www.combinatorics.ir

Transactions on Combinatorics
ISSN (print): 2251-8657, ISSN (on-line): 2251-8665
Vol. 7 No. 1 (2018), pp. 37-50.

www.ui.ac.ir

PD-SETS FOR CODES RELATED TO FLAG-TRANSITIVE SYMMETRIC DESIGNS

DEAN CRNKOVIĆ* AND NINA MOSTARAC

Communicated by Behruz Tayfeh Rezaie

Abstract. For any prime p let $C_p(G)$ be the p-ary code spanned by the rows of the incidence matrix G of a graph Γ. Let Γ be the incidence graph of a flag-transitive symmetric design D. We show that any flag-transitive automorphism group of D can be used as a PD-set for full error correction for the linear code $C_p(G)$ (with any information set). It follows that such codes derived from flag-transitive symmetric designs can be decoded using permutation decoding. In that way to each flag-transitive symmetric (v, k, λ) design we associate a linear code of length vk that is permutation decodable. PD-sets obtained in the described way are usually of large cardinality. By studying codes arising from some flag-transitive symmetric designs we show that smaller PD-sets can be found for specific information sets.

1. Introduction

Recent advances in technology have produced a requirement for good error-correcting codes and efficient encoding and decoding methods. *Permutation decoding* is a decoding method introduced in 1964 by MacWilliams [9]. The algorithm uses sets of code automorphisms called PD-sets. This method can be used when a code has a sufficiently large automorphism group to ensure the existence of a PD-set. The technique is described by MacWilliams, Sloane ([10, Chapter 16]) and Huffman ([6, Chapter 8]). A survey of permutation decoding using codes that arise from combinatorial structures is given in [8].

MSC(2010): Primary: 05B05; Secondary: 20D45, 94B05.
Keywords: Code, graph, flag-transitive design, permutation decoding.
Received: 04 June 2017, Accepted: 1 July 2017.
∗Corresponding author.
DOI: http://dx.doi.org/10.22108/toc.2017.21615

.

The question is whether PD-sets exist for a certain code, because not every code is necessarily permutation decodable. In this paper we prove the existence of PD-sets for all codes generated by the incidence matrix of an incidence graph of a flag-transitive symmetric design and construct examples of such PD-sets. In that way from each flag-transitive symmetric (v, k, λ) design we construct a linear code of length vk that is permutation decodable. By studying codes arising from some flag-transitive projective planes and biplanes we found examples of smaller PD-sets for specific information sets that are more applicable in practice for permutation decoding.

We use results on codes spanned by incidence matrices of graphs, obtained by Dankelmann, Key and Rodrigues [2]. Further, we study codes arising from some flag-transitive symmetric designs, namely projective planes and biplanes given by Kantor [7] and O'Reilly-Regueiro [11].

When constructing examples we use programming packages GAP [4] and Magma [1].

2. Background and terminology

In this section we will give some basic definitions of graph theory and coding theory.

2.1. Codes.

A *code* C of length n over the alphabet Q is a subset $C \subseteq Q^n$. Elements of a code are called *codewords*. A code C is called a p-ary *linear code* of dimension m if $Q = \mathbb{F}_p$, for a prime p, and C is an m-dimensional subspace of a vector space $(\mathbb{F}_p)^n$. For $Q = \mathbb{F}_2$ a code is called *binary*.

Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n) \in \mathbb{F}_p^n$. The *Hamming distance* between words x and y is the number $d(x, y) = |\{i : x_i \neq y_i\}|$. The *minimum distance* of the code C is defined by $d = \min\{d(x, y) : x, y \in C,\ x \neq y\}$. The *weight* of a codeword x is $w(x) = d(x, 0) = |\{i : x_i \neq 0\}|$. For a *linear code* the minimum distance equals the minimum weight: $d = \min\{w(x) : x \in C, x \neq 0\}$.

A p-ary linear code of length n, dimension k, and distance d is called a $[n, k, d]_p$ code. A linear $[n, k, d]$ code can detect at most $d - 1$ errors in one codeword and correct at most $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ errors.

Two linear codes are *isomorphic* if one can be obtain from the other by permuting the coordinate positions. An *automorphism* of the code C is an isomorphism from C to C. The *generating matrix* of a code is a $k \times n$ matrix whose rows are vectors of the base of the code. Every code is isomorphic to the code with generating matrix in the *standard form*, i.e. in the form $[I_k, A]$, where I_k is an identity matrix of order k and A some $k \times (n - k)$ matrix.

2.2. Graphs.

A *graph* Γ is an ordered triplet (V, E, ψ), where V is a nonempty set of *vertices*, E is a set of *edges* disjoint with V, and ψ is an incidence function which assigns a pair of vertices (not necessarily distinct) to each edge. Graphs discussed here are undirected (assigned pair of vertices is unordered), with no loops (two distinct vertices are assigned to an edge) and no multiple edges.

The *distance* between vertices u and v of the graph Γ is defined as the length of the shortest path between u and v if they are connected and if there is no path between them then we take the distance to be equal ∞. The *diameter*, $diam(\Gamma)$, of the graph Γ is the maximum distance between two vertices of Γ. The *girth* of the graph Γ is the length of the shortest cycle in Γ and if Γ has no cycle then we define it to be equal ∞.

DOI: http://dx.doi.org/10.22108/toc.2017.21615

The *degree* of the vertex $u \in V$ is the number of vertices adjacent to u. We will denote the minimum vertex degree by $\delta(\Gamma)$. A graph is *k-regular* ($k \in \mathbb{N}_0$) if all its vertices are of a degree k.

An *adjacency matrix* of graph $\Gamma = (V, E)$ is a $|V| \times |V|$ matrix $A = [a_{ij}]$, where $a_{ij} = 1$ if vertices v_i and v_j are adjacent and $a_{ij} = 0$ otherwise. An *incidence matrix* is a $|V| \times |E|$ matrix $G = [g_{ij}]$, where $g_{ij} = 1$ if vertex v_i is on the edge e_j and $g_{ij} = 0$ otherwise.

Two graphs Γ_1 and Γ_2 are said to be *isomorphic* if there exist bijections $\theta : V(\Gamma_1) \to V(\Gamma_2)$ and $\phi : E(\Gamma_1) \to E(\Gamma_2)$ such that: $\psi_{\Gamma_1}(e) = uv$ if and only if $\psi_{\Gamma_2}(\phi(e)) = \theta(u)\theta(v)$. Such a pair of mappings (θ, ϕ) is called an *isomorphism* between Γ_1 and Γ_2. An *automorphism* of the graph Γ is an isomorphism from Γ to Γ.

A graph $\Gamma = (V, E)$ is *bipartite* if V can be partitioned into two classes such that every edge has its ends in distinct classes. A *complete bipartite graph* is a bipartite graph in which every two vertices from distinct classes are connected with an edge.

Edge connectivity $\lambda(\Gamma)$ of a connected graph Γ is the minimum number of edges that need to be removed to disconnect the graph. A *bridge* of a connected graph is an edge whose removal disconnects the graph.

