ARS COMBINATORIA 167 (2026) 181–194

Ars Combinatoria
www.combinatorialpress.com/ars

Combinatorial Press

Partial permutation decoding for codes from ovals

Jirapha Limbupasiriporn*

ABSTRACT

In finite desarguesian projective planes of prime power order q, we consider the MDS codes obtained from ovals and generate new codes for the purpose of permutation decoding. We show that those new codes are $[q^2-1, 3, (q-1)^2]_q$ codes and have s-PD-sets for $s \leq q-1$.

Keywords: projective planes, ovals, linear codes, MDS codes, permutation decoding

2020 Mathematics Subject Classification: 94B05, 94B35, 51E05, 51E15.

1. Introduction

We consider codes obtained from configurations in a finite desarguesian projective plane $PG_2(\mathbb{F}_q)$ of prime power order q. In general, configurations in finite projective geometries, specifically ovals in planes, can be used to produce codes with good parameters, including certain MDS codes. In this paper, we examine codes obtained from ovals with a view to their use in permutation decoding. We construct an MDS linear code with a generator matrix whose columns form a conic in $PG_2(\mathbb{F}_q)$, and extend this to a new linear code by augmenting the matrix with scalar multiples of each column. Furthermore, we determine the automorphism group of the new code and use it to perform permutation decoding.

The efficiency of permutation decoding is primarily determined by the size of a PD-set. For an $[n, k, d]_q$ linear code with $t = \lfloor (d-1)/2 \rfloor$, the minimum possible size for a PD-set that corrects $s \leq t$ errors is bounded below by the Gordon bound $G(t)$, as noted in Section 2. This bound can be modified for s-PD-sets used in partial permutation decoding. In [12], the lower bound is generalized for s-PD-sets, showing that $G(s) \geq s+1$.

In this work, we provide a 2-PD-set of size 5, which is close to the bound of $s+1=3$. Moreover, we obtain $(q-1)$-PD-sets that, while larger than this theoretical minimum, allow for an explicit and structured decoding process.

* Corresponding author.

Received 19 Nov 2025; Revised 20 May 2026; Accepted 30 May 2026; Published Online 17 June 2026.
DOI: 10.61091/ars167-12

The paper is organized as follows: we introduce basic terminology in Section 2 and a brief background on ovals and conics in finite projective planes in Section 3. We describe in Section 4 the structure of an MDS code $\overline{C}$ obtained from an oval in $PG_2(\mathbb{F}_q)$ and then for the purpose of permutation decoding, we construct a new code C from the code $\overline{C}$ of the same dimension as $\overline{C}$ but with length and minimum weight much greater than those of the original code $\overline{C}$. We apply, in Section 5, partial permutation decoding to the code C and construct explicit small s-PD-sets for C. The size of those s-PD sets is found to be close to the minimum bound for PD-sets. Also we obtain a $(q-1)$-PD-set for C of size depending on the order q of $PG_2(\mathbb{F}_q)$. Finally, using MAGMA results, we obtain codes from ovals in $PG_2(\mathbb{F}_q)$ for some q and show how to construct PD-sets of such codes for full error correction.

2. Preliminaries

Basic terminology and results regarding to designs, geometries, linear codes and permutation decoding can be found in [1, 2, 8].

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ with point set $\mathcal{P}$, block set $\mathcal{B}$, and incidence $\mathcal{I}$ is a t-(v, k, λ) design, where t, v, k, and λ are non-negative integers, if $\mathcal{P}$ has v points, every block in $\mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. A design is symmetric if it has the same number of points and blocks. For $n \geq 2$, a symmetric 2-$(n^2+n+1, n+1, 1)$ design is called a finite projective plane of order n with blocks called the lines of the plane.

For any finite field $\mathbb{F}_q$ of order q, the set of points and r-dimensional subspaces of an n-dimensional projective geometry $PG_n(\mathbb{F}_q)$ forms a 2-design and we will denote it by $PG_{n,r}(\mathbb{F}_q)$. In particular, we write $PG_2(\mathbb{F}_q)$ for the desarguesian projective plane $PG_{2,1}(\mathbb{F}_q)$, i.e. the design of points and 1-dimensional subspaces of the projective spaces $PG_2(\mathbb{F}_q)$. The automorphism groups of these designs are the full projective semilinear groups $P\Gamma L_n(\mathbb{F}_q)$ and are always 2-transitive on points.

All the codes here are q-ary linear codes which are subspaces of $\mathbb{F}_q^n$, an n-dimensional vector space over the finite field $\mathbb{F}_q$ of order q. The elements of the codes are codewords. The support of a vector x in $\mathbb{F}_q^n$ is the set of nonzero coordinate positions of x, and the weight of x is the cardinality of its support. If C is a q-ary linear code of length n and dimension k and with minimum weight d, then it is said to be an $[n, k, d]_q$ code. For any integer i such that $0 \leq i \leq n$, A_i denotes the number of codewords in a code C of Hamming weight i. The list of A_i for $0 \leq i \leq n$ is the weight distribution of C. A generator matrix for C is a $k \times n$ matrix whose rows form a basis for C. The dual code $C^\perp$ of the code C is the orthogonal complement of C under the standard inner product $(,)$ on $\mathbb{F}_q^n$, i.e. $C^\perp = \{x \in \mathbb{F}_q^n \mid (x, c) = 0 \text{ for all } c \in C\}$. The dual code $C^\perp$ is also linear over $\mathbb{F}_q$ and of dimension $n-k$. A check matrix for C is a generator matrix for $C^\perp$. Two linear codes are said to be isomorphic if they can be obtained from one another by permuting the coordinate positions. An automorphism of C is an isomorphism of C onto itself. Clearly any automorphism preserves each weight class of C and the set of all automorphisms of C forms a group, called the automorphism group of C and denoted

by $\mathrm{Aut}(C)$. Any code is isomorphic to a code with a generator matrix in standard form $[I_k \mid A]$, where A is a $k \times (n-k)$ matrix, and in which case $H = [-A^t \mid I_{n-k}]$ is a check matrix for C. Any k-subset of coordinate positions of C corresponding to a set of k linearly independent columns of a generator matrix G for C is an information set for C, and the set of remaining $n-k$ coordinate positions is a check set for C. If the first k coordinates of C form an information set, then its generator matrix can be reduced into standard form. The integer $n-k$ is the redundancy and the number k/n is the information rate of the code.

