ON THE AUTOMORPHISM GROUPS OF PALEY 2-DESIGNS

BLESILDA P. RAPOSA
Mathematics Department
De La Salle University
2401 Taft Avenue
1004 Manila, Philippines

ABSTRACT

We determine here the automorphism groups of Paley $2-(2q+1, q, \frac{q-1}{2})$ designs where q is a prime power such that $q \equiv 1 \pmod 4$.

1. INTRODUCTION

A special construction of Hadamard 1-designs of Paley type was given by N. Ito in [3]. Paley 2- and 3- designs are Hadamard 2- and 3- designs, respectively, which are derived from Hadamard 1-designs of Paley type [4]. The purpose of this paper is to determine the automorphism groups of Paley 2-Designs. The proof makes use of a theorem by Carlitz [2].

2. HADAMARD DESIGNS

In this section, we present the definition of Hadamard 1-, 2- and 3-designs. These concepts are defined and their relationships are expounded in [4].

Definition 2.1 Let t, υ, k, λ be positive integers such that $\upsilon > k > t \geq 1$ and $\lambda \geq 1$. The pair $D = (P, B)$ is called a $t-(\upsilon, k, \lambda)$ design or simply a $t-$ design if P is a finite set of υ elements called *points* and B consists of k-subsets of P called *blocks* and every t-subset of P is contained in precisely λ blocks.

Definition 2.2 Let $P = \{1, 2, \ldots, n, 1^\circ, 2^\circ, \ldots, n^\circ\}$ be a $2n$-set such that n is a positive multiple of four. Let $B = \{\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_1^\circ, \alpha_2^\circ, \ldots, \alpha_n^\circ\}$ be a family of n-subsets of P, with $\alpha_i^\circ = P - \alpha_i$, $1 \leq i \leq n$ The pair $D = (P, B)$ is called an *Hadamard design* if the following conditions are satisfied:

(i) Each point is contained in precisely n blocks. That is, D is a 1-design.

(ii) Each pair of points except $\{i, i^o\}$, $1 \le i \le n$, is contained in precisely $n/2$ blocks. The pair $\{i, i^o\}$, for $1 \le i \le n$, is contained in no blocks.

(iii) Each triple of points not containing $\{i, i^o\}$, $1 \le i \le n$, is contained in precisely $n/4$ blocks.

(iv) Each pair of blocks except $\{\alpha_i, \alpha_1^\circ\}$, $1 \le i \le n$, meets in precisely $n/2$ points.

(v) Each trio of blocks not containing $\{\alpha_i, \alpha_1^\circ\}$, $1 \le i \le n$, meets in precisely $n/4$ points.

Definition 2.3 Let D be an Hadamard 1-(2n,n,n) design where $n \le 8$. Let α be a fixed block of D. We define the *derived design of D with respect to the block* α denoted by $D(\alpha) = (P(\alpha), B(\alpha)$, as the design whose point set and block set are $(P(\alpha) = \alpha$ and $B(\alpha) = \{\beta \cap \alpha; \beta \in B, \beta \neq \alpha, \alpha^\circ$, respectively.

It was shown in [4] that $D(\alpha,)$ is a 3-design called an *Hadamard 3-design.*

Definition 2.4 Let D be an Hadamard 1-(2n,n,n) design where $n \le 8$. Let α be a fixed block of D and let $D(\alpha)$ be the resulting Hadamard 3-design. Let i be a fixed point of $D(\alpha)$. We define the *derived design of D* (α) *with respect to the point i,* denoted by $D(\alpha,i) = (P(\alpha,i), B(\alpha,i))$, as the design whose point set and block set are $(P(\alpha,i) = \alpha - i$ and $B(\alpha,i) = \{\beta \cap \alpha - \{i\}; i \in \beta \in B(\alpha)\}$, respectively.

From [4], $D(\alpha,i)$ is a 2-design called an *Hadamard 2-design.*

3. PALEY DESIGNS

We present here the construction of Hadamard 1-designs of Paley type given by N. Ito in [3]. We then show the points and blocks of the corresponding Hadamard 3- and 2- designs.