Remark 2.1. *A graph Γ has a bridge if and only if $\lambda(\Gamma) = 1$. For every graph Γ it is known that $\lambda(\Gamma) \leq \delta(\Gamma)$; this follows directly from the fact that removing the edges incident with a vertex of degree $\delta(\Gamma)$ disconnects the graph.*

A graph Γ is *super-λ* if $\lambda(\Gamma) = \delta(\Gamma)$ and the only edge sets of cardinality $\lambda(\Gamma)$ whose removal disconnects the graph are the sets of edges incident to a vertex of degree $\delta(\Gamma)$.

3. Codes from incidence matrices of graphs

Let G be the incidence matrix of a graph $\Gamma = (V, E)$ over the finite field $\mathbb{F}_p$, where p is a prime. We will denote by $C_p(G)$ the code that is the row-span of G over $\mathbb{F}_p$.

Theorem 3.1 (Dankelmann, Key, Rodrigues **.** *codes-from-graphs] Let $\Gamma = (V, E)$ be a connected graph and G its incidence matrix. Then:*

1. *$dim(C_2(G)) = |V| - 1$;*
2. *for odd p, $dim(C_p(G)) = |V|$ if Γ is not bipartite, and $dim(C_p(G)) = |V| - 1$ if Γ is bipartite.*

Theorem 3.2 (Dankelmann, Key, Rodrigues **.** *codes-from-graphs] Let $\Gamma = (V, E)$ be a connected graph, G a $|V| \times |E|$ incidence matrix for G. Then:*

1. *$C_2(G)$ is a $[|E|, |V| - 1, \lambda(\Gamma)]_2$ code;*
2. *if Γ is super-λ, then $C_2(G)$ is a $[|E|, |V| - 1, \delta(\Gamma)]_2$ code, and the minimum words are the rows of G of weight $\delta(\Gamma)$.*

It follows that for a graph Γ for which $\delta(\Gamma) = \lambda(\Gamma)$, the minimum weight of the binary code $C_2(G)$ from the incidence matrix of a graph equals the minimum degree of the vertices of the graph $\delta(\Gamma)$.

DOI: http://dx.doi.org/10.22108/toc.2017.21615

Theorem 3.3 (Dankelmann, Key, Rodrigues **.** *codes-from-graphs] Let* $\Gamma = (V, E)$ *be a connected bipartite graph,* G *a* $|V| \times |E|$ *incidence matrix for* G*, and* p *an odd prime. Then:*

(1) $C_p(G)$ *is a* $[|E|, |V| - 1, \lambda(\Gamma)]_p$ *code;*

(2) *if* Γ *is super-*λ*, then* $C_p(G)$ *is a* $[|E|, |V| - 1, \delta(\Gamma)]_p$ *code, and the minimum words are the non-zero scalar multiples of the rows of* G *of weight* $\delta(\Gamma)$*.*

Theorem 3.4 (Dankelmann, Key, Rodrigues **.** *codes-from-graphs] Let* $\Gamma = (V, E)$ *be a connected bipartite graph. Then* $\lambda(\Gamma) = \delta(\Gamma)$ *if one of the following conditions holds:*

(1) V *consists of at most two orbits under* $Aut(\Gamma)$*, and in particular if* Γ *is vertex-transitive;*

(2) *every two vertices in one of the two partite sets of* Γ *have a common neighbour;*

(3) $diam(\Gamma) \leq 3$*;*

(4) Γ *is* k*-regular and* $k \geq \frac{n+1}{4}$*;*

(5) Γ *has girth* g *and* $diam(\Gamma) \leq g - 1$*.*

If $\delta(\Gamma) = \lambda(\Gamma)$ *and* Γ *satisfies one of the following conditions then* Γ *is super-*λ*:*

(1a) Γ *is vertex-transitive;*

(2a) Γ *is* k*-regular and* $k \geq \frac{n+3}{4}$*.*

4. Flag-transitive automorphism groups of symmetric designs as PD-sets

In this section we show that a code spanned by the incidence matrix of the incidence graph of a flag-transitive symmetric design posseses a PD-set, i.e. the code allows permutation decoding.

4.1. PD-sets and permutation decoding.

Let $C \subseteq \mathbb{F}_p^n$ be a linear $[n, k, d]$ code. For $I \subseteq \{1, \ldots, n\}$ let $p_I : \mathbb{F}_p^n \to \mathbb{F}_p^{|I|}$, $x \mapsto x|_I$, be an I-projection of $\mathbb{F}_p^n$. Then I is called an *information set* for C if $|I| = k$ and $p_I(C) = \mathbb{F}_p^{|I|}$. The set of the first k coordinates for a code with a generating matrix in the standard form is an *information set*.

Let $C \subseteq \mathbb{F}_p^n$ be a linear $[n, k, d]$ code that can correct at most t errors (i.e. t-error-correcting code) and let I be an information set for C. A subset $S \subseteq \mathrm{Aut}C$ is called a *PD-set* for C if for every subset $B \subseteq \{1, \ldots, n\}$ for which $|B| \leq t$ there exists an automorphism $\sigma \in S$ such that $\sigma(B) \cap I = \emptyset$. This means that $S \subseteq \mathrm{Aut}C$ is a PD-set for C if every t-set of coordinate positions can be moved by at least one element of S out of the information set I.

The algorithm of permutation decoding (see [10], [6]) uses PD-sets and it is more efficient the smaller the size of a PD-set is. A lower bound on the size of a PD-set is given in the following theorem and it is due to Gordon [5].

Theorem 4.1 (The Gordon bound)**.** *If* S *is a PD-set for an* $[n, k, d]$ *code* C *that can correct* t *errors,* $r = n - k$*, then:*

$$|S| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil .$$

DOI: http://dx.doi.org/10.22108/toc.2017.21615

4.2. **Flag-transitive symmetric designs.** A *symmetric* (v, k, λ)*-design* is an incidence structure $D = (P, B, I)$ which consists of the set of points P, the set of blocks B and an incidence relation I between P and B such that $|P| = |B| = v$, every block is incident with exactly k points, and every pair of points is incident with exactly λ blocks ($\lambda > 0$). A symmetric $(v, k, 1)$-design is called a *projective plane* of order $k-1$, and a symmetric $(v, k, 2)$-design is called a *biplane*.

Let $D = \{P, B, I\}$ be a symmetric design, and let $P = \{x_1, \ldots, x_v\}$ and $B = \{B_1, \ldots, B_v\}$ be its sets of points and blocks, respectively. The *incidence matrix* of the symmetric design D is a $v \times v$ matrix $A = [a_{ij}]$, where $a_{ij} = 1$ if $x_i \in B_j$ and $a_{ij} = 0$ if $x_i \notin B_j$.

An *incidence graph* or a *Levi graph* of a symmetric design (or any incidence structure) is a graph whose vertices are points and blocks of the design, and edges are incident point-block pairs (i.e. flags of the design).

