A SURVEY OF SEQUENCEABLE GROUPS AND THEIR APPLICATIONS

by

Lai So

B.Sc., Simon Fraser University, 1978

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in the Department

of

Mathematics

SIMON FRASER UNIVERSITY

February 1983

APPROVAL

Name: Lai So

Degree: Master of Science

Title of Thesis: A Survey of Sequenceable Groups and Their Applications

Examining Committee:

Chairman: B.S. Thomson

B.R. Alspach
Senior Supervisor

H. Gerber
Examining Committee

D. Ryeburn
Examining Committee

K. Heinrich

External Examiner

Date Approved: December 17, 1982

Title of Thesis/Dissertation:

A SURVEY OF SEQUENCEABLE GROUPS
AND THEIR APPLICATIONS

Author:
(signature)

LAI SO
(name)

April 6, 1983
(date)

ABSTRACT

A finite group G of order n is called a sequenceable group if all its elements can be arranged into a sequence $a_1, a_2, \ldots, a_n$ such that the partial products $a_1, a_1a_2, \ldots$ $\ldots, a_1a_2\ldots a_n$ are all distinct.

In Chapter one, we give some sufficient and necessary conditions of the sequenceable group. In Chapter two, a complete characterization of sequenceable abelian groups is given. Though the problem of determining which non-abelian groups G are sequenceable is unsolved at the present time, we know that there are infinitely many non-abelian sequenceable groups. This is discussed in Chapter three. In Chapter four, the definition of sequenceable is extended to symmetric and strong symmetric sequenceable groups. In the last chapter, we give some applications of sequenceable groups to Latin squares, Howell designs and Graph theory.

ACKNOWLEDGEMENTS

I would like to acknowledge the aid and guidance from Dr. B. Alspach, and Dr. K. Heinrich for providing the materials. A special thanks goes to M. Chan for typing this thesis.

TABLE OF CONTENTS

Chapter 5 Page

Applications of sequenceable group

LIST OF FIGURES

Page

CHAPTER ONE

Introduction

A finite group G of order n which possesses the property that all its element can be arranged into a sequence $a_1, a_2, a_3, \ldots, a_n$ in such a way that its partial products $a_1, a_1a_2, a_1a_2a_3, \ldots, a_1a_2\ldots a_n$ are all distinct is called a sequenceable group.

Basil Gordon, who has investigated the problem of sequenceable groups, completely determined all the finite sequenceable abelian groups. However, for the non-abelian case, it is still not completely solved at the present time. At the very beginning mathematicians either used computer or trial and error to find the sequencings. Later they derived methods to construct sequencings. B.A. Anderson, Basil Gordon, J. Dénes, Richard Friedlander, A.D. Keedwell, N.S. Mendelsohn, E. Török and L.L. Wang, are the mathematicians who worked on the non-abelian case. Even though this problem is not completely solved, we at least know that there exists an infinite number of sequenceable non-abelian groups of odd order and even order.

If we add some restrictions to the sequencing of the sequenceable group, we will have sequencings which we call symmetric sequencings and strong symmetric sequencings.

There are some applications of sequenceable groups. We can use the sequencing to construct complete Latin squares, Hamiltonian decompositions of an n-complete graph, construction of Howell designs, etc.

Before we go to the next chapter, we give some necessary and sufficient conditions for a group to be sequenceable which were shown by J. Dénes and E. Török[7].

Theorem 1.1 : A finite group $(G,\cdot)$ is sequenceable if and only if there exists an arrangemenet of its element $a_1,a_2,...,a_n$ such that $a_1=e$(the identity of G) and for any integers i,j, $1\leq i\leq n-1$, $2\leq i+j\leq n$, $a_{i+1}...a_{i+j}\neq e$.

Proof : We define $b_r=a_1a_2...a_r$ for $1\leq r\leq n$. A group is sequenceable if and only if there exists a sequence $a_1,a_2,...,a_n$ such that $b_1,b_2,...,b_n$ are all different. The latter holds if and only if $b_i\neq b_{i+j}$ for $1\leq i\leq n-1$, $2\leq i+j\leq n$ which holds if and only if $b_i^{-1}b_{i+j}\neq e$ which in turn holds if and only if $a_{i+1}a_{i+2}...a_{i+j}\neq e$ for $1\leq i\leq n-1$, $2\leq i+j\leq n$. □

Theorem 1.2 : A finite group $(G,\cdot)$ is sequenceable if and only if there exists an arrangement of its elements $b_1,b_2,...,b_n$ such that $b_{i-1}^{-1}b_i=b_{j-1}^{-1}b_j$ implies $i=j$.

Proof : Suppose the group is sequenceable with a sequencing $a_1,a_2,...,a_n$. Define $b_r=a_1a_2...a_r$. Then $b_{i-1}^{-1}b_i=a_i$.

Since $a_i=a_j$ implies $i=j$, $b_{i-1}^{-1}b_i=b_{j-1}^{-1}b_j$ implies $i=j$.

Conversely, assume there exists an arrangement of its elements $b_1,b_2,\ldots,b_n$ such that $b_{i-1}^{-1}b_i=b_{j-1}^{-1}b_j$ implies $i=j$. Define

$$a_1 = e$$

$$a_2 = b_1^{-1}b_2$$

$$\vdots$$

$$a_i = b_{i-1}^{-1}b_i$$

$$\vdots$$

and

$$a_n = b_{n-1}^{-1}b_n.$$

Then the a_i's are all different and

$$a_1 = b_1^{-1}b_1 = e$$

$$a_1a_2 = b_1^{-1}b_1b_1^{-1}b_2 = b_1^{-1}b_2$$

$$a_1a_2a_3 = b_1^{-1}b_3$$

$$\vdots$$

$$a_1\ldots a_i = b_1^{-1}b_i$$

$$\vdots$$

and

$a_1 \ldots a_n = b_1^{-1} b_n$.

They are all different because $b_1, b_2, \ldots, b_n$ are different elements of G. Hence the arrangement $a_1, a_2, \ldots, a_n$ of the elements of G is a sequencing of G. □

Theorem 1.3 : Let G be a finite sequenceable group of order n and Φ be an automorphism of G. Then $a_1, a_2, \ldots, a_n$ is a sequencing of G if and only if $\Phi(a_1), \Phi(a_2), \ldots, \Phi(a_n)$ is a sequencing of G.

Proof : Note that if Φ is an automorphism of G, then Φ^{-1} also is an automorphism. Thus $a_1, a_2, \ldots, a_n$ is a sequencing if and only if $a_1, a_1a_2, \ldots, a_1a_2 \ldots a_n$ are all distinct which is true if and only if $\Phi(a_1), \Phi(a_1a_2), \ldots, \Phi(a_1a_2 \ldots a_n)$ are all distinct. This is true if and only if $\Phi(a_1), \Phi(a_1)\Phi(a_2), \ldots, \Phi(a_1)\Phi(a_2) \ldots \Phi(a_n)$ are all distinct and in turn if and only if $\Phi(a_1), \Phi(a_2), \ldots, \Phi(a_n)$ is a sequencing of G. □

Theorem 1.4 : Let $(G, \cdot)$ be a sequenceable group of order n having a normal subgroup H of order h. Let us represent the elements of the factor group G/H by $H_1, H_2, \ldots, H_k$, $k=n/h$, where H_1 represents the identity of G/H. Then there exists an arrangement $a_1', a_2', \ldots, a_n'$ of $H_1, H_2, \ldots, H_k$ such that

(i) $a_1' = H_1$,

(ii) H_i $(i=1,2,\ldots,k)$ appears exactly h times among the a_j' $(j=1,2,\ldots,n)$, and

(iii) H_i $(i=1,2,\ldots,k)$ appears exactly h times among the elements $a_1'a_2'\ldots a_j'$ $(j=1,2,\ldots,n)$.

Proof : Let $b_i=a_1\ldots a_i$, $1\le i\le n$, where $a_1,a_2,\ldots,a_n$ is a sequencing of G, and Φ be the natural homomorphism of G onto G/H defined by $\Phi(a)=aH$ for any $a\in G$. We know H_i are all mutually disjoint, $\bigcup_{i=1}^{n} H_i=G$ and $aH=H_i$ if $a\in H_i$. Therefore the sequence $a_1H=a_1', a_2H=a_2', \ldots, a_nH=a_n'$ consists of h H_i's for $1\le i\le k$. The sequence $b_1H, b_2H, \ldots, b_nH$ also consists of h H_i's for $1\le i\le k$. Thus the theorem is proved. □

In the following theorem, we let

$E_i = \{\{a_1,a_2,\ldots,a_i\}: a_ja_{j+1}\ldots a_i = e$ for some integer j $1\le j\le i$ and $a_ta_{t+1}\ldots a_k\ne e$ when $1\le t\le k<i\}$ where $a_i\in G\backslash\{e\}$ and e_i denote the number of the elements in E_i.

Theorem 1.5 : Let $(G,\cdot)$ be a group of order n with identity e. Then the group $(G,\cdot)$ is sequenceable if and only if $e_2(n-3)! + e_3(n-4)! + \ldots + e_{n-1}<(n-1)!$

Proof : Let us consider the set $G\backslash\{e\}$ and let us call an arrangement of its elements $a_1,a_2,\ldots,a_{n-1}$ wrong if there exists i,k such that $a_ia_{i+1}\ldots a_{i+k}=e$ for $1\le i\le n-2$, $2\le i+k\le n-1$.

The total number of all distinct arrangements of the set $G\backslash\{e\}=(n-1)!$. By Theorem 1.1, the group is sequenceable if and only if the number of wrong arrangements is less than $(n-1)!$.

Let $a_1,a_2,\ldots,a_i$ belong to E_i, this ordered arrangement can be completed into a permutation of all the elements of the set $G\backslash\{e\}$ in $(n-1-i)!$ different ways, and all these permutations are different wrong arrangements. Thus, this contributes $e_i(n-1-i)!$ wrong arrangements of the $n-1$ distinct elements of $G\backslash\{e\}$.

However, if $a_1,a_2,\ldots,a_{n-1}$ is a wrong arrangement, then there exists at least one pair of positive integers u,v $1\le u<v\le n-1$ such that $a_u a_{u+1}\ldots a_v=e$. Let us choose of all possible pairs the pair with the property that v is minimal, and denote this pair by $\bar{u},\bar{v}$. Then $a_1a_2\ldots a_{\bar{v}}\in E_{\bar{v}}$, and $a_1a_2\ldots a_{\bar{v}}\ldots a_m\notin E_m$ for $m>\bar{v}$ because $a_{\bar{u}}a_{\bar{u}+1}\ldots a_{\bar{v}}=e$. Since $\bar{v}$ is minimal, $a_1,a_2,\ldots,a_t\notin E_t$ for $t<\bar{v}$. Hence given any wrong arrangement $a_1,a_2,\ldots,a_{n-1}$, there exists exactly one positive integer v such that $a_1,a_2,\ldots,a_v\in E_v$. Then the total number of wrong arrangements is $e_2(n-3)!+e_3(n-4)!+\ldots$ $\ldots+e_{n-2}(1)!+e_{n-1}$. The proof is finished. □

By the last theorem, we can derive an algorithm to decide whether or not a group is sequenceable. A group is sequenceable if and only if its elements can be arranged so that

$$\begin{gathered} a_0 = e \\ a_1, a_2 \notin E_2 \\ a_1, a_2, a_3 \notin E_3 \\ \vdots \\ a_1, a_2, \dots, a_{n-1} \notin E_{n-1} \end{gathered}$$

where $a_0, a_1, \dots, a_n$ are all distinct.

Let $a_0, a_1, \dots, a_k$ be an arrangement of the group elements with the following properties:

$a_0 = e,$

$a_1 \neq e,$

$a_2 \neq e, a_1, a_1^{-1}$ such that $a_1, a_2 \notin E_2,$

$a_3 \neq e, a_1, a_2, (a_1 a_2)^{-1}, a_2^{-1}$ such that $a_1, a_2, a_3 \notin E_3,$

$\vdots$

$a_k \neq e, a_1, a_2, \dots, a_{k-1}, (a_1 a_2 \dots a_{k-1})^{-1}, (a_2 a_3 \dots a_{k-1})^{-1}, \dots$

$\dots, a_{k-1}^{-1}$ such that $a_1, a_2, \dots, a_k \notin E_k.$

This means that $E_i = \phi$, $1 \le i \le n-1$. The product $a_1 a_2 \dots a_k$ is called k-sequenceable if the elements $e, a_1, \dots, a_{k-1}, (a_1 a_2 \dots a_{k-1})^{-1}, \dots, a_{k-1}^{-1}$ exhaust all the elements of the group. We continue the procedure in the above way. If we can get an (n-1)-sequenceable product, then the group is sequenceable and the (n-1)-sequenceable product is the required sequencing.

CHAPTER TWO

Sequences in Abelian Groups with Distinct Partial Products

Sequenceable abelian groups have been completely characterized by Basil Gordon [9]. In this section, the necessary and sufficient conditions for an Abelian group to be sequenceable are given and proved in detail.

Before we state and prove B. Gordon's Theorem, we introduce the notion of a complete mapping of a finite group and then state and prove four lemmas which will simplify the proof of the main theorem of this section.

Definition 2.1 : A complete mapping of a finite group G is a one-one mapping θ of G onto G such that the mapping $\eta(g)=g\theta(g)$ is a one-one mapping of G onto G.

Lemma 2.1: If G is a group of odd order, then G has a complete mapping.

Proof : Suppose G is a group of odd order and let $g\in G$ be an element of order $2t-1$. If $h=g^t$, then $h^2=g^{2t}=g^{2t-1}g=g$. Therefore h is a square root of g. Further, if $k\in G$ and $k^2=g$, we have $(k^2)^{2t-1}=g^{2t-1}$ which implies $k^{4t-2}=e$, the identity element of G. Since the order of an element is a factor of the order of the group, the order of k

must be odd. Hence, we have $k^{2t-1}=e$ gives $k=k^{2t}=g^{t}=h$. Thus, h is the unique square root of g. It follows that in a group of odd order with elements $g_1, g_2, \ldots, g_n$, $g_i^2=g_j^2$ only if $i=j$. Define $\theta(g_i)=g_i$ for $i=1,2,\ldots,n$. We have $\eta(g_i)=g_i^2$ $(i=1,2,\ldots,n)$. Since $\eta(g_i)=\eta(g_j)$ implies $g_i^2=g_j^2$ which implies $g_i=g_j$, we have that η is one-one. Then the identity mapping θ is a complete mapping. □

<u>Lemma 2.2</u> : If the group G has a complete mapping, then there exists an ordering of the elements of G such that $g_1 g_2 \ldots g_n$ is the identity element.

<u>Proof</u> : Let $G=\{g_1, g_2, \ldots, g_n\}$ and $g_1=e$. Assume $\theta(g)$ is a complete mapping of G. Define $\theta^*(g)=\theta(g)\theta(e)^{-1}$. Then $\theta^*(g)$ is one-one for $\theta^*(g_i)=\theta^*(g_j)$ implies $\theta(g_i)\theta(e)^{-1}=\theta(g_j)\theta(e)^{-1}$ which implies $\theta(g_i)=\theta(g_j)$. We have $g_i=g_j$. Also $\eta^*(g)$ is one-one because $\eta^*(g_i)=\eta^*(g_j)$ implies $g_i\theta^*(g_i)=g_j\theta^*(g_j)$ which implies $g_i\theta(g_i)\theta(e)^{-1}=g_j\theta(g_j)\theta(e)^{-1}$ which implies $\eta(g_i)=\eta(g_j)$. We have $g_i=g_j$. Note that $\theta^*(e)=\theta(e)\theta(e)^{-1}=e$ and $\eta^*(e)=e\theta^*(e)=ee=e$. Thus, without loss of generality, we can take $\theta(e)=\eta(e)=e$. Then $\eta(g_i)=g_i\theta(g_i)\neq e$ for $g_i\neq e$. Now consider $g_2\theta(g_2)=\eta(g_2)\neq e$ so that $g_2^{-1}\neq\theta(g_2)$. This means that $\theta(g_2)^{-1}$ occurs among $G\backslash\{e,g_2\}$. Then let $\theta(g_2)^{-1}=g_3$. We form the product $g_2\theta(g_2)g_3\theta(g_3)$. We continue in this manner and eventually

reach a product

(1) $g_2\theta(g_2)g_3\theta(g_3)\ldots g_s\theta(g_s)=e$ where $\theta(g_{i-1})=g_i^{-1}$ for $i=3,\ldots,s$ and $\theta(g_s)=g_2^{-1}$.

If $s=n$, the theorem is proved. This is because θ is a complete mapping and $\eta(g_1),\eta(g_2),\ldots,\eta(g_s)=\eta(g_n)$ is an ordering of the elements of G such that $\eta(g_1)\eta(g_2)\ldots$ $\ldots\eta(g_n)=g_1\theta(g_1)g_2\theta(g_2)\ldots g_n\theta(g_n)=e$.

If $s<n$, we repeat the process beginning with $g_{s+1}\theta(g_{s+1})$, where g_{s+1} is an element of G distinct from $g_1,g_2,\ldots,g_s$. Finally we arrive at a series of cycles similar to the above whose product is the identity element. Thus, we have $\eta(g_1)\eta(g_2)\ldots\eta(g_n)=g_1\theta(g_1)g_2\theta(g_2)\ldots g_n\theta(g_n)=e$. Then $\eta(g_1),\eta(g_2),\ldots,\eta(g_n)$ is the required ordering of G. □

Lemma 2.3 : If the product of all elements of the abelian group G is not the identity, then G has the form A×B with A cyclic of order 2^k, $k>0$, and B of odd order.

Proof : Since the product of all elements of G is not the identity, then there exists no ordering of the elements of G such that $g_1g_2\ldots g_n=e$. By Lemma 2.2, G has no complete mapping. By Lemma 2.1, G is of even order. Then G has the form A×B with A cyclic of order 2^k, $k>0$, and B of odd order. □

Lemma 2.4 : If j is any positive integer, and $\delta_1,\delta_2,\ldots,\delta_m$

are positive integers, then there exist unique integers $j_0, j_1, \ldots, j_m$ such that

$$j \equiv j_0 \pmod{\delta_1\delta_2\ldots\delta_m},$$

$$j_0 = j_1+j_2\delta_1+j_3\delta_1\delta_2+\ldots+j_m\delta_1\delta_2\ldots\delta_{m-1},$$

$$0 \le j_1 < \delta_1,$$

$$0 \le j_2 < \delta_2,$$

$$\vdots$$

$$0 \le j_m < \delta_m.$$

Proof : The proof of the existence and uniqueness of the expansion is entirely analogous to the expansion of an integer in powers of a number base. Since j and $\delta_1\delta_2\ldots\delta_m$ are positive integers, then by the Division Algorithm, there exist unique integers q_0 and j_0, $0 \le j_0 < \delta_1\delta_2\ldots\delta_m$, such that $j=j_0+q_0\delta_1\delta_2\ldots\delta_m$. That is, $j \equiv j_0 \pmod{\delta_1\delta_2\ldots\delta_m}$. Similarly, for integers j_0 and δ_1 there exist unique integers q_1 and j_1, $0 \le j_1 < \delta_1$, such that $j_0=j_1+q_1\delta_1$. For integers q_1 and δ_2 there exist unique integers q_2 and j_2, $0 \le j_2 < \delta_2$, such that $q_1=j_2+q_2\delta_2$. Therefore

$$j_0 = j_1+q_1\delta_1 = j_1+(j_2+q_2\delta_2)\delta_1 = j_1+j_2\delta_1+q_2\delta_1\delta_2.$$

We now continue this process. Finally we obtain

$$j_0 = j_1+j_2\delta_1+j_3\delta_1\delta_2+\ldots+q_{m-1}\delta_1\delta_2\ldots\delta_{m-1} \text{ where}$$

$$0\le j_i<\delta_i,\ i=1,2,\ldots,m-1.$$

Since $0\le j_0<\delta_1\delta_2\ldots\delta_m$, then

$$j_0-j_1-j_2\delta_1-\ldots-j_{m-1}\delta_1\delta_2\ldots\delta_{m-2}$$

$$= q_{m-1}\delta_1\delta_2\ldots\delta_{m-1}<\delta_1\delta_2\ldots\delta_{m-1}\delta_m$$

so that $0\le q_{m-1}<\delta_m$. We replace q_{m-1} by j_m. The lemma is proved. □

Next we are going to prove B. Gordon's Theorem. The necessary condition of the theorem is simple to prove. For the sufficiency, B. Gordon, using the elements of a basis of the group, constructed the desired sequencing.

