Some Related Designs of Paley 2-designs of *QN*-type

Blessilda P. Raposa
Mathematics Department, De La Salle University
2401 Taft Avenue, 1004 Manila, Philippines

Keywords: *2-designs, Paley 2-designs of QN-type, dual, complement, self-dual, isomorphism*

Paley 2-designs of QN-type are symmetric $2-\left(2q+1, q, \frac{q-1}{2}\right)$ *designs where q is a prime power such that* $q \equiv 1 (\mathrm{mod}\ 4)$. *The main results of this paper show that the Paley 2-designs of QN-type and their complements are self-dual.*

INTRODUCTION

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

A 2 - (v,k,λ)design is said to be *symmetric* if $|P| = |B|$. Otherwise, it is called *non-symmetric*.

Example 1

Consider the design $D = (P, B)$ where $P = \{1,2,3,4,5,6,7,8,9,10,11\}$ and B consists of the following blocks:

$\alpha_1 = \{1, 2, 3, 7, 10\}$ $\alpha_2 = \{1, 2, 6, 9, 11\}$
$\alpha_3 = \{1, 3, 4, 5, 9\}$ $\alpha_4 = \{1, 4, 6, 7, 8\}$
$\alpha_5 = \{1, 5, 8, 10, 11\}$ $\alpha_6 = \{2, 3, 4, 8, 11\}$
$\alpha_7 = \{2, 4, 5, 6, 10\}$ $\alpha_8 = \{2, 5, 7, 8, 9\}$
$\alpha_9 = \{3, 5, 6, 7, 11\}$ $\alpha_{10} = \{3, 6, 8, 9, 10\}$
$\alpha_{11} = \{4, 7, 9, 10, 11\}$

Observe that the above design D has 11 points and that every block has 5 points in it. It is also straightforward to check that every pair of points is in 2 blocks. For example, the pair of points $\{1,2\}$ can be found in α_1 and α_2. Thus, we say that D is a 2-(11, 5, 2) design. Moreover, D is symmetric since the number of points and the number of blocks are equal.

If D and D' are two designs, we define an *isomorphism* $\phi: D \rightarrow D'$ to be a one-to-one mapping of points of D onto points of D' such that $p \in \alpha$ in D if and only if $\phi(p) \in \phi(\alpha)$ in D'. If there exists an isomorphism from D to D', then we say that D and D' are *isomorphic*, denoted by $D \cong D'$.

Example 2

Let D' be the design where $P = \{1,2,3,4,5,6,7,8,9,10,11\}$ and B consists of the following blocks:

$\beta_1 = \{1, 2, 4, 5, 6\}$ $\beta_2 = \{1, 2, 7, 9, 10\}$
$\beta_3 = \{1, 3, 4, 7, 8\}$ $\beta_4 = \{1, 3, 5, 9, 11\}$
$\beta_5 = \{1, 6, 8, 10, 11\}$ $\beta_6 = \{2, 3, 5, 8, 10\}$

$\beta_7 = \{2, 3, 6, 7, 11\}$ $\beta_8 = \{2, 4, 8, 9, 11\}$
$\beta_9 = \{3, 4, 6, 9, 10\}$ $\beta_{10} = \{4, 5, 7, 10, 11\}$
$\beta_{11} = \{5, 6, 7, 8, 9\}$

It can be verified that the 2-(11,5,2) design D of Example 1 and D' are isomorphic designs. Consider the mapping ϕ given below.

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 11 & 5 & 1 & 6 & 8 & 7 & 3 & 2 & 10 & 9 & 4 \end{pmatrix}$$

The notation assigns to each point a of D in the first row, its corresponding image $\phi(a)$ in D' directly below it in the second row. Thus $\phi(1) = 11$, $\phi(2) = 5$, and so on. The mapping ϕ induces a mapping of blocks from D to D' given as follows.

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} \\ \beta_4 & \beta_{10} & \beta_5 & \beta_7 & \beta_8 & \beta_1 & \beta_{11} & \beta_6 & \beta_3 & \beta_2 & \beta_9 \end{pmatrix}$$

Since ϕ maps points to points in such a way that blocks are mapped to blocks, we conclude that ϕ is an isomorphism and that $D \cong D'$.

Given a 2- (v,k,λ) design, there are several designs which are related to it or which can be constructed from it. We consider two of them, namely, the dual and the complement.

The *dual* of a design D, denoted by D^T, is the design whose points and blocks are the blocks and points of D, respectively. Incidence in D^T is defined as follows: The point α is in the block a of D^T if and only if $a \in \alpha$ in D. If $D \cong D^T$, then we say that D is *self-dual*.

