PERMUTATIONS WITH A DISTINCT DIVISOR PROPERTY

Mohammad Javaheri and Nikolai A. Krylov

ABSTRACT. A finite group of order n is said to have the distinct divisor property (DDP) if there exists a permutation $g_1, \ldots, g_n$ of its elements such that $g_i^{-1} g_{i+1} \neq g_j^{-1} g_{j+1}$ for all $1 \leq i < j < n$. We show that an abelian group is DDP if and only if it has a unique element of order 2. We also describe a construction of DDP groups via group extensions by abelian groups and show that there exist infinitely many non abelian DDP groups.

1. Introduction

A Costas array of order n is a permutation $x_1, \ldots, x_n$ of $\{1, 2, \ldots, n\}$ such that the $\binom{n}{2}$ vectors $(j-i, x_j-x_i)$, $i \neq j$, are all distinct. Costas arrays were first studied by John P. Costas for their applications in sonar and radar [3,4]. Several algebraic constructions of Costas arrays exist for special orders n, such as Welch, Logarithmic Welch, and Lempel constructions [8,9,10]. Through exhaustive computer searches, all Costas arrays of order $n \leq 29$ have been found [5]. However, the problem of finding Costas arrays for larger orders becomes computationally very difficult. The weaker notion of *DDP permutation* requires only the consecutive *distinct difference property* i.e., $x_{i+1} - x_i \neq x_{j+1} - x_j$ for all $1 \leq i < j < n$. By recursive constructions, an abundance of DDP permutations can be found, at least 2^n, of order n [1].

In this paper, we are interested in a notion slightly stronger than DDP.

Definition 1.1. A DDP sequence mod a positive integer n is a permutation $x_0, \ldots, x_{n-1}$ of the elements of $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ such that $x_0 = 0$ and $x_{i+1} - x_i \not\equiv x_{j+1} - x_j \pmod{n}$ for all $0 \leq i < j < n - 1$.

The first example of a DDP sequence mod 12 was introduced by F. H. Klein in 1925 as the all-interval twelve-tone row, series, or chord

$$F, E, C, A, G, D, A\flat, D\flat, E\flat, G\flat, B\flat, C\flat,$$

named the *Mutterakkord* (Mother chord) [12]. In integers mod 12, this sequence reads

$$0, 11, 7, 4, 2, 9, 3, 8, 10, 1, 5, 6,$$

and the sequence of consecutive differences mod 12 is given by 11, 8, 9, 10,7, 6, 5, 2, 3, 4, 1, which are all distinct. By 1952, there were 18 known examples of all-interval series [6]. In 1965, IBM 7094 listed all of the 3856 examples of all-interval rows [2]. Another example of an eleven-interval, twelve-tone row is the *Grandmother* chord, invented by Nicolas Slonimsky in 1938 [13].
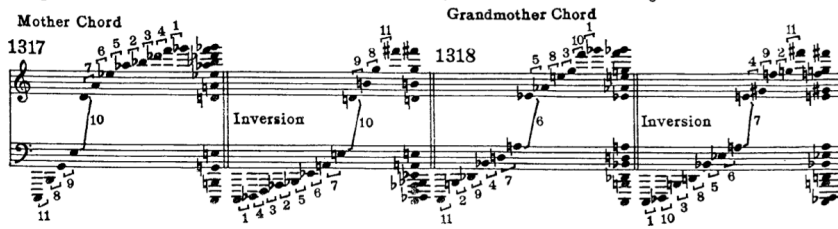

FIGURE 1. An image of the Mother chord and Grandmother chord in Slonimsky's *Thesaurus of Scales and Melodic Patterns* (p. 185).

The Grandmother chord has the additional property that the intervals are odd and even alternately, and the odd intervals decrease by one whole-tone, while the even intervals increase by one whole-tone. In integers mod 12, the grandmother chord is

$$0, 11, 1, 10, 2, 9, 3, 8, 4, 7, 5, 6,$$

where the sequence of consecutive differences mod 12 is given by 11, 2, 9, 4, 7, 6, 5, 8, 3, 10, 1. Inspired by Slonimsky's Grandmother chord, we define the Slonimsky sequence modulo n by letting

$$s_i = (-1)^i \lceil i/2 \rceil = \begin{cases} i/2 & \text{if } i \text{ is even;} \\ n - (i+1)/2 & \text{if } i \text{ is odd.} \end{cases} \tag{1}$$

Then the sequence $s_0, \ldots, s_{n-1}$ is a DDP sequence modulo n if and only if n is even. If $x_0, \ldots, x_{n-1}$ is a DDP sequence modulo n, then the sequence $rx_0, \ldots, rx_{n-1}$ is also a DDP sequence modulo n for each r with $\gcd(r, n) = 1$. Therefore, there are at least $\phi(n)$ DDP sequences mod an even integer n. The numbers of DDP sequences mod even integers are given by the sequence [7,11]

$https://oeis.org/A141599 A141599 : 1, 2, 4, 24, 288, 3856, 89328, 2755968, 103653120, \ldots.$

There are no DDP sequences modulo n for odd values of n (see Lemma 4.1).

In our next definition, we generalize Definition 1.1, which pertains to the group $(\mathbb{Z}_n, +)$, to any finite group G.

Definition 1.2. Let G be a finite group with n elements. We say a permutation $g_0, \ldots, g_{n-1}$ of elements of G has the *distinct divisor property* (DDP) or $g_0, \ldots, g_{n-1}$ is a DDP sequence, if $g_0 = 1_G$ and $g_i^{-1} g_{i+1} \neq g_j^{-1} g_{j+1}$ for all $0 \leq i < j < n-1$. The set of all DDP sequences in G is denoted by $\mathcal{O}_G$. We say G is a DDP group if $\mathcal{O}_G \neq \emptyset$.