Theorem 2.5 : A finite abelian group G is sequenceable if and only if G is the direct product of two groups A and B, where A is cyclic of order 2^k, $k>0$, and B is of odd order.

Proof : To see the necessity of the condition, suppose that G is sequenceable and let $a_1,a_2,\ldots,a_n$ be an ordering of the elements of G with distinct partial products. Define $b_i=a_1a_2\ldots a_i$ for each integer i, $1\le i\le n$. If $a_i=e$ for some $i>1$, then $b_{i-1}=a_1a_2\ldots a_{i-1}=a_1a_2\ldots a_{i-1}e=a_1a_2\ldots$ $\ldots a_{i-1}a_i=b_i$, contrary to our assumption and therefore we have $a_1=b_1=e$. Hence $b_n \neq e$, that is, the product of all elements of G is not the identity. By Lemma 2.3, G has the form A×B with A cyclic of order 2^k, $k>0$, and B of odd order.

To prove sufficiency of the condition, suppose that $G=A\times B$ with A and B as in the statement of the theorem. We then show that G is sequenceable by constructing an ordering $a_1,a_2,\ldots,a_n$ of its elements with distinct partial products. From the general theory of abelian groups, it is known that G has a basis of the form $c_0,c_1,\ldots,c_m$, where c_0 is of order 2^k, and where the orders $\delta_1,\delta_2,\ldots,\delta_m$ of $c_1,c_2,\ldots,c_m$ are odd positive integers each of which divides the next, that is, $\delta_i | \delta_{i+1}$ for $0<i<m$. By Lemma 2.2, if j is any positive integer, then there exist unique integers $j_0,j_1,\ldots,j_m$ such that

$$j \equiv j_0 \pmod{\delta_1\delta_2\ldots\delta_m},$$

$$j_0 = j_1+j_2\delta_1+j_3\delta_1\delta_2+\ldots+j_m\delta_1\delta_2\ldots\delta_{m-1},$$

$$0 \leq j_1 < \delta_1,$$

$$(1) \qquad 0 \leq j_2 < \delta_1,$$

$$\vdots$$

$$0 \leq j_m < \delta_m.$$

We are now in a position to define the desired sequencing of G. It is convenient to define the products $b_1, b_2, \ldots, b_n$ directly, to prove they are all distinct, and then to verify that the corresponding a_i, as calculated from the formula $a_1=e$, $a_i=b_{i-1}^{-1}b_i$, are all distinct.

If i is of the form 2j+1 $(0\le j<n/2)$, let

$$b_{2j+1} = c_0^{-j} c_1^{-j_1} c_2^{-j_2} \ldots c_m^{-j_m},$$

where $j_1, j_2, \ldots, j_m$ are the integers defined in (1). On the other hand, if i is of the form 2j+2 $(0\le j<n/2)$, let

$$b_{2j+2} = c_0^{j+1} c_1^{j_1+1} c_2^{j_2+1} \ldots c_m^{j_m+1} .$$

Now, we are going to prove the elements $b_1, b_2, \ldots, b_n$ defined above are all distinct.

Suppose $b_s=b_t$ with s=2u+1 and t=2v+1. Then $c_0^{-u} c_1^{-u_1} c_2^{-u_2} \ldots c_m^{-u_m} = c_0^{-v} c_1^{-v_1} c_2^{-v_2} \ldots c_m^{-v_m}$. Hence

$$\begin{array}{llll} & -u \equiv -v \pmod{2^k} & \text{or equivalently} & u \equiv v \pmod{2^k}, \\ & -u_1 \equiv -v_1 \pmod{\delta_1} & \text{or} & u_1 \equiv v_1 \pmod{\delta_1}, \\ (2) & \vdots & & \vdots \\ & -u_m \equiv -v_m \pmod{\delta_m} & \text{or} & u_m \equiv v_m \pmod{\delta_m}. \end{array}$$

From the inequalities in (1), then $0\le u_i<\delta_i$ and $0\le v_i<\delta_i$ for each integer i, $1\le i\le m$. We conclude that $u_1=v_1$,

$u_2=v_2,\ldots,u_m=v_m$. Since $u_0=u_1+u_2\delta_1+u_3\delta_1\delta_2+\ldots+u_m\delta_1\delta_2\ldots\delta_{m-1}$ and $v_0=v_1+v_2\delta_1+v_3\delta_1\delta_2+\ldots+v_m\delta_1\delta_2\ldots\delta_{m-1}$, we have $u_0=v_0$ so that $u\equiv v \pmod{\delta_1\delta_2\ldots\delta_m}$. Together with the first congruence of (2) and since $(2^k,\delta_1\delta_2\ldots\delta_m)=1$, this gives $u\equiv v \pmod{2^k\delta_1\delta_2\ldots\delta_m}$. Thus $u\equiv v \pmod{n}$, which implies $u=v$.

Suppose $b_s=b_t$ with $s=2u+2$ and $t=2v+2$. Then $c_0^{u+1}c_1^{u_1+1}c_2^{u_2+1}\ldots c_m^{u_m+1}=c_0^{v+1}c_1^{v_1+1}c_2^{v_2+1}\ldots c_m^{v_m+1}$ and

$$
(3)\quad
\begin{array}{lcl}
u+1 \equiv v+1 \pmod{2^k} & \text{or equivalently} & u \equiv v \pmod{2^k}, \\
u_1+1 \equiv v_1+1 \pmod{\delta_1} & \text{or} & u_1 \equiv v_1 \pmod{\delta_1}, \\
\vdots & & \vdots \\
u_m+1 \equiv v_m+1 \pmod{\delta_m} & \text{or} & u_m \equiv v_m \pmod{\delta_m}.
\end{array}
$$

In a fashion similar to the above, $b_{2u+2}=b_{2v+2}$ implies $u=v$.

Finally, suppose $b_s=b_t$ with $s=2u+1$ and $t=2v+2$. Then $c_0^{-u}c_1^{-u_1}c_2^{-u_2}\ldots c_m^{-u_m}=c_0^{v+1}c_1^{v_1+1}c_2^{v_2+1}\ldots c_m^{v_m+1}$ and

$$
\begin{array}{l}
-u \equiv v+1 \pmod{2^k}, \\
-u_1 \equiv v_1+1 \pmod{\delta_1}, \\
\vdots \\
-u_m \equiv v_m+1 \pmod{\delta_m},
\end{array}
$$

or equivalently

$$
(4)\qquad
\begin{aligned}
u+v+1 &\equiv 0 \pmod{2^k},\\
u_1+v_1+1 &\equiv 0 \pmod{\delta_1},\\
&\vdots\\
u_m+v_m+1 &\equiv 0 \pmod{\delta_m}.
\end{aligned}
$$

Since $0\le u_i<\delta_i$ and $0\le v_i<\delta_i$, we have $0<u_i+v_i+1\le 2(\delta_i-1)+1<2\delta_i$ for each integer, $1\le i\le m$. This together with the congruences (4) forces us to have

$$
\begin{aligned}
u_1+v_1+1 &= \delta_1,\\
u_2+v_2+1 &= \delta_2,\\
&\vdots\\
u_m+v_m+1 &= \delta_m.
\end{aligned}
$$

Multiplying the (i+1)'st equation of this system by $\delta_1\delta_2\ldots\delta_i$, $1\le i<m$, we obtain

$$
\begin{aligned}
u_1+v_1+1 &= \delta_1,\\
\delta_1(u_2+v_2+1) &= \delta_1\delta_2,\\
\delta_1\delta_2(u_3+v_3+1) &= \delta_1\delta_2\delta_3,\\
&\vdots\\
\delta_1\delta_2\ldots\delta_{m-1}(u_m+v_m+1) &= \delta_1\delta_2\ldots\delta_{m-1}\delta_m.
\end{aligned}
$$

Adding them together gives us

$$
(u_1+v_1+1)+\delta_1(u_2+v_2+1)+\delta_1\delta_2(u_3+v_3+1)+\ldots
$$

$$
+\delta_1\delta_2\ldots\delta_{m-1}(u_m+v_m+1) = \delta_1+\delta_1\delta_2+\delta_1\delta_2\delta_3+\ldots+\delta_1\delta_2\delta_3\ldots\delta_m.
$$

Simplifying we get

$$(u_1+\delta_1u_2+\delta_1\delta_2u_3+\dots+\delta_1\delta_2\dots\delta_{m-1}u_m)$$
$$+(v_1+\delta_1v_2+\delta_1\delta_2v_3+\dots+\delta_1\delta_2\dots\delta_{m-1}v_m)+1 = \delta_1\delta_2\delta_3\dots\delta_m,$$

that is, $u_0+v_0+1 = \delta_1\delta_2\delta_3\dots\delta_m$. Since $u\equiv u_0 \pmod{\delta_1\delta_2\dots\delta_m}$ and $v\equiv u_0 \pmod{\delta_1\delta_2\dots\delta_m}$, then $u+v+1\equiv u_0+v_0+1 \pmod{\delta_1\delta_2\dots\delta_m}$. But $u_0+v_0+1 = \delta_1\delta_2\dots\delta_m$ so that $u+v+1\equiv 0 \pmod{\delta_1\delta_2\dots\delta_m}$. Combining this with the first congruence of (4), we find that $u+v+1\equiv 0 \pmod{2^k\delta_1\delta_2\dots\delta_m}$ because $(2^k,\delta_1\delta_2\dots\delta_m)=1$. Therefore $u+v+1\equiv 0 \pmod{n}$, which on account of the inequalities $0\le u<n/2$ and $0\le v<n/2$ implies that $0<u+v+1<n$ which is impossible. Hence, the elements $b_1,b_2,\dots,b_n$ are all distinct.

Next we calculate $a_1,a_2,\dots,a_n$. If $i=2j+2$ $(0\le j<n/2)$, then

$$a_i = b_{i-1}^{-1}b_i = (c_0^{-j}c_1^{-j_1}c_2^{-j_2}\dots c_m^{-j_m})^{-1}(c_0^{j+1}c_1^{j_1+1}c_2^{j_2+1}\dots c_m^{j_m+1})$$
$$= c_0^{2j+1}c_1^{2j_1+1}\dots c_m^{2j_m+1}.$$

These are all different by the same argument as above. If $i=2j+1$ and $j_1\ne 0$, then $j \equiv j_0 \pmod{\delta_1\delta_2\dots\delta_m}$, $j_0 = j_1+j_2\delta_1+j_3\delta_1\delta_2+\dots+j_m\delta_1\delta_2\dots\delta_{m-1}$ and $0\le j_1<\delta_i$, for

$i=1,2,\ldots,m$, imply $j-1 \equiv j_0-1 \pmod{\delta_1\delta_2\ldots\delta_m}$ and

$j_0-1 = (j_1-1)+j_2\delta_1+j_3\delta_1\delta_2+\ldots+j_m\delta_1\delta_2\ldots\delta_{m-1}$ with $0\le j_1-1<\delta_1$

and $0\le j_i<\delta_i$ where $i=2,3,\ldots,m$. Then

$$a_i = b_{i-1}^{-1}b_i = b_{2j}^{-1}b_{2j+1} = b_{2(j-1)+2}^{-1}b_{2j+1}$$

$$= (c_0^{(j-1)+1}c_1^{(j_1-1)+1}c_2^{j_2+1}\ldots c_m^{j_m+1})^{-1}c_0^{-j}c_1^{-j_1}c_2^{-j_2}\ldots c_m^{-j_m}$$

$$= c_0^{-2j}c_1^{-2j_1}c_2^{-2j_2-1}c_3^{-2j_3-1}\ldots c_m^{-2j_m-1}.$$

If $i=2j+1$ and $j_1=0$ but $j_2\neq 0$, then $j \equiv j_0 \pmod{\delta_1\delta_2\ldots\delta_m}$,

$j_0 = j_2\delta_1+j_3\delta_1\delta_2+\ldots+j_m\delta_1\delta_2\ldots\delta_{m-1}$ and $0\le j_i<\delta_i$ for $i=2,3,\ldots,m$,

imply $j-1 \equiv j_0-1 \pmod{\delta_1\delta_2\ldots\delta_m}$ and

$$j_0-1 = -1+j_2\delta_1+j_3\delta_1\delta_2+\ldots+j_m\delta_1\delta_2\ldots\delta_{m-1}$$

$$= (\delta_1-1)+(j_2-1)\delta_1+j_3\delta_1\delta_2+\ldots+j_m\delta_1\delta_2\ldots\delta_{m-1}$$

with $0\le\delta_1-1<\delta_1$, $0\le j_2-1<\delta_2$ and $0\le j_i<\delta_i$ where $i=3,4,\ldots,m$. Then

$$a_i=b_{i-1}^{-1}b_i$$

$$=(c_0^{(j-1)+1}c_1^{(j_1-1)+1}c_2^{(j_2-2)+1}c_3^{j_3+1}\ldots c_m^{j_m+1})^{-1}c_0^{-j}c_2^{-j_2}c_3^{-j_3}\ldots c_m^{-j_m}$$

$$= c_0^{-2j}c_2^{-2j_2}c_3^{-2j_3-1}\ldots c_m^{-2j_m-1}.$$

Similarly, if $j_1=j_2\dots=j_{t-1}=0$ but $j_t\neq 0$, then

$$a_i = c_0^{-2j} c_t^{-2j_t} c_{t+1}^{-2j_{t+1}-1} \dots c_m^{-2j_m-1} .$$

These a_i's are obviously distinct from each other by the same reasoning as before. Because of the exponent of c_0, they are also distinct from the a_i with i even. This completes the proof of the theorem. □

Example :

Consider the group $G=Z_2\times Z_3\times Z_3$. We use basis elements c_0, c_1 and c_2 of orders 2, 3, and 3, respectively. Using the notation (α,β,γ) for the elements $c_0^{\alpha}c_1^{\beta}c_2^{\gamma}$ where $c_0=(1,0,0)$, $c_1=(0,1,0)$, $c_2=(0,0,1)$ and $\delta_1=3$, $\delta_2=3$ the sequences a_i and b_i are then the following:

i	j	j_0	j_1	j_2	b_i	a_i
$1 = 2\cdot 0+1$	0	0	0	0	(0,0,0)	(0,0,0)
$2 = 2\cdot 0+2$	0	0	0	0	(1,1,1)	(1,1,1)
$3 = 2\cdot 1+1$	1	1	1	0	(1,2,0)	(0,1,2)
$4 = 2\cdot 1+2$	1	1	1	0	(0,2,1)	(1,0,1)
$5 = 2\cdot 2+1$	2	2	2	0	(0,1,0)	(0,2,2)
$6 = 2\cdot 2+2$	2	2	2	0	(1,0,1)	(1,2,1)
$7 = 2\cdot 3+1$	3	3	0	1	(1,0,2)	(0,0,1)
$8 = 2\cdot 3+2$	3	3	0	1	(0,1,2)	(1,1,0)
$9 = 2\cdot 4+1$	4	4	1	1	(0,2,2)	(0,1,0)
$10 = 2\cdot 4+2$	4	4	1	1	(1,2,2)	(1,0,0)

11 = 2·5+1	5	5	2	1	(1,1,2)	(0,2,0)
12 = 2·5+2	5	5	2	1	(0,0,2)	(1,2,0)
13 = 2·6+1	6	6	0	2	(0,0,1)	(0,0,2)
14 = 2·6+2	6	6	0	2	(1,1,0)	(1,1,2)
15 = 2·7+1	7	7	1	2	(1,2,1)	(0,1,1)
16 = 2·7+2	7	7	1	2	(0,2,0)	(1,0,2)
17 = 2·8+1	8	8	2	2	(0,1,1)	(0,2,1)
18 = 2·8+2	8	8	2	2	(1,0,0,)	(1,2,2)

In the lemma below, p(A) denotes the product of all elements of A where A is a subset of elements of the group G.

Lemma 2.6 : An abelian group G has exactly one element of order 2 if and only if the product of all n distinct elements of G is not the identity element of G.

Proof : Let the set H consist of the identity and all the elements of G of order 2. Then H is a subgroup of G. This follows because $e\epsilon H$ and if a, $b\epsilon H$, then $(ab^{-1})^2 = a^2(b^{-1})^2 = a^2(b^2)^{-1} = e$ so that $ab^{-1}\epsilon H$. If $a\epsilon G$ is of order greater than 2, $a \neq a^{-1}$. Thus, both a and a^{-1} appear in p(G) and hence p(G)=p(H).

Let n(G) be the number of elements of order 2 in G. Suppose n(G)=1, then p(G)=p(H)≠e. Suppose n(G)=0, then p(G)=e because H={e}. Suppose n(G)>1. Then H has order greater than 2 so that H has order 2^k, $k>1$. Then H has k generators $g_1, g_2, \ldots, g_k$ and every element of H has an unique representation in the form $g_1^{n_1} g_2^{n_2} \ldots g_k^{n_k}$ where n_i is 0 or 1. Hence $p(H) = \Pi(g_1^{n_1} g_1^{n_2} \ldots g_k^{n_k})$, where the product is over the distinct k-tuples $(n_1, n_2, \ldots, n_k)$ with each n_i taking the value 0 or 1. Then $p(H)=(g_1 g_2 \ldots g_k)^m$ where $m=2^{k-1}$ and since $k>1$, we have $p(H)=e$. This proves the lemma.□

From Theorem 2.5, we know that the abelian group G is sequenceable if and only if the product of all elements of G is not the identity. Together with the above lemma, we can state that "a finite abelian group G is sequenceable if and only if the abelian group has an unique element of order 2."

Before finishing this chapter, we give a simple method to construct a sequencing of an abelian group of even order Z_{2m}.

