Partial permutation decoding for codes from Paley graphs*

J. D. Key and J. Limbupasiriporn
Department of Mathematical Sciences
Clemson University
Clemson SC 29634, U.S.A.

April 26, 2004

Abstract

We examine codes from the Paley graphs for the purpose of permutation decoding and observe that after a certain length, PD-sets to correct errors up to the code's error-capability will not exist. In this paper we construct small sets of permutations for correcting two errors by permutation decoding for the case where the codes have prime length.

1 Introduction

An algorithm for decoding codes that have a large automorphism group was introduced by MacWilliams [11], where it was applied mostly to classes of cyclic codes, and the Golay codes. It involves choosing appropriate information sets for the code and finding a set of automorphisms (called a PD-set) that satisfies particular conditions.

Appropriate information sets and PD-sets for infinite classes of binary codes defined by some regular graphs (triangular graphs, lattice graphs and graphs from triples) with a symmetric group as an automorphism group were found in [8, 9, 7]. In [6] the p-ary codes from desarguesian planes were examined and it was observed that for planes of sufficiently large order no PD-sets could exist. For this a lower bound on the size of a PD-set was used: see Section 2. In that paper the notion of an s-PD-set was introduced, to correct s errors, where s is not necessarily the full error-correction capability of the code. Small 2-PD-sets were found for the codes from desarguesian projective and affine planes of prime order.

*This work was supported by the DoD Multidisciplinary University Research Initiative (MURI) program administered by the Office of Naval Research under Grant N00014-00-1-0565, and NSF grant #9730992.

Here (and in [10]) we look at the similar problem for the codes from Paley graphs and we prove the following, which applies to these codes:

Theorem 1 *Let $C = [n, k, d]_q$ be a cyclic code of prime length n over the field $\mathbb{F}_q$ of order q, where $n \equiv 1 \pmod 8$, $(n, q) = 1$ and $d \geq 5$. Label the coordinate positions $0, 1, \ldots, n-1$ and suppose that $0, 1, \ldots, k-1$ form the information symbols. Let $\tau_{a,b} : i \mapsto ai + b$ for $a, b \in \mathbb{F}_n$ and a a nonzero-square and suppose that $\tau_{a,b} \in Aut(C)$ for all such $a, b \in \mathbb{F}_n$. Then*

(1) if $k = \frac{n-1}{2}$ the set

$$\{\tau_{1,b} \mid b \in \{0, k\}\} \cup \{\tau_{k,b} \mid b \in \{k, 2k, \frac{3k}{2}, \frac{k}{2} - 1\}\}$$

is a 2-PD-set of size 6 for C;

(2) if $k = \frac{n+1}{2}$ the set

$$\{\tau_{1,b} \mid b \in \{0, 1, k, k-1, n-1\}\} \cup \{\tau_{k,b} \mid b \in \{0, k, k-1, \frac{k-1}{2}, \frac{3k-1}{2}\}\}$$

is a 2-PD-set of size 10 for C.

Corollaries 2, 3 in Section 4 then state this result explicitly for the codes from Paley graphs when the length is prime. Note that a similar result holds for 3-PD-sets, although in that case the size of the 3-PD-set depends on the length of the code; this can be found in [10].

The organization of the paper is as follows: in Section 2 we give the general background; in Section 3 we define the Paley graphs and their codes, giving some of the well-known properties that we will be needing; in Section 4 we prove the theorem; in Section 5 we give tables to show that PD-sets to decode all errors do not exist after a certain length.

2 Background and terminology

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, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. The **code C_F of the design** $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F.

All the codes here are **linear codes**, i.e. subspaces of the ambient vector space. If a code C over a field of order q is of length n, dimension k, and minimum weight d, then we write $[n, k, d]_q$ to show this information. A **generator matrix** for the code is a $k \times n$ matrix made up of a basis for C. The **dual** or **orthogonal** code $C^{\perp}$ is the orthogonal under the standard inner product $(,)$, i.e. $C^{\perp} = \{v \in$

$F^n | (v, c) = 0$ for all $c \in C\}$. A **check** (or **parity-check**) matrix for C is a generator matrix H for $C^\perp$. If c is a codeword then the **support** of c is the set of non-zero coordinate positions of c. The all-one vector will be denoted by $\jmath$, and is the vector with all entries equal to 1. Two linear codes of the same length and over the same field are **isomorphic** if they can be obtained from one another by permuting the coordinate positions. An **automorphism** of a code C is an isomorphism from C to C. The automorphism group will be denoted by $\mathrm{Aut}(C)$. A code of length n is **cyclic** if $\mathrm{Aut}(C)$ contains a cycle of length n.