The following result shows that if a linear code C has minimum weight d, then d is the smallest number of linearly dependent columns of its parity-check matrix. Furthemore, it provides the determination of minimum weight of a linear code using a check matrix, see [6].

Result 2.1. Let C be a linear code with parity check matrix H. Then the minimum weight of C is d if and only if any $d-1$ columns of H are linearly independent but some d columns are linearly dependent.

For any $[n,k,d]_q$ code C, one of the simplest upper bound on the size of C is given by the Singleton bound, $d \leq n-k+1$. Any linear code for which equality holds in the Singleton bound is called a maximum distance separable code, abbreviated as MDS code. It is known that a linear code is MDS if and only if its dual is MDS. Moreover, an MDS code of length n and dimension k has precisely k distinct nonzero weights, $d, d+1, \ldots, n$, and the weight distribution of the code is given by $A_0 = 1$, $A_i = 0$ for $1 \leq i < d$, and for each i such that $d \leq i \leq n$,

$$A_i = \binom{n}{i} \sum_{j=0}^{i-d} (-1)^j \binom{i}{j} \left(q^{i+1-d-j} - 1\right), \tag{1}$$

see [1, Chapter 2] or [13, Chapter 11].

For decoding, we want to determine, from a received vector, which codeword in C was sent. The minimum weight of C completely determines the error-detecting and error-correcting capabilities of the code, i.e. C can detect up to $d-1$ errors or correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.

Permutation decoding is a decoding technique described fully in MacWilliams and Sloane [13, Chapter 16] and Huffman [7, Section 8]. It uses a set S of automorphisms of a t-error-correcting $[n,k,d]_q$ code C, called a PD-set, such that every t-set of coordinate positions for C is moved by at least one member of S into the check positions for C. The existence of a PD-set for C depends on the choice of information and check sets for the codes. If C has a PD-set S and redundancy r, then a lower bound on the size of S can be determined by a Gordon bound, due to Gordon [5], from a formula due to Schönheim [14], and quoted and proved in [7]. That bound is given as follows:

$$|S| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil = G(t). \tag{2}$$

In [10, 11], the notion of partial permutation decoding for codes was introduced to correct small numbers of errors less than the full error-correction capability of the code. Thus for $s \leq t$, an s-PD-set for a t-error-correcting code C is similarly defined to be a set of automorphisms of C such that every s-set of coordinate positions is moved by at least one member of the set into the check positions. The minimum size of an s-PD-set can also be computed by the Gordon bound quoted above with replacing t by s in the formula for $G(s)$.

The algorithm for permutation decoding can be stated as follows: given a t-error-correcting $[n, k, d]_q$ code C with generator matrix G and check matrix H both in standard form and with the first k coordinate positions corresponding to the information symbols, let $S = \{g_1, g_2, \ldots, g_m\}$ be a PD-set for C and encode any vector v of length k as vG. If x is sent and y is received with at most t errors, then firstly compute the syndromes $H(yg_i)^T$ for $i = 1, 2, \ldots, m$ until an i is found such that the weight of this vector is t or less, then compute the codeword c that has the same information symbols as yg_i, and finally decode y as cg_i^{-1}.

3. Ovals and conics

A brief description of background on ovals and conics in a finite projective plane is provided, see Assmus and Key [1, Chapter 3] or Hughes and Piper [9, Chapter 2] for further discussion.

An oval $\mathcal{O}$ in a finite projective plane Π of order q is a set of points of Π such that lines meet $\mathcal{O}$ in at most two points, and which is maximal with this property. It follows that $\mathcal{O}$ consists of $q + 1$ points if q is odd and $q + 2$ points if q is even, in which case ovals are also called hyperovals. A conic in a projective plane is the set of all zeros of a non-degenerate quadratic form. A conic in the desarguesian projective plane $PG_2(\mathbb{F}_q)$ of order q has $q + 1$ points. All conics in $PG_2(\mathbb{F}_q)$ are equivalent, and hence, we need only consider the conic with equation $y^2 = xz$. The number of solutions of this is $q + 1$ and lines meet it in at most two points. Thus in the odd case, conics give ovals. In the q even case, the $q + 1$ tangents to a conic meet in a point, and this can be added to the set to give an oval (hyperoval). An oval from a conic is called a regular oval. Segre [15] showed that in $PG_2(\mathbb{F}_q)$ with q odd, every oval is regular. When q is even and $q \geq 16$, there are families of hyperovals that are not regular.

From the canonical form given above, a conic $\mathcal{C}$ in $PG_2(\mathbb{F}_q)$ consists of the point $(1, 0, 0)$ and all points of the form $(y^2, y, 1)$ for $y \in \mathbb{F}_q$ so that

$$\begin{aligned} \mathcal{C} &= \{(x, y, z) \in PG_2(\mathbb{F}_q) \mid y^2 = xz\} \\ &= \{(1, 0, 0)\} \cup \{(y^2, y, 1) \mid y \in \mathbb{F}_q\}. \end{aligned} \tag{3}$$

These points can also be represented in parametric coordinates by identifying the point $(1, 0, 0)$ with a new symbol ∞ and the point $(y^2, y, 1)$ with the element y in $\mathbb{F}_q$. The elements of the projective general linear group $PGL_3(\mathbb{F}_q)$ that fix the conic form a subgroup G of $PGL_3(\mathbb{F}_q)$. This group G is 3-transitive on the points of the conic $\mathcal{C}$ and its elements

are defined on $PG_2(\mathbb{F}_q)$ by

$$T(a,b,c,d) = \begin{bmatrix} a^2 & ac & c^2 \\ 2ab & ad+bc & 2cd \\ b^2 & bd & d^2 \end{bmatrix}, \tag{4}$$

for all $a,b,c,d \in \mathbb{F}_q$ such that $ad-bc \neq 0$. The group G induces a group of permutations on the $q+1$ points in $\mathcal{C}$ given in parametric form as

$$\tau_{a,b,c,d} : y \mapsto \frac{ay+b}{cy+d}, \tag{5}$$

for all $y \in \mathbb{F}_q \cup \{\infty\}$ and $a,b,c,d \in \mathbb{F}_q$ such that $ad-bc \neq 0$. Since the parametric coordinates for $\mathcal{C}$ can also be defined as for the projective line, it follows that the group G is isomorphic to the projective semilinear group $P\Gamma L_2(\mathbb{F}_q)$.