Let the elements of Z_{2m} be $0,1,2,\ldots,2m-1$. We claim that $S: 0,1,2m-2,3,2m-4,5,2m-6,7,2m-8,9,\ldots,4,2m-3,2,2m-1$ is a sequencing of Z_{2m}. Obviously, the elements of S are all distinct. The partial sum P is of the form $0,1,2m-1,2,2m-2,3,\ldots,m+2,m-1,m+1,m$ and they are all distinct. Thus, S is a sequencing of Z_{2m}.

CHAPTER THREE

Non-abelian Sequenceable Groups

At the present time, the problem of determining the sequenceable non-abelian groups is still unsolved. Different mathematicians have used different methods to construct sequencings for non-abelian groups. We know only that there exist an infinite number of sequenceable non-abelian groups.

Basil Gordon first constructed a sequencing of a non-abelian group of order 10. N.S. Mendelsohn heuristically found five sequencings of a non-abelian group of order 21. J. Dénes and E. Török used a computer to show that for all non-abelian groups of order $n \leq 14$, the only non-abelian sequenceable groups were the dihedral groups, D_5, D_6, and D_7. They also found a sequencings of D_8 and 15 sequencings of a non-abelian group of order 21. Lawrence Wang also used a computer to test the finite group G where G of order pq is generated by a, b with $a^p=b^q=1$, $a^{-1}ba=b^r$ where r is a positive integer, p, q are primes, $q\equiv 1 \pmod p$ and $r^p\equiv 1 \pmod q$. He ran the program for n=6, 10, and 21, which were known to be sequenceable already. He also tested for some other n and found that for n=39, 55, 57, these groups are also sequenceable. B.A. Anderson derived a technique to find a sequencing of D_p where $p>3$ is an odd prime with primitive root r such that $3r\equiv -1 \pmod p$ and he gave sequencings for D_5, D_{11}, and D_{17}. Finally, Richard Friedlander derived a method to construct a sequencing for D_n where n is a prime congruent to 1 modulo 4.

At last we have an infinite family of sequenceable non-abelian groups. A.D. Keedwell had constructed a sequencing of a non-abelian group of order 27. Recently he showed that if p is an odd prime which has 2 as a primitive root and q is another odd prime of the form q=2ph+1, then the non-abelian group of order pq is sequenceable.

We first give some basic definitions.

Definition 3.1 : A dihedral group D_n is the group generated by two elements a, b where $a^2=b^n=1$ and $ab=b^{-1}a$.

Then D_n has order 2n and for any a, $b \in D_n$, $b^j=ab^{-j}$ for any j. If $H=\langle b\rangle$, H is a normal subgroup of D_n, and the factor group $D_n/H=\{H,H_1\}$ where $H_1^2=H$.

Let $G=\langle a,b\rangle$ be a non-abelian group of order pq, p<q where p and q are distinct odd primes satisfying the relations $a^p=b^q=1$ and $ba=ab^s$ with $s^p \equiv 1 \pmod{q}$. Then $(a^u b^v)(a^x b^y) = a^{u+x} b^{vs^x+y}$. Also, $H=\langle b\rangle$ is a normal subgroup of order q and the number of its Sylow p-subgroups is 1+pk=q. Therefore, (q-1) is divisible by p. Since q is odd, 2p divides (q-1) so q=2ph+1 for some integer h.

Definition 3.2 : A map Φ of group G into G' is a homomorphism if for any a, b belonging to G, $\Phi(ab)=(\Phi a)(\Phi b)$.

The natural homomorphism $\Phi:G\to G/H$ is a homomorphism defined by $\Phi(a)=aH$ where $a\in G$. If $G=\langle a,b\rangle$ such that $a^p=b^q=1$, $ba=ab^s$ where $s^p\equiv 1 \pmod q$ and $H=\langle b\rangle$, then the natural homomorphism $\Phi:G\to G/H$ maps G onto the cyclic group of order p with elements $1=H$, $x=aH$, $x^2=a^2H$, ... , $x^{p-1}=a^{p-1}H$.

Definition 3.3 : GH[p] denotes the set of residue classes modulo the prime p.

Definition 3.4 : A generator x of the cyclic multiplicative group of order p-1 of GF[p] is called a primitive root of GF[p].

For example, when p=11, the cyclic multiplicative group can be generated by 2 because the powers $2^0\equiv 1$, $2^1\equiv 2$, $2^2\equiv 4$, $2^3\equiv 8$, $2^4\equiv 5$, $2^5\equiv 10$, $2^6\equiv 9$, $2^7\equiv 7$, $2^8\equiv 3$, $2^9\equiv 6 \pmod{11}$ give all the p-1=10 non-zero residue classes $\overline{1},\overline{2},\ldots,\overline{10}$.

Definition 3.5 : Let G be a group of order n, H be a normal subgroup of G of order h, and let $G/H=\{x_1,x_2,\ldots,x_t\}$ such that $t=n/h$. A sequence S of length n consisting of elements from G/H is called a quotient sequencing of G if each x_j, $1\le j\le t$, occurs h times in both S and the sequence of partial products of S.

By Theorem 1.4, we have the following statement. Let H be a normal subgroup of G and Φ be the natural homomorphism defined by $\Phi(x)=xH$ for $x\in G$. If S is a sequencing of G, then the image of S under Φ is a quotient sequencing of G. This gives us a method to search for a sequencing of G. We can select a normal subgroup H of G, list all quotient sequencing of G, and lift these quotient sequencings back to G hoping that one of these forms a sequencing of G. If all the liftings fail to form a sequencing, then G is not sequenceable.

<u>Example</u> : Let $G = S_3 = \{e,(12),(13),(23),(123),(132)\}$
and $H = A_3 = \{e,(132),(132)\}$.
So $S_3/A_3 = \{A_3,\{(12),(13),(23)\}\}$.

For simplicity let $S_3/A_3 = \{1,x\}$ where $\{e,(123),(132)\} = 1$ and $\{(12),(13),(23)\} = x$. Then $\Phi(e) = \Phi(123) = \Phi(132) = 1$ and $\Phi(12) = \Phi(13) = \Phi(23) = x$, where Φ is the natural homomorphism. A quotient sequencing Q of S_3/A_3 is a sequence of length 6 such that Q and its sequence of partial products is made up of three 1's and three x's. After checking all the combinations, we find that there are 4 quotient sequencings:

1,1,x,1,x,x; 1,1,x,x,x,1; 1,x,1,x,1,x; 1,x,x,1,x,1.

In order to get a sequencing of S_3, the first 1 in the quotient must lift back to the identity e of S_3. Using the automorphisms of the group, we know that there exist inner automorphisms Φ_1, Φ_2 such that $\Phi_1(123)=(132)$ or $\Phi_2(123)=(132)$ and $\Phi_1(13)=(12)$, $\Phi_2(23)=(12)$. Then we can assume that the second 1 lifts back to (123), and the first x lifts back to (12). Then the third 1 must lift to (132). Now, we have a partial sequence e, (123), (12), (132). The partial products are e, (123), (23), (13). However, if we put on a fifth element of either (13) or (23), we repeat a partial product e or (123), respectively. Therefore, the first quotient sequencing fails to lift back to a sequencing of S_3. Similarly, all the other quotient sequencings fail too. We conclude that S_3 is not a sequenceable group.

§3.1 Sequencings of some non-abelian groups of even order

Suppose D_n is a dihedral group. Let $H=\langle b\rangle$. Then $D_n/H=\{H,H_1\}$ such that $H_1^2=H$. For simplicity we let $H=1$, $H_1=x$. By the method described above, in order to find a sequencing of D_n, we investigate the quotient sequencings of D_n/H. Lifting the quotient sequencings back to D_n, we hope that one of the liftings is a sequencing of D_n. Since $\langle b\rangle=\{e,b,b^2,\ldots,b^{n-1}\}$, the image of all these elements under the natural homomorphism Φ is 1, and the image of $\{a,ab,ab^2,\ldots,ab^{n-1}\}$ is x. Then the quotient sequencing of D_n is a sequence of n 1's and n x's. For the case of D_5, Richard Friedlander found that the quotient sequencing 1,1,1,x,x,x,x,x,1,1 could be lifted back to give a sequencing of D_5.

One general form of a quotient sequencing of D_n which may give a sequencing of D_n is

$$(1)\qquad \overbrace{1,1,\ldots,1}^{k+1},\overbrace{x,x,\ldots,x}^{2k+1},\overbrace{1,1,\ldots,1}^{k}$$

with $n=2k+1$. The sequence of partial products is

$$(2)\qquad \overbrace{1,1,\dots,1}^{k+1},\overbrace{x,1,x,1,\dots,1,x}^{2k+1},\overbrace{x,x,\dots,x}^{k}$$

The original arrangement of the elements of D_n having (1) as its quotient sequencing is of the form

$$b^{a_1},b^{a_2},\dots,b^{a_{k+1}},ab^{t_1},ab^{t_2},ab^{t_3},\dots,ab^{t_{2k+1}},b^{r_1}b^{r_2},\dots,b^{r_k}.$$

Its partial products in D_n are of the form

$$b^{a_1},b^{a_1+a_2},\dots,b^{S_A},ab^{t_1-S_A},b^{t_2-t_1+S_A},ab^{t_3-t_2+t_1-S_A},$$

$$b^{t_4-t_3+t_2-t_1+S_A},\dots,ab^{S_T-S_A},ab^{S_T-S_A+r_1},ab^{S_T-S_A+r_1+r_2},\dots$$

$\dots,ab^{S_T-S_A+r_1+r_2+\dots+r_k}$. Where $A=\{a_1,a_2,\dots,a_{k+1}\}$, $T=\{t_1,t_2,\dots,t_{2k+1}\}$, $R=\{r_1,r_2,\dots,r_k\}$ are sequences of integers modulo n, and $S_A=a_1+a_2+\dots+a_{k+1}$, $S_T=t_{2k+1}-t_{2k}+\dots+t_3-t_2+t_1$.

Let $D=\{d_1,\dots,d_k\}$ and $E=\{e_0,e_1,\dots,e_k\}$ such that

$$d_i=t_{2i}-t_{2i-1},\ 1\le i\le k,$$

$$(3)\ e_0=t_1-S_A \text{ and}$$

$$e_i=t_{2i+1}-t_{2i},\ 1\le i\le k.$$

Let $(A,D)=\{a_1,a_2,\dots,a_{k+1},d_1,d_2,\dots,d_k\}$,

$(E,R)=\{e_0,e_1,\dots,e_k,r_1,r_2,\dots,r_k\}$ and

$(E\wedge D)=\{e_0,d_1,e_1,d_2,e_2,\dots,d_k,e_k\}$.

Then the arrangement of all the elements in D_n reduces to

$$(4)\quad b^{a_1},b^{a_2},\dots,b^{a_{k+1}},ab^{e_0+S_A},ab^{e_0+d_1+S_A},ab^{e_0+d_1+e_1+S_A},\dots$$
$$\dots,ab^{e_0+d_1+e_1+\dots+d_k+e_k+S_A},b^{r_1},b^{r_2},\dots,b^{r_k}$$

and the sequence of partial products in D_n reduces to

$$(5)\quad b^{a_1},b^{a_1+a_2},b^{a_1+a_2+a_3},\dots,b^{S_A},ab^{e_0},b^{S_A+d_1},ab^{e_0+e_1},$$
$$b^{S_A+d_1+d_2},\dots,ab^{e_0+e_1+\dots+e_k},ab^{e_0+e_1+\dots+e_k+r_1},\dots$$
$$\dots,ab^{e_0+e_1+\dots+e_k+r_1+r_2+\dots+r_k}.$$

Then we have the following theorem.

<u>Theorem 3.1</u> : Let G be the dihedral group of order 2n, n=2k+1. Suppose there exist sequences of integers $A=\{a_1,a_2,\dots,a_{k+1}\}$, $R=\{r_1,r_2,\dots,r_k\}$, $D=\{d_1,d_2,\dots,d_k\}$ and $E=\{e_0,e_1,\dots,e_k\}$ such that

$d_i = t_{2i}-t_{2i-1}$, $1\le i\le k$,

$e_0 = t_i-S_A$ where $S_A = a_1+a_2+\dots+a_{k+1}$,

$e_1 = t_{2i+1}-t_{2i}$, $1\le i\le k$, and satisfying conditions:

(i) $a_1,a_2,\dots,a_{k+1},r_1,r_2,\dots,r_k$ are all distinct modulo n,

(ii) the elements of P(A,D), the sequence of partial sums of (A,D), are all distinct modulo n,

(iii) the elements of $P(E\wedge D)$ are all distinct modulo n, and

(iv) the elements of P(E,R) are all distinct modulo n.

Then there exists a sequencing of D_n.

<u>Proof</u> : Conditions (i) and (iii) guarantee that elements

of (4) are all distinct and conditions (ii) and (iv) guarantee that elements of (5) are all distinct. Then (4) is a sequencing of D_n. □

We are at the point of seeking values of n such that there exist the sequences A,R,D,E satisfying all the conditions as described in the above result. Richard Friedlander was sucessful in choosing the sequences A,R,D,E when n is a prime congruent to 1 modulo 4. We have the following theorem.

Theorem 3.2[8] : The group D_n where n is a prime and $n \equiv 1 \pmod 4$ is sequenceable.

Proof : Since n is odd we write $n=2k+1$. Let $A = \{0,2,\ldots,2k\}$, $R = \{1,3,5,\ldots,2k-1\}$, $D = \{-h,-3h,-5h,\ldots,-(2k-1)h\}$ and $E = \{0,2h,4h,\ldots,2kh\}$ where the Legendre symbol $(h|n)=-1$.

In order to show D_n is sequenceable, it suffices to show all these sequences satisfy conditions (i), (ii), (iii) and (iv) as described in Theorem 3.1.

(i) Obviously all the elements of A and R are distinct modulo n.

(ii) We have to show that the elements of P(A,D), the sequence of partial sums of (A,D), are distinct modulo n. Suppose the partial sums of (A,D) are not all distinct.

Case 1. Two equal partial sums are from the A part. Then there exist i, k such that

$0+2+4+\ldots+2i \equiv 0+2+\ldots+2j \pmod{n}$ where $0 \le i \le j \le (n-1)/2$.

Thus, $i(i+1) \equiv j(j+1) \pmod{n}$ so that $(j-i)(j+i+1) \equiv 0 \pmod{n}$.

This implies $i=j$ so that all the partial sums from A are distinct.

Case 2. Two equal partial sums are from the D part. Then there exist i, j such that

$S_A-(h+3h+\ldots+(2i-1)h) \equiv S_A-(h+3h+\ldots+(2j-1)h) \pmod{n}$

where $1 \le i \le j \le (n-1)/2$.

Then $h+3h+\ldots+(2i-1)h \equiv h+3h+\ldots+(2j-1)h \pmod{n}$ so that

$i^2h \equiv j^2h \pmod{n}$ or $(i+j)(i-j)h \equiv 0 \pmod{n}$.

This implies $i=j$ and all partial sums from D distinct.

Case 3. Assume one partial sum from A and one from D are equal. Then there exist i, j such that

$0+2+4+\ldots+2i \equiv S_A-(h+3h+\ldots+(2j-1)h) \pmod{n}$

where $0 \le i \le (n-1)/2=k$ and $1 \le j \le (n-1)/2=k$.

Thus $i(i+1) \equiv S_A-j^2h \pmod{n}$.

Since $S_A = \sum_{i=0}^{k} 2i = k(k+1)$ and $n = 2k+1$,

then $4S_A = 4k^2+4k$ (1)

and $n^2 = 4k^2+4k+1$. (2)

Combining (1) and (2), we have $4S_A = n^2-1$.

Then $4i(i+1) \equiv 4(S_A-j^2h) \pmod n$ or

$4i(i+1) \equiv n^2-1-4j^2h \pmod n$ or

$(2i+1)^2 \equiv -4j^2h \pmod n$

which implies $(-h|n)=1$. This is impossible as $(h|n)=-1$ and $n\equiv 1 \pmod 4$.

(iii) Now $E\wedge D = \{0,-h,2h,-3h,4h,\ldots,-(2k-1)h,2kh\}$ so that $P(E\wedge D) = \{0,-h,h,-2h,2h,\ldots,-kh,kh\}$. Since $(h,n)=1$, they are all distinct modulo n.

(iv) This is similar to (ii).

Now $(E,R) = \{0,2h,4h,\ldots,2kh,1,3,5,\ldots,2k-1\}$.

Case 1. Two partial sums are both from the E part. Then there exist i, j such that

$(i+1)ih \equiv (j+1)jh \pmod n$ where $0\leq i<j\leq k=(n-1)/2$.

Hence $(i-j)(i+j+1)h \equiv 0 \pmod n$ and it is impossible as n is a prime.

Case 2. Two partial sums are both from the R part. Then there exist i, j such that

$(k+1)kh+i^2 \equiv (k+1)kh+j^2 \pmod n$ where $0\leq i<j\leq k$

so that $(i-j)(i+j) \equiv 0 \pmod n$. This is impossible.

Case 3. One partial sum is from A and the other is from R. Then there exist i and j such that

$(i+1)ih \equiv (k+1)kh+j^2 \pmod n$ where $0\leq i\leq k$, $0\leq j\leq k$.

Then $4(i+1)ih \equiv 4(k+1)kh+4j^2 \pmod n$ or

$$4(i+1)ih \equiv (n^2-1)h+4j^2 \pmod{n} \text{ or}$$

$$4(i+1)ih \equiv -h+4j^2 \pmod{n}.$$

So $4j^2 \equiv 4(2j+1)^2 h \pmod{n}$ which implies $(h|n)=1$. This is a contradiction and the proof is finished. □

Example : We find a sequencing of D_{13}. We have $n=13$, $k=6$ and $(2|13)=-1$. We take $h=2$. The sequences A,R,D,E are

$$A = \{0,2,4,6,8,10,12\},$$

$$R = \{1,3,5,7,9,11\},$$

$$D = \{11,7,3,12,8,4\},$$

$$E = \{0,4,8,12,3,7,11\} \text{ and } S_A \equiv 3 \pmod{13}.$$

Then we use $d_i = t_{2i}-t_{2i-1}$, $1\le i\le 6$,

$$e_0 = t_1-S_A,$$

$$e_i = t_{2i+1}-t_{2i}, \quad 1\le i\le 6,$$

to solve for the sequence $T=\{3,1,5,12,7,10,9,8,11,6,0,4,2\}$. We know the sequences A, T and R and a sequencing of D_{13} is

$e,b^2,b^4,b^6,b^8,b^{10},b^{12},ab^3,ab,ab^5,ab^{12},ab^7,ab^{10},ab^9,ab^8,$
$ab^{11},ab^6,a,ab^4,ab^2,b,b^3,b^5,b^7,b^9,b^{11}.$

The partial products are

$e,b^2,b^6,b^{12},b^7,b^4,b^3,a,b,ab^4,b^8,ab^{12},b^{11},ab^{11},b^{10},ab,$
$b^5,ab^8,b^9,ab^6,ab^7,ab^{10},ab^2,ab^9,ab^5,ab^3.$

J. Dénes and E. Török tested all the non-abelian groups of order $n\le 12$ on the ICT 1905 computer, and found that only D_5 and D_6 were sequenceable. Because it took 45-55 minutes to test for $n=12$, for $n>12$, the program only ran for a certain period of time or found a sequencing. It was found that D_7 and D_8 are also sequenceable. These are the results.