For odd values of n, instead of distinct consecutive differences, the sequence (1) has distinct consecutive *signed* differences. This motivates the following definition.

Definition 1.3. Let $p_0, \ldots, p_{n-1}$ be a permutation of elements of an abelian group G with $p_0 = 0$. The sequence of signed differences is defined by $h_0 = 0$ and $h_i = (-1)^{i-1}(p_{i-1} - p_i)$ for $1 \leq i < n$. We say $p_0, \ldots, p_{n-1}$ is a *Slonimsky* sequence if the following conditions hold:

  i) $h_i \neq h_j$ for all $0 \leq i < j < n$.
  ii) $h_i + h_{n-i} = 0$ for all $0 < i < n$.
  iii) $p_i + p_{n-i-1} = p_{n-1}$ for all $0 \leq i < n$, where we refer to p_{n-1} as the last term of the sequence.

For example, the following sequence is a Slonimsky sequence in $\mathbb{Z}_7$:

$$0, 6, 1, 5, 2, 4, 3,$$

and its sequence of signed differences is 0, 1, 2, 3, 4, 5, 6. Slonimsky sequences in odd abelian groups play an important role in constructing DDP sequences via group extensions, and we study them in Section 2.

This is how this paper is organized. In Section 2, we show that every odd abelian group has a Slonimsky sequence. In Section 3, we use the existence of Slonimsky sequences in odd abelian groups to show that every central extension of an even DDP group by an odd abelian group is DDP (see Cor. 3.3). We also show that for every odd nilpotent group G and an even DDP group K, the direct product $G \times K$ is DDP (see Theorem 3.4). In particular, $G \times \mathbb{Z}_{2^m}$ is DDP for every odd nilpotent group G and every integer $m \geq 1$.

In Section 4, we show that a finite abelian group is DDP if and only if it has a unique element of order 2. We also find a lower bound on the number of DDP sequences in an abelian group G in terms of the prime factorization of its order. In particular, we will show that if $n = 2^m k l$ for $m \geq 1$ and relatively prime odd integers k, l, then there are at least $(2k)^{l-1}$ DDP sequences modulo n (see Cor.

4.5). Finally, in Section 5, we will show that there are infinitely many non abelian DDP groups.

2. Slonimsky sequences in abelian groups

In this section, we prove that every abelian odd group has a Slonimsky sequence. This result will only be needed in the proof of Theorem 3.2 and can be skipped in a first reading. We begin with the cyclic case.

Lemma 2.1. *If n is odd, then $G = (\mathbb{Z}_n, +)$ has a Slonimsky sequence with the last term $(n-1)/2$.*

Proof. Let $p_i = (-1)^i \lceil i/2 \rceil \mod n$ for $0 \le i \le n-1$. Then, for $1 \le i \le n-1$, we have

$$h_i = (-1)^{i-1}(p_{i-1} - p_i) = (-1)^{i-1}\left((-1)^{i-1}\lceil (i-1)/2 \rceil - (-1)^i \lceil i/2 \rceil\right)$$
$$= \lceil (i-1)/2 \rceil + \lceil i/2 \rceil = i,$$

hence property (i) in Definition 1.3 holds. Moreover, $h_i + h_{n-i} = i + n - i = 0$ (mod n) and $p_i + p_{n-i-1} = (-1)^i \lceil i/2 \rceil + (-1)^{n-i-1} \lceil (n-i-1)/2 \rceil = (n-1)/2$ whether i is even or odd. It follows that $p_0, \ldots, p_{n-1}$ is a Slonimsky sequence. $\square$

Theorem 2.2. *Let $G = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_d}$ be an odd abelian group. Then there exists a Slonimsky sequence in G with the last term*

$$((m_1 - 1)/2, \ldots, (m_d - 1)/2).$$

Proof. Proof is by induction on d. The claim for $d = 1$ follows from Lemma 2.1. For $d > 1$, let $H = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_{d-1}}$ and $m_d = m = 2l - 1$. By the inductive hypothesis for H, there exists a Slonimsky sequence $p_0, \ldots, p_{n-1}$ in H with signed differences $h_0, \ldots, h_{n-1}$ such that

$$h_i + h_{n-i} = 0, \ \forall i \in \{1, \ldots, n-1\}; \tag{2}$$
$$p_i + p_{n-i-1} = ((m_1 - 1)/2, \ldots, (m_{d-1} - 1)/2), \ \forall i \in \{0, \ldots, n-1\}. \tag{3}$$

In order to define the Slonimsky sequence $P_0, \ldots, P_{mn-1}$ in $G = H \times \mathbb{Z}_m$, we first define its sequence of signed differences g_i, $1 \le i \le mn$, in G as follows. For $1 \le i \le mn$, write $i = qn + r$, where $0 \le q \le m - 1$ and $0 \le r \le n - 1$. If $r = 0$, we let $g_i = (0_H, q) \in H \times \mathbb{Z}_m$, and if $0 < r \le m - 1$, we let

$$g_i = \left(h_r, (-1)^q l + 2\lceil q/2 \rceil\right).$$

We first show that $g_0, \ldots, g_{mn-1}$ is a permutation of elements of G. Suppose $g_i = g_j$, where $i = qn + r$ and $j = pn + t$. If $r = 0$, then $g_j = g_i = (0_H, q)$