4. Codes from ovals

We generate a new code based on the MDS code obtained from a matrix whose columns form a conic in $PG_2(\mathbb{F}_q)$. Consider a $3 \times (q+1)$ matrix $\overline{G}$ with entries in $\mathbb{F}_q$ given by

$$\overline{G} = \begin{bmatrix} 1 & 1 & \cdots & 1 & 1 & 0 \\ y_1 & y_2 & \cdots & y_{q-1} & 0 & 0 \\ y_1^2 & y_2^2 & \cdots & y_{q-1}^2 & 0 & 1 \end{bmatrix}, \tag{6}$$

where the y_i's are distinct non-zero elements of $\mathbb{F}_q$. Let $\overline{C}$ be the code over $\mathbb{F}_q$ with generator matrix $\overline{G}$. Note that if we regard the columns of $\overline{G}$ as points in $PG_2(\mathbb{F}_q)$, then these points, when reversing the coordinate positions, form the conic $\mathcal{C}$ as given in (3). Since every conic is an oval, no three points of $\mathcal{C}$ are on the same line, which implies that every three columns of $\overline{G}$ are linearly independent. Moreover, since every four columns of $\overline{G}$ are linearly dependent, it follows from Result 2.1 that the minimum weight of the dual code $\overline{C}^{\perp}$ is 4. Hence $\overline{C}^{\perp}$ is a $[q+1, q-2, 4]_q$ MDS code, and its dual $\overline{C}$ is a $[q+1, 3, q-1]_q$ MDS code. Note that $\overline{C}^{\perp}$ is the code of the largest length with minimum distance 4 and redundancy 3.

We take the points in the conic $\mathcal{C}$ as the coordinate positions of the code $\overline{C}$ with the order corresponding to the columns of $\overline{G}$. Recall that the points in $\mathcal{C}$ can be represented in parametric form by the elements of $\mathbb{F}_q \cup \{\infty\}$. Although $P\Gamma L_2(\mathbb{F}_q)$ is an automorphism group of $\mathcal{C}$, it cannot be an automorphism group of the code $\overline{C}$ when $q > 3$. This is because the collineation $\tau = \tau_{0,1,1,0} : y \mapsto y^{-1}$ of $P\Gamma L_2(\mathbb{F}_q)$ does not preserve the code $\overline{C}$. In particular, τ maps the first row vector $u = (1,1,\ldots,1,1,0)$ of $\overline{G}$ into $u^\tau = (1,1,\ldots,1,0,1)$, which is not in a row span of $\overline{G}$. Thus $u^\tau \notin \overline{C}$. In fact, the collineations of $P\Gamma L_2(\mathbb{F}_q)$ as given in (5) map $\overline{C}$ onto another code equivalent to $\overline{C}$.

We now construct a new code from the code $\overline{C}$. Let G be a $3 \times (q^2-1)$ matrix consisting of $3 \times (q-1)$ submatrices B_i, for $i \in \{1,2,\ldots,q,\infty\}$, whose columns are obtained by multiplying the i^{th} column of $\overline{G}$ by the distinct non-zero elements of $\mathbb{F}_q$, i.e.

$$G = \begin{bmatrix} B_1 & B_2 & \cdots & B_q & B_\infty \end{bmatrix} \tag{7}$$

where

$$B_\infty = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 1 & \delta_1 & \cdots & \delta_{q-2} \end{bmatrix}, \tag{8}$$

$$B_i = \begin{bmatrix} 1 & \delta_1 & \cdots & \delta_{q-2} \\ y_i & \delta_1 y_i & \cdots & \delta_{q-2} y_i \\ y_i^2 & \delta_1 y_i^2 & \cdots & \delta_{q-2} y_i^2 \end{bmatrix}, \tag{9}$$

for $1 \leq i \leq q$ with $\delta_0 = 1$ and δ_j, for $1 \leq j \leq q-2$, the distinct non-zero elements of $\mathbb{F}_q$. Let C be the code over $\mathbb{F}_q$ with generator matrix G. As the underlying code $\overline{C}$ is a $[q+1, 3, q-1]_q$-MDS code, it has exactly three distinct nonzero weights, $q-1$, q and $q+1$. According to the formula in (1), the weight distribution of the code $\overline{C}$ is listed in Table 1. Further, since the generator matrix G for the code C is obtained by augmenting $(q-1)$ nonzero columns to each column of $\overline{G}$, all nonzero codewords in C have weights $(q-1)^2$, $q(q-1)$ or q^2-1. The weight distribution of C is obtained from that of $\overline{C}$ as shown in Table 2. Thus C is a $[q^2-1, 3, (q-1)^2]_q$ code. By Result 2.1, the dual code $C^\perp$ is a $[q^2-1, q^2-4, 2]_q$ code. Note that C can correct up to $\frac{(q-1)^2-2}{2}$ errors if q is odd, and $\frac{(q-1)^2-1}{2}$ errors if q is even.

Table 1. Weight distribution of the $[q+1, 3, q-1]_q$-MDS code $\overline{C}$

i	$q-1$	q	$q+1$
A_i	$\frac{q(q^2-1)}{2}$	q^2-1	$\frac{q(q-1)^2}{2}$

Table 2. Weight distribution of the new code C

i	$(q-1)^2$	$q(q-1)$	q^2-1
A_i	$\frac{q(q^2-1)}{2}$	q^2-1	$\frac{q(q-1)^2}{2}$

As described in Section 3, the group in $PGL_3(\mathbb{F}_q)$ that fixes the conic will be examined to see if it is an automorphism group of the code C. Recall that a permutation matrix is a square matrix with exactly one 1 in each row and each column and 0 elsewhere. The following result shows how to determine an automorphism group of a code: see MacWilliams and Sloane [13, Chapter 8].

Result 4.1. Let C be an $[n, k]_q$ code with generator matrix G. Let P be an $n \times n$ permutation matrix and ρ the corresponding permutation. Then ρ is in $\mathrm{Aut}(C)$ if and only if there exists an invertible $k \times k$ matrix A such that $AG = GP$.