Dihedral group D_3:

The number of partial sequencings of length 3 obtained was 18,
of length 4 was 12, and
of length 5 was 0.

The group is not sequenceable (total number of products tested was 30).

Dihedral group D_4:

The number of partial sequencings of length 4 obtained was 20,
of length 5 was 152,
of length 6 was 270, and
of length 7 was 0.

The group is not sequenceable (total number of products tested was 448).

Quaternion group Q_3 of order 8:

The number of partial sequencings of length 4 obtained was 72,
of length 5 was 216,
of length 6 was 48, and
of length 7 was 0.

The group is not sequenceable (total number of products tested was 336).

Dihedral group D_5:

The number of partial sequencings of length 5 obtained was 280,
of length 6 was 1920,
of length 7 was 3920,
of length 8 was 2240, and
of length 9 was 320.

The group is sequenceable (total number of products tested was 8680). One of the sequencings of length 10 is $e,b,b^2,a,ab,ab^4,ab^2,ab^3,b^3,b^4$. The partial product sequence is $e,b,b^3,ab^2,b^4,a,b^2,ab,ab^4,ab^3$.

Dihedral group D_6:

The number of partial sequencings of length 6 obtained was 936,
of length 7 was 17520,
of length 8 was 71580,
of length 9 was 108840,
of length 10 was 57312, and
of length 11 was 3072.

The group is sequenceable (total number of products tested was 259,260). One of the sequencings of length 12 is $e,b,b^2,a,b^3,ab^2,ab,ab^4,ab^3,b^4,b^5,ab^5$. The partial products are $e,b,b^3,ab^3,a,b^2,ab^5,b^5,ab^4,ab^2,ab,b^4$.

Group $G=\{b,a:b^3=a^4=e,ba=ab^{-1}\}$ of order 12:

The number of partial sequencings of length 6 obtained was 1152,
of length 7 was 14832,

of length 8 was 64560,
of length 9 was 85824,
of length 10 was 39792, and
of length 11 was 0.

The group is not sequenceable (total number of products tested was 206,160).

Alternating group A_4 of order 12:
The number of partial sequencings of length 6 obtained was 1032,
of length 7 was 16224,
of length 8 was 63480,
of length 9 was 91248,
of length 10 was 41472, and
of length 11 was 0.

The group is not sequenceable (total number of products tested was 213,456).

For the dihedral group D_7 which is sequenceable, one of the sequencing is $e,b,b^2,b^3,a,b^4,b^6,b^5,ab^6,ab^3,ab^4,ab,ab^5,ab^2$. The partial products are $e,b,b^3,b^6,ab,ab^5,ab^4,ab^2,b^4,ab^6,b^5,ab^3,b^2,a$.

For the dihedral group D_8 which is sequenceable, one of the sequencings is $e,b,b^2,b^3,a,b^4,b^5,b^6,ab^5,ab^4,b^7,ab^6,ab^3,ab,ab^2,$ ab^7. The partial products are $e,b,b^3,b^6,ab^2,ab^6,ab^3,ab,b^4,a,$ $ab^7,b^7,ab^4,b^5,ab^5,b^2$.

As mentioned earlier in this chapter, B.A. Anderson introduced a method to construct sequencings of some dihedral groups of order 2p where p is an odd prime. He succeeded in sequencing D_5, D_{11}, D_{17} and D_{23} by this method.

We know that D_p is generated by two elements a, b such that $a^2=b^p=e$ and $a^{-1}ba=b^{-1}$. The elements of D_p either have order 1, (the identity); order p,($Z_p\backslash\{e\}$, Z_p the cyclic subgroup generated by b) or order 2,($D_p\backslash Z_p$). Suppose $S:a_0,a_1,\ldots,a_{2p-1}$ is a sequencing of D_p. Then there is a corresponding string $T:n(a_0),n(a_1),\ldots,n(a_{2p-1})$ where for $1\leq i\leq 2p-1$, $n(a_i)$ is the order of a_i. We know that

$$T:1,\overbrace{p,p,\ldots,p}^{(p-1)/2},\overbrace{2,2,\ldots,2}^{p},\overbrace{p,p,\ldots,p}^{(p-1)/2}$$

could be a string for some sequencings of D_p.

Anderson's method of construction is to split the sequencing into three separated parts. He first considers the middle part which contains all elements with order 2. After sequencing the middle part he considers the first part and the sequencing of the first part induces a sequencing of the last part.

Let $c_i = a_0a_1\ldots a_i$ and $t = (p-1)/2$. Then

$$P:c_0,c_1,\ldots,c_t,c_{t+1},c_{t+2},\ldots,c_{t+p},c_{t+p+1},\ldots,c_{2p-1}$$

is the sequence of partial products of S and

$c_0,c_1,\ldots,c_t$ belong to Z_p,

$c_{t+2},c_{t+4},\ldots,c_{t+p-1}$ belong to Z_p,

$c_{t+1},c_{t+3},\ldots,c_{t+p}$ belong to $D_p\backslash Z_p$, and

$c_{t+p+1},c_{t+p+2},\ldots,c_{2p-1}$ belong to $D_p\backslash Z_p$.

Definition 3.6 : Suppose $r=2s+1$, where s is any positive integer, and G is an abelian group of order r. $S=\{\{x_i,y_i\}:1\le i\le s\}$ is a starter for G if every nonzero element of G occurs as (i) an element of some paris of S and (ii) a difference of some pairs of S.

If $x_i+y_i=0$ for $1\le i\le s$, then we call S the patterned starter for G.

Theorem 3.3 : Suppose $p>3$ is an odd prime with primitive root r, n is a positive integer such that $(n,p-1)=1$, and $3r^n\equiv -1 \pmod p$. If $t=(p-1)/2$, $c_t=b^{r^s}$ for some integer s

and $c_{t+2k-1} = b^{r^{s+(k-1)n}} ab^{i_k} = ab^{r^{s+kn}}$ and

(1) $c_{t+2k} = ab^{r^{s+kn}} ab^{j_k} = b^{r^{s+kn}}$ for $1\le k\le (p-1)/2$,

then (i) $\{i_k,j_k : 1\le k\le (p-1)/2\}$ is a reduced residue system modulo p,

(ii) $b^{r^{s+[(p-1)/2]n}} a = ab^{r^s} = c_{t+p}$, and

(iii) $\{\{i_k,j_k\} : 1\le k\le (p-1)/2\}$ is a patterned starter on Z_p.

Proof : (i) We know $(a^u b^v)(a^x b^y) = a^{u+x} b^{v(-1)^x+y}$.

Then we have

$$ab^{r^{s+(k-1)n}(-1)+i_k} = ab^{r^{s+kn}} \text{ and}$$

$b^{r^{s+kn}(-1)+j_k} = b^{r^{s+kn}}$ which implies

$i_k \equiv r^{s+(k-1)n}(r^n+1) \pmod p$ $1 \le k \le (p-1)/2$ and

$j_k \equiv 2r^{s+kn} \pmod p$ $1 \le k \le (p-1)/2$.

Assume that there exist u,v, $1 \le u,v \le (p-1)/2$ and $u \ne v$ such that $r^{s+(v-1)n}(r^n+1) \equiv r^{s+(u-1)n}(r^n+1) \pmod p$. This implies $r^{vn}-r^{un} \equiv r^{vn}(1-r^{(u-v)n}) \equiv 0 \pmod p$ which yields $r^{(u-v)n} \equiv 1 \pmod p$. This is impossible for $r^t \equiv 1 \pmod p$ only if t is a multiple of $(p-1)$. It is shown similarly that j_u and j_v are distinct non-zero residues. Suppose there exist u,v where $1 \le u,v \le (p-1)/2$, $u \ne v$ such that $i_u \equiv j_v \pmod p$. Then $2r^{s+vn}-r^{s+(u-1)n}(r^n+1) \equiv 0 \pmod p$ and $r^{s+(u-1)n}(2r^{(v-u+1)n}-r^n-1) \equiv 0 \pmod p$. Since $r^{s+(u-1)n} \not\equiv 0 \pmod p$, then we have $2r^{(v-u+1)n}-r^n-1 \equiv 0 \pmod p$. However, $1 \le u,v \le (p-1)/2$ and $u \ne v$, so that $v-u$ can take on any value from $1,2,\ldots,p-2$ modulo $(p-1)$ except $(p-1)/2$. Then the same is true of $(v-u)n$ for $(n,p-1)=1$. From our assumption, $3r^n+1 \equiv 0 \pmod p$. It is equivalent to $-3r^n-1 \equiv 0 \pmod p$ or $r^n[2r^{(p-1)/2}-1]-1 \equiv 0 \pmod p$ for $r^{(p-1)/2} \equiv -1 \pmod p$ or $2r^{(p-1)/2+n}-r^n-1 \equiv 0 \pmod p$ which means that $2r^{(v-u)n\ +n}-r^n-1 \equiv 0 \pmod p$ has no solution. Therefore, all i_u and j_v are distinct $\pmod p$.

(ii) Now

$$b^{r^{s+[(p-1)/2]n}}a = a^2b^{r^{s+[(p-1)/2]n}}a$$

$$= ab^{r^{s+[(p-1)/2]n}(-1)}$$

$$= ab^{-r^{s+[(p-1)/2]n}}.$$

Since $(p-1,n)=1$, then n is odd. Then we have

$$b^{r^{s+[(p-1)/2]n}}a = ab^{r^s}..$$

(iii) From (i), we can show similarly that the differences of i_k and j_k are all distinct. What we have to prove is that

$$(i_k+j_k) \equiv 0 \pmod p \text{ for } 1 \leq k \leq (p-1)/2, \text{ or}$$

$$\begin{aligned}(i_k+j_k) &\equiv r^{s+(k-1)n}(r^n+1)+2r^{s+kn} \\ &\equiv r^{s+(k-1)n}+3r^{s+kn} \\ &\equiv r^{s+(k-1)n}(1+3r^n) \\ &\equiv 0 \pmod p \text{ for } 3r^n \equiv -1 \pmod p. \ \square\end{aligned}$$

Let us consider D_{11}, then $p=11$. Let $r=7$, $n=1$, and $s=4$. Then $c_t = b^{r^s} = b^3$, $c_{t+2k-1} = ab^{r^{s+kn}} = ab^{7^{4+k}} = ab^{3+k}$,

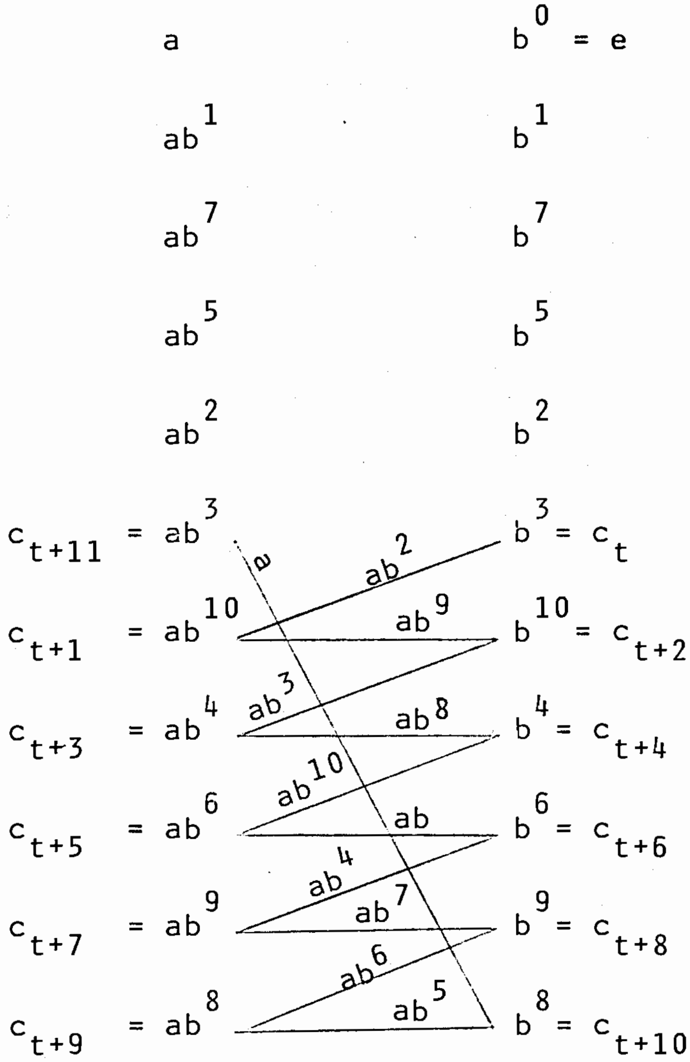
$c_{t+2k} = b^{r^{s+kn}} = b^{7^{4+k}} = b^{3+k}$ for $1 \leq k \leq 5$,

$c_{t+11} = ab^{r^s} = ab^3$, $a_{t+1} = ab^2$, $a_{t+2} = ab^9$, $a_{t+3} = ab^3$,

$a_{t+4} = ab^8$, $a_{t+5} = ab^{10}$, $a_{t+6} = ab$, $a_{t+7} = ab^4$,

$a_{t+8} = ab^7$, $a_{t+9} = ab^6$, $a_{t+10} = ab^5$ and $a_{t+11} = a$.

We have the following picture.



Now $\{i_k : 1 \le k \le 5\} = \{2,3,10,4,6\}$, $\{j_k : 1 \le k \le 5\} = \{9,8,1,7,5\}$ $\{i_k, j_k : 1 \le k \le 5\}$ is a reduced residue system modulo 11. Also, $\{\{i_k, j_k\} : 1 \le k \le 5\}$ is the patterned starter on Z_{11}.

Assuming the above conditions hold, we have the partial sequencing of the elements of $D_p \backslash Z_p$. In order to complete the sequencing, we have to order the elements of Z_p.

Obviously, the first part of the partial product starts at e, and ends at b^{r^s}. Suppose F is a choice function on the patterned starter of Z_p. Let F^* be a sequence of F with 0 as the first element. If $F^* = \{0 = f_0, f_1, f_2, \ldots, f_{(p-1)/2}\}$,

then for $0 \le i \le (p-1)/2 = t$, define $g(i) = \sum_{j=0}^{i} f_j$ and $c_i = b^{g(i)}$.

Suppose F^* has the property that $c_t = b^{r^s}$ and $\{e, c_1, \ldots, c_{t-1}\}$ is exactly the set of elements of Z_p that do not appear as partial products. That is, $\{c_1, c_2, \ldots, c_{t-1}\} \cap \{c_{t+2k} : 1 \le k \le (p-1)/2\} = \phi$. Then sequencing of F^* will match up with the middle part. Also we can use F^* to finish the remainder of D_p.

Let $-F^* = \{-f_{(p-1)/2}, \ldots, -f_2, -f_1\}$ and for $1 \le i \le (p-1)/2 = t$

define $h(i) = \sum_{j=t-(i-1)}^{t} -f_j$ and $c_{t+p+i} = ab^{r^s+h(i)}$ and $h(0) = 0$. The

elements of F^* and $-F^*$ give us all elements of Z_p as F is a choice function of the patterned starter. And for

$1 \le i \le (p-1)/2$, $g(t-i) = \sum_{j=0}^{t} f_j - f_{t-i+1} - f_{t-i+2} - \ldots - f_t = r^s + h(i)$.

Then we see that the c_{t+p+i}'s are exactly the elements of $D_p \backslash Z_p$ not appearing as c_{t+2k-1}, $1 \le k \le (p-1)/2$.

Again, suupose $p=11$, $r=7$, $n=1$, $c_t=b^3$, $F^*=\{0,7,5,1,3,9\}$, and $-F^*=\{2,8,10,6,4\}$. Then $c_0=b^0$, $c_1=b^7$, $c_2=b^1$, $c_3=b^2$, $c_4=b^5$, $c_5=b^3$ and $c_{16}=ab^3$, $c_{17}=ab^5$, $c_{18}=ab^2$, $c_{19}=ab^1$, $c_{20}=ab^7$, $c_{21}=a$.

The sequencing of D_{11} can be determined completed by giving p, r, n, c_t and F^*.

B.A. Anderson using the above method, found sequencings of D_5, D_{11}, D_{17}, and D_{23} by hand. We have

D_5: $p=5$, $r=3$, $n=1$, $c_t=b^3$ and $F^*=\{0,1,2\}$.

D_{11}: $p=11$, $r=7$, $n=1$, $c_t=b^3$ and $F^*=\{0,7,5,1,3,9\}$.

D_{17}: $p=17$, $r=11$, $n=1$, $c_t=b^3$ and $F^*=\{0,5,6,14,13,15,16,9,10\}$.

D_{23}: $p=23$, $r=15$, $n=1$, $c_t=b^3$ and $F^*=\{0,4,7,2,17,18,15,1,20,9,13,12\}$.

§3.2 Sequencings of non-abelian groups of order pq

Now, we consider the groups G of order pq, such that G is generated by a and b satisfying the relations $b^p=a^q=e$, $ab=ba^r$ where e is the identity, r is a positive integer, p, q are primes, $q\equiv 1 \pmod p$ and $r^p\equiv 1 \pmod q$.

Lawrence Wang used a computer to test for sequenceability for $n=6$, 10, and 21, for which the answers were known. He also succeeded in finding sequencings for $n=39$ ($p=3$, $q=13$, $r=13$), $n=55$ ($p=5$, $q=11$, $r=3$), and $n=57$ ($p=3$, $q=19$, $r=7$).

A.D. Keedwell found a sequencing for $G=\{a,b:a^9=b^3=e, ab=ba^4\}$ by trial and error. The sequencing is e, b^2a^6, ba, a^7, ba^7, b^2a^8, b^2a^7, a^4, b, b^2a^5, a, a^2, a^5, ba^2, ba^4, a^3, b^2a^2, b^2, b^2a^4, a^8, b^2a^3, ba^6, b^2a, ba^3, ba^8, ba^5, a^6 and the partial products are e, b^2a^6, b^2a^4, b^2, ba^6, ba^7, a^8, ba^3, ba^2, ba^5, ba^8, a, a^3, b, a^2, b^2a^2, b^2a^8, a^7, a^4, ba, b^2a, b^2a^3, ba^4, b^2a^5, a^5, a^6, b^2a^7.

J.Dénes and E. Török used computers to generate 15 sequencings of the group $G=\{a, b:b^3=a^7=e, ab=ba^2\}$. N.S. Mendelsohn succeeded in obtaining some sequencings of the non-abelian group G of order 21. Then the group $G=\langle a,b\rangle$ is a case of order pq such that $b^p=a^q=1$, $ab=ba^r$, $r^p\equiv 1 \pmod q$ where p and q are both prime and $q\equiv 1 \pmod p$. The following is the method Mendelsohn used to sequence the group G mentioned above with $p = 3$, $q = 7$.

Let S be a set of all transformations of the form $(x)T_{u,v}\equiv ux+v \pmod q$ where $u=1,2,\ldots,q-1$, and $v=0,1,2,\ldots,q-1$. Obviously, S is a group of order $(q-1)q$.

