let $W_1^+ = \{\hat{\alpha}^{i+(\delta+1)/2}[y, \hat{\alpha}^{(\delta+1)/2}y, -y(1+\hat{\alpha}^{(\delta+1)/2})] : 0 \le i < (\delta-1)/2\}$ where y is the odd solution of the equation $x(1+\hat{\alpha}^{(\delta+1)/2}) \equiv 2 \pmod v$, and let $W_1^- = \{\hat{\alpha}^{i+(\delta+1)/2}[y, -\hat{\alpha}^{(\delta+1)/2}y, -y(1-\hat{\alpha}^{(\delta+1)/2})] : 0 \le i < (\delta-1)/2\}$, where y is the odd solution of the equation $x(1-\hat{\alpha}^{(\delta+1)/2}) \equiv 2 \pmod v$. Clearly, $x(1+\hat{\alpha}^{(\delta+1)/2}) \equiv 2 \pmod v$, has a unique

solution z modulo $p = v/2$. Since $1 + \hat{\alpha}^{(\delta+1)/2}$ modulo v is even, z and $z + p$ are the solutions of the same equation modulo v. Similar considerations lead to the conclusion that $x(1 - \hat{\alpha}^{(\delta+1)/2}) \equiv 2 (\text{mod } v)$ has a unique odd solution modulo v. Now, let W_1 equals either W_1^+ or W_1^-, $W_2 = \{\hat{\alpha}^{3i}\{2, 2\alpha, -2(1 + \alpha)\} : 0 \leq i < (\delta + 1)/6\}$, and $W^* = W_1 \cup W_2$.

THEOREM 5. *For $v = 22 + 48k$, where $k \equiv 0$ or 2 (mod 5), if $o(\hat{\alpha}) = \delta$ the set W^* of $(n - 5)/6$ vertices from $Q(v)$ has property D.*

Proof. Assume $W^* = W_1^+ \cup W_2$. Since $o(\hat{\alpha}) = \delta$, we can set $\gamma = \hat{\alpha}$ in the set W and therefore $W_2 \subseteq W$ and by Lemma 18 it has property D. All the vertices from W_1^+ belong to the orbit $[\hat{\alpha}^{(\delta+1)/2}]$ of $Q_1(v)$. As mentioned before (Lemma 4), 1 appears exactly twice in the vertices from each orbit of $Q_1(v)$, and from the properties of the automorphism it follows that each odd number t appears twice in the orbit $[\hat{\alpha}^{(\delta+1)/2}]$. It is easy to see that t appears in the vertices $u = [\hat{\alpha}^{(\delta+1)/2}t, t, -t(1 + \hat{\alpha}^{(\delta+1)/2})]$, and $\hat{\alpha}^{(\delta+1)/2}\, u$. Since $(\hat{\alpha}^{(\delta+1)/2})^2$ is equal to $\hat{\alpha}$ it follows that W_1^+ contains exactly one of these two vertices. Combining this with the fact that each even number appears exactly once in each orbit of $Q_1(v)$ we conclude that W_1^+ has property D.

Let y be the odd solution of the equation $x(1 + \hat{\alpha}^{(\delta+1)/2}) \equiv 2 (\text{mod } v)$. The difference pairs that W_1^+ induces contain only the following even numbers,

$$\left\{ \pm y(1 + \hat{\alpha}^{(\delta+1)/2})\hat{\alpha}^{i+(\delta+1)/2} : 0 \leq i < \frac{\delta - 1}{2} \right\} = \left\{ \pm 2\hat{\alpha}^{i+(\delta+1)/2} : 0 \leq i < \frac{\delta - 1}{2} \right\} =$$

$$\left\{ \pm 2(\hat{\alpha}^{(\delta+1)/2})^{2i+1} : 0 \leq i < \frac{\delta - 1}{2} \right\}.$$

The difference pairs induced by W_2 contain the following even numbers,

$$\left\{ \pm 2\hat{\alpha}^i : 0 \leq i < \frac{\delta + 1}{2} \right\} = \left\{ \pm 2(\hat{\alpha}^{(\delta+1)/2})^{2i} : 0 \leq i < \frac{\delta + 1}{2} \right\}$$

and therefore both sets are disjoint.

The same arguments hold for $W^* = W_1^- \cup W_2$. □

A *k-isolated 1-factor* in a graph $G = (V, E)$ is a subgraph $G' = (V, E')$ such that the degree of k vertices in G' is 0, and the degree of all the other vertices is 1. A k-isolated 1-factor of $Q(v)$ is said to have property D if the set of isolated vertices has property D. Our purpose is to find an $(n - 5)/6$-isolated 1-factor with property D in $Q(v)$. The edges of a k-isolated 1-factor with property D in $Q(v)$, will be the base DQs of the form $<x, y, x, z>$ of B_2. The $(n - 5)/6$ base $\overline{\text{DT}}$s $\{x, y, z\}$ of B_1 will be chosen from the isolated vertices, one from each vertex. Each one of the $\overline{\text{DT}}$s represented by the vertex can be chosen.

THEOREM 6. *If* $v \equiv 22$ *or* $118 \pmod{240}$, *and the order of* $\alpha = (1 + \sqrt{5})/2$ *is not* 5, 10 (*if* $n > 23$), 7 *or* 14, *and* I_p, $v = 2p$, *does not contain any proper subset closed under unsigned inverse besides* $\{\alpha - 1, \alpha\}$, *then* $Q_2(v)$ *has an* $(n + 1)/24$*-isolated* 1*-factor with property D.*

Proof. As proved in Lemma 18 W has property D. By Lemma 17 all the DTs in W belong to cycles in $Q_2(v)$ of length s, where $s = o(\hat{\alpha})$. Lemma 17 also implies that the DTs from W appear in the following vertices in these cycles (r and s are as defined in Lemma 17),

$$W = \left\{ v_k^t \colon 0 \le t \le r - 1,\ k = 3i,\ 0 \le i < \left\lfloor \frac{s}{3} \right\rfloor \right\}$$

Now, for odd $\lfloor s/3 \rfloor$, let $m = \lfloor s/3 \rfloor$ and $m = \lfloor s/3 \rfloor - 1$ otherwise. By Theorem 4 and Lemma 17, it is clear that the first m vertices from W on each such cycle can be completed to an isolated 1-factor of $Q_2(v)$. A simple calculation shows that unless the order of $(1 + \sqrt{5})/2$ is 5, 10 (if $n > 23$), 7 or 14, the number of isolated vertices, rm, is at least $(\delta + 1)/6$. Hence, $Q_2(v)$ has an $(n + 1)/24$-isolated 1-factor with property D. □

In Theorem 5, we showed that when $o(\hat{\alpha}) = \delta$, each set W^* has size $(n - 5)/6$ and property D. In Theorem 6 we have constructed an $(n + 1)/24$-isolated factor with property D of $Q_2(v)$. When $o(\hat{\alpha}) = \delta$ the $(n + 1)/24$ isolated vertices from $Q_2(v)$ belong to W_2. To complete the construction of the code we have to show that after removing the $(n - 7)/8 = (\delta - 1)/2$ vertices that belong to W_1 from $Q_1(v)$, the rest of $Q_1(v)$ contains a 1-factor. We believe that there are many different 1-factors in the subgraph of $Q_1(v)$ induced by the remaining vertices. We used a check program that checks if one certain type of a 1-factor exists in the above subgraph.