which implies that $t = 0$, hence $g_j = (0_H, p)$, and so $p = q \Rightarrow i = j$. Thus, suppose that $r, t \neq 0$. It follows from $g_i = g_j$ that $h_r = h_t$, and so $r = t$. It also follows from $g_i = g_j$ that $(-1)^q l + 2\lceil q/2 \rceil = (-1)^p l + 2\lceil p/2 \rceil$. If $p - q$ is odd, we conclude that $|2\lceil q/2 \rceil - 2\lceil p/2 \rceil| = 2l$, which is a contradiction, since $2\lceil p/2 \rceil, 2\lceil q/2 \rceil \in \{0, 2, \ldots, 2l - 2\}$. If $p - q$ is even, we conclude that $2\lceil q/2 \rceil = 2\lceil p/2 \rceil$, which implies that $p = q \Rightarrow i = j$. Therefore, $g_0, \ldots, g_{mn-1}$ is a permutation of elements of G.

Next, we define $P_i = \sum_{k=0}^{i} (-1)^k g_k$ and show that $P_0, \ldots, P_{mn-1}$ is a Slonimsky sequence in G. A simple induction shows that for $i = qn + r$ with $0 \leq q \leq m - 1$ and $0 \leq r \leq n - 1$, we have

$$
P_i = \begin{cases}
(p_r, q/2) & \text{if } q \text{ is even and } r \text{ is even;} \\
(p_r, -l - q/2) & \text{if } q \text{ is even and } r \text{ is odd;} \\
(p_{n-r-1}, -(q+1)/2) & \text{if } q \text{ is odd and } r \text{ is even;} \\
(p_{n-r-1}, -l + (q+1)/2) & \text{if } q \text{ is odd and } r \text{ is odd.}
\end{cases}
$$

We need to show that $P_0, \ldots, P_{mn-1}$ is a permutation of elements of G. Suppose that $P_i = P_j$ for $i = qn + r$ and $j = pn + t$. If r, t are both even or both odd, from $P_i = P_j$, we conclude that $p = q$. Thus, without loss of generality, suppose that p is even and q is odd. Then $p_t = p_{n-r-1}$ and so $t = n - r - 1$ which implies that t and r are both even or both odd. If they are both odd, then $p/2 = -l + (q+1)/2$ modulo m, and if they are both even, then $-l - p/2 = -(q+1)/2$ modulo m. In either case we gave $p/2 - (q+1)/2 = -l \pmod{m}$, which is a contradiction since $1 - l \leq p/2 - (q+1)/2 \leq l - 2$.

Next, we show that $g_i + g_{mn-i} = 0$ for all $1 \leq i \leq mn - 1$. Let $i = qn + r$, where $0 \leq q \leq n - 1$ and $0 \leq r \leq m - 1$. So we can write $mn - i = (m - q - 1)n + n - r$. Suppose $r \neq 0$. Then

$$
g_i + g_{mn-i} = (h_r, (-1)^q l + 2\lceil q/2 \rceil) + \left(h_{n-r}, (-1)^{m-q-1} l + 2\lceil (m-q-1)/2 \rceil \right).
$$

Since $h_r + h_{n-r} = 0$ and $m - 1$ is even, this simplifies to

$$
g_i + g_{mn-i} = (0, (-1)^q 2l + 2\lceil q/2 \rceil + 2\lceil (-q/2) \rceil - 1) = (0, 0) \in H \times \mathbb{Z}_m.
$$

If $r = 0$, then $g_i = (0, q)$ and one writes $mn - i = (m - q)n$. Therefore, $g_{mn-i} = (0, m - q)$ which again leads to $g_i + g_{mn-i} = (0, 0)$.

Finally, we claim that $P_i + P_{mn-i-1} = ((m_1 - 1)/2, \ldots, (m_d - 1)/2)$ for all $i \in \{0, \ldots, mn - 1\}$. We have $p_r + p_{m-r-1} = ((m_1 - 1)/2, \ldots, (m_{d-1} - 1)/2)$ for all $r = 0, \ldots, m - 1$ by the inductive hypothesis. Let $i = qn + r$, and so

$mn - i - 1 = (m - q - 1)n + n - r - 1$. If q is even and r is odd, then

$$P_i + P_{mn-i-1} = (p_r + p_{n-r-1}, (m-1)/2)$$
$$= ((m_1 - 1)/2, \ldots, (m_{d-1} - 1)/2, (m-1)/2).$$

The claim in other cases follows similarly. □

3. Central extensions

In this section, we describe a construction of DDP sequences via group extensions. Let G be a group extension of H by N i.e., suppose that $1 \to N \to G \xrightarrow{\pi} H \to 1$ is a short exact sequence. We will describe an algorithm to *lift* a DDP sequence in H to G. By a lift of the DDP sequence $h_1, \ldots, h_{|H|}$ in H to G, we mean a DDP sequence $g_1, \ldots, g_{|G|}$ such that $\pi(g_i) = h_i$ for $i = 1, \ldots, |H|$.

It turns out that in order for our algorithm of lifting a DDP sequence from H to G work, the group $N = \ker(\pi)$ must contain no *real* elements of G except the identity.

Definition 3.1. An element $h \in G$ is said to be a *real* element of G if there exists $g \in G$ such that $g^{-1}hg = h^{-1}$. We denote the set of real elements of G by $\mathcal{R}(G)$.