Any code is isomorphic to a code with generator matrix in so-called **standard form**, i.e. the form $[I_k \,|\, A]$; a check matrix then is given by $[-A^T \,|\, I_{n-k}]$. The first k coordinates are the **information symbols** and the last $n-k$ coordinates are the **check symbols**.

The graphs, $\Gamma = (V, E)$ with vertex set V and edge set E, discussed here are undirected with no loops. A graph is **regular** if all the vertices have the same valency. The **adjacency matrix** A of a graph of order n is an $n \times n$ matrix with entries a_{ij} such that $a_{ij} = 1$ if vertices v_i and v_j are adjacent, and $a_{ij} = 0$ otherwise. The p**-rank** of the matrix A, denoted by $rank_p(A)$, is the dimension of the row space of A over the finite field of p elements. A **strongly regular graph** Γ of type (n, k, λ, μ) is a regular graph of order n with valency k which is such that any two adjacent vertices are together adjacent to λ vertices and any two non-adjacent vertices are together adjacent to μ vertices. The complement of the graph Γ is also a strongly regular of type $(n, n-k-1, n-2k+\mu-2, n-2k+\lambda)$. If A is the adjacency matrix of the graph Γ, then A has three distinct eigenvalues; one of which is the valency k of A with the corresponding eigenvector the all-one vector, and the other two eigenvalues of A, say r and s, where $r > s$, satisfy the equation

$$x^2 + (\mu - \lambda)x + (\mu - k) = 0. \tag{1}$$

It can be shown, see [4], that the eigenvalues r and s of A are integers, unless they have the same multiplicity. If r and s have the same multiplicity then the graph Γ is of type $(n, \frac{n-1}{2}, \frac{n-1}{4} - 1, \frac{n-1}{4})$ and its complement has the same type as Γ. Moreover, the p-rank of A can be computed as follows: see [2] and [4].

Result 1 *If A is the adjacency matrix of a strongly regular graph of type (n, k, λ, μ) and the eigenvalues of A that satisfy the equation (1) have the same multiplicity then*

$$rank_p(A) = \begin{cases} n & \text{if } p \nmid k\mu, \\ n-1 & \text{if } p | k \text{ but } p \nmid \mu, \\ \frac{n-1}{2} & \text{if } p | \mu. \end{cases}$$

Permutation decoding was first developed by MacWilliams [11]. It involves finding a set of automorphisms of a code such that the set satisfies certain conditions that allow it to be used for decoding; such a set is called a PD-set. The method is described fully in MacWilliams and Sloane [12, Chapter 15] and Huffman [5, Section 8]. In [6] the definition of PD-sets was extended to that of s-PD-sets for s-error-correction:

Definition 1 *If C is a t-error-correcting code with information set $\mathcal{I}$ and check set $\mathcal{C}$, then a* **PD-set** *for C is a set $\mathcal{S}$ of automorphisms of C which is such that every t-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into the check positions $\mathcal{C}$.*

*For $s \leq t$ an s-***PD-set** *is a set $\mathcal{S}$ of automorphisms of C which is such that every s-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into $\mathcal{C}$.*

That a PD-set will fully use the error-correction potential of the code follows easily and is proved in Huffman [5, Theorem 8.1]. That an s-PD-set will correct s errors also follows, and we restate this result in order to use our s-PD-sets for s-error-correction, where $s \leq t$:

Result 2 *Let C be an $[n, k, d]_q$ t-error-correcting code. Suppose H is a check matrix for C in standard form, i.e. such that I_{n-k} is in the redundancy positions. Let $y = c + e$ be a vector, where $c \in C$ and e has weight $s \leq t$. Then the information symbols in y are correct if and only if the weight of the syndrome Hy^T of y is $\leq s$.*

The algorithm for permutation decoding is as follows: we have a t-error-correcting $[n, k, d]_q$ code C with check matrix H in standard form. Thus the generator matrix $G = [I_k|A]$ and $H = [A^T|I_{n-k}]$, for some A, and the first k coordinate positions correspond to the information symbols. Any vector v of length k is encoded as vG. Suppose x is sent and y is received and at most s errors occur, where $s \leq t$. Let $\mathcal{S} = \{g_1, \dots, g_m\}$ be an s-PD-set. Compute the syndromes $H(yg_i)^T$ for $i = 1, \dots, m$ until an i is found such that the weight of this vector is s or less. Compute the codeword c that has the same information symbols as yg_i and decode y as cg_i^{-1}.

Such sets might not exist at all, and the property of having a PD-set might not be invariant under isomorphism of codes, i.e. it depends on the choice of $\mathcal{I}$ and $\mathcal{C}$. Furthermore, there is a bound on the minimum size that the set $\mathcal{S}$ may have, due to Gordon [3], from a formula due to Schönheim [13], and quoted and proved in [5]:

Result 3 *If $\mathcal{S}$ is a PD-set for a t-error-correcting $[n, k, d]_q$ code C, and $r = n-k$, then*

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

This result can be adapted to s-PD-sets for $s \leq t$ by replacing t by s in the formula.