By Theorem 1, $Q_1(v)$ can be factored into δ isomorphic paths, h_i, $0 \le i < \delta$ of even length $\delta - 1$. Since $o(\hat{\alpha}) = \delta$, we set $h_i = \hat{\alpha}^i h_o$. The h_is contain only third and second derivative edges. It is not difficult to show that each two of the h_is are connected by exactly one first derivative edge, the location of which can be calculated. In order to find a 1-factor in the subgraph induced by all the vertices which are not *isolated*, we use the first derivative edges. Recall that the $(\delta - 1)/2$ vertices from $Q_1(v)$ that belong to W_1 were taken from a single orbit (either $[\hat{\alpha}^{(\delta+1)/2}]$ or $[-\hat{\alpha}^{(\delta+1)/2}]$). Hence, the $(\delta - 1)/2$ vertices which belong to W_1 appear in the same location in each h_i, $0 \le i < (\delta - 1)/2$. The h_is are of even length and therefore by taking out those vertices we are left with $(\delta - 1)/2$ paths of odd length, $h_{i,odd}$, and $(\delta - 1)/2$ paths of even length, $h_{i,even}$, $0 \le i < (\delta - 1)/2$. $(\delta - 1)/2$ is even and hence the paths h_i, $0 \le i < (\delta - 1)/2$ can be partitioned into pairs, (h_i, h_j), $i \ne j$. In our check program we allowed only pairs such that $2(i - j)$ divides $(\delta - 1)/2$, so that we have only to check one such pair, h_0 and its pair mate, and by the automorphism properties the situation is exactly the same with all the other $(\delta - 5)/4$ pairs. From now on we refer only to the pair h_0, h_i. Both h_0 and h_i have a single first derivative edge connecting them to a third path h_k, $k \notin \{0, i\}$. The check program goes through all the possible pairs of i and k, and checks if the first derivative edges leave h_0 and h_i from even locations in $h_{0,odd}$ *and* $h_{i,odd}$ and reaches h_k in one even location and one odd location in $h_{k,even}$, where the even location is before the odd one. In this case we have an $(n - 5)/6$-isolated 1-factor in $Q(v)$. The scenario is depicted in Figure 1.

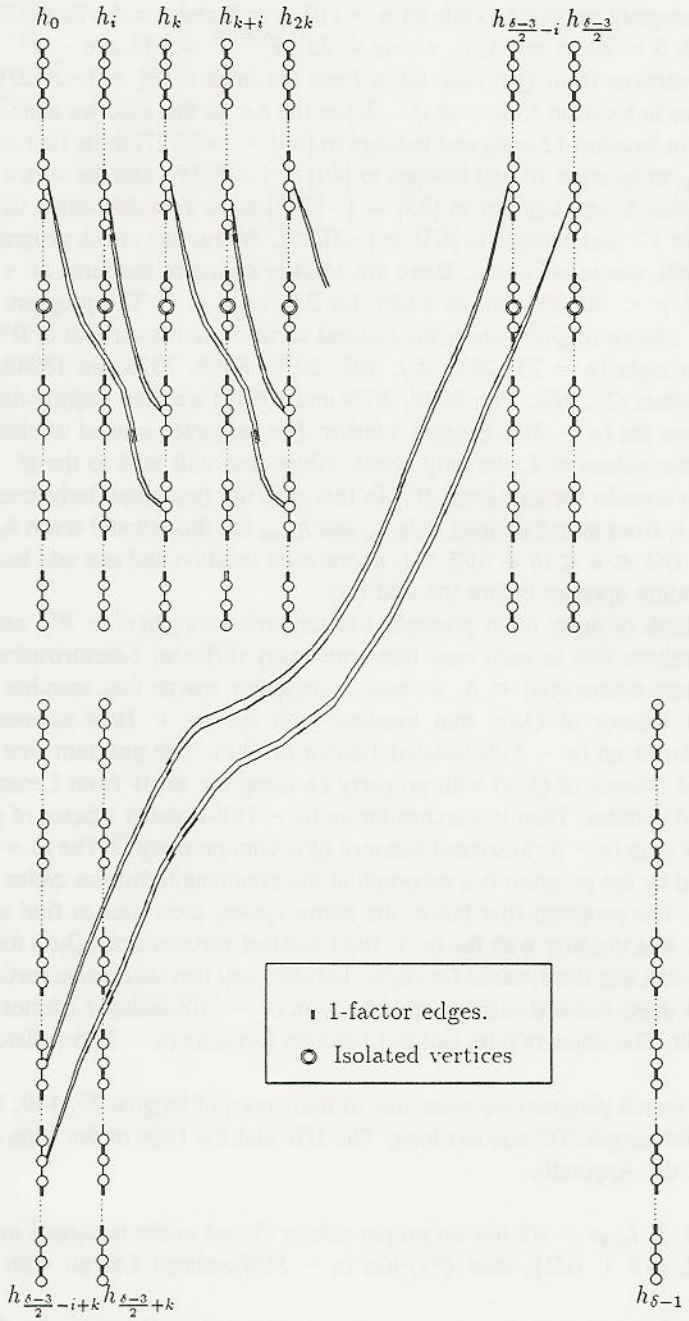
h_0
h_i
h_k
h_{k+i}
h_{2k}
$h_{\frac{\delta-3}{2}-i}$
$h_{\frac{\delta-3}{2}}$
1-factor edges.
Isolated vertices
$h_{\frac{\delta-3}{2}-i+k}$
$h_{\frac{\delta-3}{2}+k}$
$h_{\delta-1}$

Figure 1.

