5-2013

On an Additive Characterization of a Skew Hadamard (n, n−1/ 2 , n−3 4)-Difference Set in an Abelian Group

John McSorley
Southern Illinois University Carbondale, jmcsorley@math.siu.edu

On an Additive Characterization of a Skew Hadamard $(n, \frac{n-1}{2}, \frac{n-3}{4})$-Difference Set in an Abelian Group

John P. McSorley
Department of Mathematics
Mailcode 4408
Southern Illinois University
Carbondale. IL 62901-4408
mcsorley60@hotmail.com

Abstract

We give a combinatorial proof of an additive characterization of a skew Hadamard $(n, \frac{n-1}{2}, \frac{n-3}{4})$-difference set in an abelian group G. This research was motivated by the $p = 4k + 3$ case of Theorem 2.2 of Monico and Elia [4] concerning an additive characterization of quadratic residues in $\mathbb{Z}_p$. We then use the known classification of skew $(n, \frac{n-1}{2}, \frac{n-3}{4})$-difference sets in $\mathbb{Z}_n$ to give a result for integers $n = 4k + 3$ that strengthens and provides an alternative proof of the $p = 4k + 3$ case of Theorem 2.2 of [4].

Keywords: abelian group; difference set; skew; Hadamard; additive characterization; quadratic residues

1 Introduction: difference sets in G and an additive characterization of Q in $\mathbb{Z}_p$

Let G be an abelian group of order n written additively, with identity 0, and let $G^* = G \backslash \{0\}$. Let $\mathbb{Z}_n$ denote the integers modulo n. For most of this paper n will be an integer of the form $n = 4k + 3$, with $k \geq 1$. We also use $[n] = \{1, 2, \ldots, n\}$.

We start with some Definitions, see p.298 and p.356 of Beth, Jungnickel and Lenz [1]:

Definitions 1.1 (n, κ, λ)-difference set in G, skew

(1) A (n, κ, λ)-*difference set* in G is a κ-subset $D = \{d_1, d_2, \ldots, d_\kappa\} \subseteq G$ with the property that every $g \in G^*$ occurs exactly λ times as a difference $d_i - d_j$ for $d_i, d_j \in D$, and $1 \leq i, j \leq \kappa$, where $i \neq j$.

(2) A (n, κ, λ)-difference set D is *skew* if $G = \{0\} \cup D \cup -D$ is a partition of G.

Example 1.2 $G = \mathbb{Z}_{11}$. $D = \{1, 3, 4, 5, 9\}$ is a $(11, 5, 2)$-difference set. Also D is skew because $\mathbb{Z}_{11} = \{0\} \cup \{1, 3, 4, 5, 9\} \cup \{2, 6, 7, 8, 10\}$ is a partition of $\mathbb{Z}_{11}$.

Now let $p = 4k + 3$ be a prime, with $k \geq 1$. Let Q be the set of quadratic residues in $\mathbb{Z}_p$, and N be the set of quadratic non-residues. We have $Q = -N$, and $|Q| = |N| = \frac{p-1}{2}$, and $\mathbb{Z}_p = \{0\} \cup Q \cup -Q$ is a partition of $\mathbb{Z}_p$.

In Theorem 2.2 of Monico and Elia [4] the following characterization is proved:

Let $p = 4k+3$ be prime and let $d_p = \frac{p+1}{4}$. Suppose $A \subset \mathbb{Z}_p^*$ and $B = \mathbb{Z}_p^* \setminus A$. Then $A = Q$, the set of quadratic residues of $\mathbb{Z}_p$, if and only if

1. $|A| = \frac{p-1}{2}$,
2. $1 \in A$,
3. *every $a \in A$ can be written as an ordered sum of two elements from A in exactly $d_p - 1$ ways, and*
4. *every $b \in B$ can be written as an ordered sum of two elements from A in exactly d_p ways.*

In §2, motivated by this Theorem, we present our main result (Theorem 2.2) which gives an additive characterization of a skew $(n, \frac{n-1}{2}, \frac{n-3}{4})$-difference set in G. The proof of this result is purely combinatorial.

In §3, we use the known classification of skew $(n, \frac{n-1}{2}, \frac{n-3}{4})$-difference sets in $G = \mathbb{Z}_n$ to give our Theorem 3.4 that strengthens and provides an alternative proof for the $p = 4k + 3$ case of Theorem 2.2 of [4]. (The other case of Theorem 2.2 of [4] involves primes $p = 4k + 1$.)