It is easily checked that an incidence graph Γ of a symmetric (v, k, λ)-design is bipartite (partition parts are sets of points and blocks of the design) and k-regular (every point is incident with k blocks and every block is incident with k points).

Remark 4.2. *An incidence graph* Γ *of a symmetric* (v, k, λ)*-design has diameter* $\mathrm{diam}(\Gamma) = 3$.

Proof. There are three possible cases:

(i) $d(u, v) = 1 \;\Leftrightarrow\; (u, v)$ is a flag,

(ii) $d(u, v) = 2 \;\Leftrightarrow\; (u, v)$ are two distinct points or two distinct blocks;

(iii) $d(u, v) = 3 \;\Leftrightarrow\; (u, v)$ are a nonincident point and block (an antiflag).

□

An *automorphism* of a symmetric design is a permutation of points which sends blocks to blocks. The set of all automorphisms of a design forms a group which is called the *full automorphism group* of the design. Every subgroup of the full automorphism group is called an *automorphism group*.

A permutation group G is *transitive* on points of the set Ω if and only if

$$\forall \alpha, \beta \in \Omega,\ \exists g \in G \text{ such that } g(\alpha) = \beta.$$

A *flag* of a symmetric design is an incident point-block pair. An automorphism group of a symmetric design D is called *flag-transitive* if it is transitive on flags of D. The classification of flag-transitive symmetric designs is still an open problem. H. Davies [3] proved that for a given $\lambda > 1$ there are finitely many (v, k, λ)-designs (not necessarily symmetric) admitting a flag-transitive imprimitive automorphism group, by proving that in that case k is bounded. Some further results towards the classification of flag-transitive symmetric designs can be found in [12] and [11].

Dankelmann, Key and Rodrigues have shown in [2, Result 7] the following result.

Theorem 4.3. *Let* $\Gamma = (V, E)$ *be a* k*-regular graph with the automorphism group* A *transitive on edges and let* G *be an incidence matrix of* Γ*. If* $C = C_p(G)$ *is a* $[|E|, |V| - \varepsilon, k]_p$ *code, where* p *is a prime and* $\varepsilon \in \{0, 1, \ldots, |V| - 1\}$*, then any transitive subgroup of* A *is a PD-set for full error correction for* C*.*

DOI: http://dx.doi.org/10.22108/toc.2017.21615

Theorem 4.3 applied to an incidence graph of a flag-transitive symmetric design leads to the following main result of this paper.

Theorem 4.4. *Let $\Gamma = (V, E)$ be an incidence graph of a symmetric (v, k, λ)-design D with flag-transitive automorphism group A and let G be an incidence matrix for Γ. Then $C = C_p(G)$ is a $[|E|, |V| - 1, k]_p$ code, for any prime p, and any flag transitive subgroup of A can serve as a PD-set (for any information set) for full error correction for the code C.*

Proof. Γ is a connected and bipartite graph, so by Theorem 3.3 and Theorem 3.4 it follows that $C_p(G)$ is a code with parameters $[|E|, |V| - 1, \lambda]_p$. Since $diam(\Gamma) = 3$ and every two vertices from the same partition class have a common neighbour, Theorem 3.4 implies that $\lambda = \delta$. Γ is k-regular, so the minimum degree of Γ is $\delta = k$. Hence, it follows that $C_p(G)$ is a $[|E|, |V| - 1, k]_p$ code, for any prime p. The group A is flag-transitive on D, so A is transitive on the edges of Γ. We can now apply Theorem 4.3 to finish the proof. □

5. **Examples**

For the following computational results we use programming packages GAP [4] and Magma [1].

We will first look at examples of flag-transitive symmetric designs with $\lambda = 1$, i.e. flag-transitive projective planes. Then we will examine flag-transitive symmetric designs with $\lambda = 2$, i.e. flag-transitive biplanes. We will find all flag-transitive subgroups of the full automorphism groups of the designs. These subgroups are PD-sets for the codes obtained from the designs (for any information set).

Parameters of the linear $[n, k, d]_p$ code obtained from a flag-transitive symmetric (v, k', λ)-design in the described way can be calculated as follows: the length is $n = v \cdot k'$ (i.e. the number of flags), the dimension is $k = 2v - 1$ and the minimum weight $d = k'$.

5.1. **Flag-transitive projective planes.** The following theorem is due to W. Kantor [7]:

Theorem 5.1. *If D is a projective plane of order n admitting a flag-transitive automorphism group A, then either:*

(i) *D is Desarguesian and $A \triangleright PSL(3, n)$, or*

(ii) *A is a sharply flag-transitive Frobenius group of odd order $(n^2 + n + 1)(n + 1)$ and $n^2 + n + 1$ is a prime.*

We will examine three examples of flag-transitive projective planes, namely the symmetric designs with parameters (7,3,1), (13,4,1) and (21,5,1). These planes are $PG_2(GF(q))$ for $q = 2, 3, 4$. Information about PD-sets from flag-transitive automorphism groups of these projective planes are given in Table 1.

DOI: http://dx.doi.org/10.22108/toc.2017.21615

TABLE 1. Flag-transitive automorphism groups of projective planes as PD-sets

i	Flag-transitive projective plane D_i	Code $C_p(G_i)$	Gordon bound g_i	Orders of all flag-transitive subgroups of automorphism group A_i
1	$(7, 3, 1)$	[21,13,3]	3	21,168
2	$(13, 4, 1)$	[52,25,4]	2	5616
3	$(21, 5, 1)$	[105,41,5]	4	20160, 40320, 60480, 120960

PD-sets that are found guarantee that the corresponding code can be decoded with permutation decoding technique. But, those flag-transitive subgroups, i.e. PD-sets, are of large order, much larger than the Gordon bound. However, we have found smaller PD-sets for the mentioned codes for specific information sets, as shown in Table 2.

TABLE 2. Smallest PD-sets found in codes obtained from projective planes D_1, D_2, D_3

i	Flag-transitive projective plane D_i	Code $C_2(G_i)$	Gordon bound g_i	Smallest PD-set found in A_i
1	$(7, 3, 1)$	[21,13,3]	3	4
2	$(13, 4, 1)$	[52,25,4]	2	4
3	$(21, 5, 1)$	[105,41,5]	4	64

Some smaller PD-sets for binary codes $C_2(G)$ for the projective planes are listed in Table 2 and given in examples below.

In the table, the first two examples correct only one error, so PD-sets are not required, when simply using the syndrome would suffice for decoding (see, for example, [6, p.177]). Thus Eg.1 and 2 are simply academic, and of no practical use.

Note that the coordinate positions $1, 2, \dots, n$ from the given information sets, that are permuted by the automorphisms of the code, correspond to the flags of the initial symmetric design. More precisely, the correspondence is given by:

$$\begin{array}{ccc}
1 & \equiv & (\text{"first point from the first block", "first block"}) \\
2 & \equiv & (\text{"second point from the first block", "first block"}) \\
\vdots & & \\
k' & \equiv & (\text{"}k'\text{-th point from the first block", "first block"}) \\
k'+1 & \equiv & (\text{"first point from the second block", "second block"}) \\
\vdots & & \\
2k' & \equiv & (\text{"}k'\text{-th point from the second block", "second block"}) \\
\vdots & & \\
n = v \cdot k' & \equiv & (\text{"}k'\text{-th point from the }v\text{-th block", "}v\text{-th block"})
\end{array}$$

DOI: http://dx.doi.org/10.22108/toc.2017.21615

where the blocks and the points are taken in the order in which they are listed in the set of blocks.