Let N be a normal subgroup of G. If the only real element of G in N is 1_G i.e., $N \cap \mathcal{R}(G) = \{1_G\}$, then

$$\forall h \in N \backslash \{1_G\} \ \forall g \in G : hgh \neq g, \tag{4}$$

or equivalently, for abelian N,

$$\forall g \in G \ \forall h_1, h_2 \in N : h_1 \neq h_2 \Rightarrow h_1 g h_1 \neq h_2 g h_2.$$

If N is contained in the center of G, then the condition $N \cap \mathcal{R}(G) = \{1_G\}$ is equivalent to N having odd order.

Theorem 3.2. *Let $\pi : G \to H$ be an epimorphism such that $\ker(\pi)$ is an abelian group of odd order m with $\ker(\pi) \cap \mathcal{R}(G) = \{1_G\}$. If H is an even DDP group, then G is an even DDP group. More precisely, let $p_0, \ldots, p_{n-1}$ be a DDP sequence in H. Then there exist at least $(2m)^{(n-1-e)/2}$ DDP sequences $P_0, \ldots, P_{mn-1}$ in G such that $\pi(P_i) = p_i$ for all $i = 0, \ldots, n-1$, where e is the number of elements of order 2 in H. In particular*

$$|\mathcal{O}_G| \geq |\mathcal{O}_H| \times (2m)^{(n-1-e)/2}.$$

Proof. Let $p_0, \ldots, p_{n-1}$ be a DDP sequence in H. We define $h_0 = 1_H$ and $h_r = p_{r-1}^{-1} p_r$ for $1 \leq r \leq n - 1$. We define a bijection $\sigma : \{0, \ldots, n-1\} \to \{0, \ldots, n-1\}$

by letting $\sigma(r)$ to be the unique number in $\{0, \ldots, n-1\}$ such that $h_{\sigma(r)} = h_r^{-1}$. Let

$$I = \{0 \leq r \leq n-1 : \sigma(r) = r\},$$

and let A be a set obtained by including exactly one of r or $\sigma(r)$ for every $r \in \{0, \ldots, n-1\} \backslash I$, and define $B = \{0, \ldots, n-1\} \backslash (A \cup I)$. Clearly, $0 \in I$ and there are $2^{(n-|I|)/2}$ choices for A.

Let also $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$ be a Slonimsky sequence in $N = \ker(\pi)$; such a special DDP sequence exists by Theorem 2.2, since N has odd order. Let $\beta_0, \ldots, \beta_{m-1}$ be the sequence of signed differences. Let us denote the element α_{m-1} by y_N. By the definition of Slonimsky sequence, one has

$$\alpha_i \alpha_{m-1-i} = y_N = \alpha_{m-1}, \ \forall i \in \{0, \ldots, m-1\}, \tag{5}$$

$$\beta_i \beta_{m-i} = 1_N, \ \forall i \in \{1, \ldots, m-1\}, \tag{6}$$

where 1_N denotes the identity element of N. In order to define the sequence $P_0, \ldots, P_{mn-1}$, we first define its sequence of consecutive differences $g_0, \ldots, g_{mn-1}$ as follows. For each $r \in A$, we let g_r be an arbitrary element of $\pi^{-1}(h_r)$. For $r \in B$, by our choice of A and I, there exists a unique $s \in A$ such that $r = \sigma(s)$; then, we let

$$g_r = g_{\sigma(s)} = \begin{cases} g_s^{-1} & \text{if } s + \sigma(s) \text{ is odd}; \\ y_N g_s^{-1} y_N & \text{if } s \text{ and } \sigma(s) \text{ are both odd}; \\ y_N^{-1} g_s^{-1} y_N^{-1} & \text{if } s \text{ and } \sigma(s) \text{ are both even}. \end{cases} \tag{7}$$

To define g_r for $r \in I$, choose $f_r \in \pi^{-1}(h_r)$ to be arbitrary. Then one can show that

$$\pi^{-1}(h_r) = \{\alpha_i f_r \alpha_i \mid i \in \{1, \ldots, m\} \text{ and } \alpha_i \in N\},$$

and hence there exists $v_r \in N$ such that $f_r^{-1} = v_r f_r v_r$, since $\pi(f_r^{-1}) = h_r = \pi(f_r)$. Then, choose $w_r \in N$ such that $w_r^2 = v_r y_N^{(-1)^{r+1}}$, and let $g_r = w_r f_r w_r$. It follows from this definition that

$$g_r^{-1} = \begin{cases} y_N g_r y_N & \text{if } r \in I \text{ is even}; \\ y_N^{-1} g_r y_N^{-1} & \text{if } r \in I \text{ is odd}. \end{cases}$$

Next, we define g_i for all $n \leq i \leq mn-1$. The idea is to present $g_0, \ldots, g_{mn-1}$ as a union of m blocks each containing n elements so that π maps each block onto H, alternating in increasing (for even blocks) or decreasing (for odd blocks) order of indices. To be more precise, by the Euclidean algorithm, there exist unique integers

$0 \le r \le n - 1$ and $0 \le q \le m - 1$ such that $i = nq + r$. If $r = 0$, let $g_i = \beta_q$. If $r \ge 1$, let

$$
g_i = \begin{cases}
\alpha_q g_{n-r}^{-1} \alpha_q & \text{if } q \text{ is odd and } r \text{ is odd;} \\
\alpha_q^{-1} g_{n-r}^{-1} \alpha_q^{-1} & \text{if } q \text{ is odd and } r \text{ is even;} \\
\alpha_q^{-1} g_r \alpha_q^{-1} & \text{if } q \text{ is even and } r \text{ is odd;} \\
\alpha_q g_r \alpha_q & \text{if } q \text{ is even and } r \text{ is even.}
\end{cases} \tag{8}
$$