Example 3

The dual of the 2-(11,5,2) design D of Example 1 is given below. Its point set is $P^T = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8, \alpha_9, \alpha_{10}, \alpha_{11}\}$ and the blocks are:

$1 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$ $2 = \{\alpha_1, \alpha_2, \alpha_6, \alpha_7, \alpha_8\}$
$3 = \{\alpha_1, \alpha_3, \alpha_6, \alpha_9, \alpha_{10}\}$ $4 = \{\alpha_3, \alpha_4, \alpha_6, \alpha_7, \alpha_{11}\}$
$5 = \{\alpha_3, \alpha_5, \alpha_7, \alpha_8, \alpha_9\}$ $6 = \{\alpha_2, \alpha_4, \alpha_7, \alpha_9, \alpha_{10}\}$
$7 = \{\alpha_1, \alpha_4, \alpha_8, \alpha_9, \alpha_{11}\}$ $8 = \{\alpha_4, \alpha_5, \alpha_6, \alpha_8, \alpha_{10}\}$
$9 = \{\alpha_2, \alpha_3, \alpha_8, \alpha_{10}, \alpha_{11}\}$ $10 = \{\alpha_1, \alpha_5, \alpha_7, \alpha_{10}, \alpha_{11}\}$
$11 = \{\alpha_2, \alpha_5, \alpha_6, \alpha_9, \alpha_{11}\}$

The 2-(11,5,2) design D is self-dual. Consider the mapping ϕ: $D \rightarrow D^T$ given by

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ \alpha_2 & \alpha_6 & \alpha_9 & \alpha_{10} & \alpha_4 & \alpha_8 & \alpha_{11} & \alpha_3 & \alpha_7 & \alpha_5 & \alpha_1 \end{pmatrix}$$

This then induces the following mapping of blocks.

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} \\ 11 & 2 & 6 & 9 & 1 & 3 & 8 & 4 & 7 & 5 & 10 \end{pmatrix}$$

Clearly, ϕ is an isomorphism and $D \cong D^T$. Hence, D is self-dual.

The next related design that we are going to consider is the complement of a design. If D is a 2-design, then its *complement*, denoted by D^c, is the design whose points are the points of D and for each block α^c of D^c, the point $p \in \alpha^c$ in D^c if and only if $p \notin \alpha$ in D.

Example 4

The complement D^c of the 2-(11,5,2) design D of Example has point set $P^c = \{1,2,3,4,5,6,7,8,9,10,11\}$ and its blocks are as follows:

$$\alpha_1^c = \{4, 5, 6, 8, 9, 11\}$$

$\alpha_2^c = \{3, 4, 5, 7, 8, 10\}$

$\alpha_3^c = \{2, 6, 7, 8, 10, 11\}$

$\alpha_4^c = \{2, 3, 5, 9, 10, 11\}$

$\alpha_5^c = \{2, 3, 4, 6, 7, 9\}$

$\alpha_6^c = \{1, 5, 6, 7, 9, 10\}$

$\alpha_7^c = \{1, 3, 7, 8, 9, 11\}$

$\alpha_8^c = \{1, 3, 4, 6, 10, 11\}$

$\alpha_9^c = \{1, 2, 4, 8, 9, 10\}$

$\alpha_{10}^c = \{1, 2, 4, 5, 7, 11\}$

$\alpha_{11}^c = \{1, 2, 3, 5, 6, 8\}$

SOME KNOWN RESULTS

In this section, we consider some known results about the related designs of a given 2- (v,k,λ) design D. The proofs of these theorems are found in [1].

We recall that v represents the number of points in D, k denotes the number of points in a block and that λ is the number of blocks containing two distinct points. We let b denote the number of blocks in D and let r denote the number of blocks through a point.

Theorem 1. If D is a symmetric 2- (v,k,λ) design, then its dual D^T is again a symmetric 2- (v,k,λ) design.

Observe that the dual of the 2-(11,5,2) design given in Example 3 is again a symmetric 2-(11,5,2) design.

Theorem 2. If D is a 2- (v,k,λ) design with $2 \leq k \leq v - 2$, then its complement D^c is a $2 - (v, v-k, b - 2r + \lambda)$ design.

The 2- (11, 5, 2) design has $b = 11$ and $r = 5$. Thus, in Example 4, one can verify that the complement of the 2-(11,5,2) design is a 2-(11, 6, 3) design.

PALEY 2-DESIGNS OF *QN*-TYPE

In this section, we give the construction of the Paley 2-designs of *QN*-type as described by N. Ito in [2].