3 Paley graphs

Let n be a prime power with $n \equiv 1 \pmod 4$. The **Paley graph**, denoted by $P(n)$, has the finite field $\mathbb{F}_n$ of order n as vertex set and two vertices x and y are adjacent if and only if $x - y$ is a non-zero square in $\mathbb{F}_n$. Since $n \equiv 1 \pmod 4$, -1 is a square in $\mathbb{F}_n$. The condition that -1 is a square in $\mathbb{F}_n$ is required to ensure that xy is an edge if and only if yx is. Thus $P(n)$ is well-defined. The Paley graph is a strongly regular graph of type $(n, \frac{n-1}{2}, \frac{n-1}{4} - 1, \frac{n-1}{4})$ and is isomorphic to its complement.

The Paley graph $P(n)$ can be viewed as a 1-$(n, \frac{n-1}{2}, \frac{n-1}{2})$ design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ with point set $\mathcal{P} = \mathbb{F}_n$ and block set $\mathcal{B} = \{B_x \mid x \in \mathbb{F}_n\}$, where

$$B_x = \{y \in \mathbb{F}_n \mid y - x \text{ is a non-zero square in } \mathbb{F}_n\}$$

for all $x \in \mathbb{F}_n$. An incidence matrix for $\mathcal{D}$ with blocks B_x in the same ordering as the points x, is an adjacency matrix A of $P(n)$. The code C of the Paley graph $P(n)$ over $\mathbb{F}_p$ is the subspace of $\mathbb{F}_p^n$ spanned by the rows of A. Thus the dimension of C is the p-rank of A and the minimum distance d of C is at most $\frac{n-1}{2}$, the valency of $P(n)$. Result 1 implies that if p divides $\frac{n-1}{2}$ but does not divide $\frac{n-1}{4}$ then C is a trivial code, so from now on we suppose that p divides $\frac{n-1}{4}$.

Note that of course much is known about the codes here, since they are the well-known quadratic residue codes and can be read about in many places, and for example in [12] or [14]. Here we will summarize those properties we require for the permutation decoding, but more detail can also be found in [10]. The dual codes are the codes of the non-residues together with $\jmath$: see also [1, Chapter 2].

In case of $p = 2$, we first note that the parameter $\mu = \frac{n-1}{4}$ is odd if $n \equiv 5 \pmod 8$ and is even if $n \equiv 1 \pmod 8$. Thus the dimension of the binary code C of $P(n)$ is $n - 1$ if $n \equiv 5 \pmod 8$ and is $\frac{n-1}{2}$ if $n \equiv 1 \pmod 8$.

Let $n = q^e$ for some prime q. For any $\sigma \in Aut(\mathbb{F}_n)$ and $a, b \in \mathbb{F}_n$ with a a non-zero square, we define the map $\tau_{a,b,\sigma}$ on $\mathbb{F}_n$ by

$$\tau_{a,b,\sigma} : x \mapsto ax^{\sigma} + b, \tag{2}$$

for $x \in \mathbb{F}_n$.

Result 4 *If C is the p-ary code of the Paley graph of order n, $n \equiv 1 \pmod 4$, where p divides $\frac{n-1}{4}$ and where $n = q^e$ for some prime q, then the set*

$$G = \{\tau_{a,b,\sigma} \mid \sigma \in Aut(\mathbb{F}_n),\ a, b \in \mathbb{F}_n,\ a \text{ a non-zero square}\} \tag{3}$$

is an automorphism group of C of order $\frac{1}{2}en(n-1)$, where $\tau_{a,b,\sigma}$ is defined as in (2).

This is well-known and can be found in any text on quadratic residue codes.

Note: The group G in Result 4 is transitive but not 2-transitive.

4 2-PD-sets for Paley graphs of prime order

Now we take the Paley graphs $P(n)$ of prime order n, where $n \equiv 1 \pmod 8$, and let C be the p-ary code of $P(n)$, where the prime p divides $\frac{n-1}{4}$. Thus C is cyclic and a $[n, \frac{n-1}{2}]_p$ code by Result 1. Let $k = \frac{n-1}{2}$. Since the codes are quadratic residue codes, the minimum weight d of the code C satisfies the square-root bound, i.e. $d^2 \geq n$, so that $\sqrt{n} \leq d \leq k$: see [1, Chapter 2], for example. Note also that since $n \equiv 1 \pmod 8$, 2 is a square in $\mathbb{F}_n$.

We order the coordinate positions of the cyclic code C as $0, 1, 2, \cdots, n-1$, and take the set

$$\mathcal{I} = \{0, 1, \ldots, k-1\} \tag{4}$$

for the information set and the set

$$\mathcal{C} = \{k, k+1, \ldots, n-1\} \tag{5}$$

for the check set of C.