Let H be a set of transformations defined by $(x)T_{r^n,s} = r^nx+s$ where r is an integer $r^p\equiv 1 \pmod q$, $n=0,1,2,\ldots,p-1$, and $s=0,1,2,\ldots,q-1$. We see that H is a subgroup of S of order pq.

We represent the element $T_{r^n,s}$ of H by (n,s). Then

$$\begin{aligned}(x)(u,v)(g,h) &= (x)T_{r^u,v}T_{r^g,h}\\ &= (r^ux+v)T_{r^g,h}\\ &= r^g(r^ux+v)+h\\ &= r^{u+g}x+vr^g+h\\ &= (u+g,vr^g+h).\end{aligned}$$

The rule of multiplication of any two elements of H is $(u,v)(g,h) = (u+g,vr^g+h)$.

Define a mapping $\Phi G \to S$ by $\Phi(a^u b^v) = (u,v)$ for any $a^u b^v$ in G. It is clear that it is one-one and onto. Let $a^u b^v$ and $a^g b^h$ in G. Then

$$\begin{aligned}\Phi(a^u b^v a^g b^h) &= \Phi(a^{u+g} b^{vr^g+h}) \\ &= (u+g, vr^g+h) \\ &= (u,v)(g,h) \\ &= \Phi(a^u b^v)\Phi(a^g b^h) \text{ and}\end{aligned}$$

then Φ is an isomorphism.

Therefore if we can find a sequencing of S, it is the same as finding a sequencing of G. In order to get a sequencing of S, we arrange the first elements of the ordered-pair (u,v), so that 0,1,2,...,p-1, each appears q times and the differences of successive pairs also appear q times. We do the same thing to the second elements of the ordered pairs. However, it is not easy to arrange the second elements. Since we know that T is a sequencing of G if and only if $\Phi(T)$ is a sequencing of G where Φ is an automorphism of G, we can use the automorphism group of S to reduce the number of possible sequences to be considered. For the case of p=3, q=7, Mendelsohn obtained five sequencings heuristically. They are all listed in the following table.

I	G	II	III	IV	V
(0,0)	b^0a^0	(0,0)	(0,0)	(0,0)	(0,0)
(1,0)	b^1a^0	(0,1)	(0,1)	(0,3)	(0,3)
(1,1)	b^1a^1	(1,2)	(1,2)	(1,6)	(1,6)
(0,4)	b^0a^4	(2,6)	(2,6)	(1,0)	(1,0)
(1,3)	b^1a^3	(1,3)	(1,3)	(2,2)	(2,2)
(0,2)	b^0a^2	(0,2)	(0,2)	(1,1)	(1,1)
(2,2)	b^2a^2	(0,4)	(0,4)	(0,1)	(0,1)
(2,4)	b^2a^4	(1,5)	(1,5)	(2,5)	(2,5)
(0,5)	b^0a^5	(1,1)	(1,1)	(2,0)	(2,0)
(0,1)	b^0a^1	(0,5)	(0,5)	(0,4)	(0,4)
(2,6)	b^2a^6	(2,4)	(1,4)	(1,2)	(2,4)
(2,5)	b^2a^5	(2,1)	(2,0)	(0,6)	(1,5)
(2,3)	b^2a^3	(1,0)	(0,3)	(1,4)	(1,3)
(1,4)	b^1a^4	(1,6)	(2,1)	(1,3)	(1,2)
(2,0)	b^2a^0	(2,3)	(2,5)	(2,4)	(2,3)
(1,5)	b^1a^5	(1,4)	(2,4)	(1,5)	(1,4)
(2,1)	b^2a^1	(2,2)	(2,2)	(2,5)	(2,6)
(0,3)	b^0a^3	(0,3)	(1,6)	(2,1)	(0,6)
(1,2)	b^1a^2	(2,0)	(2,3)	(2,6)	(2,1)
(1,6)	b^1a^6	(2,5)	(1,0)	(2,3)	(0,5)
(0,6)	b^0a^6	(0,6)	(0,6)	(0,2)	(0,2)

A.D. Keedwell has shown that for an odd prime p with 2 as a primitive root and for another odd prime q of the form q=2ph+1, then the group of order pq is sequenceable. In particular, all non-abelian groups of order 3q except D_3, and all non-abelian groups of orders 5q, 11q, and 13q are sequenceable.

The method that A.D. Keedwell used to show the sequencings exist is by making use of the property that the image under the natural homomorphism $\Phi:G\to G/H$ of a sequencing of G is a quotient sequencing of G. He claimed a particular sequence is a quotient sequencing of the group G of order pq with 2 as a primitive root of GF[p] and then he constructed a sequencing of the group for which the above sequencing is the quotient sequencing under the mapping $\Phi:G\to G/H$. He first solved the case with p=3 and then generalized to all odd primes p.

Definition 3.8 : A group G of order n is said to have a near-sequencing if its elements can be arranged in a sequence $a_0=e$, a_1, a_2, ..., a_{n-1} in such a way that the partial products $a_0=e$, a_0a_1, $a_0a_1a_2$, ..., $a_0a_1a_2\ldots a_{n-2}$ are all distinct and the product $a_0a_1a_2\ldots a_{n-1}=e$.

Lemma 3.4 : If q is an odd prime, then the cyclic group $(Z_q,+)$ possesses near-sequencings.

Proof : Let $(Z_q,+)$ be the additive group of the field GF[q]. Let r be a primitive root of GF[q]. We claim that the sequence $0, r^h-r^{h-1}, r^{h+1}-r^h, \ldots, r^{q-2}-r^{q-3}, 1-r^{q-2}, r-1, \ldots, r^{h-1}-r^{h-2}$ is a near-sequencing of $(Z_q,+)$. They are all distinct. Each non-zero element is of the form $r^i(r-1)$, $1\leq i\leq q-1$. If there exist i and j such that $r^i(r-1)\equiv r^j(r-1) \pmod q$, then $r^{1-j}\equiv 1 \pmod q$. This is impossible for the range of i, unless i=j. The partial sums of the sequence are $0, r^h-r^{h-1}, r^{h+1}-r^{h-1}, \ldots, r^{q-2}-r^{h-1}, 1-r^{h-1}, r-r^{2-1}, \ldots, r^{h-2}-r^{h-1}, 0$. They are all distinct except the first and the last one because all non-zero elements are of the form r^i-r^{h-1} and $1\leq i\leq q-1$ and $i\neq h-1$. Also note that the element which does not occur as a partial sum is $-r^{h-1}$. □

Let the image of the natural homomorphism $\Phi:G\rightarrow G/H$ be $\{1,x,x^2,\ldots,x^{p-1}\}$ where $H=\{a:a^q\}=e$. We are going to produce a quotient sequencing for the construction of the sequencing of G.

Lemma 3.5 : Let p be an odd prime such that 2 is a primitive root of the Galois field GF[p]. Then the non-abelian group of order pq where q is an odd prime greater than p has a quotient sequencing.

Proof : We know that q=2ph+1 for some integer h. Let t be an element in GF[q] satisfying the condition $2t\equiv 1 \pmod p$. Then $(2t)^i\equiv 2^i t^i \equiv 1 \pmod p$. If $t^i\equiv 1 \pmod p$, then $2^i\equiv 1 \pmod p$. That is, $2^i - t^i \equiv 0 \pmod p$ which implies t is also a primitive root of GF[p].

We show the following sequence is a quotient sequencing.

(i) A sequence of 2ph 1's followed by x, followed by a sequence of 2ph-1, copies of the sequence x^{t-1}, x^{t^2-t}, $x^{t^3-t^2}$, ..., $x^{t^{p-2}-t^{p-3}}$, $x^{1-t^{p-2}}$, followed by x^{t-1}, x^{t^2-1}, $x^{t^3-t^2}$, ..., $x^{t^{p-2}-t^{p-3}}$, 1, x^2, x^4, ..., $x^{2^{p-2}}$, $x^{1-t^{p-2}}$ where all indices are computed modulo p.

(ii) The partial products are 2ph 1's followed by a sequence of 2ph-1, copies of the sequence x, x^t, x^{t^2}, x^{t^3}, ..., $x^{t^{p-2}}$ followed by the sequence x, x^t, x^{t^2}, ..., $x^{t^{p-1}}$, $x^{t^{p-2}}$, $x^{t^{p-2}}$, $x^{t^{p-3}}$, $x^{t^{p-4}}$, ..., x^{t^2}, x^t, x, 1. This arises from the fact that $2t\equiv 1 \pmod p$ implies $2^{p-2}t^{p-2}\equiv 1 \pmod p$ so that $t^{p-2}\equiv 2 \pmod p$.

For (i), observe that $t-1$, t^2-t, ..., $t^{p-2}-t^{p-3}$, $t^{1-t^{p-2}}$ are all distinct. The reason is similar to that used in Lemma 3.4. Also, $2\equiv t^{p-1}$, $2^2\equiv t^{p-2}$, ..., $2^{p-2}\equiv 1 \pmod p$ are also distinct.

For (ii), we note that $1 \equiv t^{p-1}, t, t^2, \ldots, t^{p-2}$ are all distinct non-zero elements of GF[p] as t is a primitive root of GF[p]. Therefore, the sequencing (i) is a quotient sequencing for 1 and each distinct power of x occurs exactly $2ph+1=q$ times in both sequences (i) and (ii). □

Now we are going to show that for the case $p=3$, the group G of order 3q has a sequencing.

<u>Theorem 3.6</u> : Let $G = \{a, b : a^q = b^3 = e, ab = ba^s\}$ be a non-abelian group of order 3q, where $s^p \equiv 1 \pmod q$ and 2 be a primitive root of GF[p]. Then G is sequenceable.

<u>Proof</u> :We are going to show the following ordering of G is a sequencing of G.

	Quotient Sequencing	Sequencing	Partial Products
	1	e	e
	1	$a^{r^h-r^{h-1}}$	$a^{r^h-r^{h-1}}$
2ph times	1	$a^{r^{h+1}-r^h}$	$a^{r^{h+1}-r^{h-1}}$
	.		
	.		
	.		
	.		
	1	$a^{r^{h-2}-r^{h-3}}$	$a^{r^{h-2}-r^{h-1}}$
	x	ba^{α}	$ba^{(r^{h-2}-r^{h-1})s+\alpha}$

$$\begin{array}{lll}
x & ba^{\alpha_1} & b^2a^{(r^{h-2}-r^{h-1})s^2+\alpha s+\alpha_1} \\[1ex]
x^2 & b^2a^{\beta_1} & ba^{(r^{h-2}-r^{h-1})s+\alpha+(\alpha_1 s^2+\beta_1)} \\[1ex]
x & ba^{\alpha_2} & b^2a^{(r^{h-2}-r^{h-1})s^2+\alpha s+\alpha_1+(\beta_1 s+\alpha_2)} \\[1ex]
x^2 & b^2a^{\beta_2} & ba^{(r^{h-2}-r^{h-1})s+\alpha+(\alpha_1 s^2+\beta_1)+(\alpha_2 s^2+\beta_2)} \\[1ex]
x & ba^{\alpha_3} & b^2a^{(r^{h-2}-r^{h-1})s^2+\alpha s+\alpha_1+(\beta_1 s+\alpha_2)+(\beta_2 s+\alpha_3)} \\
\cdot & & \\
\cdot & & \\
\cdot & & \\
\cdot & & \\
x^2 & b^2a^{\beta_{q-2}} & ba^{(r^{h-2}-r^{h-1})s+\alpha+\sum_{i=1}^{q-2}(\alpha_i s^2+\beta_i)} \\[1ex]
x & ba^{\alpha_{q-1}} & b^2a^{(r^{h-2}-r^{h-1})s^2+\alpha s+\alpha_1+\sum_{i=1}^{q-2}(\beta_i s+\alpha_{i+1})} \\[1ex]
1 & a^{\mu} & b^2a^{(r^{h-2}-r^{h-1})s^2+\alpha s+\alpha_1+\mu+\sum_{i=1}^{q-2}(\beta_i s+\alpha_{i+1})} \\[1ex]
x^2 & b^2a^{\beta_{q-1}} & ba^{(r^{h-2}-r^{h-1})s+\alpha+\beta_{q-1}+(\alpha_{q-1}+\mu)s^2+\sum_{i=1}^{q-2}(\alpha_i s^2+\beta_i)} \\[1ex]
x^2 & b^2a^{\beta_q} & a^{(r^{h-2}-r^{h-1})+(\alpha+\beta_{q-1})s^2+(\alpha_{q-1}+\mu)s+\beta_q+\sum_{i=1}^{q-2}(\alpha_i s+\beta_i s^2)}
\end{array}$$

If the ordering described above is a sequencing, the following conditions have to be satisfied:

(i) The elements $\alpha, \alpha_1, \ldots, \alpha_{q-1}$ must be all distinct.

(ii) The elements $\beta_1, \beta_2, \ldots, \beta_q$ must be all distinct.

(iii) $\mu = r^{h-1}-r^{h-2}$.

(iv) The elements 0, $\alpha_1 s^2+\beta_1$, $(\alpha_1 s^2+\beta_1)+(\alpha_2 s^2+\beta_2)$, ...

$$\ldots, \sum_{i=1}^{q-2}(\alpha_i s^2+\beta_i),\ (\alpha_{q-1}+\mu)s^2+\beta_{q-1}+\sum_{i=1}^{q-2}(\alpha_i s^2+\beta_i)$$

are all distinct.

(v) The elements 0, $\beta_1 s+\alpha_2$, $(\beta_1 s+\alpha_2)+(\beta_2 s+\alpha_3)$, ...

$$\ldots, \sum_{i=1}^{q-2}(\beta_i s+\alpha_{i+1}),\ \mu+\sum_{i=1}^{q-2}(\beta_i s+\alpha_{i+1})$$ are all distinct.

(vi) $$(r^{h-2}-r^{h-1})+(\alpha+\beta_{q-1})s^2+(\alpha_{q-1}+\mu)s+\beta_q+\sum_{i=1}^{q-2}(\alpha_i s+\beta_i s^2)$$

$= -r^{h-1}$ for $-r^{h-1}$ is the element which differs from

e, $a^{r^h-r^{h-1}}$, $a^{r^{h+1}-r^{h-1}}$, ..., $a^{r^{h-2}-r^{h-1}}$, and

(vii) $s^2+s+1 \equiv 0 \pmod{q}$ for $s^3 \equiv 1 \pmod{q}$ implies $(s-1)(s^2+s+1) \equiv 0 \pmod{q}$ which implies $(s^2+s+1) \equiv 0 \pmod{q}$ as $s \neq 1$.

Let t be a primitive root of GF[q] and let the following hold: $\alpha_1 s^2+\beta_1 = t^l-t^{l-1}$,

$$\alpha_2 s^2+\beta_2 = t(t^l-t^{l-1}) = t^{l+1}-t^l,$$

$$\vdots$$

$$\alpha_{q-2}s^2+\beta_{q-2} = t^{q-3}(t^l-t^{l-1}) = t^{q-3+l}-t^{q-4+l} = t^{l-2}-t^{l-3},$$

and $(\alpha_{q-1}+\mu)2 + \beta_{q-1} = -t^{l-2}$.

Then $0 = 0$,

$$\alpha_1 s^2+\beta_1 = t^l - t^{l-1},$$

$$(\alpha_1 s^2+\beta_1)+(\alpha_2 s^2+\beta_2) = t^{l+1}-t^{l-1},$$

$$(\alpha_1 s^2+\beta_1)+(\alpha_2 s^2+\beta_2)+(\alpha_3 s^2+\beta_3) = t^{l+2}-t^{l-1},$$

$$\vdots$$

$$\sum_{i=1}^{q-2}(\alpha_i s^2+\beta_i) = t^{l-2}-t^{l-1}, \text{ and}$$

$$(\alpha_{q-1}+\mu)s^2+\beta_{q-1}+\sum_{i=1}^{q-2}(\alpha_i s^2+\beta_i) = 0-t^{l-1}.$$

Obviously all these elements are different and condition (iv) is satisfied.

With the above assumption, we can have $\alpha_{i+1} = t\alpha_i$ and $\beta_{i+1} = t\beta_i$ for $i=1,2,...,q-3$. Hence $\alpha_{i+1} = t^i\alpha_1$ and $\beta_{i+1} = t^i\beta_1$ for $i=1,2,...,q-3$.

In order to meet condition (i), we can choose $\alpha_{q-1} = t^{q-2}\alpha_1$ and $\alpha=0$. In order to meet condition (ii), we can let $\beta_{q-1}, \beta_q \in \{0, t^{q-2}\beta_1\}$ and $\beta_{q-1} \neq \beta_q$.

For condition (v), we let

$$\beta_1 s+\alpha_2 = t^u(t^l-t^{l-1}) = t^u(\alpha_1 s^2+\beta_1),$$

$$\beta_2 s+\alpha_3 = t^u(t^{l+1}-t^l) = t^u(\alpha_2 s^2+\beta_2),$$

$$\vdots$$

$$\beta_{q-2}s+\alpha_{q-1} = t^u(t^{l-2}-t^{l-3}) = t^u(\alpha_{q-1}s^2+\beta_{q-2}), \text{ and}$$

$$\mu = -t^{u+l-2}.$$

Then we have $0 = 0$,

$$\beta_1 s+\alpha_2 = t^u(t^l-t^{l-1}),$$

$$(\beta_1 s+\alpha_2)+(\beta_2 s+\alpha_3) = t^u(t^{l+1}-t^{l-1}),$$

$$(\beta_1 s+\alpha_2)+(\beta_2 s+\alpha_3)+(\beta_3 s+\alpha_4) = t^u(t^{l+2}-t^{l-1}),$$

$$\vdots$$

$$\sum_{i=1}^{q-2}(\beta_i s+\alpha_i+1) = t^u(t^{l-2}-t^{l-1}), \text{ and}$$

$$\mu+\sum_{i=1}^{q-2}(\beta_i s+\alpha_i+1) = -t^{u+l-1} = t^u(0-t^{l-1}).$$

They are all distinct elements of GF[q].

In order to have condition (vi) be satisfied, we must have $0 = r^{h-2}+(\alpha+\beta_{q-1}+\beta_1+\beta_2+\ldots+\beta_{q-2})s^2+(\mu+\alpha_1+\alpha_2+\ldots+\alpha_{q-1})s+\beta_q$. From (i), $\alpha_1,\alpha_2,\ldots,\alpha_{q-1}$ are all distinct modulo q so we have $\sum_{i=1}^{q-1}\alpha_i = [(q-1)/2]q \equiv 0 \pmod q$ and from (ii), $\beta_{q-1}+\beta_q+\beta_1+\beta_2+\ldots+\beta_{q-2} = [(q-2)/2]q \equiv 0 \pmod q$.

Therefore, we have $0 = r^{h-2}+(\alpha-\beta_q)s^2+\mu s+\beta_q$ with $\alpha=0$.