We claim that the sequence $P_i = \prod_{k=0}^{i} g_k$, $0 \le i \le mn - 1$, is a DDP sequence. We prove by induction on $0 \le i \le mn - 1$ that for $i = nq + r$, we have

$$
P_i = \begin{cases}
P_{n-r-1}\alpha_q & \text{if } q \text{ is odd and } r \text{ is odd;} \\
P_{n-r-1}\alpha_q^{-1} & \text{if } q \text{ is odd and } r \text{ is even;} \\
P_r \alpha_q^{-1} & \text{if } q \text{ is even and } r \text{ is odd;} \\
P_r \alpha_q & \text{if } q \text{ is even and } r \text{ is even.}
\end{cases} \tag{9}
$$

The claim is clearly true for all $0 \le i \le n - 1$. Suppose the claim is true for $i = nq + r$. Suppose that q and r are both odd. The proof in all other cases is similar. If $r = n - 1$ then

$$P_{i+1} = P_i g_{i+1} = (P_0 \alpha_q)\beta_{q+1} = P_0 \alpha_{q+1}$$

as claimed. If $0 \le r < n - 1$. Then $i + 1 = nq + (r + 1)$ and we have

$$P_{i+1} = P_i g_{i+1} = (P_{n-r-1}\alpha_q)(\alpha_q^{-1} g_{n-r-1}^{-1} \alpha_q^{-1}) = P_{n-r-2}\alpha_q^{-1}$$

as claimed. It follows from (9) that $P_i \ne P_j$ for $0 \le i < j \le mn - 1$. To see this, suppose $P_i = P_j$ for $i = nq_1 + r_1$ and $j = nq_2 + r_2$. Suppose that q_1 and q_2 are even. The proof in other cases is similar. Then $p_{r_1} = \pi(P_i) = \pi(P_j) = p_{r_2}$ which implies that $r_1 = r_2 = r$. But then $\alpha_{q_1} = (P_r^{-1}P_i)^{\pm 1} = (P_r^{-1}P_j)^{\pm 1} = \alpha_{q_2}$, and so $q_1 = q_2$, hence $i = j$.

Next, we show that $g_i \ne g_j$ for all $0 \le i < j \le mn - 1$. On the contrary, suppose that $g_i = g_j$ for $i = qn + r$ and $j = pn + s$ where $1 \le r, s < n$. There are two cases:

Case 1. $p \equiv q \pmod 2$. If p, q are both even, then $h_r = \pi(g_i) = \pi(g_j) = h_s$, and if p, q are both odd, then $h_{n-r} = \pi(g_i)^{-1} = \pi(g_j)^{-1} = h_{n-s}$. In either case, we conclude that $r = s$. If r is even, this implies that $\alpha_p g_r \alpha_p = \alpha_q g_r \alpha_q$ (if p, q are even) or $\alpha_q^{-1} g_{n-r}^{-1} \alpha_q^{-1} = \alpha_p^{-1} g_{n-r}^{-1} \alpha_p^{-1}$ (if p, q are odd). In either case, since $N \cap \mathcal{R}(G) = \{1_G\}$, we must have $p = q$, and so $i = j$.

Case 2. Without loss of generality, suppose q is even and p is odd. Then $\alpha_q^{\pm 1} g_r \alpha_q^{\pm 1} = \alpha_p^{\pm 1} g_{n-s}^{-1} \alpha_p^{\pm 1}$. By projecting onto H via π, we must have $h_r = h_{n-s}^{-1}$. If $r = n - s \in I$, then r and s are both even or both odd. If they are both even,

it follows from $g_i = g_j$ that $\alpha_q g_r \alpha_q = \alpha_p^{-1} g_r^{-1} \alpha_p^{-1}$ which implies that $\alpha_p \alpha_q = y_N$, which is a contradiction, since p and q have different parity. If r and s are both odd, then $\alpha_q^{-1} g_r \alpha_q^{-1} = \alpha_p g_r^{-1} \alpha_p$ which leads to the same contradiction.

Thus, suppose $r \in A \cup B$. Without loss of generality, suppose $r \in A$, and so $n - s = \sigma(r) \in B$. If both r and s are odd, according to Eq. (7) we have $\alpha_q^{-1} g_r \alpha_q^{-1} = \alpha_p g_{\sigma(r)}^{-1} \alpha_p = \alpha_p y_N^{-1} g_r y_N^{-1} \alpha_p$, which implies $\alpha_p \alpha_q = y_N$, a contradiction. Similarly, if r and s are both even, we have $\alpha_q g_r \alpha_q = \alpha_p^{-1} g_{\sigma(r)}^{-1} \alpha_p^{-1} = \alpha_p^{-1} y_N g_r y_N \alpha_p^{-1}$, which again implies $\alpha_p \alpha_q = y_N$, a contradiction. If r is odd and $\sigma(r)$ is even, then $\alpha_q^{-1} g_r \alpha_q^{-1} = \alpha_p^{-1} g_{\sigma(r)}^{-1} \alpha_p^{-1} = \alpha_p^{-1} g_r \alpha_p^{-1}$ which implies that $\alpha_p = \alpha_q$, a contradiction. Finally, if r is even and $\sigma(r)$ is odd, then $\alpha_q g_r \alpha_q = \alpha_p g_{\sigma(r)}^{-1} \alpha_p = \alpha_p g_r \alpha_p$ which implies that $\alpha_q = \alpha_p$, a contradiction.