Using the program we found a code for $n = 119$, $w = 4$ and $d = 4$ with 67850 codewords. For $n = 119$, $\delta = 29$, $\alpha = 93$, $\hat{\alpha} = -\alpha = 25$, $\hat{\alpha}^{(\delta+1)/2} = 113$ and $-\hat{\alpha}^{(\delta+1)/2} = 5$. All the isolated vertices from $Q_1(v)$ are taken from the orbit $[113] = [-29/27] = [\hat{\alpha}^{(\delta+1)/2}]$ which appears in location 13 (out of $0 \ldots 27$) in the h_is. In this case we connect the vertex that appears in location 12 in h_0 and belongs to $[69] = [-25/27]$ to its first derivative that appears in h_{16} in location 16 and belongs to $[49] = [-33/35]$; and the vertex that appears in h_7 in location 8, and belongs to $[55] = [-17/19]$ to its first derivative that appears in h_{16} in location 17, and belongs to $[63] = [-37/35]$. We ran the check program for values of $n < 600000$, where $o(\hat{\alpha}) = \delta$. There are 1624 primes p of the form $11 + 24k$, $k \equiv 0$ or 2(mod 5), $p < 300000$, out of which for 246 $o(\hat{\alpha}) = \delta$. The program found $(n - 5)/6$-isolated 1-factor of $Q(v)$, where the isolated vertices are the vertices of W^* for all these values except eight ($n = 23$, 263, 359, 503, 2039, 3863, 7079 and 13943). For six of these eight values (23, 263, 359, 2039, 7079 and 13943) we used slightly different structure to achieve the $(n - 5)/6$-isolated 1-factor. For example, instead of checking all the $\delta - 2$ possible values of k, we only check values that will lead to the $(\delta + 1)/2$ paths which do not contain vertices from W_1. In this case the first edge derivative still have to leave h_0 and h_i from even locations in $h_{0,odd}$ and $h_{i,odd}$ but they should reach h_k (rather than $h_{k,odd}$), $(\delta - 1)/2 \leq k < (\delta + 3)/2 + i$, in one even location and one odd location, where the even location appears before the odd one.

One can think of many other possible 1-factorizations of $Q_1(v) - W_1$, and as we said before, we believe that in each case there are many different 1-factorizations.

For the cases where $o(\hat{\alpha}) < \delta$, we have a computer search that searches for an $(n - 7)/8$-isolated 1-factor of $Q_1(v)$ that together with the $(n + 1)/24$-isolated 1-factor of Theorem 6 forms an $(n - 5)/6$-isolated 1-factor of $Q(v)$. The program first builds $(n + 1)/24$-isolated 1-factor of $Q_2(v)$ with property D, using the set W from Lemma 18, as the set of isolated vertices. Then it searches for an $(n - 7)/8$-isolated 1-factor of $Q_1(v)$, whose union with W is an $(n - 5)/6$-isolated factor of $Q(v)$ with property D. The $(n - 7)/8$-isolated 1-factor found by the program is a subgraph of the even length disjoint cycles of $Q_1(v)$ (see Lemma 10). The program first builds the above cycles, then tries to find a set of $(n - 7)/8$ vertices, that together with the $(n + 1)/24$-isolated vertices from $Q_2(v)$ form a set with property D, such that the distance (in edges) between any two successive vertices in a cycle is odd. After those isolated vertices are found, an $(n - 7)/8$-isolated 1-factor of $Q_1(v)$ can be easily built. The union of both isolated 1-factors forms an $(n - 5)/6$-isolated 1-factor in $Q(v)$.

Using the search program we were able to find codes of lengths 23, 119, 263 and 359. The search for length 503 was too long. The DTs and the DQs of the code of length 23, are given in the Appendix.

Conjecture 1. If I_p, $p = v/2$ has no proper subset closed under unsigned inverse, except $\{(\sqrt{5} - 1)/2, (\sqrt{5} + 1)/2\}$, then $Q(v)$ has $(n - 5)/6$-isolated 1-factor with property D.

Using the above two constructions we found extended cyclic codes for 244 values of $n < 600000$.

7. Other 1-Rotational Packings of Quadruples

In this section we discuss possible constructions of extended cyclic codes for all the other cases of $n \equiv 5 \pmod 6$. To achieve the upper bound of $(n-1)(n^2-3n-4)/24$, except for $n \equiv 23 \pmod{24}$ the code must contain some cycles which are not of full length.

(1) for $n \equiv 5 \pmod{24}$, the code must contain one cycle of length $(n-1)/4$.
(2) for $n \equiv 11 \pmod{24}$, the code must contain at least one cycle of length $(n-1)/2$.
(3) for $n \equiv 17 \pmod{24}$, the code must contain one cycle of length $(n-1)/4$, and at least one cycle of length $(n-1)/2$.

We believe in all these cases there exist codes in which all the other cycles are of full length. A cycle of length $(n-1)/4$, is induced by the DQ $<(n-1)/4, (n-1)/4, (n-1)/4, (n-1)/4>$, and it contains the DT $<(n-1)/4, (n-1)/4, (n-1)/2>$. A cycle of length $(n-1)/2$, is induced by the DQ $<i, j, i, j>$, where $i + j = (n-1)/2$, and it contains the DTs $<i, j, (n-1)/2>$ and $<j, i, (n-1)/2>$. Note that the construction we used, matched all triples of the form $<i, j, (n-1)/2>$, with the triples $<i, i, n-1-2i>$ and $<j, j, n-1-2j>$, to create all the quadruples of the form $<i, i, j, j>$. Thus, in all the cases where an optimal extended cyclic code must contain a cycle of length $(n-1)/2$, i.e., when $n \equiv 11$ or $17 \pmod{24}$, the code cannot include all the DQs of the form $<i, i, j, j>$.

In the cases where $n \equiv 5 \pmod{24}$, the DQ $<(n-1)/4, (n-1)/4, (n-1)/4, (n-1)/4>$, induced by the DT $<(n-1)/4, (n-1)/4, (n-1)/2>$, must be added to the code. Thus, $(n-5)/4$ DQs of the form $<i, i, j, j>$ containing all the DTs of the form $<i, i, n-1-2i>$ and $<i, j, (n-1)/2>$, can be added to the code, and the vertex set of $Q(n-1)$ remains the same. The size of the vertex set of $Q(n-1)$ in this case is $((n-5)(n-6))/12$, out of which an $(n-5)/6$-isolated 1-factor should be picked. In this case $Q_1(n-1)$ contains $((n-5)(n-3))/16$ vertices, and it should have an $(n-5)/8$-isolated 1-factor. The size of $Q_2(n-1)$ is $((n-5)(n-15))/48$, and it should have an $(n-5)/24$-isolated 1-factor. Since for $n \equiv 5 \pmod{48}$ the sizes of both graphs and the sizes of the isolated factors are even, the construction is feasible. For $n \equiv 29 \pmod{48}$ the graphs contain odd numbers of vertices, and the sizes of the isolated factors are odd too, thus the construction is feasible in this case too. But in this case, since $n \equiv 5 \pmod{24}$, $(n-1)/2 \equiv 2 \pmod{12}$, which is not a prime, the isolated factors should be picked in a different way.

Using a search program, that finds an $(n-5)/6$-isolated 1-factor of an hypergraph, whose vertices are all the DTs and edges are all the DQs, we were able to find an optimal extended cyclic code of length $n = 29$, weight $w = 4$, and minimum Hamming distance $d = 4$, of size 875 (see the Appendix), thus proving that $A(29, 4, 4) \geq 875$. This code contains all the DQs of the form $<i, i, j, j>$. Our search program uses a heuristic used by Diener [24] and Phelps [21] for the purpose of enumerating cyclic SQSs.