Since n is a prime the only automorphism of $\mathbb{F}_n$ is the identity, so we write

$$\tau_{a,b} : x \mapsto ax + b, \tag{6}$$

where $a, b \in \mathbb{F}_n$ with a a nonzero-square, and we denote $\tau_{a,0}$ by τ_a for all non-zero squares $a \in \mathbb{F}_n$.

Also note that since 2 and $n-1$ are squares in $\mathbb{F}_n$, it follows that if $k = \frac{n-1}{2}$ then $2k = n-1$ which implies that k is a square in $\mathbb{F}_n$. Also, if $k = \frac{n+1}{2}$ then $2k = n+1 \equiv 1 \pmod n$ which implies that k is a square in $\mathbb{F}_n$.

We first note that a 2-PD-set will exist for the code $C = [n, \frac{n-1}{2}]_p$ of $P(n)$ since $\frac{n-1}{2} < \frac{n}{2}$, and by [11] the cyclic group T of S_n, generated by the cyclic permutation $x \mapsto x+1$, will form a 2-PD-set for C.

For the dual code $C^{\perp} = [n, \frac{n+1}{2}]_p$, we have the following result, see [6], to ensure the existence of a 2-PD-set for $C^{\perp}$.

Result 5 *Let $C = [n, k, d]_q$ be a cyclic code of odd length n over the field $\mathbb{F}_q$ of order q, where $k = \frac{n+1}{2}, (n, q) = 1$ and $d \geq 5$. Label the coordinate positions $0, 1, \ldots, n-1$ and suppose that $0, 1, \ldots, k-1$ form the information symbols. Let $A = Aut(C) \leq S_n$, and let $\tau : i \mapsto i+1$ and $\mu : i \mapsto qi$, working modulo n. If $T =< \tau >$ then $S = T \cup \mu T$ will form a 2-PD-set of $2n$ elements for C, unless $q \equiv \pm 1 \pmod n$.*

Note: The lower bounds of the size of 2-PD-sets for the code and its dual of the Paley graph $P(n)$ are 4 and 7, respectively, as follows immediately from Result 3. The sizes of 2-PD-sets that we obtain in Theorem 1 are close to these bounds.

Proof of Theorem 1:

We need to show in (1) and (2) that for every pair of coordinate positions i and j there is an element in S that maps the two positions into the check positions

$\mathcal{C}$ as given in (5). It is clear that if i and j are in the check positions, i.e. $k \leq i < j \leq n-1$, then the identity element τ_1 will keep these in $\mathcal{C}$.

To prove (1), take $k = \frac{n-1}{2}$. If i and j are such that $0 \leq i < j \leq k-1$ then the element $\tau_{1,k}$ will map i and j into $\mathcal{C}$ since $k \leq i+k < j+k \leq 2k-1 = n-2$.

We now consider four distinct cases for i and j, where $0 \leq i \leq k-1$ and $k \leq j \leq n-1$. Note first that k is even since $n \equiv 1 \pmod 4$. The elements $\tau_{k,2k}$, $\tau_{k,\frac{3k}{2}}$, $\tau_{k,\frac{k}{2}-1}$, or $\tau_{k,k}$ will map both i and j into the check set $\mathcal{C}$ depending on whether i and j are even or not. Throughout the proof of (i), let $i = 2r$ if i is even and $i = 2r+1$ otherwise for some $0 \leq r \leq \frac{k-2}{2}$, and let $j = 2s$ for some $\frac{k}{2} \leq s \leq k$, if j is even and $j = 2s+1$ for some $\frac{k}{2} \leq s \leq k-1$, otherwise.

Case 1: i and j are even. Then

$$i\tau_{k,2k} = ki + 2k \equiv n - r - 1 \text{ (mod } n)$$

and

$$j\tau_{k,2k} = kj + 2k \equiv n - s - 1 \text{ (mod } n).$$

Since $0 \leq r \leq \frac{k-2}{2}$ and $\frac{k}{2} \leq s \leq k$, it follows that $k \leq n - \frac{k}{2} = \frac{3k+2}{2} \leq n-r-1 \leq n-1$ and $n-k-1 = k \leq n-s-1 \leq n-\frac{k}{2}-1 = \frac{3k}{2} \leq n-1$, which shows that these automorphisms will map the pair into the check positions.