Let q be a prime power such that $q \equiv 1 (\mathrm{mod}\ 4)$ 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 two disjoint copies of $GF(q)$, namely $GF(q)_1$ and $GF(q)_2$. For any $a \in GF(q)$, the two mappings which map a to a_1 and a_2 are isomorphisms. For a subset $S \subseteq GF(q)$, and for $i = 1,2$, the set S_i is the image in $GF(q)_i$ of S under the *ith* mapping. The *coset* $Q + a = \{x + a \mid x \in Q\}$. We define $Q_i + a_i$ as $(Q+a)_i$. The cosets $N + a$ and $N_i + a_i$ are defined analogously.

Let $D=(P,B)$ be such that
$P = GF(q)_1 \cup GF(q)_2 \cup \{t\}$ and
$B = \{\alpha, \beta(a), \gamma(a) \mid a \in GF(q)\}$ where

$$\alpha = GF(q)_2\,;$$

$$\beta(a) = (Q_1 + a_1) \cup \{a_1\} \cup (Q_2 + a_2); \text{ and}$$

$$\gamma(a) = (Q_1 + a_1) \cup \{t\} \cup (N_2 + a_2).$$

Then D is a symmetric

$$2 - \left(2q + 1,\ q,\ \frac{q-1}{2}\right)$$

design of Paley QN-type or simply a *Paley 2-design of QN-type.*

Example 5

Let $q = 5$. The quadratic residues of $GF(5)$ are

1 and 4. The non-quadratic residues are 2 and 3. Thus $Q = \{1,4\}$ and $N = \{2,3\}$. The blocks of the corresponding Paley 2-design of *QN*-type are given as follows:

$$\begin{aligned}
\alpha &= \{0_2, 1_2, 2_2, 3_2, 4_2\}\\
\beta(0) &= \{1_1, 4_1, 0_1, 1_2, 4_2\}\\
\beta(1) &= \{2_1, 0_1, 1_1, 2_2, 0_2\}\\
\beta(2) &= \{3_1, 1_1, 2_1, 3_2, 1_2\}\\
\beta(3) &= \{4_1, 2_1, 3_1, 4_2, 2_2\}\\
\beta(4) &= \{0_1, 3_1, 4_1, 0_2, 3_2\}\\
\gamma(0) &= \{1_1, 4_1, \mathrm{t}, 2_2, 3_2\}\\
\gamma(1) &= \{2_1, 0_1, \mathrm{t}, 3_2, 4_2\}\\
\gamma(2) &= \{3_1, 1_1, \mathrm{t}, 4_2, 0_2\}\\
\gamma(3) &= \{4_1, 2_1, \mathrm{t}, 0_2, 1_2\}\\
\gamma(4) &= \{0_1, 3_1, \mathrm{t}, 1_2, 2_2\}
\end{aligned}$$

We distinguish the Paley 2-designs of *QN*-type from the other family of designs which some literature refer to as Paley 2-designs. The latter Paley 2-designs are also called *designs of quadratic residue type*. Their point set is $GF(q)$ for q a prime power and $q \equiv 3 \pmod 4$ and their blocks are cosets of the set of quadratic residues of $GF(q)$. The blocks of the Paley 2-designs of *QN*-type consist of both cosets of quadratic residues (Q) and non-quadratic residues (N), hence the name. Although the number of points in the Paley 2-designs of *QN*-type is $2q + 1 \equiv 3 \pmod 4$, it is not always a prime power. The only time when the two Paley 2-designs are isomorphic is when the number of points is 11.

SELF-DUALITY OF THE PALEY 2-DESIGNS OF *QN*-TYPE AND THEIR COMPLEMENTS

The main objective of this section is to show that the Paley 2-Designs of *QN*-type and their complements are self-dual. Henceforth, all occurrences of q will mean that $q = p^n$, $q \equiv 1 \pmod 4$, where p is a prime number and n is a positive integer.

Theorem 3

The Paley 2- designs of *QN*-type are self-dual.

Proof:

We first construct the dual D^T of D, the Paley

$$2-\left(2q+1,\, q,\, \frac{q-1}{2}\right)$$

design of *QN*-type. The point set P^T of D^T consists of $\{\alpha\} \cup \{\beta(a) \mid a \in GF(q)\} \cup \{\gamma(a) \mid a \in GF(q)\}$. The blocks of D^T are:

$t = \{\gamma(a) \mid a \in GF(q)\}$;

$a_1 = \{\beta(a)\} \cup \{\beta(b) \mid a \in Q+b\} \cup \{\gamma(b) \mid a \in Q+b\}$, where $a_1 \in GF(q)_1$;

$a_2 = \{\alpha\} \cup \{\beta(b) \mid a \in Q+b\} \cup \{\gamma(b) \mid a \in N+b\}$, where $a_2 \in GF(q)_2$.