We have shown that $P_0, \ldots, P_{mn-1}$ is a DDP sequence in G with $\pi(P_i) = p_i$ for all $0 \le i \le n - 1$. Recall that in constructing the set A, we have two choices per each pair $(r, \sigma(r))$. Moreover, for each $r \in A$, we have m choices in defining g_r. It follows that there are at least $(2m)^{|A|} = (2m)^{(n-|I|)/2}$ DDP sequences which are lifts of a given DDP sequence in H. Since I is comprised of 1_H and elements of order 2, each DDP sequence in H has at least $(2m)^{(n-e-1)/2}$ lifts to G, where e is the number of elements of order 2 in H. $\qquad\square$

Corollary 3.3. *Every central extension of an even DDP group by an odd abelian group is a DDP group.*

Proof. Let N be an odd abelian group and H be an even DDP group. Suppose that $\pi : G \to H$ is an epimorphism with $\ker(\pi) \cong N$. We need to show that G is a DDP group. Since $\ker(\pi)$ is an odd abelian group and, by the definition of central extension, the normal subgroup $\ker(\pi)$ lies in the center of G, one has $\ker(\pi) \cap \mathcal{R}_G = \{1_G\}$, the conditions of Theorem 3.2 hold, hence G is an even DDP group. $\qquad\square$

Theorem 3.4. *Let G be a finite odd nilpotent group and K be an even DDP group. Then $G \times K$ is a DDP group.*

Proof. Let $Z_0 \lhd Z_1 \lhd \cdots \lhd Z_n = G$ be the upper central series of G. We prove by a finite reverse induction on $0 \le i \le n$ that $(G/Z_i) \times K$ is a DDP group. The claim is clearly true for $i = n$. Suppose we have proved that $(G/Z_{i+1}) \times K$ is DDP for $0 \le i < n$ and we show that $(G/Z_i) \times K$ is DDP. Consider the epimorphism

$$\pi_i : \frac{G}{Z_i} \times K \to \frac{G}{Z_{i+1}} \times K, \ \pi_i(g + Z_i, \ k) := (g + Z_{i+1}, \ k)$$

induced by the inclusion $Z_i \hookrightarrow Z_{i+1}$. By the inductive hypothesis $G/(Z_{i+1}) \times K$ is DDP. Moreover, $\ker(\pi_i) \cong (Z_{i+1}/Z_i) \times \{1_K\}$ which is contained in the center of

$G/Z_i \times K$. It then follows from Corollary 3.3 that $(G/Z_i) \times K$ is DDP. When $i = 0$, we conclude that $G \times K$ is DDP. $\qquad\square$

4. The abelian case

In this section, we determine all finite abelian DDP groups. We begin with describing an obstruction to the existence of a DDP sequence in the abelian case. For an abelian group G, we use 0_G (or simply 0) to denote its identity element.

Lemma 4.1. *If G is an abelian DDP group, then it has a unique element of order 2.*

Proof. Let $x_1, \ldots, x_k$ be a DDP sequence in G. Then we have

$$-x_1 + x_k = \sum_{i=1}^{k-1}(-x_i + x_{i+1}) = \sum_{g \in G} g. \qquad (10)$$

Now let us assume to the contrary that either G has odd order or it has more than one element of order 2. Firstly, if G has odd order, we have $2\sum_{g \in G} g = \sum_{g \in G} g + \sum_{g \in G}(-g) = 0_G$, and (10) implies that $x_k = x_1$, which is not allowed. Secondly, if G has more than one element of order 2, then one can write $G = \mathbb{Z}_m \times \mathbb{Z}_n \times H$ for even integers m, n, and an abelian group H. But then

$$\sum_{g \in G} g = \left(mn|H|/2, mn|H|/2, mn\sum_{h \in H} h \right) = (0_{\mathbb{Z}_m}, 0_{\mathbb{Z}_n}, 0_H) = 0_G \in G,$$

since $\sum_{i \in \mathbb{Z}_n} i = n(n-1)/2 = n/2$ modulo n and $2\sum_{h \in H} h = 0_H$. Now it follows again from (10) that

$$-x_1 + x_k = 0_G,$$

which contradicts the assumption that $x_1, \ldots, x_k$ are distinct. $\qquad\square$

In the next lemma we consider the group $(\mathbb{Z}_n, +)$ where $n = 2^m$.

Lemma 4.2. *Let $n = 2^m$, where m is a positive natural number. Then the following statements hold.*

    a) *The sequence $x_i = i(i+1)/2$, $0 \le i \le n-1$, is a DDP sequence modulo n for all $m \ge 1$.*

    b) *The sequence*

$$y_i = \begin{cases} i(i+1)/2 & \text{if } 0 \le i < 2^{m-2} \text{ or } 3 \cdot 2^{m-2} \le i < 2^m, \\ i(i+1)/2 + 2^{m-1} & \text{if } 2^{m-2} \le i < 3 \cdot 2^{m-2}, \end{cases}$$

    is a DDP sequence modulo n for all $m \ge 2$.

Proof. Since $x_{i+1} - x_i = i+1$, part (a) is equivalent to the claim that $i \mapsto i(i+1)/2$ is a bijection on $\mathbb{Z}_n$. If $n = 2^m$, then the map $i \mapsto i(i+1)/2$ is a one-to-one map modulo n. To see this, suppose $i(i+1)/2 \equiv j(j+1)/2 \pmod{2^m}$ for $0 \le i < j < 2^m$, and we derive a contradiction. It follows that $i(i+1) \equiv j(j+1) \pmod{2^{m+1}}$, and so $(j-i)(i+j+1) \equiv 0 \pmod{2^{m+1}}$. If $j-i$ is odd, then $i+j+1 \equiv 0 \pmod{2^{m+1}}$, a contradiction with $i+j < 2^{m+1}$. On the other hand, if $j-i$ is even, then $i+j+1$ is odd, and so $j-i \equiv 0 \pmod{2^{m+1}}$, a contradiction with $0 < j-i < 2^m$. It follows that $i \mapsto i(i+1)/2$ is one-to-one, hence a bijection, on $\mathbb{Z}_n$.