We regard the columns of the matrix G, as given in (7), as points in $PG_2(\mathbb{F}_q)$ with multiplicity $q-1$ and take them as the coordinate positions of C with the order corresponding to the columns of G. In other words, the coordinate positions of C are given by the multiset $\mathcal{P}$ of points in the conic $\mathcal{C}$ as given in (3). For convenience, we denote by P_∞

the point $(1,0,0)$ and by P_y the point $(y^2,y,1)$ for all $y \in \mathbb{F}_q$. For each δ in $\mathbb{F}_q^\times$ (the set of nonzero elements in $\mathbb{F}_q$) and each y in $\mathbb{F}_q \cup \{\infty\}$, the point δP_y is a scalar multiple of P_y. Then

$$\mathcal{P} = \{\delta P_y \mid y \in \mathbb{F}_q \cup \{\infty\},\ \delta \in \mathbb{F}_q^\times\}. \tag{10}$$

Note that for any $a,b,c,d \in \mathbb{F}_q$ with $ad-bc \neq 0$, the collineation $T(a,b,c,d)$ defined as in (4) maps the points in $\mathcal{P}$ into the following:

$$(P_\infty)T(a,b,c,d) = \begin{cases} c^2 P_{ac^{-1}} & \text{if } c \neq 0, \\ a^2 P_\infty & \text{if } c = 0, \end{cases}$$

$$(P_y)T(a,b,c,d) = \begin{cases} (cy+d)^2 P_{\frac{ay+b}{cy+d}} & \text{if } cy+d \neq 0, \\ (ay+b)^2 P_\infty & \text{if } cy+d = 0. \end{cases}$$

Thus $T(a,b,c,d)$ acts imprimitively on the blocks B_i for $i \in \{1,2,\ldots,q,\infty\}$.

Now, let $K = G^t T(a,b,c,d)$. Then K^t is a $3 \times (q^2-1)$ matrix obtained from G by rearranging its columns. Thus K can be written as $K = PG^t$, where P is a $(q^2-1) \times (q^2-1)$ permutation matrix, and hence, $K^t = T(a,b,c,d)^t G = GP^t$. From Result 4.1, the corresponding permutation of $\mathcal{P}$ is in $\mathrm{Aut}(C)$. This implies that $T(a,b,c,d)$ is an automorphism of C. Therefore, we have the following:

Proposition 4.2. *The code C with generator matrix G given in (7) is a $[q^2-1,3,(q-1)^2]_q$ code over $\mathbb{F}_q$ and the set*

$$\mathcal{A} = \{T(a,b,c,d) \mid a,b,c,d \in \mathbb{F}_q,\ ad-bc \neq 0\}, \tag{11}$$

is an automorphism group of C where $T(a,b,c,d)$ is defined as in (4).

Note 4.3. 1. $T(a,b,c,d) = T(a',b',c',d')$ if and only if $a' = \pm a$, $b' = \pm b$, $c' = \pm c$, and $d' = \pm d$.

2. The order of the automorphism group $\mathcal{A}$ is $\frac{1}{2}q(q-1)(q^2-1)$ if q is odd, and $q(q-1)(q^2-1)$ if q is even.

5. s-PD-sets

We examine partial permutation decoding for the code C over $\mathbb{F}_q$ as given in Section 4 with a particular information set and then determine computationally if C has PD-sets for full error correction in small cases.

Consider the generator matrix G for the code C as given in (7). Since the first three columns of G are linearly dependent, G cannot reduce into standard form. Note that any two columns in the same block of G are linearly dependent. It follows that the information symbols for C must be taken from the points in the set $\mathcal{P}$ of coordinate positions, as given in (10), that correspond to the columns of G from different blocks B_i's.

Now we take the points $P_1, P_\omega, P_{\omega^2}$ as information symbols and the remaining points in $\mathcal{P}$ as check symbols for C, where ω is a primitive element of $\mathbb{F}_q$. Thus if we reorder

the columns of G so that the first three columns correspond to these information symbols and the rest correspond to the check symbols, we will obtain the generator matrix for C in standard form. Although the order of the information and check positions is not important, we rearrange them so that a new generator matrix G for C is in the following form:

$$G = \left[\begin{array}{ccc|ccccccc} 1 & 1 & 1 & & & & & & & \\ 1 & \omega & \omega^2 & B_1^* & B_\omega^* & B_{\omega^2}^* & B_{\omega^3} & \cdots & B_{\omega^{q-2}} & B_0 & B_\infty \\ 1 & \omega^2 & \omega^4 & & & & & & & \end{array}\right], \tag{12}$$

where, for each $y \in \mathbb{F}_q$, B_y and B_∞ are given as in (8) and (9), and B_y^* is a $3 \times (q-2)$ matrix obtained from B_y by deleting the first column.

Using G given in (12) as a generator matrix for the code C, permutation decoding can be applied. We begin with considering s-PD-sets for C where $s < t$, with t the full error-correction capability of the code. Since the automorphism group $\mathcal{A}$ of C in Proposition 4.2 is 3-transitive, $\mathcal{A}$ itself is a 3-PD-set for C. Notice that the size of $\mathcal{A}$ is quite large compared to the minimum lower bound on the size of a 3-PD-set, which is 4 by (2). Theorem 5.1 below gives 2- and 3-PD-sets for C of size close to the minimum bounds. Note that the minimum size of a 2-PD-set for C is 3.

Before proceeding further, we let

$$\mathcal{B}_y = \{\delta P_y \mid \delta \in \mathbb{F}_q^\times\}, \tag{13}$$

for all $y \in \mathbb{F}_q \cup \{\infty\}$. We say a point in the set $\mathcal{P}$ to be error-free if an error does not occur at that point, and a subset of $\mathcal{P}$ is said to be error-free if every point in the set is error-free. Note that for $q = 2$ or 3, the underlying code $\overline{C}$ is a trivial MDS code. However, when $q = 4$ or 5, the new code possesses a PD-set for full error-correction as discussed later.