Clearly, the block t has q elements. Since both Q and N have $\frac{q-1}{2}$ elements, each of the cosets $Q+b$ and $N+b$ also has $\frac{q-1}{2}$ elements. Thus, each block of D^T has q elements.

Consider the mapping $\phi : P \to P^T$ such that

$$\phi:\begin{cases} t\to\alpha & \\ a_1\to\beta(a) & \text{for all } a_1 \in GF(q)_1 \\ a_2\to\gamma(a) & \text{for all } a_2 \in GF(q)_2 \end{cases}$$

Then ϕ induces the following mapping of blocks:

$$\phi:\begin{cases} \alpha\to t & \\ \beta(a)\to a_1 & \text{for all } a \in GF(q) \\ \gamma(a)\to a_2 & \text{for all } a \in GF(q) \end{cases}$$

To see this, we first note that the block α in D consists of all the elements of $GF(q)_2$. Now, ϕ maps points in $GF(q)_2$ to blocks of the form $\gamma(a)$. In D^T, the block which contains all points of the form $\gamma(a)$ is t. Thus α is mapped to t.

Next, a block of the form $\beta(a)$ in D consists of $(Q_1+a_1) \cup \{a_1\} \cup (Q_2+a_2)$. The point a_1 is mapped to $\beta(a)$, a point b_1 belonging to Q_1+a_1 is mapped to $\beta(b)$ and a point b_2 belonging to Q_2+a_2 is mapped to $\gamma(b)$. Thus, the block $\beta(a)$ in D is mapped to the block a_1 in D^T.

Finally, a block of the form $\gamma(a)$ in D consists of $(Q_1+a_1) \cup \{t\} \cup (N_2+a_2)$. The point t is mapped to α. A point b_1 belonging to Q_1+a_1 is mapped to $\beta(b)$. A point b_2 belonging to N_2+a_2 is mapped to $\gamma(b)$. The block in D^T, consisting of such points $\alpha, \beta(b)$ and $\gamma(b)$ is a_2. Thus, the block $\gamma(a)$ in D is mapped to the block a_2 in D^T.

Since ϕ is a one-to-one onto mapping of points to points which maps blocks to blocks, it is an isomorphism. Thus, we have $D \cong D^T$ and D is self-dual.

The following theorem is considered as folklore in Design Theory. Its proof, however, is not contained in most of the books in basic Design Theory , so we present its proof here for completeness.

Theorem 4. If D is a symmetric 2- (v,k,λ) design which is self-dual, then its complement, D^c is also self-dual.

Proof: Let ϕ be an isomorphism between D and D^T. Then this implies $a \in \alpha$ in D if and only if $\phi(a) \in \phi(\alpha)$ in D^T. We claim that ϕ also induces an isomorphism between D^c and $[D^c]^T$. That is, we want to show that $b \in \alpha^c$ in D^c if and only if $\phi(b) \in \phi(\alpha^c)$ in $[D^c]^T$.

We first show $\phi(\alpha^c) = [\phi(\alpha)]^c$. The element $x \in \phi(\alpha^c)$ if and only if there exists $b \in \alpha^c$ such that $\phi(b) = x$. Since ϕ is an isomorphism, $b \in \alpha^c$ if and only if $\phi(b) \notin \phi(\alpha\ )$. But $\phi(b) \notin \phi(\alpha\ )$ if and only if $\phi(b) = x \in [\phi(\alpha)]^c$.

Let $b \in \alpha^c$ in D^c. Suppose $\phi(b) \notin \phi(\alpha^c) = [\phi(\alpha)]^c$. Then $\phi(b) \in \phi(\alpha\ )$. But this would imply $b \in \alpha$, a contradiction.

Suppose $\phi(b) \in \phi(\alpha^c)$ but $b \notin \alpha^c$. Then $b \in \alpha$ and this implies $\phi(b) \in \phi(\alpha\ )$, again a contradiction.

Thus, we have shown $b \in \alpha^c$ in D^c if and only if $\phi(b) \in \phi(\alpha^c)$ in $[D^c]^T$. Hence, ϕ is an isomorphism between D^c and $[D^c]^T$. Therefore, D^c is also self-dual.

Corollary 5. The complement of a Paley 2-design of *QN*-type is also self-dual.

Proof: This follows immediately from Theorems 3 and 4.

REFERENCES

1 Hughes, D. R. and Piper, F.C., *Design Theory*, Cambridge University Press, (1985).

2 Ito N. , On Hadamard Groups II, Journal of Algebra, Vol. 169, No. 3, 936-942 (1994).