For $n \equiv 47 \pmod{48}$ the size of vertex set of $Q_1(n-1)$, is $((n-3)(n-7))/16$, thus $Q_1(v)$ contains an even number of vertices. But, like in the case of $n \equiv 23 \pmod{48}$, it should have an $(n-7)/8$-isolated 1-factor, and since $(n-7)/8$ is odd when $n \equiv 47 \pmod{48}$, this is clearly impossible. Hence, the code cannot include all the DQs of the form $<i, i, j, j>$.

The other cases of $n \equiv 23 \pmod{48}$ are the cases when $n \equiv 167$ or $215 \pmod{240}$. In these cases the graph $OQ_2(n-1) - \{[2]\}$ has a 1-factor, provided again that $I_{(n-1)/2}$ does not contain any proper subset closed under unsigned inverse (the proof is slightly different from the proof of Theorem 4), but the $(n+1)/24$-isolated 1-factor from $Q_2(v)$ should be chosen in a different way. Using a search program we found an extended cyclic code with $n = 167$, $w = 4$ and $d = 4$ that contains 189,406 words. The program finds the cycles in $Q_1(166)$ with the techniques implied by the proof of Lemma 10. In this case, only one cycle that contains 6806 vertices is created. $Q_2(166)$ also contains a Hamiltonian cycle, whose length is 2241, and the program found a 27-isolated 1-factor in $Q(166)$.

8. S-cyclic $SQS(4p)$

The analysis of Köhler orbit graph and the analysis of the sequence in Lemma 6 can be used also for generating S-cyclic $SQS(4p)$, for p prime, $p \equiv 5 \pmod{12}$. Our code $C = C_o \cup C_1$, where C_0 contains all the DQs of the form $<i, i, j, j>$ as in Section 2. Note that $<p, p, p, p>$ is a DQ in C_0.

The set T_n, $n = 4p$, and the graph $Q(4p)$ are defined as in Section 3. T_n is partitioned into three subsets:

1. $\{<x, y, z> : 2 \nmid x,\ 2 \nmid y,$ and $2|z\}$
2. $\{<x, y, z> : 4 \nmid x,\ 4 \nmid y,\ 2|x,\ 2|y,$ and $4|z\}$
3. $\{<x, y, z> : 4|x,\ 4|y,$ and $4|z\}$

$Q(4p)$ is partitioned into three subgraphs, $Q_i(4p)$, $1 \le i \le 3$, contains vertices from the set i. Note that in $Q(4p)$ there is no edge connecting vertex from $Q_i(4p)$ to $Q_j(4p)$ for $i \neq j$. One can easily verify that

LEMMA 19. *$Q_2(4p)$ is isomorphic to $Q_1(2p)$, and $Q_3(4p)$ is isomorphic to $Q_2(2p)$*

By combining Lemma 19, and the results of Siemon [19], we infer

COROLLARY 7.

1. *$Q_2(4p)$ has a 1-factor.*
2. *If I_p, $p = n/4$, contains no proper subset closed under unsigned inverse beside $\{\alpha - 1, \alpha\}$, where $\alpha = (1 + \sqrt{5})/2$, then $Q_3(4p)$ has a 1-factor.*

Now, we have to show that $Q_1(4p)$ has a 1-factor. Recall that $E(m)$ is the multiplicative group of residues between 1 and $m - 1$ modulo m, relatively prime to m.

LEMMA 20. *There exists an element $w \in E(4p)$ such that $o(w) = 2\delta$, $\delta = (p-1)/2$, and $w^{\delta} \equiv 2p - 1 \pmod{4p}$.*

Proof. Let w be a generator of $E(2p)$. Therefore $o(w) = 2\delta$ in $E(2p)$ and $w^\delta \equiv -1 \pmod{2p}$. Hence, w^δ can be equal either to $2p - 1$ or to $4p - 1$ modulo $4p$.

$$w^\delta = (1 + (w - 1))^\delta = \sum_{i=0}^{\delta} \binom{\delta}{i} (w - 1)^i = 1 + \sum_{i=1}^{\delta} \binom{\delta}{i} (w - 1)^i$$

Since $w - 1$ and δ are even, $\Sigma_{i=1}^{\delta} \binom{\delta}{i} (w - 1)^i$ is divisible by 4 and therefore $w^\delta \equiv 1 \pmod 4$. Hence, $w^\delta \equiv 2p - 1 \pmod{4p}$, and $o(w) = 2\delta$ in $E(4p)$. □

Let $E^+(4p) = \{w^i : 0 \le i \le 2\delta - 1\}$ be the cyclic subgroup of $E(4p)$ generated by an element $w \in E(4p)$, $o(w) = 2\delta$, and $w^\delta \equiv 2p - 1 \pmod{4p}$. Since $4p - 1 \notin E^+(4p)$, we have

$$E(4p) = E^+(4p) \cup E^-(4p),$$

where $E^-(4p) = \{-w^i : 0 \le i \le 2\delta - 1\}$. Let U be the automorphism group of $Q_1(4p)$ defined in Section 4. Since $m\{x, y, z\} = -m\{x, y, z\}$, $U = \{\tilde{m} : m \in E^+(4p)\}$, where $\tilde{m}$ is the automorphism defined by $\tilde{m} : \{x, y, z\} \to m\{x, y, z\}$, it follows that $|U| = 2\delta$. Since $-1 \notin E^+(4p)$ it follows that

LEMMA 21. *The orbit of* $\{x, y, z\} \in T_n$ *under* U *is*

$$\{x, y, z\}U = \{\tilde{w}^i(\{x, y, z\}) : 0 \le i \le 2\delta - 1\},$$

where w *is a generator of* $E^+(4p)$.

Henceforth, let w be a generator of $E^+(4p)$.

LEMMA 22. *The orbits of* U *on* $Q_1(4p)$ *are*

(1) $\{[\pm w^i]\}_{i=1}^{\delta-1}$ *each one of length* 2δ.
(2) $[-w^\delta] = [2p + 1]$ *of length* δ.
(3) $[p]$, $[3p]$ *of length* 2δ.

Proof. Since $-1 \notin E^+(4p)$ one can prove similarly to Lemma 4 that the elements of (1) and (2) are distinct. Since there is no i, such that $w^i = p$ or $3p$, and since $px = -3px$ for $x \in E(4p)$, it follows that (3) contains two distinct orbits, which do not appear in (1) and (2). Clearly only odd numbers can represent orbits in $Q_1(4p)$. The only odd numbers which are not covered in (1), (2) and (3), or by their inverses are 1, -1 and $2p - 1$. The orbit [1] contains all the DTs of the form $\{i, i, n - 2i\}$ such that i is odd: and the orbit $[2p - 1]$ contains all the DTs of the form $\{i, j, 2p\}$ such that i and j are odd. These DTs do not belong to T_n. Finally $[-1]$ does not represent an orbit. Hence, (1), (2) and (3) are all the representatives of the orbits of $Q_1(4p)$.