Case 2: i is even and j is odd. Then

$$i\tau_{k,\frac{3k}{2}} = ki + \frac{3k}{2} = k(2r) + \frac{3k}{2} \equiv \frac{3k}{2} - r \pmod n$$

and

$$j\tau_{k,\frac{3k}{2}} = kj + \frac{3k}{2} = k(2s+1) + \frac{3k}{2} \equiv \frac{5k}{2} - s \pmod n.$$

Since $0 \leq r \leq \frac{k-2}{2}$ and $\frac{k}{2} \leq s \leq k-1$, it follows that $\frac{3k}{2} - \frac{k-2}{2} = k+1 \leq \frac{3k}{2} - r \leq \frac{3k}{2} \leq n-1$ and $k \leq \frac{5k}{2} - (k-1) = \frac{3k+2}{2} \leq \frac{5k}{2} - s \leq \frac{5k}{2} - \frac{k}{2} = 2k = n-1$, which completes this case.

Case 3: i is odd and j is even. Then

$$i\tau_{k,\frac{k}{2}-1} = ki + \frac{k}{2} - 1 = k(2r+1) + \frac{k}{2} - 1 \equiv \frac{3k-2}{2} - r \pmod n$$

and

$$j\tau_{k,\frac{k}{2}-1} = kj + \frac{k}{2} - 1 = k(2s) + \frac{k}{2} - 1 \equiv \frac{5k}{2} - s \pmod n.$$

Since $0 \leq r \leq \frac{k-2}{2}$ and $\frac{k}{2} \leq s \leq k$, it follows that $\frac{3k-2}{2} - \frac{k-2}{2} = k \leq \frac{3k-2}{2} - r \leq \frac{3k-2}{2} \leq n-1$ and $k \leq \frac{5k}{2} - k = \frac{3k}{2} \leq \frac{5k}{2} - s \leq \frac{5k}{2} - \frac{k}{2} = 2k = n-1$, completing this case.

Case 4: i and j are odd. Then

$$i\tau_{k,k} = ki + k = k(2r+1) + k \equiv 2k - r \text{ (mod } n)$$

and

$$j\tau_{k,k} = kj + k = k(2s+1) + k \equiv 2k - s \text{ (mod } n).$$

Since $0 \leq r \leq \frac{k-2}{2}$ and $\frac{k}{2} \leq s \leq k-1$, it follows that $k \leq 2k - \frac{k-2}{2} = \frac{3k+2}{2} \leq 2k - r \leq 2k = n-1$ and $2k-(k-1) = k+1 \leq 2k-s \leq 2k - \frac{k}{2} = \frac{3k}{2} \leq n-1$. This completes the proof for $k = \frac{n-1}{2}$, i.e. the given set is a 2-PD-set for this value of k.

To prove (2), we take $k = \frac{n+1}{2}$ and consider three distinct cases of i, where $0 \leq i \leq k-1$, and for each case we consider the various possibilities for j, where $i < j \leq n$. Note that k is odd.

Case 1: $i = 0$. If $1 \leq j \leq k-2$ then $i\tau_{1,k} = k$ and $k+1 \leq j+k = j\tau_{1,k} \leq 2k-2 = n-1$.

If $j = k-1$ then $i\tau_{k,k} = k$ and

$$j\tau_{k,k} = kj + k = k^2 \equiv \frac{3k-1}{2} \pmod{n},$$

and $k \leq \frac{3k-1}{2} \leq n-1$.

If $j = k$ then $i\tau_{k,\frac{3k-1}{2}} = \frac{3k-1}{2} \geq k$ and

$$j\tau_{k,\frac{3k-1}{2}} = kj + \frac{3k-1}{2} = k^2 + \frac{3k-1}{2} \equiv k \text{ (mod } n).$$

If $k+1 \leq j \leq n-1$, we write $j = k+s$ for some $1 \leq s \leq k-2$, so

$$j\tau_{1,n-1} = j + n - 1 = n + (k+s-1) \equiv k+s-1 \text{ (mod } n)$$

and $k \leq k+s-1 \leq 2k-3 = n-2$.

Thus the elements $\tau_{1,k}, \tau_{k,k}, \tau_{k,\frac{3k-2}{2}}$ or $\tau_{1,n-1}$ will map both i and j into the check set $\mathcal{C}$.

Case 2: $i = k-1$. If $k \leq j \leq n-2$, we write $j = k+s$ for some $0 \leq s \leq k-3$, so

$$i\tau_{1,1} = i + 1 = k \quad \text{and} \quad j\tau_{1,1} = j + 1 = k + s + 1$$

where $k+1 \leq k+s+1 \leq n-1$.

If $j = n-1$ then

$$i\tau_{k,k-1} = ki + k - 1 = k^2 - 1 = \equiv \frac{3k-3}{2} \pmod{n}$$

and

$$j\tau_{k,k-1} = kj + k - 1 = k(n-1) + k - 1 \equiv n - 1 \text{ (mod } n).$$

Note that $k \leq \frac{3k-3}{2} \leq n-1$.

Thus $\tau_{1,1}$ or $\tau_{k,k-1}$ will map i and j into the check set $\mathcal{C}$.