Example 1. *Let D_1 be a symmetric $(7,3,1)$-design with the set of points $P_1 = \{1,2,3,4,5,6,7\}$ and the set of blocks $B_1 = \{\{1,2,3\},\{1,4,5\},\{1,6,7\},\{2,4,7\},\{2,5,6\},\{3,4,6\},\{3,5,7\}\}$. For the corresponding $[21,13,3]_2$ code the Gordon bound is $g_1 = 3$, and there are exactly 2752512 PD-sets of size 4 for the information set $I_1 = \{1,2,3,4,5,6,7,8,9,10,13,16,19\}$. PD-set of size 3 has not been found, but not all subsets of A_1 of size 3 were checked. One of the PD-sets of size 4 for I_1 is a group S_1 generated by the permutation $a = (1,13,20,9)(2,14,21,7)(3,15,19,8)(4,10,6,12)(5,11)(16,18)$.*

Example 2. *Let D_2 be a symmetric $(13,4,1)$-design with the set of points $P_2 = \{1,2,3,\ldots,13\}$ and the set of blocks $B_2 = \{\{1,2,3,4\},\{1,5,6,7\},\{1,8,9,10\},\{1,11,12,13\},\{2,5,9,11\}, \{2,6,8,13\}, \{2,7,10,12\}, \{3,5,10,13\},\{3,6,9,12\},\{3,7,8,11\},\{4,5,8,12\}, \{4,6,10,11\}, \{4,7,9,13\}\}$. For the corresponding $[52,25,4]_2$ code the Gordon bound is $g_2 = 2$. We have found a PD-set of size 4 for the information set $I_2 = \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,21,25,29,33,37,41,45,49\}$. We didn't find PD-sets of size 2, or 3, but not all subsets of A_2 of those sizes were checked. The found PD-set of size 4 for I_2 is a group S_2 generated by the element b:*

$b = (1,15,42,17)(2,13,44,18)(3,16,43,19)(4,14,41,20)(5,28,6,25)(7,27)(8,26)(9,36,30,21)$
$(10,35,29,24)(11,33,32,23)(12,34,31,22)(37,52,39,51)(38,50)(40,49)(45,48)(46,47)$.

Example 3. *Let D_3 be a symmetric $(21,5,1)$-design with the set of points $P_3 = \{1,2,3,\ldots,21\}$ and the set of blocks:*

$B_3 = \{\{1,2,3,4,5\},\{1,6,7,8,9\},\{1,10,11,12,13\},\{1,14,19,20,21\},\{1,15,16,17,18\}, \{2,6,12,14,15\},$
$\{2,7,10,18,21\},\{2,8,11,17,20\},\{2,9,13,16,19\}, \{3,6,13,17,21\}, \{3,7,11,14,16\},\{3,8,10,15,19\},$
$\{3,9,12,18,20\},\{4,6,11,18,19\},\{4,7,13,15,20\}, \{4,8,12,16,21\},\{4,9,10,14,17\},\{5,6,10,16,20\},$
$\{5,7,12,17,19\},\{5,8,13,14,18\}, \{5,9,11,15,21\}\}$.

For the corresponding $[105,41,5]_2$ code the Gordon bound is $g_3 = 4$. We have found a PD-set of size 64 for the information set $I_3 = \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25, 26,31,36,41,46,51,56,61,66,71,76,81,86,91,96,101\}$. It is a permutation group generated by the following six elements:

$c_1 = (1,5)(2,4)(6,91)(7,94)(8,92)(9,95)(10,93)(11,101)(12,104)(13,103)(14,102)(15,105)$
$(16,96)(17,99)(18,97)(19,100)(20,98)(21,86)(22,88)(23,89)(24,87)(25,90)(26,81)(27,85)$
$(28,82)(29,84)(30,83)(31,71)(32,72)(33,74)(34,75)(35,73)(36,66)(37,70)(38,68)(39,67)$
$(40,69)(41,76)(42,78)(43,80)(44,79)(45,77)(47,49)(48,50)(57,60)(58,59)(62,63)(64,65)$,
$c_2 = (1,73)(2,75)(3,72)(4,71)(5,74)(6,48)(7,47)(8,46)(9,49)(10,50)(11,15)(12,14)(16,43)$
$(17,44)(18,45)(19,41)(20,42)(21,98)(22,96)(23,99)(24,97)(25,100)(26,90)(27,87)(28,88)$
$(29,89)(30,86)(31,65)(32,61)(33,63)(34,64)(35,62)(36,40)(37,39)(51,52)(54,55)(56,92)$
$(57,94)(58,93)(59,91)(60,95)(76,81)(77,85)(78,83)(79,84)(80,82)(101,104)(102,105)$,
$c_3 = (1,57)(2,58)(3,56)(4,59)(5,60)(6,9)(7,10)(11,37)(12,36)(13,38)(14,39)(15,40)(16,97)$
$(17,99)(18,96)(19,98)(20,100)(21,77)(22,76)(23,79)(24,78)(25,80)(26,83)(27,82)(28,85)$
$(29,84)(30,81)(31,33)(34,35)(41,88)(42,87)(43,90)(44,89)(45,86)(46,61)(47,62)(48,65)$

DOI: http://dx.doi.org/10.22108/toc.2017.21615

$(49,63)(50,64)(66,104)(67,102)(68,103)(69,105)(70,101)(71,74)(73,75)(91,95)(93,94)$,
$c_4 = (1,48)(2,49)(3,46)(4,47)(5,50)(6,73)(7,71)(8,72)(9,75)(10,74)(11,15)(12,14)(16,98)$
$(17,99)(18,100)(19,97)(20,96)(21,43)(22,42)(23,44)(24,41)(25,45)(26,85)(27,81)(28,83)$
$(29,84)(30,82)(31,94)(32,92)(33,93)(34,95)(35,91)(36,39)(37,40)(56,61)(57,65)(58,63)$
$(59,62)(60,64)(66,67)(69,70)(76,87)(77,90)(78,88)(79,89)(80,86)(101,105)(102,104)$,
$c_5 = (1,63)(2,65)(3,61)(4,64)(5,62)(6,93)(7,95)(8,92)(9,94)(10,91)(11,14)(12,15)(16,28)$
$(17,29)(18,27)(19,26)(20,30)(21,78)(22,80)(23,79)(24,77)(25,76)(31,75)(32,72)(33,73)$
$(34,71)(35,74)(36,40)(37,39)(41,90)(42,86)(43,88)(44,89)(45,87)(46,56)(47,60)(48,58)$
$(49,57)(50,59)(66,69)(67,70)(81,100)(82,96)(83,98)(84,99)(85,97)(101,102)(104,105)$,
$c_6 = (1,16)(2,19)(3,17)(4,18)(5,20)(6,21)(7,25)(8,23)(9,24)(10,22)(26,65)(27,64)(28,63)$
$(29,61)(30,62)(31,90)(32,89)(33,88)(34,87)(35,86)(36,40)(37,39)(41,75)(42,74)(43,73)$
$(44,72)(45,71)(46,99)(47,100)(48,98)(49,97)(50,96)(51,54)(52,55)(56,84)(57,85)(58,83)$
$(59,82)(60,81)(66,70)(67,69)(76,95)(77,94)(78,93)(79,92)(80,91)(101,105)(102,104)$.