For part (b), one verifies that the sequence of consecutive differences of $y_0, \dots, y_{n-1}$ is given by

$$0, 1, 2, \dots, 2^{m-2}-1, 3 \cdot 2^{m-2}, 2^{m-2}+1, \dots, 3 \cdot 2^{m-2}-1, 2^{m-2}, 3 \cdot 2^{m-2}+1, \dots, 2^m-1,$$

which is obtained from the sequence $0, 1, \dots, 2^m - 1$ by exchanging 2^{m-2} and the product $3 \cdot 2^{m-2}$, hence $y_0, \dots, y_{n-1}$ is a DDP sequence. $\qquad\square$

Corollary 4.3. *If $n = 2^m$, $m \ge 3$, then $|\mathcal{O}_{\mathbb{Z}_n}| \ge n$.*

Proof. For $m \ge 3$, the two DDP sequences in Lemma 4.2 are distinct. Moreover, $rx_0, \dots, rx_{n-1}$, and $ry_0, \dots, ry_{n-1}$, are DDP sequences for every odd number $r \in \mathbb{Z}_n$, and the corollary follows. $\qquad\square$

Theorem 4.4. *Let G be an abelian group. Then G is a DDP group if and only if G has exactly one element of order 2.*

Proof. In light of Lemma 4.1, it is left to show that if $G = H \times \mathbb{Z}_{2^m}$, where $m \ge 1$ and H is an odd abelian group, then G is DDP. Since H is an odd nilpotent group and $\mathbb{Z}_{2^m}$ is an even DDP group by Lemma 4.2, the claim follows from Theorem 3.4. $\qquad\square$

Corollary 4.5. *Let $c_1 = 1$, $c_2 = 2$, and $c_m = 2^m$ for $m \ge 3$. If $G = \mathbb{Z}_{2^m} \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ where $n_1, \dots, n_k$ are odd integers and $m \ge 1$, then*

$$|\mathcal{O}_G| \ge c_m \times (2n_1)^{2^{m-1}-1} \times (2n_2)^{2^{m-1}n_1-1} \cdots (2n_k)^{2^{m-1}n_1 \cdots n_{k-1}-1}.$$

In particular, if an abelian group G has size $2^m kl$, where $m \ge 1$ and k, l are relatively prime odd integers, then $|\mathcal{O}_G| \ge (2k)^{l-1}$.

Proof. Proof is by induction on k. If $k = 0$, the claim follows from Lemma 4.2. For the inductive step, let $G = \mathbb{Z}_{n_{k+1}} \times H$, where by the inductive hypothesis

$$|\mathcal{O}_H| \ge c_m \times (2n_1)^{2^{m-1}-1} \times (2n_2)^{2^{m-1}n_1-1} \cdots (2n_k)^{2^{m-1}n_1 \cdots n_{k-1}-1}.$$

By Theorem 3.2, we have

$$|\mathcal{O}_G| \geq (2n_{k+1})^{(|H|-1-e)/2}|\mathcal{O}_H|,$$

where e is the number of elements of order 2. It follows from $G = \mathbb{Z}_{2^m} \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ that one has $e = 1$, and the claim follows. The last claim of the Corollary 4.5 follows from $G \cong \mathbb{Z}_{2^m} \times \mathbb{Z}_k \times \mathbb{Z}_l$. $\qquad\square$

5. The non abelian case

Computer searches show that the smallest non abelian DDP group is the dihedral group D_5, which has 320 DDP sequences. If we present D_5 in terms of generators and relations as

$$D_5 \cong \langle a, b \mid a^5 = b^2 = 1, \ aba = b \rangle,$$

an example of a DDP sequence in D_5 is

$$1, a, a^3, ba^3, a^2, b, a^4, ba^4, ba^2, ba,$$

with the corresponding sequence of distinct divisors

$$1, a, a^2, ba, b, ba^2, ba^4, ba^3, a^3, a^4.$$

The group D_6 has 3072 DDP sequences, and the alternating group on four elements A_4 has 2304 DDP sequences.

Computer searches also confirm that D_7 is a DDP group, and we conjecture that D_n is a DDP group for all $n \geq 5$. As we noted in Lemma 4.1, an abelian group of odd order is not DDP. However, the next example shows that in the non abelian case, DDP groups of odd order do exist.

Example 5.1. Let $G = \mathbb{Z}_7 \rtimes \mathbb{Z}_3$ be the non abelian group of order 21. G is the smallest non abelian group of odd order. In generators and relations, G is given by

$$G \cong \langle a, b \mid a^7 = b^3 = 1, \ a^2 b = ba \rangle.$$

The following sequence is a DDP sequence in G:

$$1, a, ba^6, ba^2, a^3, a^5, b, b^2 a^4, ba^4, b^2 a^2, ba^5, ba^3, a^6, b^2 a^3, ba, b^2, b^2 a^6, a^2, b^2 a, b^2 a^5, a^4,$$

where the sequence of distinct divisors is given by

$$1, a, ba^2, a^3, b^2 a^6, a^2, ba, ba^4, b^2 a^3, b, b^2 a, a^5, b^2, b^2 a^5, b^2 a^2, ba^3, a^6, ba^6, b^2 a^4, a^4, ba^5.$$

The next lemma provides a construction of DDP groups via semidirect products. Consider for example the semidirect product $G = \mathbb{Z}_9 \rtimes_\phi \mathbb{Z}_6$, where $\phi : \mathbb{Z}_6 \to Aut(\mathbb{Z}_9)$ is defined by

$$\phi_t(j) := \begin{cases} j & \text{if } t \equiv 0 \pmod 3; \\ 4j & \text{if } t \equiv 1 \pmod 3; \\ 7j & \text{if } t \equiv 2 \pmod 3. \end{cases}$$

Then G is a DDP group by the following lemma.