Let q be a prime power such that $q \equiv 1 \pmod 4$ and let $GF(q)$ be the field of q elements. Let Q and N denote the sets of quadratic residues and non-quadratic residues respectively, of the multiplicative group $GF(q)^*$. We introduce a new symbol t. Then consider four disjoint copies of $GF(q) \cup \{t\}$,namely, $GF(q)_1 \cup \{t_1\}$, $GF(q)_1^* \cup \{t_1^*\}$, $GF(q)_2 \cup \{t_2^*\}$, and $GF(q)_2^* \cup \{t_2^*\}$. For any $a \in$, $GF(q)$, the four mappings which map a to a_1, a_1^*, a_2, a_2^*, respectively are isomorphisms.

We let

$$
\begin{aligned}
P(q) &= \{t_1\} \cup GF(q)_1 \cup \{t_1^*\} \cup GF(q_1)^* \cup \{t_2\}\ GF(q)_2 \cup \{t_2^*\} \cup GF(q)_2^*;\\
\beta_1(t) &= \{t_1\} \cup GF(q)_1 \cup \{t_2^*\} \cup GF(q)_2;\\
\beta_1(a) &= \{t_1\} \cup Q_1 + a_1 \cup \{a_1\} \cup N_1^* + a_1^* \cup \{t_2\} \cup Q_2 + a_2 \cup \{a_2^*\}\\
&\quad \cup N_2^* + a_2^* \text{ where } a \text{ runs over } GF(q);\\
\beta_2(t) &= \{t_1^*\} \cup GF(q)_1 + \cup \{t_2^*\} \cup GF(q_2^*);\\
\beta_2(a) &= \{t_1\} \cup Q_1 + a_1 \cup \{a_1^*\} \cup N_1^* + a_1^* \cup \{t_2^*\} \cup Q_2^* + a_2^* \cup \{a_2^*\}\\
&\quad \cup N_2 + a_2 \text{ where } a \text{ runs over } GF(q);
\end{aligned}
$$

Then we let $\beta_i(a)^c = P(q) - \beta_i(a)$; $i = 1, 2$ and $\beta_i(t)^c = P(q) - \beta_i(t)$; $i = 1, 2$. Furthermore, we let $B(q) = \{\beta_i(t), \beta_i(a), \beta_i(t)^c, \beta_i(a)^c$ where a runs over $GF(q)$ and $i = 1, 2$.

Then $D(q) = (P(q), B(q))$ is an Hadamard 1-design and is called an *Hadamard 1-design of Paley type* [3].

Consider now the derived design of $D(q)$ with respect to the block $\beta_i(t)$, denoted by $D(\beta_i(t)) = (P(\beta_1(t)), B(\beta_1(t)))$. Then $P(\beta_1(t)) = \beta_1(t)$ and $B(\beta_1(t)) = \{\alpha, \beta(a), g(a), \alpha^c, \beta(a)^c, g(a)^c\}$ where the blocks

$$
\begin{aligned}
\alpha &= GF(q)_2 \cup \{t_1\};\\
\beta(a) &= Q_1 + a_1 \cup \{a_1\} \cup Q_2 + a_2 \cup \{t_1\};\\
g(a) &= Q_1 + a_1 \cup \{t_2^*\} \cup N_2 + a_2 \cup \{t_1\};
\end{aligned}
$$

are such that a runs over $GF(q)$ and δ^c denotes the complement of the block δ with respect to the point set $P(\beta_1(t))$.

Then from Section 2, $D(\beta_1(t))$ is an Hadamard $3-(2q+2, q+1, \frac{q-1}{2}$ design which we shall call an *Hadamard 3-design of Paley type.*

Next, we consider the derived design of $D(\beta_1(t))$ with respect to the point t1 denoted by $D(\beta_1(t), t_1) = (P(\beta_1(t), t_1), B(\beta_1(t), t_1))$. We then have $P(\beta_1(t), t_1) = GF(q_1) \cup GF(q_2) \cup \{t_2^*\}$ and $B(\beta_1(t), t_1) = \{\alpha', \beta'(a), g'(a^c\}$ where the blocks

$$
\begin{aligned}
\alpha' &= GF(q)_2;\\
\beta'a) &= Q_1 + a_1 \cup \{a_1\} \cup Q_2 + a_2; \text{ and}\\
g'(a) &= Q_1 + a_1 \cup \{t_2^*\} \cup N_2 + a_2;
\end{aligned}
$$

are such that a runs over $GF(q)$.