To calculate the length of orbits from (1) and (2) we use a method similar to the proof of Lemma 3, but in this case if $w^r x = y$, $w^r y = x$, and $w^r z = z$ (or $w^r x = -y$, $w^r y = -x$ and $w^r z = z$), then $w^{2r} = 1$, and $r = \delta$. Hence, $w^\delta x = y$ or $w^\delta x = -y$, and therefore

either $[x, y, z] \in [w^\delta]$ or $[x, y, z] \in [-w^\delta]$. Since $w^\delta = 2p - 1$ and $-w^\delta = 2p + 1$ it follows that $[-w^\delta] = [2p + 1]$ is of length δ. We already showed that the orbit $[w^\delta] = [2p - 1]$ does not belong to $OQ_1(4p)$. Hence, the only orbit from (1) and (2) of length δ is $[-w^\delta] = [2p + 1]$, and all the orbits from (1) are of length 2δ.

For the orbits $[p]$ and $[3p]$, note that the first element in each DT in these orbits is relatively prime to p and the second is a multiple of p. These orbits have length 2δ since $-1 \notin E^+(4p)$, $E^+(4p) = \{w^i : 0 \leq i \leq 2\delta - 1\}$. □

We next define the orbit graph of U on $Q_1(4p)$, in a similar way to Section 5. We show that $OQ_1(4p)$ contains a Hamiltonian path.

LEMMA 23.

(1) $[2p + 1]$ *is adjacent only to* $[2p - 3]$, *and each vertex from* $[2p + 1]$ *is connected to two vertices* $u, v \in [2p - 3]$, *such that* $u = w^\delta v$.
(2) $[p]$ *and* $[3p]$ *are adjacent.*
(3) *Let* v *be a vertex from* $[p]$ or $[3p]$, *then* $v''' = w^\delta v$.

Proof.

(1) $[2p + 1]' = [2p - 1]$ which does not belong to $OQ_1(4p)$. $(2p + 1)^{-1} \equiv 2p + 1 \pmod{4p}$, and hence $[2p + 1]'' = [2p + 1]''' = [2p - 3]$. Consider a vertex $t \in [2p + 1]$, $t = w^i[1, 2p + 1, 2p - 2]$, $0 \leq i \leq \delta - 1$. $t'' = w^i[1, 2p - 3, 2p + 2]$ and $t''' = w^i[2p - 1, 3, 2p - 2] = (2p - 1)w^i[1, 2p - 3, 2p + 2] = w^\delta t''$.
(2) $[p]' = [-p] = [3p]$.
(3) Consider a vertex $v \in [p]$. $v = [x, px, -x(p + 1)]$. $v''' = [x(2p - 1), px, x(p + 1)] = (2p - 1)[x, px, -x(p + 1)] = w^\delta v$. The proof for $v \in [3p]$ is similar. □

Let $\{x_i\}$, and $\{y_i\}$, $0 \leq i \leq 2\delta - 1$ be the sequences defined as follows

$$x_i = \begin{cases} 1 & \text{if } i = 0 \\ -(x_{i-1} + 2) & \text{if } i \text{ is odd} \\ x_{i-1}^{-1} & \text{if } i \neq 0 \text{ and } i \text{ is even} \end{cases}$$

$$y_i = \begin{cases} 2p + 1 & \text{if } i = 0 \\ -(y_{i-1} + 2) & \text{if } i \text{ is odd} \\ y_{i-1}^{-1} & \text{if } i \neq 0 \text{ and } i \text{ is even} \end{cases}$$

where the computations are done modulo $4p$. Similarly to the proof of Lemma 6 one can prove,

LEMMA 24. *The sequences* $\{x_i\}$ *and* $\{y_i\}$ *has the following properties:*

(1) *All the* x_i*s and the* y_i*s are odd.*

(2) *For* $0 \le j \le \delta/2 - 1$,

$$x_{4j+1} = -\frac{3+4j}{1+4j};\ x_{4j+2} = -\frac{1+4j}{3+4j};\ x_{4j+3} = -\frac{5+4j}{3+4j};\ x_{4j+4} = -\frac{3+4j}{5+4_j}$$

$$y_{4j+1} = 2p - \frac{3+4j}{1+4j};\ y_{4j+2} = 2p - \frac{1+4j}{3+4j};\ y_{4j+3} = 2p - \frac{5+4j}{3+4j};\ y_{4j+4} = 2p - \frac{3+4j}{5+4j}$$

(3) $x_{2\delta-1} = p$, and $y_{2\delta-1} = 3p$.
(4) *All the* x_i*s and the* y_i*s are distinct.*
(5) *When i is odd,* x_i *is the second derivative of* x_{i-1}, y_i *is the second derivative of* y_{i-1}, x_i *is the third derivative of* x_{i-2}, *and* y_i *is the third derivative of* y_{i-2}.

From Lemmas 23 and 24, and the fact that $[z] = [z^{-1}]$ we infer

LEMMA 25. *The path*

$$\mathbf{Oh} \triangleq [x_2] - [x_3] - [x_6] - [x_7] - \ldots - [x_{2\delta-2}] - [x_{2\delta-1}] - [y_{2\delta-1}] - [y_{2\delta-2}] - \ldots - [y_7] - [y_6] - [y_3] - [y_2] - [2p+1] =$$

$$\left[-\frac{1}{3}\right] - \left[-\frac{5}{3}\right] - \left[-\frac{5}{7}\right] - \left[-\frac{9}{7}\right] - \ldots - \left[-\frac{p-4}{p-2}\right] - \left[-\frac{p}{p-2} = p\right] -$$

$$\left[2p - \frac{p}{p-2} = 3p\right] - \left[2p - \frac{p-4}{p-2}\right] - \ldots - \left[2p - \frac{9}{7}\right] - \left[2p - \frac{5}{7}\right] -$$

$$\left[2p - \frac{5}{3}\right] - \left[2p - \frac{1}{3}\right] - [2p+1]$$

is a Hamiltonian path in $OQ_1(4p)$.

Note that by the definition of the sequences $\{x_i\}$ and $\{y_i\}$, and of **Oh**, the numerator of the fraction representing orbits in the path is congruent to 1 modulo 4, and the denominator is congruent to 3 modulo 4. An edge between orbits that belong to the same sequence ($\{x_i\}$ or $\{y_i\}$) with equal numerators is a second derivative edge, and an edge between orbits that belong to the same sequence with equal denominators is a third derivative edge. The edge between $[p]$ and $[3p]$ is a first derivative edge, and the edge connecting $[2p+1]$ and $[2p-3] = [2p-1/3]$ is a third derivative edge.

Before we proceed we define the following set $\{h_i\}_{i=0}^{2\delta-1}$ of isomorphic paths in $Q_1(4p)$. Each path h_i contains one vertex from each orbit of $Q_1(4p)$ and the order between the vertices in each path h_i is identical to the order between the orbits in **Oh**.