5.2. **Flag-transitive biplanes.** There are only six known flag-transitive biplanes. We will apply the described construction of PD-sets on five of them, since the sixth flag-transitive biplane has parameters $(37,9,2)$ and hence produces the incidence graph with 333 edges which appears to be too demanding for the required computation. The information about flag-transitive biplanes and their full automorphism groups and point stabilizers is given in [11]. All flag-transitive subgroups of their full automorphism group are PD-sets for the code obtained from a design, for any information set. The information about PD-sets from flag-transitive automorphism groups of biplanes is given in Table 3.

TABLE 3. Flag-transitive automorphism groups of biplanes as PD-sets

i	Flag-transitive symmetric design D_i, full automorphism group A_i, point stabilizer	Code $C_p(G_i)$	Gordon bound g_i	Orders of all flag-transitive subgroups of A_i
4	$(4,3,2)$, S_4, S_3	$[12,7,3]$	3	12, 24
5	$(7,4,2)$, $PSL_2(7)$, S_4	$[28,13,4]$	2	168
6	$(11,5,2)$, $PSL_2(11)$, A_5	$[55,21,5]$	4	55, 660
7	$(16,6,2)$, 2^4S_6, S_6	$[96,31,6]$	3	$96,192,288,384,$ $576,768,960,1152,$ $1920,5760,11520$
8	$(16,6,2)$, $(\mathbb{Z}_2\times\mathbb{Z}_8)(S_2.4)$, $(S_2.4)$	$[96,31,6]$	3	384, 768

Again, these flag-transitive subgroups as PD-sets are of large order. We have also found smaller PD-sets for the mentioned codes, for specific information sets, as shown in Table 4.

DOI: http://dx.doi.org/10.22108/toc.2017.21615

Table 4. Smallest PD-sets found in codes obtained from biplanes $D_4, \ldots, D_8$

i	Flag-transitive design D_i	Code $C_2(G_i)$	Gordon bound g_i	Smallest PD-set found in A_i
4	$(4, 3, 2)$	[12,7,3]	3	3
5	$(7, 4, 2)$	[28,13,4]	2	3
6	$(11, 5, 2)$	[55,21,5]	4	10
7	$(16, 6, 2)$	[96,31,6]	3	12
8	$(16, 6, 2)$	[96,31,6]	3	9

In *Example* 5 only the full automorphism group of the design D_5 is flag-transitive. In *Examples* 4, 6 and 8 there is one more flag-transitive subgroup, besides the full automorphism group. In *Example* 7. there are 11 flag-transitive subgroups of the full automorphism group of D_7. Some smaller PD-sets for binary codes $C_2(G)$ for biplanes listed in Table 3 are given in examples below and listed in Table 4.

Examples 4 and 5 correct just a single error, so permutation decoding is of no practical use.

Example 4. *Let D_4 be a symmetric $(4, 3, 2)$-design with the set of points $P_4 = \{1, 2, 3, 4\}$ and the set of blocks $B_4 = \{\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}\}$. For the corresponding binary $[12, 7, 3]_2$ code the Gordon bound is $g_4 = 3$, and there are exactly 128 PD-sets of size 3 for the information set $I_4 = \{1, 2, 3, 4, 6, 7, 10\}$. One of the PD-sets for I_4 is $S_4 = \{(1, 2, 5, 4)(3, 10, 6, 7)(8, 11, 12, 9)$, $(1, 5, 12, 8)(2, 6, 11, 7)(3, 4, 10, 9)$, $(1, 6, 8, 10)(2, 4, 9, 11)(3, 5, 7, 12)\}$.*

Example 5. *Let D_5 be a symmetric $(7, 4, 2)$-design with the point set $P_5 = \{1, 2, 3, 4, 5, 6, 7\}$ and the blocks $B_5 = \{\{1, 2, 3, 4\}, \{1, 3, 5, 6\}, \{1, 2, 5, 7\}, \{1, 4, 6, 7\}, \{2, 3, 6, 7\}, \{2, 4, 5, 6\}, \{3, 4, 5, 7\}\}$. There are no PD-sets of size $g_5 = 2$ for the corresponding binary $[28, 13, 4]_2$ code for the information set $I_5 = \{1, 2, 3, 4, 5, 7, 8, 9, 12, 13, 17, 21, 25\}$. But, there are exactly 90944 PD-sets of size 3 for I_5. One of them is*

$S_5 = \{(1, 3, 25, 28, 12, 9)(2, 6, 26, 20, 11, 13)\ (4, 18, 27, 16, 10, 5)(7, 14, 17)(8, 22, 19, 23, 15, 21),$
$(1, 6)(2, 7, 4, 8)(3, 5)(9, 25, 13, 18)(10, 27, 14, 19)(11, 26, 15, 17)(12, 28, 16, 20)(21, 23, 22, 24),$
$(1, 7, 28, 17)(2, 5, 27, 20)(3, 6, 25, 18)(4, 8, 26, 19)(9, 11, 12, 10)(13, 23, 16, 21)(14, 24)(15, 22)\}.$

Example 6. *Let D_6 be a symmetric $(11, 5, 2)$-design with the set of points $P_6 = \{1, 2, 3, \ldots, 11\}$ and the set of blocks $B_6 = \{\{1, 3, 4, 5, 9\}, \{2, 4, 5, 6, 10\}, \{3, 5, 6, 7, 11\}, \{1, 4, 6, 7, 8\}, \{2, 5, 7, 8, 9\}, \{3, 6, 8, 9, 10\}, \{4, 7, 9, 10, 11\}, \{1, 5, 8, 10, 11\}, \{1, 2, 6, 9, 11\}, \{1, 2, 3, 7, 10\}, \{2, 3, 4, 8, 11\}\}$. We haven't found PD-sets of size $g_6 = 4$ for the corresponding $[55, 21, 5]_2$ code for the information set $I_6 = \{1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 14, 15, 16, 20, 21, 26, 31, 36, 41, 46, 51\}$, but not all subsets of the automorphism group A_6 of the code of size 4 were checked. No subgroups of A_6 of order 4, 5 or 6 are PD-sets for I_6. But, there are exactly 24 subgroups of A_6 of order 10 that are PD-sets for I_6. One of them is the permutation group generated by generators d and e given below:*

DOI: http://dx.doi.org/10.22108/toc.2017.21615

$d = (2,16)(3,46)(4,36)(5,41)(6,34)(7,50)(8,39)(9,30)(11,20)(12,38)(13,28)(14,54)(15,24)$
$(17,48)(18,26)(19,52)(21,35)(22,40)(23,55)(25,45)(29,43)(31,47)(32,51)(33,42)(49,53)$,
$e = (1,10,44,37,27)(2,7,42,40,28)(3,6,45,38,26)(4,9,41,39,29)(5,8,43,36,30)(11,17,47,35,24)$
$(12,18,46,34,25)(13,16,50,33,22)(14,19,49,32,23)(15,20,48,31,21)(51,55,54,52,53)$.