Again from Section 2, $D(\beta_1(t), t_1)$ is an Hadamard $2-(2q+1), q+1, \frac{q-1}{2}$ design which we shall call an *Hadamard 2-design of Paley type.*

We note here that these families of Paley designs are distinct from the designs of quadratic residue type which some literature also refer to as Paley designs. *Designs of quadratic residue type* have point set equal to $GF(q)$ for q a prime power and $q \equiv 3 \pmod 4$. Its blocks are of the form $Q + a$, where Q denotes the set of quadratic residues of $GF(q)$ and a runs over $GF(q)$. Note that while the number of points in *our* Paley designs is $2q + 1 \equiv 3 \pmod 4$, $2q + 1$ is not always a prime power. The only time when *our* Paley designs and designs of quadratic residues type are isomorphic is when the number of points is 11.

4. AUTOMORPHISM GROUPS OF PALEY 2-DESIGNS

In this section, we determine the automorphism groups of the Paley 2-designs.

4.1 The case $q = 5$.

We first consider the case when $q = 5$. That is, we consider the Paley 2-(11,5,2) design which is isomorphic to the design of quadratic residue type for $q = 11$.

Its automorphism group is of order $660 = 2^2 \times 3 \times 5 \times 11$. Its generators are

$$\begin{aligned} a &= (0_1, 1_1)(3_1, t_2^*)(0_2, 2_2)(1_2, 4_2), \\ b &= (2_1, 4_1)(3_1, t_2^*)(0_2, 4_2)(1_2, 2_2), \\ c &= (1_1, 4_1, 1_2)(2_1, 3_2, t_2^*)(3_1, 2_2, 0_2) \text{ and} \\ d &= (2_1, 2_2, 0_2)(3_1, 3_2, t_2^*)(4_1, 4_2, 1_2) \end{aligned}$$

The group contains an 11-cycle $(1_1, 2_1, 3_1, 3_2, 2_2, 4_2, 0_1, 3_2, 4_1, t_2^*, 0_2)$ and is transtive. The group was first discovered by Todd [6].

4.2 The case q > 5

Henceforth, the Paley 2-designs we will consider will have $q \geq 9$.

Let $q = p^n$, $q \equiv 1 \pmod 4$, where p is prime and n is a natural number. Let a, b be fixed elements of $GF(q)$ such that a is a nonzero square. Let $D' = (P', B')$ denote a Paley 2-design. We define $\pi_{a,b,j}$: $P' \to P'$ such that

$$\pi_{a,b,j}: \begin{cases} x \to & a_i x^{p^j} + b_i \text{ if } x \in GF(q)_i,\ i = 1,2;\ 1 \leq j \leq n, \\ t_2^* \to & t_2^*. \end{cases}$$

Theorem 4.1 *The set* $G = \{\pi_{a,b,j} : a, b \in GF(q)$ *is nonzero square,* $1 \leq j \leq n\}$ *is an automorphism group for the Paley 2-designs.*

Proof. Clearly, every $\pi_{a,b,j}$ maps every point of $GF(q)_2$ to a point in $GF(q)_2$, or equivalently, the block $GF(q)_2$ is fixed by G.

Next, the point $x \in Q + y$ iff $x = d + y$ for a nonzero square d. Hence $\pi_{a,b,j}$: $x \to ax^{p^j} + b = ad^{p^j} + ay^{p^j} + b \in Q + (ay^{p^j} + b)$. Thus, the block $[Q_1 + y_1 \cup \{y_1\} \cup Q_2 + y_2]$ is mapped to the block $[Q_1 + (a_1 y_1^{p^j} + b_1) \cup \{a_1 y_1^{p^j} + b_1\}] \cup Q_2 + (a_2 y_2^{p^j} + b_2)]$

Similarly, the point $x \in N + y$ iff $x = n + y$ for a nonquadratic residue n. Thus, $\pi_{a,b,j}$: $x \to ax^{p^j} + b = an^{p^j} + ay^{p^j} + b \in N + (ay^{p^j} + b)$. Thus, the block $[Q_1 + y_1 \cup \{t_2^*\} \cup N_2 + y_2]$ is mapped to the block $[Q_1 + (a_1 y_1^{p^j} + b_1) \cup \{t_2^*\} \cup N_2 + (a_2 y_2^{p^j} + b_2)]$. □

Next, we show that G is *the* automorphism group of the Paley 2-designs for $q \geq 9$. We first need the following lemmas.