$h_0 = [-3, 1, 2] - [-3, 5, -2] - \ldots - [-(p-2), p-4, 2] - [-(p-2), p, -2] - [p-2, p, 2p+2] - [p-2, 2p-(p-4), 2p-2] - \ldots - [3, 2p-5, 2p+2] - [3, 2p-1, 2p-2] - [1, 2p+1, 2p-2]$

and $h_i = w^i h_0$, $0 \le i \le 2\delta - 1$. $v_{[x],i}$ will denote the vertex from h_i that belongs to orbit $[x]$. Note that by Lemma 23(1) and the properties of U, h_i and $h_{i+\delta}$, $0 \le i \le \delta - 1$ share the last vertex, i.e., $w^i[2p + 1, 1, 2p - 2]$. Apart from this vertex, each other vertex of $Q_1(4p)$ appears exactly once in one of the h_is. Let H_i, $0 \le i \le \delta - 1$, be the path defined by concatenating h_i with the reverse path of $h_{i+\delta}$, where the vertex $w^i[2p + 1, 1, 2p - 2]$ is taken only once. Clearly all the H_is are disjoint, and their union covers the vertices in $Q_1(4p)$.

LEMMA 26. $v'_{[-(p-4)/p-2)],i} = v_{[f],i+l}$, *where* $w^l = 3$ *or* -3, *and* $f = 2p - \frac{\frac{p-2}{3}}{\frac{p+4}{3}}$.

Proof. For the vertex $v_{[-(p-4)/(p-2)],i} = w^i[p - 4, -(p - 2), 2]$, $(w^i[-(p - 2), p - 4, 2])' = w^i[p - 2, p - 4, 2p + 6] = 3w^i\,[(p - 2)/3, 2p - (p + 4)/3, 2p + 2] = w^{i+l}v_{[f],0} = v_{[f],i+l}$. □

LEMMA 27. $o(3)$ *and* $o(-3)$ *modulo* $4p$ *are divisible by* 4.

Proof. Since

$$\left(\frac{3}{p}\right) = \left(\frac{3}{5 + 12k}\right) = \left(\frac{3}{5}\right) = -1$$

it follows that $o(3)$ modulo p is even. Since $p \equiv 1 \pmod 4$ it follows that -1 is a quadratic residue modulo p, and since $o(3)$ is even modulo p, it follows that $3^i \equiv -1 \pmod p$ for some even i and hence $o(3)$ modulo p is divisible by 4. The same argument holds for -3. Thus $o(3)$ and $o(-3)$ modulo $4p$ are divisible by 4. □

LEMMA 28. *Let* l *be as in Lemma* 26. *The set* $\{H_i\}_{i=0}^{\delta-1}$ *can be partitioned to two disjoint sets, such that for* $0 \le i \le \delta - 1$, H_i *is in the first set and* H_{i+l} *belongs to the second* (*where subscripts are taken modulo* δ).

Proof. Note that since h_i and $h_{i+\delta}$ belong to H_i we only have to show that the smallest m such that $ml \equiv 0 \pmod \delta$ is even. This follows immediately from the fact that $w^l \in \{3, -3\}$ and $o(3)$ and $o(-3)$ modulo $4p$ is divisible by 4. □

LEMMA 29. *Let* l *be as in Lemma* 26. *The subgraph induced by the vertices of* H_0 *and* H_l *has a* 1*-factor.*

Proof.

1. First we construct a cycle by connecting $v_{[-(p-4)/(p-2)],0}$ and $v_{[-(p-4)/(p-2)],\delta}$ to their first derivatives $v_{[f],l}$ and $v_{[f],l+\delta}$ respectively (see Lemma 26). Since the cycle contains two vertices from $[2p + 1]$, the same number of vertices from h_0 and h_δ, and the same number of vertices from h_l and $h_{l+\delta}$, it follows that the length of the cycle is even.

2. The rest of the subgraph is decomposed into the following paths

$$v_{\left[-\frac{1}{3}\right],l} - v_{\left[-\frac{5}{3}\right],l} - \cdots - v_{\left[\frac{-p-4}{p-6}\right],l} - v_{\left[\frac{-p-4}{p-2}\right],l} - v_{[p],l}$$

$$v_{\left[-\frac{1}{3}\right],l+\delta} - v_{\left[-\frac{5}{3}\right],l+\delta} - \cdots - v_{\left[\frac{-p-4}{p-6}\right],l+\delta} - v_{\left[\frac{-p-4}{p-2}\right],l+\delta} - v_{[p],l+\delta}$$

$$v_{\left[-\frac{1}{3}\right],0} - v_{\left[-\frac{5}{3}\right],0} - \cdots - v_{\left[\frac{-p-8}{p-6}\right],0} - v_{\left[\frac{-p-4}{p-6}\right],0}$$

$$v_{\left[-\frac{1}{3}\right],\delta} - v_{\left[-\frac{5}{3}\right],\delta} - \cdots - v_{\left[\frac{-p-8}{p-6}\right],\delta} - v_{\left[\frac{-p-4}{p-6}\right],\delta}$$

$$v_{\left[2p-\frac{\frac{p+10}{3}}{\frac{p+4}{3}}\right],l} - \cdots - v_{\left[2p-\frac{p-4}{p-6}\right],l} - v_{\left[2p-\frac{p-4}{p-2}\right],l}$$

$$v_{\left[2p-\frac{\frac{p+10}{3}}{\frac{p+4}{3}}\right],l+\delta} - \cdots - v_{\left[2p-\frac{p-4}{p-6}\right],l+\delta} - v_{\left[2p-\frac{p-4}{p-2}\right],l+\delta}$$

These paths are of even length since they begin and end with the same derivative edges (second or third).

3. The only two vertices which remain are $v_{[3p],l}$ and $v_{[3p],l+\delta}$, which are connected by Lemma 23(3).

The scenario is depicted in Figure 2. □

From Lemmas 28, 29 and the automorphism properties we conclude

THEOREM 7. *$Q_1(4p)$ has a 1-factor.*

COROLLARY 8. If I_p, $p = n/4$, *contains no proper subset closed under unsigned inverse beside* $\{\alpha - 1, \alpha\}$, *where* $\alpha = (1 + \sqrt{5})/2$, *then there exists an S-cyclic SQS(4p) with* $p \equiv 5 \pmod{12}$.

As said before, it was verified that for $p < 1500000$, I_p contains no proper subset closed under unsigned inverse.