Case 3: $1 \leq i \leq k-2$. If j is such that $i < j \leq k-1$ then $\tau_{1,k-1}$ will map both i and j into the check set $\mathcal{C}$ since $k \leq i+k-1 < j+k-1 \leq 2k-2 = n-1$.

Suppose that $k \leq j \leq n-1$. Let $i = 2r+2$ for some $0 \leq r \leq \frac{k-5}{2}$, if i is even and $i = 2r+1$ for some $0 \leq r \leq \frac{k-3}{2}$, otherwise, and let $j = k+2s+1$ for some $0 \leq s \leq \frac{k-3}{2}$, if j is even and $j = k+2s$ for some $0 \leq s \leq \frac{k-3}{2}$, otherwise. The following show that $\tau_{k,k-1}$, $\tau_{k,\frac{3k-1}{2}}$, $\tau_{k,\frac{k-1}{2}}$, or τ_k will map both i and j into the check set $\mathcal{C}$:

- i and j are even. Then

$$i\tau_{k,k-1} = ki + k - 1 = k(2r+2) + k - 1 \equiv k + r \text{ (mod } n)$$

and

$$j\tau_{k,k-1} = kj + k - 1 = k(k+2s+1) + k - 1 \equiv \frac{3k-1}{2} + s \pmod{n}.$$

Since $\leq r \leq \frac{k-5}{2}$ and $0 \leq \frac{k-3}{2}$, it follows that $k \leq k+r \leq k + \frac{k-5}{2} = \frac{3k-5}{2} = 2k-2 \leq n-1$ and $\frac{3k-1}{2} \leq \frac{3k-1}{2} + s \leq \frac{3k-1}{2} + \frac{k-3}{2} = n-1$.

- i is even and j is odd. Then

$$i\tau_{k,\frac{3k-1}{2}} = ki + \frac{3k-1}{2} = k(2r+2) + \frac{3k-1}{2} \equiv \frac{3k+1}{2} + r \pmod{n}$$

and

$$j\tau_{k,\frac{3k-1}{2}} = kj + \frac{3k-1}{2} = k(k+2s) + \frac{3k-1}{2} \equiv k + s \text{ (mod } n).$$

Since $0 \leq r \leq \frac{k-5}{2}$ and $0 \leq s \leq \frac{k-3}{2}$, it follows that $k \leq \frac{3k+1}{2} \leq \frac{3k+1}{2} + r \leq \frac{3k+1}{2} + \frac{k-5}{2} = n-1$ and $k \leq k+s \leq k+\frac{k-3}{2} = \frac{3k-3}{2} \leq n-1$.

- i is odd and j is even. Then

$$i\tau_{k,\frac{k-1}{2}} = ki + \frac{k-1}{2} = k(2r+1) + \frac{k-1}{2} \equiv \frac{3k-1}{2} + r \pmod{n}$$

and

$$j\tau_{k,\frac{k-1}{2}} = kj + \frac{k-1}{2} = k(k+2s+1) + \frac{k-1}{2} \equiv k + s \text{ (mod } n).$$

Since $0 \leq r \leq \frac{k-3}{2}$ and $0 \leq s \leq \frac{k-3}{2}$, it follows that $k \leq \frac{3k-1}{2} \leq \frac{3k-1}{2} + r \leq \frac{3k-1}{2} + \frac{k-3}{2} = n-1$ and $k \leq k+s \leq \frac{3k-1}{2}$.

- i and j are odd. Then

$$i\tau_k = ki = k(2r+1) = (2k)r + k \equiv k + r \text{ (mod } n)$$

and

$$j\tau_k = kj = k(k+2s) = \equiv \frac{3k-1}{2} + s \pmod{n}.$$

Since $0 \leq r \leq \frac{k-3}{2}$ and $0 \leq s \leq \frac{k-3}{2}$, it follows that $k \leq k+r \leq k + \frac{k-3}{2} = \frac{3k-1}{2} \leq n-1$ and $\frac{3k-1}{2} \leq \frac{3k-1}{2} + s \leq \frac{3k-1}{2} + \frac{k-3}{2} = 2k-2 = n-1$.

Thus the given set is a 2-PD-set for this value of k. This completes the proof of the theorem. ■

Corollary 2 *Let $P(n)$ be the Paley graph of prime order n, where $n \equiv 1$ (mod 8), and $C = [n, \frac{n-1}{2}]_p$ its code over $\mathbb{F}_p$ where p is a prime that divides $\frac{n-1}{4}$. If the information set is given as in (4), where $k = \frac{n-1}{2}$, then C has a 2-PD-set of size 6.*

Corollary 3 *Let $P(n)$ be the Paley graph of prime order n, where $n \equiv 1$ (mod 8), and $C^{\perp} = [n, \frac{n+1}{2}]_p$ the dual of its code C over $\mathbb{F}_p$ where p is a prime that divides $\frac{n-1}{4}$. If the information set for $C^{\perp}$ is given as in (4), where $k = \frac{n+1}{2}$, then $C^{\perp}$ has a 2-PD-set of size 10.*

Note: In [10] 3-PD-sets for these codes are found, using similar methods. The proofs are much longer and we do not include them here. The 3-PD-sets of the codes of the graphs are of size $4n$ for $n \equiv 1$ (mod 12) and $6n$ otherwise, where the length of the code is the prime n.