Lemma 4.2 *$GF(q)_2$ is an isolated block.*

Proof.

$GF(q)_2$ has the special property that for any other block $\alpha \in B'$, \$ a block $\beta \in B'$ such that $GF(q)_2 \cap \alpha \cap \beta = \emptyset$. That is, note that $\forall a \in GF(q)$,

$GF(q)_2 \cap [Q_1 + a_1 \cup \{a_1\} \cup Q_2 + a_2] \cap [Q_1 + a_1 \cup \{t_2^*\} \cup N_2 + a_2] = \emptyset$.

On the other hand, if we fix any other block $\gamma \in B'$, then \$$\alpha \in B'$ such that $\forall \beta \in B'$, we have

$$\gamma \cap \alpha \cap \beta \neq \emptyset. \qquad (1)$$

For example, if we choose $\gamma = [Q_1 \cup \{0_1\} \cup Q_2]$, then we can choose $\alpha = [Q_1 \cup \{t_2^*\} \cup N_2]$. Clearly, in this case, (1) is satisfied. By Theorem 4.1, the block $[Q_1 + a_1 \cup \{a_1\} \cup Q_2 + a_2]$ is equivalent to $[Q_1 \cup \{0_1\} \cup Q_2]$. That is, they have the same orbit under the group G of Theorem 4.1 Hence (1) is also satisfied by blocks of the form $[Q_1 + a_1 \cup \{a_1\} \cup Q_2 + a_2]$.

If we choose $\gamma = [Q_1 \cup \{t_2^*\} \cup N_2]$, then we can choose $\alpha = [Q_1 \cup \{0_1\} \cup Q_2]$. Thus, (1) is satisfied. By Theorem 4.1, the block $[Q_1 + a_1 \cup \{t_2^*\} \cup N_2 + a_2]$ is equivalent to $[Q_1 \cup \{t_2^*\} \cup N_2]$, hence (1) is also satisfied by blocks of the form $[Q_1 + a_1 \cup \{t_2^*\} \cup N_2 + a_2]$. L

Lemma 4.3 *t_2^* is an isolated point.*

Proof. The point t_2^* has the special property that for any other point x in $GF(q)_1$, \$ another point y in $GF(q)_2$, such that the triple of points $\{t_2^* x, y\}$ is not contained in any block. Note that $\{t_2^* a_1, a_2\}$ is not contained in any block.

On the other hand, if we fix any other point $z \in P'$, then \$$x$ in $GF(q)_1$ such that $\forall$ other point y in $GF(q)_2$, the triple $\{x, y, z\}$ is contained in some block. For example, if we choose $z = 0_1$, then choose $x = 1_1$. There exist $\frac{q-5}{4}$ cosets $Q_1 + a_1$ which contain the pair $\{0_1, 1_1\}$. Then the cosets $Q_2 + a_2$ and $N_2 + a_2$ cover $GF(q)_2$.

If z is any other point in $GF(q)_1$, say a_1, then choose $x = 0_1$. The pair $\{0_1, a_1\}$ is contained in at least $\frac{q-5}{4}$ cosets $Q_1 + b_1$. Then again the cosets $Q_2 + b_2$ and $N_2 + b_2$ cover $GF(q)_2$.

If $z = 0_2$, then choose $x = 0_2$. All blocks of the form $[Q_1 + a_1 \cup \{a_1\} \cup Q_2 + a_2]$ where $a \in Q$, contain $\{0_1, 0_2\}$. Since any pair of points in $GF(q)_2$ is in at least $\frac{q-5}{4}$ cosets $Q_2 + c_2$, then for any other $b_2 \in GF(q)_2$, the triple $\{0_1, 0_2, b_2\}$ is contained in some block $[Q_1 + a_1 \cup \{a_1\} \cup Q_2 + a_2]$ where $a \in Q$.