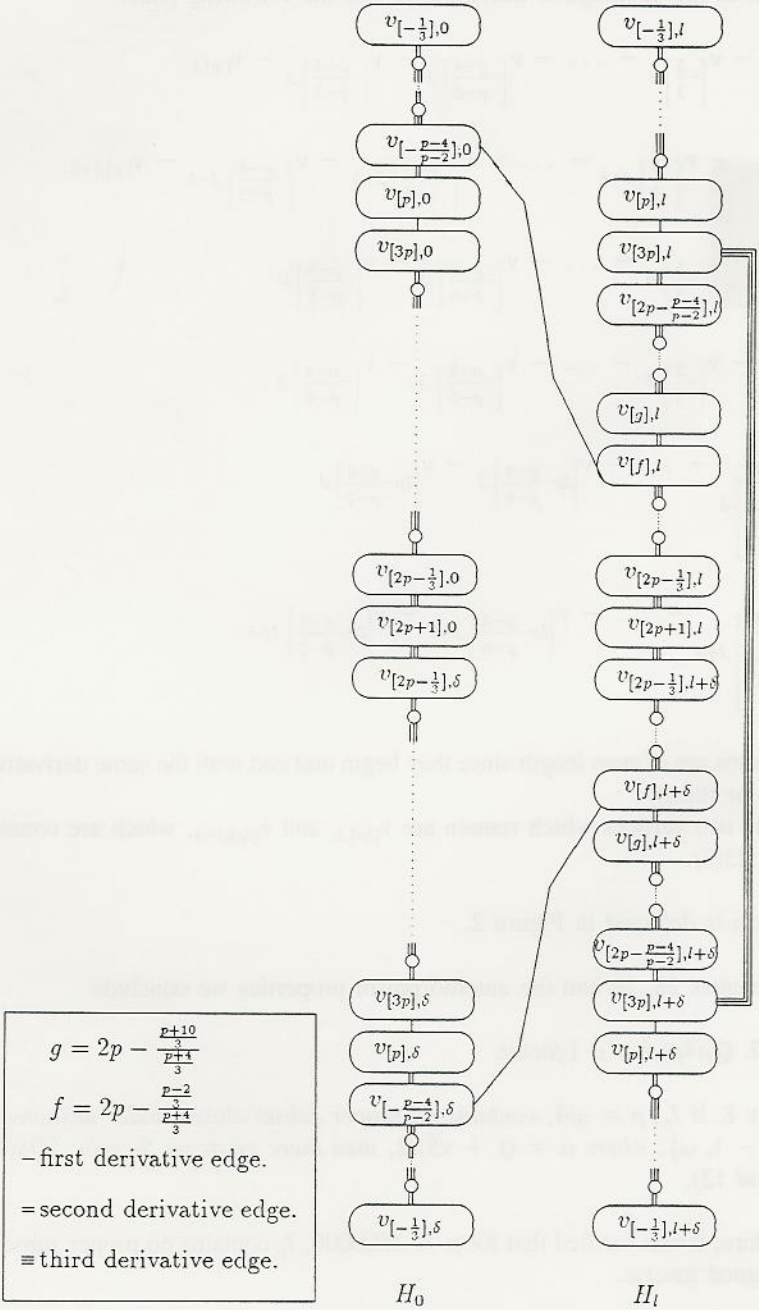
$v_{[-\frac{1}{3}],0}$
$v_{[-\frac{p-4}{p-2}],0}$
$v_{[p],0}$
$v_{[3p],0}$
$v_{[2p-\frac{1}{3}],0}$
$v_{[2p+1],0}$
$v_{[2p-\frac{1}{3}],\delta}$
$v_{[3p],\delta}$
$v_{[p],\delta}$
$v_{[-\frac{p-4}{p-2}],\delta}$
$v_{[-\frac{1}{3}],\delta}$
H_0
$v_{[-\frac{1}{3}],l}$
$v_{[p],l}$
$v_{[3p],l}$
$v_{[2p-\frac{p-4}{p-2}],l}$
$v_{[g],l}$
$v_{[f],l}$
$v_{[2p-\frac{1}{3}],l}$
$v_{[2p+1],l}$
$v_{[2p-\frac{1}{3}],l+\delta}$
$v_{[f],l+\delta}$
$v_{[g],l+\delta}$
$v_{[2p-\frac{p-4}{p-2}],l+\delta}$
$v_{[3p],l+\delta}$
$v_{[p],l+\delta}$
$v_{[-\frac{1}{3}],l+\delta}$
H_l
$g = 2p - \frac{\frac{p+10}{3}}{\frac{p+4}{3}}$
$f = 2p - \frac{\frac{p-2}{3}}{\frac{p+4}{3}}$
– first derivative edge.
= second derivative edge.
≡ third derivative edge.

Figure 2.

9. Optical Orthogonal Codes

An (n, w, λ)-*Optical Orthogonal Code* (OOC) [20] C, $n > 1$, $1 \leq w \leq n$, $0 \leq \lambda \leq w$, is a set of binary codewords of length n, with weight w satisfying:

1. for all $x \in C$, every two different cyclic shifts of x intersect in at most λ ONEs. (This implies that the orbit of every word $x \in C$ is full.)
2. for all $x, y \in C$, $x \neq y$, any two cyclic shifts of x and y intersect in at most λ ONEs.

For given n, w and λ, $\Phi(n, w, \lambda)$ denotes the largest possible size of an (n, w, λ)-OOC. An (n, w, λ)-OOC that achieves this size is *optimal*. One can easily observe that an (n, w, λ)-OOC is obtained by taking one representative from all the full length orbits of a cyclic constant weight code of length n, weight w and minimum distance $2(w - \lambda)$. Construction for OOCs can be found in [20], [25], [26].

We consider the case $\lambda = 2$ and $w = 4$. When $n \equiv 2$ or 4 (mod 6) and a 1-rotational SQS exists an optimal $(n - 1, 4, 2)$-OOC is obtained by taking one word from each orbit with ZERO in the point fixed by the rotational automorphism. A strictly cyclic SQS, is a cyclic SQS whose orbits are of full length. A necessary condition for the existence of a strictly cyclic $SQS(n)$ is $n \equiv 2$ or 10 (mod 24). When a strictly cyclic $SQS(n)$ exists it corresponds to an optimal $(n, 4, 2)$-OOC. The full orbits of S-cyclic SQS also correspond to an optimal $(n, 4, 2)$-OOC. Hence, if $n = 4p$, $p \equiv 5$ (mod 12) if I_p, contains no proper subsets closed under unsigned inverse beside $\{\alpha - 1, \alpha\}$, where $\alpha = (1 + \sqrt{5})/2$, then an optimal $(n, 4, 2)$-OOC exists.

For the cases $n = 2p$, where $p \equiv 11$ (mod 12), i.e., $n \equiv 22$ (mod 24), we used a similar analysis as in the previous sections and found more optimal $(n, 2, 4)$-OOC depending on the order of some elements.

10. Conclusion

We have constructed optimal extended cyclic constant weight codes of weight 4, minimum Hamming distance 4, and size $((n - 1)(n^2 - 3n - 4))/24$, for 246 values of the form $n \equiv 5$ (mod 6). This improves the known lower bound of $A(n, 4, 4)$ in these cases. For infinitely many value $n \equiv 5$ (mod 6) we gave enough evidence to believe that such codes exist. Lots of open ground for research remains in this area and some of the questions are easily raised from our discussion. We have used our method to construct new S-cyclic Steiner Quadruple Systems, and discussed the application of the construction in the design of optimal $(n, 2, 4)$-optical orthogonal codes.