Example 7. *Let D_7 be a symmetric $(16,6,2)$-design with the set of points $P_7 = \{1,2,3,\dots,16\}$ and blocks $B_7 = \{\{1,2,3,4,5,6\},\{1,2,13,14,15,16\},\{1,3,9,10,11,13\}, \{1,4,7,8,9,16\}$, $\{1,5,8,10,12,14\},\{1,6,7,11,12,15\},\{2,3,7,8,12,13\},\{2,4,10,11,12,16\}$, $\{2,5,7,9,11,14\},\{2,6,8,9,10,15\},\{3,4,9,12,14,15\},\{3,5,7,10,15,16\}$, $\{3,6,8,11,14,16\},\{4,5,8,11,13,15\}, \{4,6,7,10,13,14\},\{5,6,9,12,13,16\}\}$.*

The Gordon bound for the corresponding $[96,31,6]_2$ code is $g_7 = 3$. We have found 16 PD-sets of size 12 for the information set $I_7 = \{1,2,3,4,5,6,7,9,10,11,12,13,15,16,17,19,21,2225,29,31,37,43,49,55,61,67,73,79,85,91\}$. Not all subsets of size 12 (or less) were checked (as the computation becomes more difficult with a larger automorphism group). One of those PD-sets of size 12 is
$S_7 = \{(),(1,8)(3,37)(4,43)(5,49)(6,55)(9,13)(10,25)(11,31)(12,19)(14,42)(15,95)(16,89)$
$(17,83)(20,48)(21,72)(22,78)(23,96)(26,54)(27,77)(28,90)(29,65)(32,60)(33,71)(34,84)(35,66)$
$(39,67)(40,73)(41,61)(45,85)(46,79)(47,62)(51,68)(52,91)(53,80)(57,74)(58,92)(59,86)(63,94)$
$(70,87)(76,81),(1,14)(2,18)(3,13)(4,15)(5,16)(6,17)(7,38)(8,42)(9,37)(10,39)(11,40)$
$(12,41)(19,61)(20,63)(21,65)(22,66)(23,62)(24,64)(25,67)(26,70)(27,71)(28,68)(29,72)(30,69)$
$(31,73)(32,76)(33,77)(34,74)(35,78)(36,75)(43,95)(44,93)(45,91)(46,92)(47,96)(48,94)(49,89)$
$(50,88)(51,90)(52,85)(53,86)(54,87)(55,83)(56,82)(57,84)(58,79)(59,80)(60,81),(1,23,54,74)$
$(2,24,50,75)(3,20,51,76)(4,21,53,73)(5,22,49,78)(6,19,52,77)(7,93,30,56)(8,96,26,57)$
$(9,94,28,60)(10,92,25,58)(11,95,29,59)(12,91,27,55)(13,63,90,32)(14,62,87,34)(15,65,86,31)$
$(16,66,89,35)(17,61,85,33)(18,64,88,36)(37,48,68,81)(38,44,69,82)(39,46,67,79)(40,43,72,80)$
$(41,45,71,83)(42,47,70,84),(1,23,87,34)(2,93,88,82)(3,63,90,76)(4,52,86,17)(5,58,89,46)$
$(6,15,85,53)(7,24,69,36)(8,96,70,84)(9,48,68,60)(10,78,67,66)(11,12,72,71)(13,20,51,32)$
$(14,62,54,74)(16,79,49,92)(18,44,50,56)(19,21,33,31)(22,39,35,25)(26,57,42,47)(27,40,41,29)$
$(28,81,37,94)(30,75,38,64)(43,91,59,83)(45,80,55,95)(61,65,77,73),(1,26)(2,30)(3,28)(4,27)$
$(5,25)(6,29)(7,50)(8,54)(9,51)(10,49)(11,52)(12,53)(13,68)(14,70)(15,71)(16,67)(17,72)$
$(18,69)(19,80)(20,81)(21,83)(22,79)(23,84)(24,82)(31,91)(32,94)(33,95)(34,96)(35,92)(36,93)$
$(37,90)(38,88)(39,89)(40,85)(41,86)(42,87)(43,77)(44,75)(45,73)(46,78)(47,74)(48,76)(55,65)$
$(56,64)(57,62)(58,66)(59,61)(60,63),(1,34,54,62)(2,36,50,64)(3,32,51,63)(4,31,53,65)$
$(5,35,49,66)(6,33,52,61)(7,82,30,44)(8,84,26,47)(9,81,28,48)(10,79,25,46)(11,80,29,43)$
$(12,83,27,45)(13,76,90,20)(14,74,87,23)(15,73,86,21)(16,78,89,22)(17,77,85,19)(18,75,88,24)$
$(37,60,68,94)(38,56,69,93)(39,58,67,92)(40,59,72,95)(41,55,71,91)(42,57,70,96),(1,34,87,23)$
$(2,82,88,93)(3,76,90,63)(4,17,86,52)(5,46,89,58)(6,53,85,15)(7,36,69,24)(8,84,70,96)$
$(9,60,68,48)(10,66,67,78)(11,71,72,12)(13,32,51,20)(14,74,54,62)(16,92,49,79)(18,56,50,44)$
$(19,31,33,21)(22,25,35,39)(26,47,42,57)(27,29,41,40)(28,94,37,81)(30,64,38,75)(43,83,59,91)$