If z is any other point in $GF(q)_2$, say a_2, then choose $x = 1_1$. We must show that for any other point $y = b_2$ in $GF(q)_2$, there exists a block which contains the triple $\{a_2, 1_1, b_2\}$. We note that if 1_1 is contained in the coset $Q_1 + a_1$ then $a_1 - 1$ must be a square.

First, we consider the case when $a_2 \in Q_2$. If $b_2 \in Q_2$, then the block $[Q_1 \cup \{0_1\} \cup Q_2]$ contains the triple $\{a_2, 1_1, b_2\}$. If $b_2 \in N_2 \cup \{0_2\}$, then there exist at least two pairs say, $\{Q_1, Q_2\} \subseteq Q_2$ and $\{n_1, n_2\} \subseteq N_2$ such that $a_2 - b_2 = q_1 - q_2 = n_1 - n_2$. Find s such that $s = a_2 - q_1 = b_2 - q_2$. If $s - 1 \in Q_2$, then the block $[Q_1 + s_1 \cup \{s_1\} \cup Q_2 + s_2]$ contains the triple $\{a_2, 1_1, b_2\}$. Otherwise, find s such that $s = a_2 - n_1 = b_2 - n_2$ and $s - 1 \in Q_2$. Then the block $[Q_1 + s_1 \cup \{t_2^*\} \cup N_2 + s_2]$ contains the triple $\{a_2, 1_1, b_2\}$.

Next, we consider the case when a_2 is a non-square. If $b_2 \in Q_2$, then the block $[Q_1 \cup \{t_2^*\} \cup N_2]$ contains the triple $\{a_2, 1_1, b_2\}$. If $b_2 \in Q_2 \cup \{0_2\}$, then we again find two pairs $\{q_1, q_2\} \subseteq Q_2$ and $\{n_1, n_2\} \subseteq N_2$ such that $a_2 - b_2 = q_1 - q_2 = n_1 - n_2$. Then, as before we find a square $s - 1$ such that $s = a_2 - q_1 = b_2 - q_2$ or $s = a_2 - n_1 = b_2 - n_2$. Then either $[Q_1 + s_1 \cup \{s_1\} \cup Q_2 + s_2]$ or $[Q_1 + s_1 \cup \{t_2^*\} \cup N_2 + s_2]$ contains the triple $\{a_2, 1_1, b_2\}$.

Lemma 4.4 *Let* $\sigma \in Aut\ D'$.

(i) *If* $\sigma(0_1) = 0_1$ *then* $\sigma(Q_1) = (Q_1)$.

(ii) If $\sigma(x_1) = x_1\ \forall x_1 \in GF(q)_1$ *then* σ *is the identity element of* $Aut\ D'$.

Proof.

(i) By Lemmas 4.2 and 4.3, *Aut D'* must fix $GF(q)_2$ and t_2^*. Hence, it must also fix $GF(q)_1$.

Let σ be an unknown automorphism of D'. Then $\sigma\{t_2^*\} = t_2^*$. If we assume that $\sigma(0_1) = 0_1$, then this would imply that $\sigma(0_2) = 0_2$ since the triple $\{0_1, t_2^*, 0_2\}$ is not contained in any block.

We now consider the blocks containing 0_1, namely $[Q_1 \cup \{0_1\} \cup Q_2]$ and blocks of the form $[Q_1 + a_1 \cup \{a_1\} \cup Q_2 + a_2]$ and $[Q_1 + a_1 \cup \{t_2^*\} \cup N_2 + a_2]$ where $a \in Q$. Since σ fixes 0_1 and t_2^* blocks of the form $[Q_1 + a_1 \cup \{t_2^*\} \cup N_2 + a_2]$ must be mapped to blocks of the same type. Now, blocks of the type $[Q_1 + a_1 \cup \{a_1\} \cup Q_2 + a_2]$ where $a \in Q$ contain both 0_1 and 0_2 while

$[Q_1 \cup \{0_1\} \cup Q_2]$ contains only 0_1. Thus the block $[Q_1 \cup \{0_1\} \cup Q_2]$ must be fixed by σ. Hence $\sigma(Q_1) = Q_1$, $\sigma(0_1) = 0_1$and $\sigma(Q_2) = Q_2$. This then implies that $\sigma(N_1) = N_1$, $\sigma(0_2) = 0_2$, and $\sigma(N_2) = N_2$.