Now, we restate all the conditions:

To meet conditions (i), (ii) and (iv),

$$\alpha = 0,$$

$$\alpha_{i+1} = t^i\alpha_1 \text{ for } i=1,2,\ldots,q-2,$$

$$\beta_{i+1} = t^i\beta_1 \text{ for } i=1,2,\ldots,q-3,$$

$$\alpha_1s^2+\beta_1 = t^{l-1}(t-1), \text{ and}$$

$$(t^{q-2}\alpha_1+\mu)s^2+\beta_{q-1} = -t^{l-2} \text{ with}$$

$$\beta_{q-1},\ \beta_q \in \{0,t^{q-2}\beta_1\},\ \beta_{q-1} \neq \beta_q.$$

To meet conditions (iii) and (v),

$$\mu = r^{h-2}(r-1) = -t^{u+l-2} \text{ and}$$

$$\beta_1s+t\alpha_1 = t^u(\alpha_1s^2+\beta_1).$$

To meet condition (vi),

$$r^{h-2}+(\alpha-\beta_q)s^2+\mu s+\beta_q = 0 \text{ with } \alpha = 0.$$

From $\beta_1s+t\alpha_1 = t^u(\alpha_1s^2+\beta_1)$ we obtain

$$\beta_1(s-t^u) = \alpha_1(s^2t^u-t) \qquad \text{(a)}$$

From $\alpha_1 s^2+\beta_1 = t^{l-1}(t-1)$, we obtain

$$\alpha_1 = st^{l-1}(t-1)-s\beta_1. \qquad \text{(b)}$$

Substitute (b) into (a) and obtain

$$\beta_1(s-t^u) = [st^{l-1}(t-1)-s\beta_1](s^2t^u-t)$$

$$\beta_1 s-\beta_1 t^u = s^3t^{l-1}t^u(t-1)-\beta_1 t^u-st^l(t-1)+s\beta_1 t$$

$$\beta_1(s-st) = (s^2t^{l-1}t^u-t^l)(st-s)$$

$$\beta_1 = t^l-s^2t^{l-1}t^u$$

$$= t^{l-1}(t-s^2t^u). \qquad \text{(c)}$$

Substitute (c) into (b) and obtain

$$\alpha_1 = st^{l-1}(t-1)-st^{l-1}(t-s^2t^u)$$

$$= t^{l-1}(t^u-s).$$

Substitute $\alpha_1 = t^{l-1}(t^u-s)$ into the condition

$(t^{q-2}\alpha_1+\mu)s^2+\beta_{q-1} = -t^{l-2}$ yielding

$[t^{q-2}t^{l-1}(t^u-s)+\mu]s^2+\beta_{q-1} = -t^{l-2}$ which becomes

$[t^{l-2}(t^u-s)+\mu]s^2+\beta_{q-1} = -t^{l-2}$.

Multiply by s on both sides to produce $t^{u+l-2}+\mu+\beta_{q-1}s = 0$.

Then $\mu = -t^{u+l-2}$ if and only if $\beta_{q-1} = 0$.

Since β_{q-1}, $\beta_q \in \{0, t^{q-2}\beta_1\}$, then $\beta_q = t^{q-2}\beta_1$. The set of conditions reduces to

$$\alpha = 0,$$

$$\alpha_{i+1} = t^i \alpha_1 \text{ for } i = 1,2,\ldots,q-2,$$

$$\beta_{i+1} = t^i \beta_1 \text{ for } i = 1,2,\ldots,q-3,$$

$$\alpha_1 = t^{l-1}(t^u - s),$$

$$\beta_1 = t^{l-1}(t - s^2 t^u),$$

$$\beta_{q-1} = 0,$$

$$\beta_q = t^{q-2}\beta_1, \text{ and}$$

$$\mu = r^{h-2}(r-1) = -t^{u+l-2} \qquad \text{(A)}$$

$$r^{h-2} + \mu s + \beta_q(1-s^2) = 0. \qquad \text{(B)}$$

We know $\beta_q = t^{q-2}\beta_1$ which implies $\beta_q = t^{q-2}t^{l-1}(t-s^2t^u)$.

Now $\beta_1 = t^{l-1}(t-s^2t^u)$; $\mu = -t^{u+l-2}$. From (A) and (B) we obtain

$$-t^{u+l-2} + [\mu s + \beta_q(1-s^2)](r-1) = 0 \text{ or}$$

$$-t^{u+l-2} + [-t^{u+l-2}s + t^{q-2}t^{l-1}(t-s^2t^u)(1-s^2)](r-1) = 0.$$

Thus, $t^{l-1}(1-s^2t^{u-1})(1-s^2)(r-1) = t^{u+l-2}[1+s(r-1)]$

and $(1-s^2-s^2t^{u-1}+st^{u-1})(r-1) = [1+s(r-1)]t^{u-1}$

yielding $(1-s^2)(r-1) = (s^2r-s^2+1)t^{u-1}$ and

$$s^2(s-1)(r-1) = s^2(r-1+s)t^{u-1}.$$

We obtain $t^{u-1} \equiv [(s-1)(r-1)]/(r+s-1) \pmod{q}$. Since $\alpha_1 \neq 0$, $\beta_1 \neq 0$. Then from the equations for α_1 and β_1, we have $t^u \neq s$, $t^{u-1} \neq s$. Note that $t^{u-1} \neq s$ implies $s \neq (s-1)(r-1)(r-1+s)^{-1}$, $s(r-1+s) \neq (s-1)(r-1)$, and $r \neq s+2$.

Now, we can construct a sequencing as follows for a non-abelian group of order 3q, q prime and $q = 6k+1$. We choose a quadratic root of $s^2+s+1 \equiv 0 \pmod{q}$ and a primitive root r of GF[q] such that $r \neq s+2$ and $r \neq 1-s$. It is possible if $q > 7$ and $\Phi(q-1) > 2$. Otherwise, $t^{u-1} \equiv [(s-1)(r-1)]/(r+s-1) \pmod{q}$ is not finite or equal s. We choose another primitive root t of GF[q] such that $t^u \neq s$ and then calculate

$$\alpha_1 = (t^u-s)t^{l-1},\ \beta_1 = (t-s^2t^u)t^{l-1},\ \beta_q = t^{q-2}\beta_1,$$

$$\beta_{q-1} = \alpha = 0,\ r^{h-2} = -t^{u-1}(r-1)^{-1}t^{l-1},\ \text{and } \mu = r^{h-2}(r-1).$$

We choose t^{l-1} arbitrarily, and compute both $\alpha_{i+1} = t^i\alpha_1$ and $\beta_{i+1} = t^i\beta_1$. We substitute these values into the sequence. A sequencing of the non-abelian group of order 3q, q an odd prime is obtained. □

We are going to use the case $p = 3$ as a guideline to find a sequencing of the non-abelian group of order pq.

Lemma 3.7 : Let p be a prime with 2 as a primitive root of GF[p] and $2\sigma \equiv 1 \pmod{p}$. Then $\sigma^{p-r} \equiv 2^{r-1}$, $1-\sigma^{p-2} \equiv -1$ and more generally $\sigma^{p-r}-\sigma^{p-r-1} \equiv -\sigma^{p-r} \pmod{p}$.

Proof : Since $2\sigma \equiv 1 \pmod{p}$, then $(2\sigma)^{p-r} \equiv 1 \pmod{p}$ which implies

$$\begin{aligned}\sigma^{p-r} &\equiv 2^{r-p} \pmod{p}\\ &\equiv 2^{r}2^{-p} \pmod{p}\\ &\equiv 2^{r-1} \pmod{p}.\end{aligned}$$

Also, $2\sigma \equiv 1 \pmod{p}$ implies $2^{p-1}\sigma^{p-2} \equiv 2 \pmod{p}$ which is equivalent to $\sigma^{p-2} \equiv 2 \pmod{p}$. Then we have $1-\sigma^{p-2} \equiv -1 \pmod{p}$. Now $2\sigma \equiv 1 \pmod{p}$ is equivalent to $2^{p-r}\sigma^{p-r} \equiv 1 \pmod{p}$ if and only if $\sigma^{p-r} \equiv 2^{r-p} \pmod{p}$.

Similarly $\sigma^{p-r-1} \equiv 2^{r+1-p} \pmod{p}$. Then

$$\begin{aligned}\sigma^{p-r}-\sigma^{p-r-1} &\equiv 2^{r-p}(1-2)\\ &\equiv -2^{r-p}\\ &\equiv -\sigma^{p-r} \pmod{p}. \ \square\end{aligned}$$

We make use of the above lemma and the fact that if p is an odd prime such that 2 is a primitive root of the Galois field GF[p], then the non-abelian group of order pq, where q is any odd prime greater than p, has a quotient sequencing, which we have shown before, to seek a sequencing of the non-abelian group of order pq.

Theorem 3.8[12] : Let p be an odd prime which has 2 as a primitive root and let q be another odd prime of the form q=2ph+1. Then the non-abelian group of order pq is sequenceable.

Proof : For the case of p = 3, it was shown previously. Using the case p = 3 as a guideline, we are going to construct a sequencing of the non-abelian group which is of the form

$e,\ a^{r^h-r^{h-1}},\ a^{r^{h+1}-r^h},\ a^{r^{h+2}-r^{h+1}},\ \ldots,\ a^{r^{h-2}-r^{h-3}},\ b,$

$b^{\sigma-1}a^{\alpha_1^{(1)}},\ b^{\sigma^2-\sigma}a^{\alpha_1^{(2)}},\ b^{\sigma^3-\sigma^2}a^{\alpha_1^{(3)}},\ \ldots,\ b^{\sigma^{p-2}-\sigma^{p-3}}a^{\alpha_1^{(p-2)}},$

$b^{1-\sigma^{p-2}}a^{\alpha_1^{(p-1)}},\ b^{\sigma-1}a^{\alpha_2^{(1)}},\ b^{\sigma^2-\sigma}a^{\alpha_2^{(2)}},\ \ldots,\ b^{1-\sigma^{p-2}}a^{\alpha_2^{(p-1)}},$

$b^{\sigma-1}a^{\alpha_3^{(1)}},\ b^{\sigma^2-\sigma}a^{\alpha_3^{(2)}},\ \ldots,\ b^{\sigma^{p-2}-\sigma^{p-3}}a^{\alpha_{q-1}^{(p-2)}},\ a^{\mu},\ b^{\sigma^{p-2}},$

$b^{\sigma^{p-3}},\ b^{\sigma^{p-4}},\ \ldots,\ b^{\sigma},\ b^{-1}a^{\alpha_{q-1}^{(p-1)}}$, where $\mu = r^{h-1}-r^{h-2}$, σ is an element of G such that $2\sigma \equiv 1 \pmod p$.

This sequencing gives rise to the partial products which are listed in the following. We represent the element $b^v a^w$ by the ordered pair v, w and s is one of the roots or the congruence $s^p \equiv 1 \pmod q$. They are listed below.

v, w

$(0,\quad 0)$

$(0,\quad r^h-r^{h-1})$

$(0,\quad r^{h+2}-r^{h-1})$

.
.
.
.

$\vdots$

$$(\ 0,\qquad r^{h-2}-r^{h-1} = r^{*}\ )$$

$$(\ 1,\qquad r^{*}s\ )$$

$$(\ \sigma,\qquad r^{*}s^{\sigma}+\alpha_{1}^{(1)}\ )$$

$$(\ \sigma^{2},\qquad r^{*}s^{\sigma^{2}}+\alpha_{1}^{(1)}s^{\sigma^{2}-\sigma}+\alpha_{1}^{(2)}\ )$$

$$(\ \sigma^{3},\qquad r^{*}s^{\sigma^{3}}+\alpha_{1}^{(1)}s^{\sigma^{3}-\sigma}+\alpha_{1}^{(2)}s^{\sigma^{3}-\sigma^{2}}+\alpha_{1}^{(3)}\ )$$

$\vdots$

$$(\ \sigma^{p-2},\qquad r^{*}s^{\sigma^{p-2}}+\alpha_{1}^{(1)}s^{\sigma^{p-2}-\sigma}+\alpha_{1}^{(2)}s^{\sigma^{p-2}-\sigma^{2}}+\ldots+$$

$$\alpha_{1}^{(p-3)}s^{\sigma^{p-2}-\sigma^{p-3}}+\alpha_{1}^{(p-2)}\ )$$

$$(\ 1,\qquad r^{*}s+(\alpha_{1}^{(1)}s^{1-\sigma}+\alpha_{1}^{(2)}s^{1-\sigma^{2}}+\ldots+\alpha_{1}^{(p-2)}s^{1-\sigma^{p-2}}+\alpha_{1}^{(p-1)})\ )$$

$$(\ \sigma,\qquad r^{*}s^{\sigma}+\alpha_{1}^{(1)}+(\alpha_{1}^{(2)}s^{\sigma-\sigma^{2}}+\alpha_{1}^{(3)}s^{\sigma-\sigma^{3}}+\ldots+\alpha_{1}^{(p-1)}s^{\sigma-1}+\alpha_{2}^{(1)})\ )$$

$$(\ \sigma^{2},\qquad r^{*}s^{\sigma^{2}}+\alpha_{1}^{(1)}s^{\sigma^{2}-\sigma}+\alpha_{1}^{(2)}+(\alpha_{1}^{(3)}s^{\sigma^{2}-\sigma^{3}}+\ldots+\alpha_{1}^{(p-1)}s^{\sigma^{2}-1}+$$

$$\alpha_{2}^{(1)}s^{\sigma^{2}-\sigma}+\alpha_{2}^{(2)})\ )$$

$\vdots$

$$\vdots$$

$$\left(\sigma^{p-2}, \quad r^{*} s^{\sigma^{p-2}} + \alpha_1^{(1)} s^{\sigma^{p-2}-\sigma} + \alpha_1^{(2)} s^{\sigma^{p-2}-\sigma^{2}} + \ldots + \alpha_1^{(p-3)} s^{\sigma^{p-2}-\sigma^{p-3}} \right.$$

$$\left. + \ \alpha_1^{(p-2)} + \sum_{i=1}^{q-3} E_i^{(p-2)} \right)$$

$$\left(1, \quad r^{*} s + \sum_{i=1}^{q-2} E_i^{(0)} \right)$$

$$\left(\sigma, \quad r^{*} s^{\sigma} + \alpha_1^{(1)} + \sum_{i=1}^{q-2} E_i^{(1)} \right)$$

$$\left(\sigma^{2}, \quad r^{*} s^{\sigma^{2}} + \alpha_1^{(1)} s^{\sigma^{2}-\sigma} + \alpha_1^{(2)} + \sum_{i=1}^{q-2} E_i^{(2)} \right)$$

$$\vdots$$

$$\left(\sigma^{p-2}, \quad r^{*} s^{\sigma^{p-2}} + \alpha_1^{(1)} s^{\sigma^{p-2}-\sigma} + \ldots + \alpha_1^{(p-3)} s^{\sigma^{p-2}-\sigma^{p-3}} \right.$$

$$\left. + \ \alpha_1^{(p-2)} + \sum_{i=1}^{q-2} E_i^{(p-2)} \right)$$

$$\left(\sigma^{p-2}, \quad r^{*} s^{\sigma^{p-2}} + \alpha_1^{(1)} s^{\sigma^{p-2}-\sigma} + \ldots + \alpha_1^{(p-3)} s^{\sigma^{p-2}-\sigma^{p-3}} \right.$$

$$\left. + \ \alpha_1^{(p-2)} + \sum_{i=1}^{q-2} E_i^{(p-2)} + \mu \right)$$

$$\left(\sigma^{p-3}, \quad r^{*} s^{\sigma^{p-3}} + \alpha_1^{(1)} s^{\sigma^{p-3}-\sigma} + \ldots + \alpha_1^{(p-4)} s^{\sigma^{p-3}-\sigma^{p-4}} \right.$$

$$\left. + \ \alpha_1^{(p-3)} + \sum_{i=1}^{q-2} E_i^{(p-3)} + (\alpha_{q-1}^{(p-2)} + \mu) s^{\sigma^{p-2}} \right)$$

$$(\sigma^{p-4}, \quad r^{*}s^{\sigma^{p-4}}+\alpha_{1}^{(1)}s^{\sigma^{p-4}-\sigma}+\ldots+\alpha_{1}^{(p-5)}s^{\sigma^{p-4}-\sigma^{p-5}}+\alpha_{1}^{(p-4)}$$

$$+\sum_{i=1}^{q-2}E_{i}^{(p-4)}+(\alpha_{q-1}^{(p-2)}+\mu)s^{\sigma^{p-2}+\sigma^{p-3}}+\alpha_{q-1}^{(p-3)}s^{\sigma^{p-3}} \quad)$$

$$\vdots$$

$$(1, \quad r^{*}s+\sum_{i=1}^{q-2}E_{i}^{(0)}+(\alpha_{q-1}^{(p-2)}+\mu)s^{\sigma^{p-2}+\sigma^{p-3}+\ldots+\sigma^{2}+\sigma}+$$

$$+\ \alpha_{q-1}^{(p-3)}s^{\sigma^{p-3}+\sigma^{p-4}+\ldots+\sigma^{2}+\sigma}+\ldots+\alpha_{q-1}^{(2)}s^{\sigma^{2}+\sigma}+\alpha_{q-1}^{(1)}s^{\sigma}$$

$$= r^{*}s+\sum_{i=1}^{q-2}E_{i}^{(0)}+(\alpha_{q-1}^{(p-2)}+\mu)s^{1-\sigma^{p-2}}+\alpha_{q-1}^{(p-3)}s^{1-\sigma^{p-3}}+\ldots$$

$$\ldots+\alpha_{q-1}^{(2)}s^{1-\sigma^{2}}+\alpha_{q-1}^{(1)}s^{1-\sigma} \quad)$$

$$(0, \quad r^{*}+\sum_{i=1}^{q-1}(\alpha_{i}^{(1)}s^{-\sigma}+\alpha_{i}^{(2)}s^{-\sigma^{2}}+\ldots+\alpha_{i}^{(p-2)}s^{-\sigma^{p-2}}+\alpha_{i}^{(p-1)}s^{-\sigma^{p-1}} \quad)$$

$$+\ \alpha_{q-1}^{(p-1)}(1-s^{-\sigma^{p-1}})+\mu s^{-\sigma^{p-2}} \quad)$$

where $E_{i}^{(0)} = \alpha_{i}^{(1)}s^{1-\sigma}+\alpha_{i}^{(2)}s^{1-\sigma^{2}}+\alpha_{i}^{(3)}s^{1-\sigma^{3}}+\ldots+\alpha_{i}^{(p-2)}s^{1-\sigma^{p-2}}$

$$+\alpha_{i}^{(p-1)} = (t^{l}-t^{l-1})t^{i-1},$$

$$E_{i}^{(1)} = \alpha_{i}^{(2)}s^{\sigma-\sigma^{2}}+\alpha_{i}^{(3)}s^{\sigma-\sigma^{3}}+\alpha_{i}^{(4)}s^{\sigma-\sigma^{4}}+\ldots$$

$$\ldots+\alpha_{i}^{(p-1)}s^{\sigma-1}+\alpha_{i+1}^{(3)} = t^{u_{1}}(t^{l}-t^{l-1})t^{i-1},$$

$$E_i^{(2)} = \alpha_i^{(3)} s^{\sigma^2-\sigma^3} + \alpha_i^{(4)} s^{\sigma^2-\sigma^4} + \alpha_i^{(5)} s^{\sigma^2-\sigma^5} + \dots$$