DOI: http://dx.doi.org/10.22108/toc.2017.21615

$(45, 95, 55, 80)(61, 73, 77, 65)$, $(1, 42)(2, 18)(3, 9)(4, 95)(5, 89)(6, 83)(7, 38)(8, 14)(10, 67)(11, 73)$ $(12, 61)(13, 37)(15, 43)(16, 49)(17, 55)(19, 41)(20, 94)(21, 29)(22, 35)(23, 47)(24, 64)(25, 39)(26, 87)$ $(27, 33)(28, 51)(30, 69)(31, 40)(32, 81)(34, 57)(36, 75)(44, 93)(45, 52)(46, 58)(48, 63)(50, 88)(53, 59)$ $(54, 70)(56, 82)(60, 76)(62, 96)(65, 72)(66, 78)(68, 90)(71, 77)(74, 84)(79, 92)(80, 86)(85, 91)$, $(1, 47, 87, 57)(2, 44, 88, 56)(3, 48, 90, 60)(4, 45, 86, 55)(5, 46, 89, 58)(6, 43, 85, 59)(7, 64, 69, 75)$ $(8, 62, 70, 74)(9, 63, 68, 76)(10, 66, 67, 78)(11, 61, 72, 77)(12, 65, 71, 73)(13, 94, 51, 81)(14, 96, 54, 84)$ $(15, 91, 53, 83)(16, 92, 49, 79)(17, 95, 52, 80)(18, 93, 50, 82)(19, 29, 33, 40)(20, 28, 32, 37)(21, 27, 31, 41)$ $(22, 25, 35, 39)(23, 26, 34, 42)(24, 30, 36, 38)$, $(1, 47, 54, 84)(2, 64, 50, 36)(3, 94, 51, 60)(4, 29, 53, 11)$ $(5, 35, 49, 66)(6, 41, 52, 71)(7, 44, 30, 82)(8, 62, 26, 34)(9, 20, 28, 76)(10, 79, 25, 46)(12, 85, 27, 17)$ $(13, 48, 90, 81)(14, 96, 87, 57)(15, 72, 86, 40)(16, 78, 89, 22)(18, 24, 88, 75)(19, 45, 77, 83)(21, 59, 73, 95)$ $(23, 70, 74, 42)(31, 43, 65, 80)(32, 37, 63, 68)(33, 55, 61, 91)(38, 93, 69, 56)(39, 58, 67, 92)$, $(1, 54)(2, 30)$ $(3, 90)(4, 77)(5, 10)(6, 65)(7, 50)(8, 26)(9, 68)(11, 91)(12, 80)(13, 51)(14, 87)(15, 33)(16, 39)$ $(17, 21)(18, 69)(19, 53)(20, 76)(22, 46)(23, 34)(24, 82)(25, 49)(27, 43)(28, 37)(29, 55)(31, 52)(32, 63)$ $(35, 58)(36, 93)(38, 88)(40, 45)(41, 59)(42, 70)(44, 75)(47, 57)(48, 81)(56, 64)(60, 94)(61, 86)(62, 74)$ $(66, 92)(67, 89)(71, 95)(72, 83)(73, 85)(78, 79)(84, 96)\}$.

Example 8. *Let D_8 be a symmetric $(16, 6, 2)$-design with the set of points $P_8 = \{1, 2, 3, \ldots, 16\}$ and the set of blocks* $B_8 = \{\{1, 2, 3, 4, 5, 6\}, \{1, 2, 13, 14, 15, 16\}, \{1, 3, 9, 10, 11, 13\}, \{1, 4, 7, 8, 9, 16\}, \{1, 5, 8, 10, 12, 14\}, \{1, 6, 7, 11, 12, 15\}, \{2, 3, 7, 8, 10, 15\}, \{2, 4, 10, 11, 12, 16\}, \{2, 5, 7, 9, 11, 14\}, \{2, 6, 8, 9, 12, 13\}, \{3, 4, 9, 12, 14, 15\}, \{3, 5, 7, 12, 13, 16\}, \{3, 6, 8, 11, 14, 16\}, \{4, 5, 8, 11, 13, 15\}, \{4, 6, 7, 10, 13, 14\}, \{5, 6, 9, 10, 15, 16\}\}$.

For the corresponding $[96, 31, 6]_2$ code with the automorphism group A_8 the Gordon bound is $g_8 = 3$. Among all subgroups of A_8 of order 12, there are exactly 104 subgroups that are PD-sets for the information set $I_8 = \{1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 15, 16, 17, 19, 21, 22, 25, 29, 31, 37, 43, 49, 55, 61, 67, 73, 79, 85, 91\}$. *One of those PD-sets of size 12 is a permutation group generated by the following permutations:*

$f = (1, 82)(2, 81)(3, 83)(4, 79)(5, 80)(6, 84)(7, 76)(8, 75)(9, 73)(10, 77)(11, 74)(12, 78)(13, 17)$ $(14, 18)(15, 16)(19, 46)(20, 44)(21, 47)(22, 43)(23, 45)(24, 48)(25, 53)(26, 50)(27, 49)(28, 52)$ $(29, 51)(30, 54)(31, 34)(32, 36)(33, 35)(37, 57)(38, 60)(39, 59)(40, 55)(41, 58)(42, 56)(61, 89)$ $(62, 85)(63, 88)(64, 87)(65, 90)(66, 86)(67, 71)(69, 70)(92, 95)(93, 94)$,

$g = (1, 84, 69)(2, 81, 72)(3, 79, 71)(4, 83, 67)(5, 80, 68)(6, 82, 70)(7, 42, 21)(8, 40, 24)(9, 38, 20)$ $(10, 41, 23)(11, 39, 19)(12, 37, 22)(13, 66, 87)(14, 62, 89)(15, 65, 88)(16, 63, 90)(17, 64, 86)$ $(18, 61, 85)(25, 95, 51)(26, 91, 50)(27, 96, 49)(28, 93, 54)(29, 92, 53)(30, 94, 52)(31, 36, 33)$ $(32, 34, 35)(43, 57, 78)(44, 60, 73)(45, 58, 77)(46, 59, 74)(47, 56, 76)(48, 55, 75)$,

$h = (1, 53)(2, 49)(3, 52)(4, 54)(5, 50)(6, 51)(7, 46)(8, 43)(9, 45)(10, 44)(11, 47)(12, 48)(13, 17)$ $(14, 15)(16, 18)(19, 76)(20, 77)(21, 74)(22, 75)(23, 73)(24, 78)(25, 82)(26, 80)(27, 81)(28, 83)$ $(29, 84)(30, 79)(31, 34)(32, 33)(35, 36)(37, 55)(38, 58)(39, 56)(40, 57)(41, 60)(42, 59)(61, 63)$

DOI: http://dx.doi.org/10.22108/toc.2017.21615

$(62,65)(64,66)(67,93)(68,91)(69,92)(70,95)(71,94)(72,96)(85,90)(86,87)(88,89)$.

In this PD-set of size 12 *we have found six PD-sets of size* 9*. Not all subsets of size* 9 *or less were checked. One of those PD-sets of size* 9 *for* I_8 *is*