2 Skew difference sets and properties P1, P2, P3

Before the main result of this paper we need the following Lemma 2.1.

Lemma 2.1 *Let G be an abelian group of order $n \geq 1$, and let $X = \{x_1, x_2, \ldots, x_\kappa\}$ be an arbitrary κ-subset of G.*

(i) Then X is a (n, κ, λ)-difference set if and only if for every $g \in G^*$ we have $|(g + X) \cap X| = \lambda$.

(ii) Let $g \in G^*$ be arbitrary. Then $|(g - X) \cap X|$ equals the number of ordered sums $g = x_i + x_j$ where $x_i, x_j \in X$, ($x_1 = x_2$ is allowed here).

Proof. (i) Let $g \in G^*$ be arbitrary, and let $\{x_i, x_j\} \subseteq X$. Clearly $g = x_i - x_j$, if and only if $g + x_j = x_i$, if and only if $x_i \in g + X$. Thus each expression of g as a difference of two elements from X results in an element of $|(g + X) \cap X|$, and conversely. This shows the stated equivalence.

(ii) Let $g \in G^*$ be arbitrary, and let s be the number of ordered sums $g = x_i + x_j$ where $x_i, x_j \in X$.

Let $h \in (g - X) \cap X$, then $h = g - x_i = x_j$, for some $x_i, x_j \in X$. Hence $g = x_i + x_j$ is an ordered sum, where $x_i, x_j \in X$. Thus $|(g - X) \cap X| \leq s$. Conversely, an ordered sum $g = x_i + x_j$, yields $h = g - x_i = x_j$, where $h \in (g - X) \cap X$. So $s \leq |(g - X) \cap X|$. Thus $|(g - X) \cap X| = s$. ■

Inspired by Theorem 2.2 of Monico and Elia [4], we have the following main result.

Theorem 2.2 *Let G be an abelian group of order $n = 4k + 3$. Suppose $A \subset G^*$ and $B = G^* \backslash A$. Then A is a skew $(n, \frac{n-1}{2}, \frac{n-3}{4})$-difference set if and only if*

P1. $|A| = \frac{n-1}{2}$,

P2. *every $a \in A$ can be written as an ordered sum of two elements from A in exactly $\frac{n-3}{4}$ ways, and*

P3. *every $b \in B$ can be written as an ordered sum of two elements from A in exactly $\frac{n+1}{4}$ ways.*

Proof. First the forward implication: Assume A is a skew $(n, \frac{n-1}{2}, \frac{n-3}{4})$-difference set. Then $G = \{0\} \cup A \cup -A$ is a partition of G and $|A| = \frac{n-1}{2}$, so P1 is satisfied.

For any $g \in G^*$ it is straightforward to show that $G = \{g\} \cup (g + A) \cup (g - A)$ is also a partition of G.

Define $A_1 = \{g\} \cap A$, $A_2 = (g + A) \cap A$, and $A_3 = (g - A) \cap A$. We have $A = G \cap A = (\{g\} \cup (g + A) \cup (g - A)) \cap A = A_1 \cup A_2 \cup A_3$. As usual $g \in G^* = A \cup B$, and we consider two cases:

For any $g \in A$: Here $A_1 = \{g\}$, and $A = \{g\} \cup A_2 \cup A_3$ is a partition of A. Now $A_2 = (g + A) \cap A$, so $|A_2| = |(g + A) \cap A| = \frac{n-3}{4}$ using Lemma 2.1(i) and the fact that A is a $(n, \frac{n-1}{2}, \frac{n-3}{4})$-difference set. Further, $A_3 = (g - A) \cap A$ and so, from Lemma 2.1(ii), $|A_3|$ equals the number of ordered sums $g = a + a'$ where $a, a' \in A$, ($a = a'$ is allowed here). The partition of A then gives: $|A_3| = \frac{n-1}{2} - 1 - |A_2| = \frac{n-3}{4}$. Thus P2 is satisfied.

For $g \in B$: Here $A_1 = \emptyset$, and $A = A_2 \cup A_3$ is a partition of A. By a similar argument to above we have $|A_2| = \frac{n-3}{4}$, and then the partition of A gives $|A_3| = \frac{n-1}{2} - |A_2| = \frac{n+1}{4}$. Thus P3 is satisfied.