$$\dots + \alpha_{i+1}^{(1)} s^{\sigma^2-\sigma} + \alpha_{i+1}^{(2)} = t^{u_2}(t^l - t^{l-1})t^{i-1}, \text{ and}$$

$$\vdots$$

$$E_i^{(p-2)} = \alpha_i^{(p-1)} s^{\sigma^{p-2}-1} + \alpha_{i+1}^{(1)} s^{\sigma^{p-2}-\sigma} + \alpha_{i+1}^{(2)} s^{\sigma^{p-2}-\sigma^2}$$

$$+ \dots + \alpha_{i+1}^{(p-3)} s^{\sigma^{p-2}-\sigma^{p-3}} + \alpha_{i+1}^{(p-2)}$$

$$= t^{u_{p-2}}(t^l - t^{l-1})t^{i-1}.$$

We also let $\alpha_{i+1}^{(j)} = t\alpha_i^{(j)}$ for $i=1,2,\dots,q-2$ and $j=1,2,\dots,p-1$. From all the equalities above we obtain

$$E_1^{(1)} - E_1^{(0)} s^{\sigma-1} = \alpha_2^{(1)} - \alpha_1^{(1)} = (t^{u_1} - s^{\sigma-1})(t^l - t^{l-1}),$$

$$E_1^{(2)} - E_1^{(1)} s^{\sigma^2-\sigma} = \alpha_2^{(2)} - \alpha_1^{(2)} = (t^{u_2} - t^{u_1} s^{\sigma^2-\sigma})(t^l - t^{l-1}),$$

$$\vdots$$

$$E_1^{(p-2)} - E_1^{(p-3)} s^{\sigma^{p-2}-\sigma^{p-3}} = \alpha_2^{(p-2)} - \alpha_1^{(p-2)}$$

$$= (t^{u_{p-2}} - t^{u_{p-3}} s^{\sigma^{p-2}-\sigma^{p-3}})(t^l - t^{l-1}), \text{ and}$$

$$tE_1^{(0)} - E_1^{(p-2)} s^{1-\sigma^{p-2}} = t\alpha_1^{(p-1)} - \alpha_1^{(p-1)}$$

$$= (t - t^{u_{p-2}} s^{1-\sigma^{p-2}})(t^l - t^{l-1}).$$

Then $\alpha_1^{(1)} = t^{l-1}(t^{u_1} - s^{\sigma-1})$,

$$\alpha_1^{(2)} = t^{l-1}(t^{u_2} - t^{u_1} s^{\sigma^2-\sigma}),$$

$$\alpha_1^{(3)} = t^{l-1}(t^{u_3} - t^{u_2} s^{\sigma^3-\sigma^2}),$$

$$\vdots$$

$$\alpha_1^{(p-2)} = t^{l-1}(t^{u_{p-2}} - t^{u_{p-3}} s^{\sigma^{p-2}-\sigma^{p-3}}), \text{ and}$$

$$\alpha_1^{(p-1)} = t^{l-1}(t - t^{u_{p-2}} s^{1-\sigma^{p-2}}).$$

We are going to check that all the partial products of the form $b^{\sigma^j} a^{\beta_i^{(j)}}$ are different.

Case $j = p-2$, $b^{\sigma^{p-2}} a^{\beta_i^{(p-2)}}$:

$$\beta_1^{(p-2)} = r^* s^{\sigma^{p-2}} + \alpha_1^{(1)} s^{\sigma^{p-2}-\sigma} + \alpha_1^{(2)} s^{\sigma^{p-2}-\sigma^2} + \ldots$$

$$\ldots + \alpha_1^{(p-3)} s^{\sigma^{p-2}-\sigma^{p-3}} + \alpha_1^{(p-2)},$$

$$\beta_2^{(p-2)} = \beta_1^{(p-2)} + E_1^{(p-2)},$$

$$\beta_3^{(p-2)} = \beta_1^{(p-2)} + E_1^{(p-2)} + E_2^{(p-2)},$$

$$\vdots$$

$$\vdots$$

$$\beta_{q-1}^{(p-2)} = \beta_1^{(p-2)} + \sum_{i=1}^{q-2} E_i^{(p-2)}, \text{ and}$$

$$\beta_q^{(p-2)} = \beta_1^{(p-2)} + \sum_{i=1}^{q-2} E_i^{(p-2)} + \mu.$$

We notice that

$$E_1^{(p-2)} = t^{u_{p-2}}(t^{l} - t^{l-1}),$$

$$E_1^{(p-2)} + E_2^{(p-2)} = t^{u_{p-2}}(t^{l+1} - t^{l-1}),$$

$$\vdots$$

$$\sum_{i=1}^{q-2} E_i^{(p-2)} = t^{u_{p-2}}(t^{l-2} - t^{l-1}), \text{ and}$$

$$\sum_{i=1}^{q-2} E_i^{(p-2)} + \mu = t^{u_{p-2}}(-t^{l-1}), \text{ provided that } \mu = t^{u_{p-2}}(-t^{l-2}),$$

and 0 are all different. Then $b^{\sigma^{p-2}}a^{\beta_i^{(p-2)}}$ are all distinct.

Case $j = p-3$, $b^{\sigma^{p-3}}a^{\beta_i^{(p-3)}}$:

$$\beta_1^{(p-3)} = r^* s^{\sigma^{p-3}} + \alpha_1^{(1)} s^{\sigma^{p-3}-\sigma} + \alpha_1^{(2)} s^{\sigma^{p-3}-\sigma^2} + \ldots + \alpha_1^{(p-3)},$$

$$\beta_2^{(p-3)} = \beta_1^{(p-3)} + E_1^{(p-3)},$$

$$\beta_3^{(p-3)} = \beta_1^{(p-3)} + E_1^{(p-3)} + E_2^{(p-3)},$$

$$\vdots$$

$$\beta_{q-1}^{(p-3)} = \beta_1^{(p-3)} + \sum_{i=1}^{q-2} E_i^{(p-3)}, \text{ and}$$

$$\beta_q^{(p-3)} = \beta_1^{(p-3)} + \sum_{i=1}^{q-2} E_i^{(p-3)} + (\alpha_{q-1}^{(p-2)} + \mu)s^{\sigma^{p-2}}.$$

We notice that

$$E_1^{(p-3)} = t^{u_{p-3}}(t^{l} - t^{l-1}),$$

$$E_1^{(p-3)} + E_2^{u(p-3)} = t^{u_{p-3}}(t^{l+1} - t^{l-1}),$$

$$\vdots$$

$$\sum_{i=1}^{q-2} E_i^{(p-3)} = t^{u_{p-3}}(t^{l-2} - t^{l-1}), \text{ and}$$

$$\sum_{i=1}^{q-2} E_i^{(p-3)} + (\alpha_{q-1}^{(p-2)} + \mu)s^{\sigma^{p-2}}$$

$$= t^{u_{p-3}}(t^{l-2} - t^{l-1}) + (t^{q-2}\alpha^{(p-2)} + \mu)s^{\sigma^{p-2}}$$

$$= t^{u_{p-3}}(t^{l-2} - t^{l-1}) + [t^{q-2}t^{l-1}(t^{u_{p-2}} - t^{u_{p-3}}s^{\sigma^{p-2}-\sigma^{p-3}})$$

$$+ t^{l-2}(-t^{u_{p-2}})]s^{\sigma^{p-2}}$$

$$= t^{u_{p-3}}(t^{l-2} - t^{l-1}) + t^{u_{p-3}}(-t^{l-2})$$

$$= t^{u_{p-3}}(-t^{l-1})$$

and 0 are all distinct so that $b^{\sigma^{p-3}}a^{\beta_i^{(p-3)}}$ are all distinct. Similarly for the cases $j = p-4, p-5, \ldots, 1$.

Case $j = 0$, $ba^{\beta_i^{(0)}}$:

$$\beta_1^{(0)} = r^*s,$$

$$\beta_2^{(0)} = r^*s+E_1^{(0)} \quad ,$$

$$\beta_3^{(0)} = r^*s+E_1^{(0)}+E_2^{(0)},$$

$$\vdots$$

$$\beta_{q-1}^{(0)} = r^*s+\sum_{i=1}^{q-2} E_i^{(0)} \text{ and}$$

$$\beta_q^{(0)} = r^*s+\sum_{i=1}^{q-2} E_i^{(0)}+(\alpha_{q-1}^{(p-2)}+\mu)s^{1-\sigma^{p-2}}+\alpha_{q-1}^{(p-3)}s^{1-\sigma^{p-3}}$$

$$+\ldots+\alpha_{q-1}^{(2)}s^{1-\sigma^2}+\alpha_{q-1}^{(1)}s^{1-\sigma}.$$

We notice that

$$E_1^{(0)} = t^{l}-t^{l-1},$$

$$E_1^{(0)}+E_2^{(0)} = t^{l+1}-t^{l-1},$$

$$\vdots$$

$$\sum_{i=1}^{q-2} E_i^{(0)} = t^{l-2}-t^{l-1}, \text{ and}$$

$$\sum_{i=1}^{q-2} E_i^{(0)}+(\alpha_{q-1}^{(p-2)}+\mu)s^{1-\sigma^{p-2}}+\alpha_{q-1}^{(p-3)}s^{1-\sigma^{p-3}}+\dots$$

$$\dots+\alpha_{q-1}^{(2)}s^{1-\sigma^2}+\alpha_{q-1}^{(1)}s^{1-\sigma}$$

$$=(t^{l-2}-t^{l-1})+t^{l-2}[-t^{u_{p-3}}s^{\sigma^{p-2}-\sigma^{p-3}}s^{1-\sigma^{p-2}}$$

$$+(t^{u_{p-3}}-t^{u_{p-4}}s^{\sigma^{p-2}-\sigma^{p-3}})s^{1-\sigma^{p-3}}+\dots$$

$$\dots+(t^{u_2}-t^{u_1}s^{\sigma^2-\sigma})s^{1-\sigma^2}+(t^{u_1}-s^{\sigma-1})s^{1-\sigma}]$$

$$=(t^{l-2}-t^{l-1})-t^{l-2}=-t^{l-1}$$

and 0 are all distinct. Then all $ba^{\beta_i^{(0)}}$ are different.

Case $b^0a^i=0$, a alone.

Since $\sum_{i=1}^{q-1}(\alpha_i^{(1)}s^{-\sigma}+\alpha_i^{(2)}s^{-\sigma^2}+\dots+\alpha_i^{(p-2)}s^{-\sigma^{p-2}}+\alpha_i^{(p-1)}s^{-\sigma^{p-1}})=0,$

then in order to have partial products which are powers of a alone, we require that

$$r^*+\alpha_{q-1}^{(p-1)}(1-s^{-1})+\mu s^{-1}\equiv -r^{h-1}\pmod{q}.$$

We must have

$$r^{h-2}-r^{h-1}+t^{q-2}t^{l-1}(t-t^{u_{p-2}}s^{1-\sigma^{p-2}})(1-s^{-1})+(r^{h-1}-r^{h-2})s^{-2}$$

$$=-r^{h-1}.$$

At the beginning we set $\mu=r^{h-1}-r^{h-2}$, which implies $r^{h-1}-r^{h-2}=t^{u_{p-2}}(-t^{l-2})$. That is, $r^{h-2}=-t^{u_{p-2}+l-2}(r-1)^{-1}$.

We need

$$-t^{u_{p-2}+l-2}(r-1)^{-1}+t^{l-2}(t-t^{u_{p-2}}s^{1-\sigma^{p-2}})(1-s^{-1})-t^{u_{p-2}+1-2}s^{-2} = 0.$$

This is equivalent to

$$t^{u_{p-2}}[(r-1)^{-1}+s^{-1}(1-s^{-1})+s^{-2}] = t(1-s^{-1}) \text{ or}$$

$$t^{u_{p-2}-1}[(r-1)^{-1}+s^{-1}] = 1-s^{-1} \text{ or}$$

$$t^{u_{p-2}-1} = (s-1)(r-1)/(r+s-1).$$

A sequencing of a non-abelian group of order pq where 2 is a primitive root of GF[p], can be constructed as follows.

First we select one of the roots s where $s \neq 1$ of the congruence $s^p \equiv 1 \pmod q$ and also a primitive root r of GF[q] such that $r+s-1 \not\equiv 0 \pmod q$. We do so because we need $t^{u_{p-2}-1} = [(s-1)(r-1)]/(r+s-1) \neq 0$. Then select another primitive root t of GF q and integers $u_1, u_2, \ldots, u_{p-1}$ such that $t^{u_1} \neq s^{\sigma-1}$, $t^{u_2-u_1} \neq s^{\sigma^2-\sigma}$, $t^{u_3-u_2} \neq s^{\sigma^3-\sigma^2}$, $\ldots$, $t^{u_{p-2}-u_{p-3}} \neq s^{\sigma^{p-3}-\sigma^{p-2}}$, $t^{u_{p-2}-1} = [(s-1)(r-1)]/(r+s-1) \not\equiv s \pmod q$. This is because we require $\alpha_1^{(j)} \neq 0$, for $i=1,2,\ldots,p-1$. Then we can compute $\alpha_1^{(j)}$ fpr $i=1,2,\ldots,q-1$, $j=1,2,\ldots,p-1$. Eventually, we select h such that $r^{h-2}(r-1) \equiv t^{l-1}(-t^{u_{p-2}-1})$ (mod q). Arbitrarily choose an index l and we obtain a sequencing of the group. □

For example, consider the non-abelian group of order 55 where $p=5$, $q=11$ and the group relations are $ab=ba^3$, $ab^2=b^2a^9$, $ab^3=b^3a^5$, $ab^4= b^4a^4$.

We need $2\sigma\equiv1 \pmod p$ with $\sigma=3$. We may choose $s=3$ since $3^5\equiv1 \pmod{11}$ and $r=2$ which is a primitive root of GF[11] as $r+s-1\equiv4 \pmod{11}$ which is not zero. Then $t^{u_3-1} = (r-1)(s-1)/(r+s-1) \equiv 6 \pmod{11}$ so $t^{u_3-1} \neq s$. We may choose $t=2$, a primitive root of GF[11]. Then $t^{u_3} = 1$. If we choose $t^{u_1} = t^{u_2} = t^{u_3} =1$, and also $t^{l-1} = 1$, then

$$\alpha_1^{(1)} = t^{u_1}-s^{\sigma-1} = 1-3^2 = 3,$$

$$\alpha_1^{(2)} = t^{u_2}-s^{\sigma^2-\sigma} = 1-3^6 = 9,$$

$$\alpha_1^{(3)} = t^{u_3}-s^{\sigma^3-\sigma^2} = 1-3^{18} = 7,$$

$$\alpha_1^{(4)} = t-t^{u_3}s^{1-\sigma^3} = 2-3^4 = 9,$$

$$\alpha_2^{(1)} = 6, \quad \alpha_2^{(2)} = 7, \quad \alpha_2^{(3)} = 3, \quad \alpha_2^{(4)} = 7,$$

$$\alpha_3^{(1)} = 1, \quad \alpha_3^{(2)} = 3, \quad \alpha_3^{(3)} = 6, \quad \alpha_3^{(4)} = 3,$$

$$\alpha_4^{(1)} = 2, \quad \alpha_4^{(2)} = 6, \quad \alpha_4^{(3)} = 1, \quad \alpha_4^{(4)} = 6,$$

$$\alpha_5^{(1)} = 4, \quad \alpha_5^{(2)} = 1, \quad \alpha_5^{(3)} = 2, \quad \alpha_5^{(4)} = 1,$$

$$\alpha_6^{(1)} = 8, \quad \alpha_6^{(2)} = 2, \quad \alpha_6^{(3)} = 4, \quad \alpha_6^{(4)} = 2,$$

$\alpha_7^{(1)} = 5$, $\alpha_7^{(2)} = 4$, $\alpha_7^{(3)} = 8$, $\alpha_7^{(4)} = 4$,

$\alpha_8^{(1)} = 10$, $\alpha_8^{(2)} = 8$, $\alpha_8^{(3)} = 5$, $\alpha_8^{(4)} = 8$,

$\alpha_9^{(1)} = 9$, $\alpha_9^{(2)} = 5$, $\alpha_9^{(3)} = 10$, $\alpha_9^{(4)} = 5$,

$\alpha_{10}^{(1)} = 7$, $\alpha_{10}^{(2)} = 10$, $\alpha_{10}^{(3)} = 9$, and $\alpha_{10}^{(4)} = 10$.

Also we require $r^{h-1}-r^{h-2} = t^{l-1}(-t^{u_3-1})$, that is, $2^{h-2} = -6$ which implies $h = 6$. Now $ab = ba^3$, $ab^2 = b^2a^9$, $ab^3 = b^3a^5$, $ab^5 = b^4a^4$. The following is a sequencing of the non-abelian group of order 55.

Sequencing	Partial products	Sequencing (contd)	Partial products (contd)
e	e	b^4a^9	ba^8
a^{10}	a^{10}	b^2a^6	b^3a
a^9	a^8	ba^7	b^4a^{10}
a^7	a^4	b^3a^3	b^2a^9
a^3	a^7	b^4a^7	ba^{10}
a^6	a^2	b^2a	b^3a^3
a	a^3	ba^3	b^4a
a^2	a^5	b^3a^6	b^2
a^4	a^9	b^4a^3	ba^3
a^8	a^6	b^2a^2	b^3a^7
b	ba^7	ba^6	b^4a^5
b^2a^3	b^3	b^3a	b^2a^4
ba^9	b^4a^9	b^4a^6	b

Sequencing	Partial products	Sequencing (contd)	Partial products (contd)
b^3a^7	b^2a^8	b^2a^4	b^3a^4
ba	b^4a^2	b^4a^8	ba^9
b^3a^2	b^2a	b^2a^9	b^3a^2
b^4a	ba^5	ba^5	b^4
b^2a^8	b^3a^9	b^3a^{10}	b^2a^{10}
ba^2	b^4a^7	b^4a^5	ba
b^3a^4	b^2a^6	b^2a^7	b^3a^5
b^4a^2	ba^4	ba^{10}	b^4a^3
b^2a^5	b^3a^8	b^3a^9	b^2a^2
ba^4	b^4a^6	a^5	b^2a^7
b^3a^8	b^2a^5	b^2	b^4a^8
b^4a^4	ba^2	b^4	b^3a^{10}
b^2a^{10}	b^3a^6	b^3	ba^6
ba^8	b^4a^4	b^4a^{10}	a
b^3a^5	b^2a^3		

However, whether or not non-abelian groups of order pq, where 2 is not a primitive root are sequenceable is still unknown.

CHAPTER FOUR

Symmetric and Strong Symmetric Sequencings

§4.1 Symmetric sequencings

Definition 4.1 : Suppose G is a group of order 2n with identity e and unique element g^* of order 2. A sequencing $a_1 a_2, \ldots, a_{2n}$ is called a symmetric sequencing if and only if $a_{n+1} = g^*$ and $a_{n+1+i} = (a_{n+1-i})^{-1}$ for $1 \le i \le n-1$.