Theorem 5.1. *Let q be a prime power and $q \geq 7$, and let ω be a primitive element of $\mathbb{F}_q$. Let C be the $[q^2-1, 3, (q-1)^2]_q$ code over $\mathbb{F}_q$ with generator matrix G as given in (12). Take $\mathcal{I} = \{P_1, P_\omega, P_{\omega^2}\}$ as an information set for C, and let $\mathcal{A}$ be an automorphism group of C as given in (11). Then*

1. *the set*

$$\begin{aligned} S = \{&T(1,0,0,1),\ T(1,0,0,-1),\ T(1+\omega, -2\omega^2, 1+\omega^{q-2}, -(1+\omega^2)),\\ &T(\omega, -\omega^2, 1, -1+\omega-\omega^2),\ T(\omega(1+\omega), -2\omega^2, 1+\omega, -(1+\omega^2))\}, \end{aligned}$$

is a 2-PD-set of size 5 for C;

2. *the set*

$$\begin{aligned} S = \Bigg\{&T(1,0,0,1),\ T(1,0,0,-1),\ T\left(\omega, -(1+\omega), \frac{1}{\omega}, -\frac{1+\omega}{\omega}\right),\\ &T(\omega, -\omega(1+\omega), \omega, -(1+\omega)),\ T\left(\frac{1+\omega}{\omega}, -\omega, \frac{1+\omega}{\omega^2}, -\omega\right),\\ &T\left(\frac{1+\omega}{\omega^2}, -\omega, \frac{1+\omega}{\omega^3}, -\frac{1}{\omega}\right),\ T\left(\frac{\omega}{1+\omega}, \frac{\omega}{1+\omega}, \frac{1}{\omega(1+\omega)}, \frac{\omega}{1+\omega}\right)\Bigg\}. \end{aligned}$$

is a 3-PD-set of size 7 for C.

Proof. Let $\mathcal{C} = \mathcal{P}\backslash\mathcal{I}$ be the check set corresponding to the information set $\mathcal{I}$ where $\mathcal{P}$ is the set of coordinate positions of C as given in (10). We need to find collineations that map any three error-free positions in $\mathcal{P}$ into $\mathcal{I}$, i.e. collineations $T(a,b,c,d)$, for $a,b,c,d \in \mathbb{F}_q$ with $ad-bc \neq 0$, that move any two or three errors into the check positions $\mathcal{C}$. Note that if the errors are in the check positions $\mathcal{C}$, the identity map $T(1,0,0,1)$ will keep these in $\mathcal{C}$.

To prove the first part of the theorem, suppose that a pair of errors occurs at the coordinate positions Q_1 and Q_2 in $\mathcal{P}$. Let $\sigma = T(1,0,0,-1)$. Then σ sends the set $\mathcal{K} = \{P_{-1}, P_{-\omega}, P_{-\omega^2}\}$ onto the information set $\mathcal{I}$. Note that $\mathcal{K} \cap \mathcal{I} = \emptyset$ as $q \geq 7$. If $Q_1 \in \mathcal{I}$ and $Q_2 \in \mathcal{I} \cup \mathcal{B}_\infty$, where $\mathcal{B}_\infty$ is given in (13), the collineation σ will take these errors into $\mathcal{C}$.

Thus without loss of generality, assume that $Q_1 \in \mathcal{I}$ and $Q_2 \in \mathcal{C}\backslash\mathcal{B}_\infty$. We distinguish three cases for Q_1.

If $Q_1 = P_1$, then we let $\tau_1 = T(1+\omega, -2\omega^2, 1+\omega^{q-2}, -(1+\omega^2))$. So τ_1 sends the set $\mathcal{K}_1 = \left\{\frac{1}{\omega^2(1-\omega)^2}P_\omega, \frac{1}{(1-\omega)^2}P_{\omega^2}, \left(\frac{\omega}{1+\omega}\right)^2 P_\infty\right\}$ onto the information set $\mathcal{I}$. In this case, if $Q_2 \notin \mathcal{K}_1$, then $\mathcal{K}_1$ will be error-free, which implies that τ_1 maps Q_1 and Q_2 into the check positions $\mathcal{C}$. If $Q_2 \in \mathcal{K}_1$, the collineation σ given above will take the errors into $\mathcal{C}$.

If $Q_1 = P_\omega$, then we look at the collineation $\tau_2 = T(\omega, -\omega^2, 1, -1+\omega-\omega^2)$ that maps the set $\mathcal{K}_2 = \left\{\frac{1}{\omega^2(1-\omega)^2}P_1, \frac{1}{(1-\omega)^2}P_{\omega^2}, P_\infty\right\}$ onto $\mathcal{I}$. If $Q_2 \notin \mathcal{K}_2$, then τ_2 will move Q_1 and Q_2 into $\mathcal{C}$. Otherwise, the collineation σ will map the pair into $\mathcal{C}$.

If $Q_1 = P_{\omega^2}$, then we consider the collineation

$$\tau_3 = T\left(\omega(1+\omega), -2\omega^2, 1+\omega, -(1+\omega^2)\right),$$

that sends the set $\mathcal{K}_3 = \left\{\frac{1}{\omega^2(1-\omega)^2}P_1, \frac{1}{(1-\omega)^2}P_\omega, \frac{1}{(1+\omega)^2}P_\infty\right\}$ onto $\mathcal{I}$. Then τ_3 will take the errors Q_1 and Q_2 into $\mathcal{C}$ if $Q_2 \notin \mathcal{K}_3$. Otherwise, the collineation σ will map those errors into $\mathcal{C}$. This completes the proof of the first part.

For the second part of the theorem, suppose that a triple of errors occurs, from left to right, at the coordinate positions Q_1, Q_2, and Q_3 in $\mathcal{P}$. If the triple is in $\mathcal{I} \cup \mathcal{B}_0 \cup \mathcal{B}_\infty$, where $\mathcal{B}_y$, for $y \in \{0, \infty\}$, is given in (13), then the collineation $T(1,0,0,-1)$ will take it into $\mathcal{C}$. Without loss of generality, assume that $Q_1 \in \mathcal{I}$ and either Q_2 or Q_3 is in $\mathcal{C}\backslash(\mathcal{B}_0 \cup \mathcal{B}_\infty)$. We consider two cases for Q_3.

If $Q_3 \in \mathcal{B}_0 \cup \mathcal{B}_\infty$, then Q_2 must be in $\mathcal{C}\backslash(\mathcal{B}_0 \cup \mathcal{B}_\infty)$. If $Q_1 \neq P_1$, then we let

$$\sigma_1 = T\left(\omega, -(1+\omega), \frac{1}{\omega}, -\frac{1+\omega}{\omega}\right) \quad \text{and} \quad \sigma_2 = T(\omega, -\omega(1+\omega), \omega, -(1+\omega)).$$

The collineations σ_1 and σ_2 map the sets

$$\mathcal{K}_1 = \left\{P_1, \left(\frac{\omega}{1+\omega}\right)^2 P_0, \omega^2 P_\infty\right\} \quad \text{and} \quad \mathcal{K}_2 = \left\{P_1, \frac{1}{(1+\omega)^2}P_0, \left(\frac{1}{\omega^2}\right)P_\infty\right\},$$

into the information set $\mathcal{I}$, respectively. Thus if $Q_3 \notin \mathcal{K}_1$, the collineation σ_1 will move Q_1, Q_2, and Q_3 into the check positions $\mathcal{C}$. If $Q_3 \in \mathcal{K}_1$, then σ_2 will send these errors into $\mathcal{C}$.