We note that fromTheorem 4.1, *Aut D'* has a group which fixes 0_1, 0_2 and which is transitive on Q_1, N_1, Q_2, and N_2.

(ii) Now, if we assume that $\sigma(x_1) = x_1$ $\forall x_1 \in GF(q)_1$ then we get that σ is the identity permutation. This is because $\sigma(x_1) = x_1$ implies $\sigma(x_2) = x_2$ since the triple $\{x_1, t_2^*, x_2\}$ is not contained in any block.

We will also need the following restatement of a theorem by Carlitz [2]. Another proof of Carlitz' theorem has been given by Bruen and Levinger [1].

Theorem 4.5 (Carlitz) *For $q = p^n$, where p is prime and n is a positive integer, we let $f : GF(q) \to GF(q)$ be such that $f(0) = 0$ and $f(Q) = Q$. Then $f(x) = ax^{p^i}$ for some $a \in Q$, $1 \leq i \leq n$.*

Theorem 4.6 *Let D' denote a Paley $2-(2q+1, q, \frac{q-1}{2})$ design for $q = p^n$, $q \equiv 1$ (mod 4), $q \geq 9$. Then its automorphism group Aut D' is the group G of Theorem 4.1 and has order $nq\ \frac{q-1}{2}$.*

Proof. Let $\sigma \in Aut\ D'$. If $\sigma(0_1) = 0_1$, then $\sigma(Q_1) = (Q_1)$ by part (i) of Lemma 4.4. Thus, we can apply Carlitz theorem and we know that $\sigma(x) = ax^{p^i}$ for some $a \in Q$, $1 \leq i \leq n$.

Let $Sym(GF(q))$ denote the group of permutations on $GF(q)$. Now, the mapping $Aut\ D' \to Sym(GF(q))$ given by $\sigma \to \sigma|_{GF(q)_1}$ is a group homomorphism and so is $\phi : (Aut\ D')_{0_1} \to Sym(GF(q))_0$ where G_x denotes the *stabilizer* of x in G.

By Carlitz' Theorem, we know that $|Im\ \phi| = n.\ \frac{q-1}{2}$. Also, by part (ii) of Lemma 4.4, ϕ is an isomorphism. Thus, $|(Aut\ D')_{0_1}|Im\ \phi|$. By the orbit-stabilizer theorem, this implies that $|\ Aut\ D'| = q.\ |\ (Aut\ D')_{0_1}|$ since the length of the orbit of 0_1 is q. Therefore, $|Aut\ D'| = nq.\ \frac{q-1}{2}$ and $Aut\ D'$ must be the group G of Theorem 4.1. □

ACKNOWLEDGMENT

This research was done when the author visited Kyushu University in 1997 under the auspices of the Japan Society for the Promotion of Science. The author also wishes to acknowledge the many valuable suggestions of Professor Noboru

Ito in the proofs of the main results. Likewise, the author is indebted to Professor Akihiro Munemasa for his improvement of the proof of Theorem 4.1 and also for bringing Carlitz' theorem to the attention of the author.

REFERENCES

1. Bruen, A., and B. Levinger. A Theorem on Permutations of a Finite Field. *Can. J. Math.* **25**, No. 5, 1060-1065 (1973).
2. Carlitz, L. A Theorem on Permutations in a Finite Field. *Proc. Amer. Math. Soc.* **11**, 456-459 (1960).
3. Ito, N. On Hadamard Groups II, *J. of Algebra* **169**, No. 3, 936-942 (1994).
4. Ito, N., J.S.Leon, and J.Q. Longyear. Hadamard Tournaments of Order 23, *Math. J. of Okayama Univ.* **35**, 1-15 (1993).
5. Norman, C. A Characterization of the Matheiu Group M_{11}, *Math. Zeitschr.* **106**, 162-166 (1968).
6. Todd, J. A. A Combinatorial Problem. *J. Math. and Phys.* **12**, 321-333 (1933).