$S_8 = \{(1,29,69,53,84,92)(2,27,72,49,81,96)(3,30,71,52,79,94)(4,28,67,54,83,93)$
$(5,26,68,50,80,91)(6,25,70,51,82,95)(7,59,21,46,42,74)(8,57,24,43,40,78)(9,58,20,45,38,77)$
$(10,60,23,44,41,73)(11,56,19,47,39,76)(12,55,22,48,37,75)(13,64,87,17,66,86)$
$(14,65,89,15,62,88)\ (16,61,90,18,63,85)(31,35,33,34,36,32), (1,51)(2,49)(3,54)(4,52)(5,50)$
$(6,53)(7,39)(8,37)(9,41)\ (10,38)(11,42)(12,40)(13,87)(14,90)(15,85)(16,89)(17,86)(18,88)$
$(19,21)(20,23)(22,24)(25,69)\ (26,68)(27,72)(28,71)(29,70)(30,67)(31,33)(32,34)(43,55)(44,58)$
$(45,60)(46,56)(47,59)(48,57)\ (61,65)(62,63)(73,77)(74,76)(75,78)(79,93)(80,91)(81,96)(82,92)$
$(83,94)(84,95), (1,53)(2,49)\ (3,52)(4,54)(5,50)(6,51)(7,46)(8,43)(9,45)(10,44)(11,47)(12,48)$
$(13,17)(14,15)(16,18)(19,76)\ (20,77)(21,74)(22,75)(23,73)(24,78)(25,82)(26,80)(27,81)(28,83)$
$(29,84)(30,79)(31,34)(32,33)\ (35,36)(37,55)(38,58)(39,56)(40,57)(41,60)(42,59)(61,63)(62,65)$
$(64,66)(67,93)(68,91)(69,92)\ (70,95)(71,94)(72,96)(85,90)(86,87)(88,89), (1,69,84)(2,72,81)$
$(3,71,79)(4,67,83)(5,68,8)(6,70,82)\ (7,21,42)(8,24,40)(9,20,38)(10,23,41)(11,19,39)$
$(12,22,37)(13,87,66)(14,89,62)(15,88,65)\ (16,90,63)(17,86,64)(18,85,61)(25,51,95)(26,50,91)$
$(27,49,96)(28,54,93)(29,53,92)(30,52,94)\ (31,33,36)(32,35,34)(43,78,57)(44,73,60)(45,77,58)$
$(46,74,59)(47,76,56)(48,75,55), (1,70)(2,72)\ (3,67)(4,71)(5,68)(6,69)(7,47)(8,48)(9,44)(10,45)$
$(11,46)(12,43)(13,64)(14,61)(15,63)(16,65)\ (17,66)(18,62)(19,59)(20,60)(21,56)(22,57)(23,58)$
$(24,55)(25,29)(28,30)(31,35)(32,33)(34,36)\ (37,78)(38,73)(39,74)(40,75)(41,77)(42,76)(49,96)$
$(50,91)(51,92)(52,93)(53,95)(54,94)(79,83)\ (82,84)(85,89)(86,87)(88,90), (1,82)(2,81)(3,83)$
$(4,79)(5,80)(6,84)(7,76)(8,75)(9,73)(10,77)\ (11,74)(12,78)(13,17)(14,18)(15,16)(19,46)$
$(20,44)(21,47)(22,43)(23,45)(24,48)(25,53)(26,50)\ (27,49)(28,52)(29,51)(30,54)(31,34)(32,36)$
$(33,35)(37,57)(38,60)(39,59)(40,55)(41,58)(42,56)\ (61,89)(62,85)(63,88)(64,87)(65,90)(66,86)$
$(67,71)(69,70)(92,95)(93,94), (1,84,69)(2,81,72)\ (3,79,71)(4,83,67)(5,80,68)(6,82,70)$
$(7,42,21)(8,40,24)(9,38,20)(10,41,23)(11,39,19)(12,37,22)\ (13,66,87)(14,62,89)(15,65,88)$
$(16,63,90)(17,64,86)(18,61,85)(25,95,51)(26,91,50)(27,96,49)\ (28,93,54)(29,92,53)(30,94,52)$
$(31,36,33)(32,34,35)(43,57,78)(44,60,73)(45,58,77)(46,59,74)\ (47,56,76)(48,55,75),$
$(1,92,84,53,69,29)(2,96,81,49,72,27)(3,94,79,52,71,30)(4,93,83,54,67,28)$
$(5,91,80,50,68,26)(6,95,82,51,70,25)(7,74,42,46,21,59)(8,78,40,43,24,57)$
$(9,77,38,45,20,58)\ (10,73,41,44,23,60)(11,76,39,47,19,56)(12,75,37,48,22,55)$
$(13,86,66,17,87,64)(14,88,62,15,89,65)\ (16,85,63,18,90,61)(31,32,36,34,33,35),$
$(1,95)(2,96)(3,93)(4,94)(5,91)(6,92)(7,11)(8,12)(9,10)\ (13,66)(14,63)(15,61)(16,62)$
$(17,64)(18,65)(19,42)(20,41)(21,39)(22,40)(23,38)(24,37)(25,84)\ (26,80)(27,81)(28,79)(29,82)$
$(30,83)(31,36)(34,35)(43,48)(44,45)(46,47)(49,72)(50,68)(51,69)\ (52,67)(53,70)(54,71)(55,78)$
$(56,74)(57,75)(58,73)(59,76)(60,77)(85,88)(89,90)\}$.

DOI: http://dx.doi.org/10.22108/toc.2017.21615

Acknowledgments

This work has been fully supported by Croatian Science Foundation under the project 1637.

References

[1] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.*, **24** (1997) 235–265.

[2] P. Dankelmann, J. D. Key and B. G. Rodrigues, Codes from incidence matrices of graphs, *Des. Codes Cryptogr.*, **68** (2013) 373–393.

[3] D. Davies, Flag-transitivity and primitivity, *Discrete Math.*, **63** (1987) 91–91.

[4] The GAP Group, GAP - Groups, Algorithms and Programming, Version 4.4.12, available at www.gap-system.org

[5] D. M. Gordon, Minimal permutation sets for decoding the binary Golay codes, *IEEE Trans. Inform. Theory*, **28** (1982) 541–543.

[6] W. C. Huffman, Codes and groups, in: V. S. Pless, W. C. Huffman (Eds.), *Handbook of Coding Theory*, Elsevier, Amsterdam, 1998, pp. 1345–1440.

[7] W. Kantor, Automorphism Groups of Designs, *Math. Z.*, **109** (1969) 246–252 .

[8] J. D. Key, Permutation decoding for codes from designs, finite geometries and graphs, in: D. Crnković, V. Tonchev (Eds.), *Information Security, Coding Theory and Related Combinatorics*, NATO Science for Peace and Security Series - D: Information and Communication Security, **29**, IOS Press, Amsterdam, 2011, pp. 172–201.

[9] F. J. MacWilliams, Permutation decoding of systematic codes, *Bell Syst. Tech. J.*, **43** (1964) 485–505.

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1998.

[11] E. O'Reilly-Regueiro, Classification of flag-transitive symmetric designs, 6th Czech-Slovak International Symposium on Combinatorics, Graph Theory, Algorithms and Applications, *Electron. Notes Discrete Math.*, **28** (2007) 535–542.

[12] C. E. Praeger and S. Zhou, Imprimitive flag-transitive symmetric designs, *J. Combin. Theory Ser. A*, **113** (2006) 1381–1395.

Dean Crnković

Department of Mathematics, University of Rijeka, Radmile Matejčić 2, 51000 Rijeka, Croatia

Email: deanc@math.uniri.hr

Nina Mostarac

Department of Mathematics, University of Rijeka, Radmile Matejčić 2, 51000 Rijeka, Croatia

Email: nmavrovic@math.uniri.hr

DOI: http://dx.doi.org/10.22108/toc.2017.21615