Suppose now that $Q_1 = P_1$. Consider the collineations

$$\sigma_3 = T\left(\frac{1+\omega}{\omega}, -\omega, \frac{1+\omega}{\omega^2}, -\omega\right) \quad \text{and} \quad \sigma_4 = T\left(\frac{1+\omega}{\omega^2}, -\omega, \frac{1+\omega}{\omega^3}, -\frac{1}{\omega}\right),$$

that map the sets

$$\mathcal{K}_3 = \left\{P_{\omega^2}, \left(\frac{1}{\omega^2}\right)P_0, \left(\frac{\omega^2}{1+\omega}\right)^2 P_\infty\right\} \quad \text{and} \quad \mathcal{K}_4 = \left\{P_{\omega^2}, \omega^2 P_0, \left(\frac{\omega^3}{1+\omega}\right)^2 P_\infty\right\},$$

into $\mathcal{I}$, respectively. If $Q_3 \notin \mathcal{K}_3$, then σ_3 will move Q_1, Q_2, and Q_3 into $\mathcal{C}$; otherwise σ_4 will take the triple into $\mathcal{C}$.

Finally, if $Q_3 \in \mathcal{C}\backslash(\mathcal{B}_0 \cup \mathcal{B}_\infty)$, then we havae $Q_3 \in \mathcal{B}_y$ for some $y \in \mathbb{F}_q^\times \backslash \{1, \omega, \omega^2\}$. If $Q_1 \neq P_1$, the collineation σ_1 given above will take Q_1, Q_2, and Q_3 into $\mathcal{C}$. Assume that $Q_1 = P_1$. If $Q_2 \neq P_{\omega^2}$, the previous collineation σ_3 will take these errors into $\mathcal{C}$. Otherwise, the collineation $T\left(\frac{\omega}{1+\omega}, \frac{\omega}{1+\omega}, \frac{1}{\omega(1+\omega)}, \frac{\omega}{1+\omega}\right)$ that sends the set $\left\{P_\omega, \left(\frac{1+\omega}{\omega}\right)^2 P_0, (\omega(1+\omega))^2 P_\infty\right\}$ onto $\mathcal{I}$ will take the errors into $\mathcal{C}$, which complete the proof. □

We now show that the automorphism group $\mathcal{A}$ of C contains s-PD-sets for C over $\mathbb{F}_q$ where $s \leq q-1$.

Theorem 5.2. *Let q be a prime power and $q \geq 7$, and let ω be a primitive element of $\mathbb{F}_q$. Let C be the $[q^2-1, 3, (q-1)^2]$ code over $\mathbb{F}_q$ with generator matrix G as given in (12). Take $\mathcal{I} = \{P_1, P_\omega, P_{\omega^2}\}$ as an information set for C, and let $\mathcal{A}$ be an automorphism group of C as given in (11). Then C has a $(q-1)$-PD-set in $\mathcal{A}$ of size $1+\frac{1}{2}(q-1)(q-3)(q^2-5q+13)$ if q is odd, and $1+(q-1)(q-3)(q^2-5q+13)$ if q is even.*

Proof. Let $\mathcal{C} = \mathcal{P}\backslash\mathcal{I}$ be the check set corresponding to the information set $\mathcal{I}$ where $\mathcal{P}$ is the set of coordinate positions of C as given in (10). Let $\mathcal{E}$ be the set of $(q-1)$ error positions in $\mathcal{P}$. If $\mathcal{E} \cap \mathcal{I} = \emptyset$, then $\mathcal{E} \subseteq \mathcal{C}$, and hence, the identity $T(1,0,0,1)$ will keep $\mathcal{E}$ in the check positions $\mathcal{C}$.

Suppose that $\mathcal{E} \cap \mathcal{I} \neq \emptyset$. Since all the points in $\mathcal{E}$ may be in distinct sets $\mathcal{B}_y$, for $y \in \mathbb{F}_q \cup \{\infty\}$, as given in (13), it follows that the number of error-free sets $\mathcal{B}_y$ for $y \in \mathbb{F}_q \cup \{\infty\}$ is at least $(q+1)-(q-1) = 2$. Recall from the note in Section 4 that $T(a,b,c,d) = T(a',b',c',d')$ if and only if $a' = \pm a$, $b' = \pm b$, $c' = \pm c$, and $d' = \pm d$. Let $I = \{1, \omega, \omega^2\}$. Consider two cases for $\mathcal{B}_\infty$.

If $\mathcal{E} \cap \mathcal{B}_\infty = \emptyset$, then $\mathcal{B}_\infty$ is error-free, and thus, there must be $y_1 \in \mathbb{F}_q$ such that $\mathcal{B}_{y_1}$ is error-free. Suppose first that $y_1 \in I$. Pick any $y_2 \in \mathbb{F}_q \backslash I$ and $\delta \in \mathbb{F}_q^\times$ such that $\delta^2 P_{y_2} \notin \mathcal{E}$. Note that such y_2 and δ exist as the number of errors in $\mathcal{E}$ is less than the number of coordinate positions in $\mathcal{P}\backslash I$, i.e. $q-1 = |\mathcal{E}| < |\mathcal{P}\backslash I| = q^2-4$. Let $\beta = \delta(y_1 - y_2)$ and let

$$a_1 = \frac{\omega}{\beta}, \quad b_1 = \frac{\omega(\omega y_1 - (1+\omega)y_2)}{\beta}, \quad c_1 = \frac{\omega}{\beta}, \quad \text{and} \quad d_1 = \frac{y_1 - (1+\omega)y_2}{\beta}.$$

Then $a_1 d_1 - b_1 c_1 \neq 0$ as y_1 and y_2 are distinct. Let $\delta_0 = \frac{\beta}{\omega}$ and $\delta_1 = \frac{\delta}{1+\omega}$. Then we can show that the collineation $\tau_1 = T(a_1, b_1, c_1, d_1)$ maps the set $\mathcal{K}_1 = \{\delta_1^2 P_{y_1}, \delta^2 P_{y_2}, \delta_0^2 P_\infty\}$

onto $\mathcal{I}$. Since $\mathcal{K}_1$ is error-free, it follows that τ_1 moves all the errors in $\mathcal{E}$ into the check positions $\mathcal{C}$. Note that τ_1 is chosen depending on the elements y_1, y_2, and δ in $\mathbb{F}_q$. Thus the number of such collineations is $\frac{3}{2}(q-1)(q-3)$ if q is odd, and $3(q-1)(q-3)$ if q is even.