Thus P1, P2, and P3 are satisfied.

Now the backward implication: Assume $A = \{a_1, a_2, \ldots, a_{\frac{n-1}{2}}\} \subset G^*$ and $B = G^* \backslash A$ where P1, P2, and P3 are satisfied, so $|B| = \frac{n-1}{2}$.

We first show that $A \cap -A = \emptyset$.

From P2 each of the $\frac{n-1}{2}$ elements $a \in A$ can be written as an ordered sum of two elements from A in $\frac{n-3}{4}$ ways, and from P3 each of the $\frac{n-1}{2}$ elements $b \in B$ can be written as an ordered sum of two elements from A in $\frac{n+1}{4}$ ways. This gives a total of $(\frac{n-1}{2})(\frac{n-3}{4}) + (\frac{n-1}{2})(\frac{n+1}{4}) = (\frac{n-1}{2})^2$ ordered sums $a_i + a_j$, where $i, j \in [\frac{n-1}{2}]$.

Now a fixed ordered sum $a_{i'} + a_{j'} = a' \in A$ or $b' \in B$ can only appear at most once amongst these $(\frac{n-1}{2})^2$ ordered sums. But there are exactly $|A| \times |A| = (\frac{n-1}{2})^2$ ordered sums $a_i + a_j$, hence *every* ordered sum $a_i + a_j$ for all $i, j \in [\frac{n-1}{2}]$ will appear exactly once amongst the above $(\frac{n-1}{2})^2$ ordered sums. Now $0 \notin A \cup B = G^*$, and so each of the above $(\frac{n-1}{2})^2$ ordered sums $a_i + a_j \neq 0$, *i.e.*, $a_i \neq -a_j$, for all $i, j \in [\frac{n-1}{2}]$.

Hence $A \cap -A = \emptyset$, and then $G^* = A \cup -A$ is a partition of G^*. Thus $B = -A$ and $G = \{0\} \cup A \cup -A$ is a partition of G.

Now we show that A is a $(n, \frac{n-1}{2}, \frac{n-3}{4})$-difference set.

Let $g \in G^* = A \cup B$. First consider $g \in A$, say $g = a_\ell$. There are in total $\frac{n-1}{2} - 1 = \frac{n-3}{2}$ ordered sums $g = a_i + (g - a_i)$ with $a_i \in A$ and $g - a_i \in A \cup B$, one for each $i \in [\frac{n-1}{2}] \backslash \{\ell\}$. From P2 exactly $\frac{n-3}{4}$ of these ordered sums have $g - a_i \in A$, so exactly $\frac{n-3}{2} - \frac{n-3}{4} = \frac{n-3}{4}$ of them have $g - a_i \in B$. So, g can be expressed as $g = a + b$ where $a \in A$ and $b \in B$ in $\frac{n-3}{4}$ ways, but $B = -A$, so g can be expressed as $g = a - a'$ for a pair $\{a, a'\} \subseteq A$ in $\frac{n-3}{4}$ ways.

Now consider $g \in B$, so $g \notin A$. Then there are $\frac{n-1}{2}$ ordered sums $g = a_i + (g - a_i)$ with $a_i \in A$ and $g - a_i \in A \cup B$, one for each $i \in [\frac{n-1}{2}]$.

From P3 exactly $\frac{n+1}{4}$ of these ordered sums have $g - a_i \in A$, so exactly $\frac{n-1}{2} - \frac{n+1}{4} = \frac{n-3}{4}$ of them have $g - a_i \in B$. And then, as above, g can be expressed as $g = a - a'$ for a pair $\{a, a'\} \subseteq A$ in $\frac{n-3}{4}$ ways.

So every $g \in G^*$ can be expressed as $g = a - a'$ for a pair $\{a, a'\} \subseteq A$ in $\frac{n-3}{4}$ ways, *i.e.*, A is a $(n, \frac{n-1}{2}, \frac{n-3}{4})$-difference set.