Lemma 5.2. *Let $\phi : \mathbb{Z}_n \to Aut(\mathbb{Z}_m)$ be a group homomorphism such that $1 + \phi_s(1)$ is a generator of $\mathbb{Z}_m$ for all $s \in \mathbb{Z}_n$. If m is odd and n is even, then $\mathbb{Z}_m \rtimes_\phi \mathbb{Z}_n$ is a DDP group.*

Proof. Consider the projection $\pi : \mathbb{Z}_m \rtimes_\phi \mathbb{Z}_n \to \mathbb{Z}_n$ with $\ker(\pi) = \mathbb{Z}_m \times \{0\}$. The claim follows from Theorem 3.2 if we show that $\alpha g \alpha = g \Rightarrow \alpha = 0$ for all $\alpha \in \mathbb{Z}_m \times \{0\}$ and $g \in \mathbb{Z}_m \rtimes_\phi \mathbb{Z}_n$. Let $g = (r, s)$ and $\alpha = (k, 0)$. Then

$$\alpha g \alpha = (k, 0)(r, s)(k, 0) = (r + k + \phi_s(k), s) \neq (r, s),$$

since $k + \phi_s(k) \neq 0$ for all $k \neq 0$; otherwise, $k(1 + \phi_s(1)) = 0$ which contradicts the assumption. $\square$

Finally, we show that there exist infinitely many non abelian DDP groups.

Theorem 5.3. *Let p be a prime with $p \equiv 3 \pmod 4$ and let t be a primitive root modulo p. Then $\mathbb{Z}_p \rtimes_\phi \mathbb{Z}_{p-1}$ is a DDP group, where $\phi : \mathbb{Z}_{p-1} \to Aut(\mathbb{Z}_p)$ is given by $\phi_s(x) = t^{2s}x$. In particular, there exist infinitely many non abelian DDP groups.*

Proof. We first show that t^{2s} is not congruent to -1 modulo p for every $s \in \mathbb{Z}_{p-1}$. If on the contrary, $t^{2s} \equiv -1 \pmod p$, we have $4s \equiv 0 \pmod{p-1}$, which implies that $2s \equiv 0 \pmod{p-1}$ since $p \equiv 3 \pmod 4$. But then $t^{2s} \equiv 1 \pmod p$, which is a contradiction. It follows that $1 + \phi_s(1) \neq 0$ for all $s \in \mathbb{Z}_{p-1}$, and the claim follows from Lemma 5.2. $\square$

References

[1] L. M. Batten and S. Sane, *Permutations with a distinct difference property*, Discrete Math., 261 (2003), 59-67.

[2] S. Bauer-Mengelberg and M. Ferentz, *On eleven-interval twelve-tone rows*, Perspectives of New Music, 3 (1965), 93-103.

[3] J. P. Costas, *A study of a class of detection waveforms having nearly ideal range-Doppler ambiguity properties*, Proceedings of the IEEE, 72 (1984), 996-1009.

[4] J. P. Costas, Medium Constraints on Sonar Design and Performance, Tech. Rep. Class 1 Rep. R65EMH33, General Electric Company, Fairfield, CT, USA, 1965.

[5] K. Drakakis, F. Iorio, S. Rickard and J. Walsh, *Results of the enumeration of Costas arrays of order 29*, Adv. Math. Commun., 5 (2011), 547-553.

[6] H. Eimert, Lehrbuch der Zwölftontechnik, Weisbaden, Breitkopf und Härtel, 1952.

[7] E. N. Gilbert, *Latin squares which contain no repeated diagrams*, SIAM R., 7(2) (1965), 189-198.

[8] S. W. Golomb, *Algebraic constructions for Costas arrays*, J. Combin. Theory Ser. A, 37 (1984), 13-21.

[9] S. W. Golomb, *Construction of signals with favourable correlation properties*, in: A. Pott et al. (Eds.), Difference Sets, Sequences and their Correlation Properties, Kluwer, Dordrecht, 1999, 159-194.

[10] S. W. Golomb and H. Taylor, *Constructions and properties of Costas arrays*, Proceedings of the IEEE, 72(9) (1984), 1143-1163.

[11] M. Gustar, Number of Difference Sets for Permutations of $[2n]$ with Distinct Differences, The on-line encyclopedia of integer sequences, https://oeis.org/A141599, 2008.

[12] F. H. Klein, *Die Grenze der Halbtonwelt*, Die Musik, 17 (1925), 281-286.

[13] N. Slonimsky, Thesaurus of Scales and Melodic Patterns, Amsco Publications, 8th edition, New York, 1975.

Mohammad Javaheri (Corresponding Author) and **Nikolai A. Krylov**

515 Loudon Road

School of Science

Siena College

Loudonville, NY 12211, USA

e-mails: mjavaheri@siena.edu (M. Javaheri)

      nkrylov@siena.edu (N. A. Krylov)