Suppose now that $y_1 \in \mathbb{F}_q \backslash I$. Choose any $y_2 \in \mathbb{F}_q \backslash (I \cup \{y_1\})$ and $\delta \in \mathbb{F}_q^\times$ such that $\delta^2 P_{y_2} \notin \mathcal{E}$. Similarly to the proof for $y_1 \in I$, we can show that there exists a collineation that takes all the errors in $\mathcal{E}$ into $\mathcal{C}$ and that the number of such collineations is $\frac{1}{2}(q-1)(q-3)(q-4)$ if q is odd, and $(q-1)(q-3)(q-4)$ if q is even.

If $\mathcal{E} \cap \mathcal{B}_\infty \neq \emptyset$, then there must be distinct elements $y_1, y_2 \in \mathbb{F}_q$ such that $\mathcal{B}_{y_1}$ and $\mathcal{B}_{y_2}$ are error-free. Suppose that $y_1, y_2 \in I$. Pick any $y_3 \in \mathbb{F}_q \backslash I$ and $\delta \in \mathbb{F}_q^\times$ such that $\delta^2 P_{y_3} \notin \mathcal{E}$. Let $\beta = \delta(y_1 - y_3)(y_2 - y_3)$ and let

$$a_2 = \frac{-(1+\omega)y_1 + \omega y_2 + y_3}{\beta}, \quad b_2 = \frac{y_1 y_2 + \omega y_1 y_3 - (1+\omega) y_2 y_3}{\beta},$$
$$c_2 = \frac{-(1+\omega)y_1 + y_2 + \omega y_3}{\omega\beta}, \quad d_2 = \frac{\omega y_1 y_2 + y_1 y_3 - (1+\omega) y_2 y_3}{\omega\beta}.$$

Then $a_2 d_2 - b_2 c_2 \neq 0$ as y_1, y_2, and y_3 are all distinct. Let

$$\delta_1 = \frac{\delta\omega(y_2 - y_3)}{(1+\omega)(y_1 - y_2)} \quad \text{and} \quad \delta_2 = \frac{\delta\omega(y_1 - y_3)}{y_1 - y_2}.$$

Then it can be shown that $\tau_2 = T(a_2, b_2, c_2, d_2)$ sends the set $\mathcal{K}_2 = \{\delta_1^2 P_{y_1}, \delta_2^2 P_{y_2}, \delta^2 P_{y_3}\}$ onto the information set $\mathcal{I}$. Since $\mathcal{K}_2$ is error-free, it follows that τ_2 maps all the errors in $\mathcal{E}$ into $\mathcal{C}$. The number of such collineations is $\frac{3\cdot 2}{2}(q-1)(q-3)$ if q is odd, and $3\cdot 2(q-1)(q-3)$ if q is even.

Suppose that $y_1 \in I$ and $y_2 \in \mathbb{F}_q \backslash I$. Let $y_3 \in \mathbb{F}_q \backslash (I \cup \{y_2\})$ and $\delta \in \mathbb{F}_q^\times$ such that $\delta^2 P_{y_3} \notin \mathcal{E}$. Similarly to the proof for $y_1, y_2 \in I$, we have that there exists a collineation that moves all the errors in $\mathcal{E}$ into $\mathcal{C}$ and that the number of such collineations is $\frac{3}{2}(q-1)(q-3)(q-4)$ if q is odd, and $3(q-1)(q-3)(q-4)$ if q is even.

Suppose that $y_1, y_2 \in \mathbb{F}_q \backslash I$. Choose $y_3 \in \mathbb{F}_q \backslash (I \cup \{y_1, y_2\})$ and $\delta \in \mathbb{F}_q^\times$ such that $\delta^2 P_{y_3} \notin \mathcal{E}$. Similarly to the proof above, we can show that there exists a collineation that maps all the errors in $\mathcal{E}$ into $\mathcal{C}$ and that the number of such collineations is $\frac{1}{2}(q-1)(q-3)(q-4)(q-5)$ if q is odd, and $(q-1)(q-3)(q-4)(q-5)$ if q is even.

Thus the total number of possible collineations used in the first case is $\frac{1}{2}(q-1)^2(q-3)$ if q is odd, and $(q-1)^2(q-3)$ if q is even and in the second case is $\frac{1}{2}(q-1)(q-3)(q^2-6q+14)$ if q is odd, and $(q-1)(q-3)(q^2-6q+14)$ if q is even. □

Remark 5.3. The proof of Theorem 5.2 provides explicitly the process for selecting the required elements from the automorphism group $\mathcal{A}$ of C. Rather than just asserting their existence, the proof details the specific construction of these sets. While the resulting $(q-1)$-PD-sets are too large to list in their entirety, for example, containing 325 elements for the smallest odd case $q = 7$ and 1, 296 for the even case $q = 8$, the step-by-step construction provided in the proof ensures that they are fully defined and can be reconstructed for any given q.

Computationally with MAGMA [3, 4], we found PD-sets that can correct up to the full error capability for certain codes over $\mathbb{F}_q$. We obtain a $[15,3,9]_4$ code over $\mathbb{F}_4$ with a PD-set of size 11 and a $[24,3,16]_5$ code over $\mathbb{F}_5$ with a PD-set of size 80. The example below illustrates the $[15,3,9]_4$ code over $\mathbb{F}_4$ and its PD-set for full error-correction. Note that the full error-correcting capability of the code is equal to $\left\lfloor \frac{(q-1)^2-1}{2} \right\rfloor$, which is quite large compared to the length $n = q^2 - 1$ of the code.