5 Computations

In the following tables we compare the lower bound of the size of a PD-set of Result 3 for full error correction with the order of the automorphism group G of the binary code C of the Paley graph $P(n)$ of order n, where $n \equiv 1 \pmod 8$.

For n prime the code C has minimum distance d satisfying the condition $d \geq \sqrt{n}$. The full error-correction capability t of C must satisfy $t \geq t_0 = \left\lfloor \frac{\sqrt{n}-1}{2} \right\rfloor$. The lower bound s of the size of a PD-set for C is thus greater than

$$s_0 = \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t_0+1}{r-t_0+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil,$$

where the redundancy $r = n - dim(C)$. Hence we have $\frac{s}{|G|} \geq \frac{s_0}{|G|}$. The ratio of s_0 to $|G|$ is shown in Table 1. Similar results hold for the dual $C^{\perp}$ of the code C.

For $n = q^2$, where q is a prime power, the minimum distance of C is $q + 1$ (see [14]) and we used this to compute the error-correcting capability t of C and the lower bound s of the size of a PD-set in Table 2.

These results indicate that for n large the required lower bound of the size of a PD-set for full error correction for the codes of $P(n)$ is greater than the order of the automorphism group G. Consequently, a PD-set for full error correction cannot exist for these codes.

n	code parameter	t_0	r	s_0	$\frac{s_0}{\lvert G\rvert}$
17	$[17, 8, 6]$	2	9	4	0.02941176
41	$[41, 20, 10]$	4	21	28	0.03414634
73	$[73, 36, 14]$	6	37	123	0.04680365
89	$[89, 44, 18]$	8	45	531	0.13559755
97	$[97, 48, 16]$	7	49	250	0.05369416
113	$[113, 56, 16]$	7	57	250	0.03950695
137	$[137, 68, 22]$	10	69	2220	0.2382997
193	$[193, 96, \geq 13]$	5	97	124	0.00669257
233	$[233, 116, \geq 15]$	7	117	251	0.00928667
241	$[241, 120, \geq 15]$	7	121	251	0.00867911
257	$[257, 128, \geq 16]$	7	129	252	0.00766051
281	$[281, 140, \geq 16]$	7	141	252	0.00640569
313	$[313, 156, \geq 17]$	8	157	507	0.01038339
337	$[337, 168, \geq 18]$	8	169	507	0.00895507
353	$[353, 176, \geq 18]$	8	177	507	0.00816057
401	$[401, 200, \geq 20]$	9	201	1018	0.01269327
409	$[409, 204, \geq 20]$	9	205	1018	0.01220097
433	$[433, 216, \geq 20]$	9	217	1018	0.01088444
449	$[449, 224, \geq 21]$	10	225	2052	0.02040248
457	$[457, 228, \geq 21]$	10	229	2052	0.01969365
521	$[521, 260, \geq 22]$	10	261	2041	0.01506718
569	$[569, 284, \geq 23]$	11	285	4113	0.02545236
577	$[577, 288, \geq 24]$	11	289	4113	0.02475087
593	$[593, 296, \geq 24]$	11	297	4114	0.02343786
601	$[601, 300, \geq 24]$	11	301	4114	0.02281753
617	$[617, 308, \geq 24]$	11	309	4114	0.02164853
641	$[641, 320, \geq 25]$	12	321	8276	0.04034711
673	$[673, 336, \geq 25]$	12	337	8276	0.03659874
761	$[761, 380, \geq 27]$	13	381	16739	0.05788436
769	$[769, 384, \geq 27]$	13	385	16611	0.05625203
809	$[809, 404, \geq 28]$	13	405	16596	0.05077776
857	$[857, 428, \geq 29]$	14	429	33649	0.09173764
881	$[881, 440, \geq 29]$	14	441	33586	0.08664225
929	$[929, 464, \geq 30]$	14	465	33305	0.07726374
937	$[937, 468, \geq 30]$	14	469	33305	0.07594934
953	$[953, 476, \geq 30]$	14	477	33306	0.07342139
977	$[977, 488, \geq 31]$	15	489	67587	0.14175839
1009	$[1009, 504, \geq 31]$	15	505	67578	0.13288735
1033	$[1033, 516, \geq 32]$	15	517	67068	0.12582453
1049	$[1049, 524, \geq 32]$	15	525	66817	0.12155706
1097	$[1097, 548, \geq 33]$	16	549	135685	0.2257068
1129	$[1129, 564, \geq 33]$	16	565	135660	0.21304864
1153	$[1153, 576, \geq 33]$	16	577	134580	0.20264166
1193	$[1193, 596, \geq 34]$	16	597	134508	0.18917398
1201	$[1201, 600, \geq 34]$	16	601	134477	0.1866181
1217	$[1217, 608, \geq 34]$	16	609	134194	0.18135893
1249	$[1249, 624, \geq 35]$	17	625	272267	0.34933973
1289	$[1289, 644, \geq 35]$	17	645	270027	0.32528827
1297	$[1297, 648, \geq 36]$	17	649	270028	0.32128749
1321	$[1321, 660, \geq 36]$	17	661	269908	0.30957723
1361	$[1361, 680, \geq 36]$	17	681	269842	0.29156978
1409	$[1409, 704, \geq 37]$	18	705	542012	0.54641832
1433	$[1433, 716, \geq 37]$	18	717	541946	0.52819806
1481	$[1481, 740, \geq 38]$	18	729	541491	0.49408818
1489	$[1489, 744, \geq 38]$	18	745	541365	0.48867772
1553	$[1553, 776, \geq 39]$	19	777	1088771	0.90344843
1601	$[1601, 800, \geq 40]$	19	801	1087038	0.84871799
1609	$[1609, 804, \geq 40]$	19	805	1087013	0.84027733
1657	$[1657, 828, \geq 40]$	19	829	1086381	0.79182519
1697	$[1697, 848, \geq 41]$	20	849	2185245	1.5185

