Permutation decoding for codes from generalized Paley graphs

Padmapani Seneviratne[1] and Jirapha Limbupasiriporn[2]

[1] Department of Mathematics & Statistics
American University of Sharjah, UAE.
[2] Department of Mathematics
Silpakorn University, Thailand.

Abstract. Generalized Paley graphs $GP(q, S)$, where q is an odd prime power are a generalization of the well known Paley graphs $P(q)$. Codes derived from the row span of adjacency and incidence matrices from Paley graphs have been studied in [1] and [2]. We examine binary codes associated with the incidence design of the generalized Paley graph $G(q, S)$. The binary codes have the parameters $[\frac{qs}{2}, q-1, s]$, when s is even and $[qs, q-1, 2s]$, when n is odd. By finding explicit PD-sets we show that these codes can be used for permutation decoding.

Keywords: Codes, Paley graphs, Permutation decoding.

1 Extended Abstract

1.1 Generalized Paley graphs

The Paley graph of order q with q a prime power is a graph on q vertices with two vertices adjacent if their difference is a square in the finite field $\mathbb{F}_q$. This graph is undirected when $q \equiv 1 \bmod 4$. The Paley graphs $P(q)$ were first defined by Paley in [3]. Let ω be a primitive element in $\mathbb{F}_q$ and let $S = \{\omega^2, \omega^4, \ldots, \omega^{q-1} = 1\}$ be the set of non zero squares in $\mathbb{F}_q$. If $q \equiv 1 \bmod 4$ then $S = -S$.

The generalized Paley graphs were defined by Praeger and Lim in [4].

Definition 1. *Let $\mathbb{F}_q$ be a finite field of order q. Let k be a divisor of $q-1$ such that $k \geq 2$ and if q is odd, then $\frac{q-1}{k}$ is even. For any multiplicative subgroup S of $\mathbb{F}_q^{\times}$ of order $\frac{q-1}{k}$, the generalized Paley graph of $\mathbb{F}_q$ denoted $GP(q, S)$, is the graph with vertex set $\mathbb{F}_q$ and edges all pairs $[x, y]$ such that $x - y \in S$.*

Note 2. From the above definition we have:

1. If $q \equiv 1 \bmod 4$ and $k = 2$, then $GP(q, S)$ is the Paley graph $P(q)$.
2. When $|S| = \frac{q-1}{k}$ is even we have $S = -S$. Hence $GP(q, S)$ is undirected and connected.
3. When $|S|$ is odd we define $[x, y]$ an edge if and only if $x - y \in S \cup -S$.

1.2 Codes

An incidence matrix of a graph $\Gamma = (V, E)$ is a $|V| \times |E|$ matrix $B = [b_{ij}]$ such that $b_{ij} = 1$ if the vertex labelled by i is on the edge labelled by j and $b_{ij} = 0$ otherwise. If Γ is regular with valency k, then the $1-(|E|, k, 2)$ design with incidence matrix B is called the incidence design of the graph Γ.

For any incidence matrix B of a graph Γ, the code of Γ over a finite field $\mathbb{F}_q$, denoted by $C_p(B)$, is the row span of B over $\mathbb{F}_p$. When the graph is regular we can consider $C_p(B)$ as the code of the design with blocks, the rows of B.

Proposition 3. *Let $\Gamma = GP(q, S)$ be the generalized Paley graph, where q is a prime power. Let $\mathcal{G}_q$ be the incidence design of $GP(q, S)$. Then*

$$C_2(\mathcal{G}_q) = \begin{cases} [\frac{qs}{2}, q-1, s], & \textit{if } s \textit{ is even} \\ [qs, q-1, 2s], & \textit{if } s \textit{ is odd} \end{cases}$$

where $s = |S|$, and

$$C_2(\mathcal{G}_q)^{\perp} = \begin{cases} [\frac{qs}{2}, \frac{q(s-2)}{2} + 1, d], & \textit{if } s \textit{ is even} \\ [qs, q(s-1) + 1, 2s, d], & \textit{if } s \textit{ is odd} \end{cases}$$

where $d = 3$, if $GP(q, S)$ admits a 3-cycle, or $d = 4$, if $GP(q, S)$ admits a 4-cycle.

Lemma 4. *$C_2(\mathcal{G}_q)$ has a basis of minimum weight vectors.*

Lemma 5. *If $(x_1, x_2, \ldots, x_q)$ is a closed path of length q for $x_i \neq x_j$ for the generalized Paley graph $GP(q, S)$, then $\mathcal{I} = \{[x_1, x_2], [x_2, x_3], \ldots, [x_{q-2}, x_{q-1}]\}$ is an information set for $C_2(\mathcal{G}_q)$.*

1.3 Automorphisms and PD-sets

Let ω be a primitive element of $\mathbb{F}_q$. Then $S =< \omega^k >$. Let $\sigma \in Aut(\mathbb{F}_q)$ be the Frobenius automorphism of $\mathbb{F}_q$, $a \in S$ and $b \in \mathbb{F}_q$. We define the map t_b on $\mathbb{F}_q$ by $t_b : x \mapsto x + b$, for $x \in \mathbb{F}_q$. Then define

$$T = \{t_b \mid b \in \mathbb{F}_q\} \tag{1}$$

T is called the translation group $A\Gamma L(1, q)$. Next we define the map f_a on $\mathbb{F}_q$ by $f_a : x \mapsto a\sigma(x)$, for $x \in \mathbb{F}_q$. Then

$$W = \{f_a \mid a \in S\} \tag{2}$$

When q is prime, we have $\sigma = 1$, then $W = \{f_a : x \mapsto ax \mid a \in S\}$. Now W fix 0 and fix S setwise, and hence $T \rtimes W$ is a subgroup of the automorphsim group of $GP(q, S)$. When $k = 2$ and $q \equiv 1 (\bmod 4)$, $T \rtimes W$ is the automorphism group of the Paley graph $P(q)$.

Next we show that when q is prime we can find full error correcting PD-sets for the codes $C_2(\mathcal{G}_q)$.

Proposition 6. *Let $q \geq 5$ be a prime, $GP(q, S)$ be the generalized Paley graph on $\mathbb{F}_q$ and let $\mathcal{G}_q$ its incidence design. Let*

$$\mathcal{I} = \{[0,1], [1,2], \ldots, [q-2, q-1]\}$$

be the information set for $C_2(\mathcal{G}_q)$. Then the set of automorphisms $W = \{f_a : x \mapsto ax \mid a \in S\}$ is a full-error correcting PD-set for $C_2(\mathcal{G}_q)$ of size $\frac{q-1}{k}$.

References

1. D. Ghinellie and J. D. Key. Codes from incidence matrices and line graphs of Paley graphs. *Advances in mathematics of communications*, 5(2011), no.1, 93-108.
2. J. D. Key and J. Limbupasiriporn Partial permutation decoding for codes from Paley graphs. Congr. Numer. 170 (2004), 143–155.
3. R. E. A. C. Paley On orthogonal matrices. *J. Math. Phys. Mass. Inst. Tech*, 12 (1933), 311-320.
4. Cheryl E. Praeger and Tian K. Lim. On Generalised Paley Graphs and their automorphism groups. *Michigan Math. Journal*, 58, 294-308.