Example 5.4. Let ω be a primitive element of $\mathbb{F}_4$, and let $\mathcal{C}$ be the conic in $PG_2(\mathbb{F}_4)$ given by

$$\mathcal{C} = \{(1,1,1), (1,\omega,\omega^2), (1,\omega^2,\omega), (1,0,0), (0,0,1)\}.$$

Let $\overline{G}$ be the matrix defined as in (6), i.e.

$$\overline{G} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & \omega & \omega^2 & 0 & 0 \\ 1 & \omega^2 & \omega & 0 & 1 \end{bmatrix}.$$

Then the code $\overline{C}$ with generator matrix $\overline{G}$ is a $[5,3,3]$ MDS code over $\mathbb{F}_4$. We construct a new 3×15 matrix G obtained from $\overline{G}$ by multiplying each column of $\overline{G}$ by the non-zero elements of $\mathbb{F}_4$ as follows:

$$G = \left[\begin{array}{ccc|ccc|ccc|ccc|ccc} 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & 0 & 0 & 0 \\ 1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega^2 & 1 & \omega & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & \omega & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega^2 & 1 & 0 & 0 & 0 & 1 & \omega & \omega^2 \end{array}\right].$$

Let C be the code with generator matrix G. Then C is a 4-error-correcting $[15,3,9]$ code over $\mathbb{F}_4$. Take the points of $PG_2(\mathbb{F}_4)$ corresponding to the columns of G as the coordinate positions of C. Note that the reduced echelon form of G is not in standard form as shown below

$$\left[\begin{array}{ccc|ccc|ccc|ccc|ccc} 1 & \omega & \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 0 & 0 & 0 & 1 & \omega & \omega^2 & 0 & 0 & 0 & 1 & \omega & \omega^2 & \omega & \omega^2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & \omega^2 & 1 & \omega \end{array}\right].$$

We reorder the coordinate positions of C so that the corresponding columns of G are in the following order:

$$G^* = \left[\begin{array}{ccc|ccc|ccc|ccc|ccc} 1 & 1 & 1 & \omega & \omega^2 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega & \omega^2 & 0 & 0 & 0 \\ 1 & \omega & \omega^2 & \omega & \omega^2 & \omega^2 & 1 & 1 & \omega & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & \omega^2 & \omega & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 & 0 & 0 & 0 & 1 & \omega & \omega^2 \end{array}\right].$$

The code C^* with generator matrix G^* is a $[15,3,9]_4$ code and is isomorphic to the code C. Note that G^* can be reduced into standard form as follows:

$$\left[\begin{array}{ccc|ccc|ccc|ccc|ccc} 1 & 0 & 0 & \omega & \omega^2 & 0 & 0 & 0 & 0 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 0 & 1 & 0 & 0 & 0 & \omega & \omega^2 & 0 & 0 & 1 & \omega & \omega^2 & \omega & \omega^2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & \omega & \omega^2 & 1 & \omega & \omega^2 & \omega^2 & 1 & \omega \end{array}\right].$$

Then the code C^* has a PD-set for full error-correction of 11 elements given by

$$T(1,1,0,1),\ T(1,1,1,0),\ T(1,1,1,\omega),\ T(1,1,1,\omega^2),\ T(1,1,\omega,0),\ T(1,1,\omega,1),$$
$$T(1,1,\omega,\omega^2),\ T(1,1,\omega^2,0),\ T(1,1,\omega^2,1),\ T(1,1,\omega^2,\omega),\ T(1,\omega,\omega,\omega).$$

6. Conclusion

We looked at MDS codes obtained from ovals in the finite desarguesian projective plane of prime-power order q and constructed new q-ary codes from those codes. We showed that s-PD-sets can be found for the new codes where $s \leq q-1$. A question remaining from our observations is whether the new codes have PD-sets for full error correction. Although the codes have large minimum weight, indicating that they would have no such PD-sets, the examples we obtained for the finite planes of small order suggest the opposite.

Acknowledgements

The author would like to thank the anonymous reviewers for their helpful comments and suggestions. The author also acknowledges with gratitude the encouragement and valuable advice of Professor J. D. Key. This work was partially supported by the Faculty of Science, Silpakorn University.

References

[1] E. F. J. Assmus and J. D. Key. *Designs and Their Codes*, volume 103 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1993. https://doi.org/10.1017/CBO9781316529836. Second printing with corrections.

[2] E. F. J. Assmus and J. D. Key. Polynomial codes and finite geometries. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*. Volume 2, chapter 16, pages 1269–1343. Elsevier Science, Amsterdam, 1998.

[3] W. Bosma and J. Cannon. *Handbook of Magma Functions*. Department of Mathematics, University of Sydney. 2003.

[4] J. Cannon, A. Steel, and G. White. Linear codes over finite fields. In J. Cannon and W. Bosma, editors, *Handbook of Magma Functions*, pages 3951–4023. 2006.

[5] D. M. Gordon. Minimal permutation sets for decoding the binary golay codes. *IEEE Transactions on Information Theory*, 28:541–543, 1982. https://doi.org/10.1109/TIT.1982.1056504.

[6] R. Hill. *A First Course in Coding Theory*. Clarendon Press, Oxford, 1986.

[7] W. C. Huffman. Codes and groups. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*. Volume 2, chapter 17, pages 1345–1440. Elsevier Science, Amsterdam, 1998.

[8] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, Cambridge, 2003. https://doi.org/10.1017/CBO9780511807077.

[9] D. R. Hughes and F. C. Piper. *Projective Planes*, volume 6 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1973.

[10] J. D. Key and J. Limbupasiriporn. Partial permutation decoding for codes from paley graphs. *Congressus Numerantium*, 170:143–155, 2004.

[11] J. D. Key, T. P. McDonough, and V. C. Mavron. Partial permutation decoding for codes from finite planes. *European Journal of Combinatorics*, 26(5):665–682, 2005. https://doi.org/10.1016/j.ejc.2004.04.007.

[12] J. D. Key, T. P. McDonough, and V. C. Mavron. Improved partial permutation decoding for reed-muller codes. *Discrete Mathematics*, 340(4):722–728, 2017. https://doi.org/10.1016/j.disc.2016.11.031.

[13] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1983.

[14] J. Schönheim. On coverings. *Pacific Journal of Mathematics*, 14(4):1405–1411, 1964. https://doi.org/10.2140/pjm.1964.14.1405.

[15] B. Segre. Ovals in a finite projective plane. *Canadian Journal of Mathematics*, 7:414–416, 1955. https://doi.org/10.4153/CJM-1955-045-x.

Jirapha Limbupasiriporn
Department of Mathematics, Faculty of Science
Silpakorn University, Nakorn Pathom 73000, Thailand
E-mail limbupasiriporn_j@su.ac.th