From above $G = \{0\} \cup A \cup -A$ is a partition of G, so A is a skew $(n, \frac{n-1}{2}, \frac{n-3}{4})$-difference set in G. ∎

3 Classification of skew difference sets in $\mathbb{Z}_n$ and consequences

Here is an example of Theorem 2.2 of Monico and Elia [4] as mentioned in the Introduction:

Example 3.1 $p = 11$, $d_p = 3$. Here $Q = \{1, 3, 4, 5, 9\}$ and $N = \{2, 6, 7, 8, 10\}$. In the following the quadratic residues, Q, are given in the first column, and the quadratic non-residues, N, in the second:

Q		N
$1 = 3+9 = 9+3$		$2 = 1+1 = 4+9 = 9+4$
$3 = 5+9 = 9+5$		$6 = 3+3 = 1+5 = 5+1$
$4 = 1+3 = 3+1$	and	$7 = 9+9 = 3+4 = 4+3$
$5 = 1+4 = 4+1$		$8 = 4+4 = 3+5 = 5+3$
$9 = 4+5 = 5+4$		$10 = 5+5 = 1+9 = 9+1$

As usual let $p = 4k + 3$ be a prime, for $k \geq 1$. Recall Paley's result from [5] that $Q \subset \mathbb{Z}_p$ is a skew $(p, \frac{p-1}{2}, \frac{p-3}{4})$-difference set.

Skew $(n, \frac{n-1}{2}, \frac{n-3}{4})$-difference sets in $G = \mathbb{Z}_n$ are classified in Corollary 3.4 of Johnsen [2], although this classification was essentially shown in Kelly [3]. See p.356 of [1] for further discussion.

Theorem 3.2 (Johnsen) *Let D be a skew $(n, \frac{n-1}{2}, \frac{n-3}{4})$-difference set in the cyclic group $\mathbb{Z}_n$. Then $n = p = 4k + 3$ is a prime and $D = Q$ is the Paley $(p, \frac{p-1}{2}, \frac{p-3}{4})$-difference set of quadratic residues in $\mathbb{Z}_p$, or $D = N$ is the $(p, \frac{p-1}{2}, \frac{p-3}{4})$-difference set of quadratic non-residues in $\mathbb{Z}_p$.* ∎

Example 3.3 $n = p = 11$. See Examples 1.2 and 3.1: $Q = \{1, 3, 4, 5, 9\}$ and $N = \{2, 6, 7, 8, 10\}$ are the two skew $(11, 5, 2)$-difference sets in $\mathbb{Z}_{11}$.

Using our Theorem 2.2 and Theorem 3.2 and the fact that $1 \in Q$, we have the following Theorem 3.4 for integers $n = 4k + 3$. Theorem 3.4 strengthens and provides an alternative proof of the $p = 4k + 3$ case of Theorem 2.2 of Monico and Elia [4].

Theorem 3.4 *Let $n = 4k + 3$ and $d_n = \frac{n+1}{4}$. Suppose $A \subset \mathbb{Z}_n^*$ and $B = \mathbb{Z}_n^* \backslash A$. Then n is a prime p and $A = Q$ if and only if*

1. $|A| = \frac{p-1}{2}$,
2. $1 \in A$,
3. *every $a \in A$ can be written as an ordered sum of two elements from A in exactly $d_p - 1$ ways, and*
4. *every $b \in B$ can be written as an ordered sum of two elements from A in exactly d_p ways.* ■

Remark The connection between the $p = 4k + 3$ case of Theorem 2.2 of Monico and Elia [4] and skew $(n, \frac{n-1}{2}, \frac{n-3}{4})$-difference sets in $\mathbb{Z}_n$ shown in this paper seems to have been overlooked by the authors of [4], and appears to be written down here for the first time.

Acknowledgement We thank the referee for indicating that we can strengthen our Theorem 2.2 to its current general form, and for other helpful comments.

References

[1] T.Beth, D.Jungnickel, H.Lenz. Design Theory, vol.1, 2-nd Ed., Encyclopedia of Mathematics and its Applications, **69**. Cambridge Univ. Press, (1999).

[2] E.Johnsen. *Skew-Hadamard Abelian Group Difference Sets*. J. Algebra, **4**, (1966), 388–402.

[3] J.Kelly. *A Characteristic Property of Quadratic Residues*. Proc. Amer. Math. Soc., **5**, (1954), 38–46.

[4] C.Monico, M.Elia. *Note on an Additive Characterization of Quadratic Residues Modulo p*. J. Combinatorics, Information and System Sciences, **31**, (2006), 209–215.

[5] R.Paley. *On Orthogonal Matrices*. J. Math. Phys., **12**, (1933), 311–320.