Table 1: Codes of Paley graphs of prime order n

n	code parameter	t	r	s	$\frac{s}{\lvert G\rvert}$
9	$[9, 4, 4]$	1	5	2	0.02777778
25	$[25, 12, 6]$	2	13	4	0.00666667
49	$[49, 24, 8]$	3	25	12	0.00510204
81	$[81, 40, 10]$	4	41	28	0.00216049
121	$[121, 60, 12]$	5	61	60	0.00413223
169	$[169, 84, 14]$	6	85	124	0.00436743
289	$[289, 144, 18]$	8	145	5078	0.00609141
361	$[361, 180, 20]$	9	181	1018	0.00783318
529	$[529, 264, 24]$	11	265	4113	0.01472547
625	$[625, 312, 26]$	12	313	8339	0.01069103
729	$[729, 364, 28]$	13	365	16738	0.01051292
841	$[841, 420, 30]$	14	421	33660	0.04764736
961	$[961, 480, 32]$	15	481	67602	0.07327653
1369	$[1369, 684, 38]$	18	685	546989	0.29207141
1681	$[1681, 840, 42]$	20	841	2186212	0.77413246
1849	$[1849, 924, 44]$	21	925	4384853	1.2833

Table 2: Codes of Paley graphs of order q^2

References

[1] E. F. Assmus, Jr. and J. D. Key. *Designs and their Codes*. Cambridge: Cambridge University Press, 1992. Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[2] A. E. Brouwer and C. J. van Eijl. On the p-rank of the adjacency matrices of strongly regular graphs. *J. Algebraic Combin.*, 1:329–346, 1992.

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

[4] Willem H. Haemers, René Peeters, and Jeroen M. van Rijckevorsel. Binary codes of strongly regular graphs. *Des. Codes Cryptogr.*, 17:187–209, 1999.

[5] W. Cary Huffman. Codes and groups. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 1345–1440. Amsterdam: Elsevier, 1998. Volume 2, Part 2, Chapter 17.

[6] J. D. Key, T. P. McDonough, and V. C. Mavron. Partial permutation decoding of codes from finite planes. *European J. Combin.*, To appear.

[7] J. D. Key, J. Moori, and B. G. Rodrigues. Permutation decoding of binary codes from graphs on triples. *Ars Combin.* To appear.

[8] J. D. Key, J. Moori, and B. G. Rodrigues. Permutation decoding for binary codes from triangular graphs. *European J. Combin.*, 25:113–123, 2004.

[9] J. D. Key and P. Seneviratne. Permutation decoding of binary codes from lattice graphs. *Discrete Math.*, To appear.

[10] J. Limbupasiriporn. Ph.D. thesis, Clemson University, 2004.

[11] F. J. MacWilliams. Permutation decoding of systematic codes. *Bell System Tech. J.*, 43:485–505, 1964.

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

[13] J. Schönheim. On coverings. *Pacific J. Math.*, 14:1405–1411, 1964.

[14] Harold N. Ward. Quadratic residue codes and divisibility. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 827–870. Amsterdam: Elsevier, 1998. Volume 1, Part 1, Chapter 9.