Appendix

Rotational Code for $n = 23$, $w = 4$, $d = 4$

B_0	⟨1, 1, 10, 10⟩	⟨2, 2, 9, 9⟩	⟨3, 3, 8, 8⟩	⟨4, 4, 7, 7⟩
	⟨5, 5, 6, 6⟩			
B_1	⟨2, 6, 14⟩	⟨1, 3, 18⟩	⟨5, 7, 10⟩	
B_2	⟨3, 4, 3, 12⟩	⟨2, 5, 2, 13⟩	⟨3, 6, 7, 6⟩	⟨1, 9, 3, 9⟩
	⟨1, 7, 1, 13⟩	⟨1, 5, 1, 15⟩	⟨1, 4, 13, 4⟩	⟨3, 5, 9, 5⟩
	⟨1, 2, 17, 2⟩	⟨2, 8, 4, 8⟩	⟨2, 4, 12, 4⟩	

Rotational Code for $n = 29$, $w = 4$, $d = 4$

B_0	⟨7, 7, 7, 7⟩	⟨1, 1, 13, 13⟩	⟨2, 2, 12, 12⟩	⟨3, 3, 11, 11⟩
	⟨4, 4, 10, 10⟩	⟨5, 5, 9, 9⟩	⟨6, 6, 8, 8⟩	
B_1	⟨4, 8, 16⟩	⟨2, 3, 23⟩	⟨6, 9, 13⟩	⟨7, 10, 11⟩
B_2	⟨2, 4, 18, 4⟩	⟨2, 6, 2, 18⟩	⟨2, 10, 6, 10⟩	⟨1, 2, 1, 24⟩
	⟨1, 4, 19, 4⟩	⟨1, 5, 17, 5⟩	⟨1, 6, 1, 20⟩	⟨1, 8, 11, 8⟩
	⟨1, 9, 1, 17⟩	⟨3, 5, 3, 17⟩	⟨1, 11, 5, 11⟩	⟨1, 12, 3, 12⟩
	⟨2, 5, 16, 5⟩	⟨2, 7, 12, 7⟩	⟨2, 9, 2, 15⟩	⟨3, 6, 3, 16⟩
	⟨3, 4, 17, 4⟩	⟨4, 9, 4, 11⟩	⟨6, 7, 8, 7⟩	⟨5, 8, 5, 10⟩
	⟨3, 7, 3, 15⟩			

Acknowledgment

The authors thank the referees for their valuable comments. They also thank H. Siemon and A. Hartman for their help.

References

1. H. Hanani, On quadruple systems. *Canad. J. Math*, Vol. 12, (1960) pp. 145–157.
2. J. Spencer, Maximal consistent families of triples, *J. of Combinatorial Theory*, Vol. 5, (1968) pp. 1–8.
3. S.M. Johnson, Upper bounds for constant weight error-correcting codes. *Discrete Mathematics*, Vol. 3, (1972) pp. 109–124.
4. J.G. Kalbfleish and R.G. Stanton, Maximal and minimal coverings of $(k-1)$-tuples by k-tuples, *Pacific J. Math.*, Vol. 26, (1968) pp. 131–140.
5. W.H. Mills, On the covering of triples by quadruples, *Proc. of the 5th Southeastern Conference on Combinatorics Graph Theory and Computation*, Boca Raton, (1974) pp. 563–581.
6. A.E. Brouwer, On the packing of quadruples without common triples, *Ars Combinatoria*, Vol. 5, (1978) pp. 3–6.
7. W.H. Mills and R.C. Mullin, Covering and packings. In Jeffry H. Dinitz and Douglas R. Stinton, editors, *Contemporary Design Theory*, John Wiley, New York (1992) pp. 371–399.
8. M.R. Best, A(11, 4, 4)=35 or some new optimal constant weight codes. Technical Report ZN 71/77, Math. Centr. Amsterdam, (1977).
9. J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups*. Springer-Verlag, Berlin-Heidelberg, New York, (1988).

10. A.E. Brouwer, J.B. Shearer, N.J.A. Sloane, and W.D. Smith, A new table of constant weight codes, *IEEE Trans. on Inform. Theory*, IT-36, (1990) pp. 1334–1380.
11. C.C. Lindner and A. Rosa, Steiner quadruple systems—a survey, *Discrete Math.*, Vol. 22, (1978) pp. 148–171.
12. C.L. van Pul and T. Etzion, New lower bounds for constant weight codes, *IEEE Trans. on Inform. Theory*, IT-35, (1989) pp. 1324–1329.
13. K.T. Phelps. Rotational Steiner quadruple systems, *Ars Combinatoria*, Vol. 4, (1977) pp. 177–185.
14. Alan Hartman and Kevin T. Phelps, Steiner quadruple systems. In Jeffry H. Dinitz and Douglas R. Stinton, editors, *Contemporary Design Theory*, pp. 205–240. John Wiley, New York (1992).
15. E. Köhler, Zyklische quadrupelsysteme. *Abh. Sem. Univ. Hamburg*, No. 48, (1978) pp. 1–24.
16. H. Siemon, Some remarks on the construction of cyclic Steiner quadruple system, *Arch. der Math.*, Vol. 49, (1987) pp. 166–178.
17. H. Siemon, Infinite families of strictly cyclic Steiner quadruple systems, *Discrete Mathematics*, Vol. 77, (1989) pp. 307–316.
18. H. Siemon, Cyclic Steiner quadruple systems and Köhler's orbit graphs, *Designs, Codes and Cryptography*, Vol. 1, (1991) pp. 121–132.
19. H. Siemon, On the existence of cyclic Steiner quadruple systems $SQS(2p)$, *Discrete Mathematics*, Vol. 97, (1991) pp. 377–385.
20. F.R.K. Chung, J.A. Salehi, and V.K. Wei, Optical orthogonal codes: design, analysis, and applications, *IEEE Transactions on Information Theory*, 35(3), (1989) pp. 595–604.
21. K.T. Phelps, On cyclic Steiner system $S(3, 4, 20)$, *Annals of Discrete Mathematics*, Vol. 7, (1980) pp. 277–300.
22. I. Niven and H.S. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley, New York, fourth edition, (1980).
23. C. Berge, *Graphs and Hyper-Graphs*, North-Holland, Amsterdam, (1970).
24. I. Diener, On cyclic Steiner systems $S(3, 4, 22)$. *Annals of Discrete Mathematics*, Vol. 7, (1980) pp. 301–313.
25. E.F. Brickell and V.K. Wei, Optical orthogonal codes and difference families, *Proc. of the Southeastern Conference on Combinatorics Graph Theory and Algorithms*, (1987).
26. H. Chung and P.V. Kumar, Optical orthogonal codes—new bounds and an optimal construction, *IEEE Transactions on Information Theory*, 36(4), (1990) pp. 866–873.