Before proving that the abelian group of order 2n is symmetric sequenceable, we need to outline the construction of the sequencing of the appropriate abelian group by B. Gordon. Suppose G is an abelian group of order 2n. B. Gordon showed that it is sequenceable and $G = A \times B$ where A is cyclic of order 2^k, $k>0$ and B has odd order. The group G has a basis $c_0, c_1, \ldots, c_m$ where c has order 2^k and the orders $\delta_1, \delta_2, \ldots, \delta_m$ of $c_1, c_2, \ldots, c_m$ are odd positive integers such that $0<i<m$ implies $\delta_i | \delta_{i+1}$. If j is any positive integer, then there exist unique integers, $j_0, j_1, \ldots, j_m$ such that

$$j \equiv j_0 \pmod{\delta_1 \delta_2 \ldots \delta_m} \text{ and}$$

(1)

$$j_0 = j_1 + j_2 \delta_1 + j_3 \delta_1 \delta_2 + \ldots + j_m \delta_1 \delta_2 \ldots \delta_{m-1} \text{ where}$$

$$0 \le j_1 < \delta_1,\ 0 \le j_2 < \delta_2,\ \ldots,\ 0 \le j_m < \delta_m.$$

The sequence of partial products P is defined as follows:

If $i = 2j+1$, $0 \le j < n$, then $b_{2j+1} = c_0^{-j} c_1^{-j_1} c_2^{-j_2} \dots c_m^{-j_m}$ and

(2) If $i = 2j+2$, $0 \le j < n$, then $b_{2j+2} = c_0^{j+1} c_1^{j_1+1} c_2^{j_2+1} \dots c_m^{j_m+1}$.

The sequencing S of G is defined as follows:

If $j = 2j+2$, $0 \le j < n$, then

$$a_i = b_{i-1}^{-1} b_i = c_0^{2j+1} c_1^{2j_1+1} \dots c_m^{2j_m+1},$$

if $i = 2j+1$, $0 \le j < n$ and $s = \min \{r: j_r \ne 0\}$, then

(3) $$a_i = b_{i-1}^{-1} b_i = c_0^{-2j} c_s^{-2j_s} c_{s+1}^{-2j_{s+1}-1} \dots c_m^{-2j_m-1}, \text{ and}$$

in particular if $j_0 = 0$, $a_i = c_0^{-2j}$.

Let g be any element of G. Since $(g^{-1}g^*g)(g^{-1}g^*g) = e$, (recall that g^* is the unique element of order 2 in G), then $g^{-1}g^*g = g^*$ which implies $g^*g = gg^*$. So g^* is in the center of G. Thus, symmetric sequencings have the form

S: $e, a_2, \dots, a_n, a_{n+1}, a_n^{-1}, \dots, a_2^{-1}$ and have the associated partial product sequence.

P: $e, b_2, \dots, b_n, b_n g^*, b_n g^* a_n^{-1} = b_n a_n^{-1} g^*, \dots, b_n g^* a_n^{-1} a_{n-1}^{-1} \dots a_2^{-1}$

where $b_i = a_1 a_2 \dots a_i$.

Therefore, P: $e, b_2, \dots, b_n, b_n g^*, b_n a_n^{-1} g^*, \dots, b_n a_n^{-1} a_{n-1}^{-1} \dots a_2^{-1} g^*$,

can be rewritten as P: $e, b_2, \dots, b_n, b_n g^*, b_{n-1} g^*, \dots, b_2 g^*, g^*$.

B.A. Anderson is the only mathematician who did some work on symmetric sequencing. However, the purpose of the first theorem of this chapter is to show the sequencings of B. Gordon are symmetric.

Theorem 4.1 : Suppose G is a sequenceable abelian group of order 2n. Then there exists a symmetric sequencing of G.

Proof : Let $a_1, a_2, \ldots, a_n$ be the sequencing described in (3). We are going to show it is a symmetric sequencing of G.

Suppose $a_i a_k = e$. From (3) it follows that either i and k are both even or i and k are both odd. For if $i = 2j+2$, $k = 2t+1$, then $c_0^{2j+1} c_0^{-2t} = c_0^{2(j-t)+1} \neq e$ because c_0 has order 2^k, $k>0$. This contradicts $a_i a_k = e$. The case where i is odd, k is even is similar.

Now suppose $i = 2j+1$ and $k = 2l+1$, $0 \leq j,l < n$. By Definition 4.1, we only need to show that $i+k \in \{2, 2n+2\}$. The case $i+k = 2$ will happen only when $a = a = e$ as will be seen later.

If $j_0 = 0$, then $a_i = c_0^{-2j}$. Since $a_i a_k = e$, then $a_k = c_0^{2j}$ so that $l_0 = 0$. Similarly, if $l_0 = 0$, then $j_0 = 0$. In the case $j_0 \neq 0$, $l_0 \neq 0$, by (3) we have

$$a_i = c_0^{-2j} c_s^{-2j_s} c_{s+1}^{-2j_{s+1}-1} \ldots c_m^{-2j_m-1} \quad \text{and}$$

$$a_k = c_0^{-2l} c_t^{-2l_t} c_{t+1}^{-2l_{t+1}-1} \ldots c_m^{-2t_m-1} .$$

Now each δ_i is odd so that we have $s = t$, otherwise $a_k a_i \neq e$. Hence, $2(j+1) \equiv 0 \pmod{2^k}$ and

$$j_s + l_s \equiv 0 \pmod{\delta_s},$$

$$j_{s+1}+l_{s+1}+1 \equiv 0 \pmod{\delta_{s+1}},$$

$$\vdots$$

$$j_m+l_m+1 \equiv 0 \pmod{\delta_m}.$$

Thus, $j_s+l_s = \delta_s$,

$$j_{s+1}+l_{s+1}+1 = \delta_{s+1},$$

$$\vdots$$

$$j_m+l_m+1 = \delta_m$$

because $0 \le j_i < \delta_i$, $0 \le l_i < \delta_i$ $i = 1,2,\ldots,m$. We multiply the $(\delta_{s+i})^{th}$ equation by $\delta_1\ldots\delta_{s+i-1}$ and obtain

$$(j_s+l_s)\delta_1\delta_2\ldots\delta_{s-1} = \delta_1\delta_2\ldots\delta_s,$$

$$(j_{s+1}+l_{s+1}+1)\delta_1\delta_2\ldots\delta_s = \delta_1\delta_2\ldots\delta_{s+1},$$

$$\vdots$$

$$(j_m+l_m+1)\delta_1\delta_2\ldots\delta_{m-1} = \delta_1\delta_2\ldots\delta_m.$$

We add then together to obtain

$(j_s+l_s)\delta_1\delta_2\ldots\delta_{s-1} + (j_{s+1}+l_{s+1}+1)\delta_1\delta_2\ldots\delta_s +\ldots+ (j_m+l_m+1)\delta_1\delta_2\ldots \ldots\delta_{m-1} = \delta_1\delta_2\ldots\delta_s + \delta_1\delta_2\ldots\delta_{s+1} +\ldots+ \delta_1\delta_2\ldots\delta_m$ or equivalently $j_s\delta_1\delta_2\ldots\delta_{s-1} \bullet j_{s+1}\delta_1\delta_2\ldots\delta_s+\ldots+j_m\delta_1\delta_2\ldots\delta_{m-1} + l_s\delta_1\delta_2\ldots \ldots\delta_{s-1} + l_{s+1}\delta_1\delta_2\ldots\delta_s +\ldots+l_m\delta_1\delta_2\ldots\delta_{m-1} = \delta_1\delta_2\ldots\delta_{m-1}\delta_m$.

By (1) we have $j_0+l_0 = \delta_1\delta_2\ldots\delta_m$. Thus, $j+l \equiv 0 \pmod{\delta_1\delta_2\ldots\delta_m}$ and $2(j+l) \boxminus 0 \pmod{2n}$. Since $0 \le j,l < n$, we conclude that $2(j-1) = 0$ or $2(j+1) = 2n$. If $2(j+1) = 0$, then $j = 1 = 0$ which implies $a_i = a_k = e$. If $2(j+1) = 2n$, then this implies $j+1 = n$ and $i+k = 2n+2$.

The case where both i and k are even is similar. This finishes the proof. □

Now we know that the sequencings of B. Gordon are symmetric. In the following, we are going to determine some more groups which have symmetric sequencings.

Theorem 4.2[2] : If G is a sequenceable group of odd order n, then $G \times Z_2$ has a symmetric sequencing.

Proof : Since the order of G is odd, then G has no element of even order. Therefore, $G\backslash\{e\}$ can be partitioned into 2-element subsets such that each subset consists of an element and its inverse. Since G is sequenceable, it has a sequencing $e, x_2, \ldots, x_n$. Now choose one element from each 2-element subset. If x_i is a chosen element, we associate $(x_i,-1)$ with x_i. If x_i is not a chosen element, we associate $(x_i,1)$ with x. For e we associate 1 with it. Then we have a string $y_1, y_2, \ldots, y_n = (e,1),(x_2,i_2),(x_3,i_3),\ldots,(x_n,i_n)$ of elements of $G \times Z_2$. We construct a symmetric sequencing of $G \times Z_2$ by extending the above sequencing. Define $y_{n+1} = (e,-1)$ and $y_{n+1+j} = (y_{n+1-j})^{-1} = (x_{n+1-j}, i_{n+1-j})^{-1}$ which is equal to $(x_{n+1-j}^{-1}, i_{n+1-j}^{-1})$. We see that $\{y_1, y_2, \ldots, y_{2n}\} = G \times Z_2$.

Since $(x_j,i_j)(e,-1) = (e,-1)(x_j,i_j)$ for $1\le j\le 2n$, $(e,-1)$ is in the center of $G\times Z_2$. The sequence of partial products is $(e,1)$, (x_2,i_2), (x_2x_3,i_2i_3), ..., $(x_2x_3\ldots x_n,i_2i_3\ldots i_n)$, $(x_2x_3\ldots x_n,-i_2i_3\ldots i_n)$, $(x_2x_3\ldots x_{n-1},-i_2i_3\ldots i_{n-1})$, ..., $(x_2x_3,-i_2i_3)$, $(x_2,-i_2)$. They are all distinct from each other. So the partial products also include all the elements of $G\times Z_2$. Thus, $G\times Z_2$ has a symmetric sequencing. □

<u>Theorem 4.3</u>[2] : Suppose the group G has a symmetric sequencing and B is an abelian group such that $\gcd(|G|,|B|) = 1$. Then $G\times B$ has a symmetric sequencing.

<u>Proof</u> : Suppse G is of order 2n and has a symmetric sequencing. Let S_G: $x_1,x_2,\ldots,x_{2n}$ be a symmetric sequencing of G and P_G: $y_1,y_2,\ldots,y_{2n}$ be the associated partial product sequence. In order to have $(|G|,|B|) = 1$, B must be of odd order, say k. We are going to construct a symmetric sequencing $S_{G\times B}$: $a_1,a_2,\ldots,a_{2nk}$ of $G\times B$. Let $\{c_1,c_2,\ldots,c_m\}$ be a basis of B such that the orders $\delta_1,\delta_2,\ldots,\delta_m$ are odd positive integers with $0<i<m$ implying $\delta_i|\delta_{i+1}$. If j is any positive integer then there exist unique integers $j_0,j_1,\ldots,j_m$ such that $j\equiv j_0 \pmod{\delta_1\delta_2\ldots\delta_m}$ and

$$j_0 = j_1+j_2\delta_1+j_3\delta_1\delta_2+\ldots+j_m\delta_1\delta_2\ldots\delta_{m-1}$$

where $0\le j_1<\delta_1$, $0\le j_2<\delta_2$, ..., $0\le j_m<\delta_m$.

Now the partial products are defined as follow.

If $i = 2j+1$, $0 \le j < nk$, then

$$b_{2j+1} = (y_{i(\text{mod } 2n)}, c_1^{-j_1} \dots c_m^{-j_m}) \text{ and}$$

if $i = 2j+2$, $0 \le j < nk$, then

$$b_{2j+2} = (y_{i(\text{mod } 2n)}, c_1^{j_1+1} \dots c_m^{j_m+1}).$$

We are going to show all the b_i's are distinct. Suppose $b_s = b_t$ where $s = 2u+1$ and $t = 2v+1$, $0 \le u, v < nk$. Hence $2u+1 \equiv 2v+1 \pmod{2n}$, then $2u \equiv 2v \pmod{2n}$ which implies $u \equiv v \pmod{n}$. As in Theorem 4.1, $u \equiv v \pmod{k}$. Since $\gcd(n,k) = 1$, we have $u \equiv v \pmod{nk}$ and thus $u = v$. It is similar for the case $s = 2u+2$ and $t = 2v+2$, $0 \le u, v < nk$. Finally, if $s = 2u+1$ and $t = 2v+2$, then $y_s \ne y_t$ so that $b_s \ne b_t$.

Now the sequence of $S_{G \times B}$ is as follows.

If $i = 2j+2$, $0 \le j < nk$, then

$$\begin{aligned} a_i &= b_{i-1}^{-1} b_i \\ &= (y_{i-1(\text{mod } 2n)}, c_1^{-j_1} \dots c_m^{-j_m})^{-1} (y_{i(\text{mod } 2n)}, c_1^{j_1+1} \dots c_m^{j_m+1}) \\ &= (x_{i(\text{mod } 2n)}, c_1^{2j_1+1} \dots c_m^{2j_m+1}). \end{aligned}$$

If $i = 2j+1$, $0 \le j < nk$ and $s = \min\{r: j_r \ne 0\}$, then

$$a_i = b_{i-1}^{-1} b_i = (x_{i(\text{mod } 2n)}, c_s^{-2j_s} c_{s+1}^{-2j_s-1} \dots c_m^{-2j_m-1}).$$

If $j_0 = 0$, then $a_i = (x_{i(\text{mod } 2n)}, e)$.

All a_i's are distinct by an argument similar to the above in which that b_i's were shown to be distinct. Then $G \times B$ is a sequenceable group.

Choose any a_s, a_t such that $a_s a_t = e$ where a_s and a_t are in $S_{G\times B}$. Since $x_1, x_2, \ldots, x_{2n}$ is a symmetric sequencing of G, which forces either s and t are both even or s and t are both odd, we then do the same thing as in Theorem 4.1 to show that $S_{G\times B}$ is a symmetric sequencing of $G \times B$. □

From the above theorems we can conclude that abelian and non-abelian symmetric sequenceable groups of arbitrarily large even order exist.

Before we go to the next section, we take a look at a relation between symmetric sequencings and even starters.

<u>Definition 4.2</u> : Suppose G is a group of order 2n with identity e and unique element g^* of order 2. Then $E = \{\{x_i, y_i\}: 1 \le i \le n-1\}$ is a left (right) even starter for G if and only if (i) every nonidentity element of G except one denoted m, occurs as an element of some pair of E and

(ii) every nonidentity element of G except g^* occurs in $\{x_i^{-1}y_i, y_i^{-1}x_i : 1 \le i \le n-1\}$ $(\{x_i y_i^{-1}, y_i x_i^{-1} : 1 \le i \le n-1\})$.

If G is abelian, there is no distinct between left and right even starters.

<u>Theorem</u> 4.4[2] : If the group G has a symmetric sequencing

$a_1,a_2,\ldots,a_n$ then G has a left even starter.

Proof : Suppose $|G| = 2n$ and G has a symmetric sequencing with partial product sequence $b_1,b_2,\ldots,b_{2n}$. Now let

$$E = \{\{b_{2j+2},b_{2(j+1)+1}\}: 0\le j<n/2-1\}$$
$$\cup \{\{b_{2n-(2j+1)},b_{2n-2j}\}: 0\le j\le n/2-1\}$$

and let $m = b_{n+1}$ if n is odd and $m = b_n$ if n is even. When n is odd,

$$E = \{\{b_2,b_3\},\{b_4,b_5\},\ldots,\{b_{n-1},b_n\}\}$$
$$\cup \{\{b_{2n-1},b_{2n}\},\{b_{2n-3},b_{2n-2}\},\ldots,\{b_{n+2},b_{n+3}\}\}$$

and every nonidentity element of G except m occurs as an element of some pair of E. When n is even,

$$E = \{\{b_2,b_3\},\{b_4,b_5\},\ldots,\{b_{n-2},b_{n-1}\}\}$$
$$\cup \ \{\{b_{2n-1},b_{2n}\},\{b_{2n-3},b_{2n-2}\},\ldots,\{b_{n+1},b_{n+2}\}\}$$

and every nonidentity element of G except m occurs as an element of some pair of E. Now, for $0\le j\le n/2-1$,

$(b_{2j+2})^{-1}b_{2(j+1)+1} = a_{2(j+1)+1} = a_p$ where $3\le p<n+1$ and p is odd.

On the other hand, $0\le j<n/2-1$ implies

$(b_{2n-(2j+1)})^{-1}b_{2n-2j} = a_{2n-2j} = a_q$ where $n+2\le q\le 2n$ and q is even. We see that the total number of p's and q's is n-1. Since we have a symmetric sequencing, it is clear that

$$C = \{a_p:3\le p<n+1 \text{ and } p \text{ odd}\} \cup \{a_q:n+2\le q\le 2n \text{ and } q \text{ is even}\}$$

contains a set of n-1 distinct elements of $G\backslash\{e,g^*\}$. Moreover $a_i = (a_j)^{-1}$ if and only if $i+j = 2n+2$. Since the sum of two p's or two q's or a p and a q is never equal to 2n+2, no element of C is the inverse of itself or another element of C.

Thus every non-identity element of G except g^* occurs in

$$\{(b_{2j+2})^{-1}(b_{2(j+1)+1}),(b_{2(j+1)+1})^{-1}(b_{2j+2}) : 0\leq j<n/2-1\}$$

$$\cup \{(b_{2n-(2j+1)})^{-1}(b_{2n-2j}),(b_{2n-2j})^{-1}(b_{2n-(2j+1)}) : 0\leq j\leq n/2-1\}.$$

Then E is a left even starter for G. □

However, the converse is not true. That is, a group G may have even starter but have no symmetric sequencing.

<u>Example</u> : Consider the quaternion group Q_3 with generators a and b and defining relations $a^4 = e$, $b^2 = a^2$ and $ba = a^3b$. The group Q_3 is of order 8 with identity e and an unique element a^2 of order 2.

Let $E = \{\{a,ab\}, \{a^2b,a^3b\}, \{a^3,b\}\}$. It is easy to verify that E is both a left and right even starter for Q_3. It has been verified by computers that Q_3 has no sequencing. Thus it certainly has no symmetric sequencing. We can also prove algebrically that Q_3 does not have a symmetric sequencing and shall do so now.

Suppose $S : e,a_2,a_3,a_4,g^*,a_4^{-1},a_3^{-1},a_2^{-1}$ is a symmetric sequencing of Q_3. Now $Q_3/\langle a^2\rangle$

$= \{e\langle a^2\rangle, a\langle a^2\rangle, b\langle a^2\rangle, ab\langle a^2\rangle\}$

$= \{\{e,a^2\}, \{a,a^3\}, \{b,ba^2\}, \{ab,aba^2\}$

$= \{\{e,a^2\}, \{a,a^3\}, \{b,a^2b\}, \{ab,a^3b\}\}.$

Now, $\langle a^2\rangle$ is a normal subgroup of Q_3 of order 2, and we see that $Q_3/\langle a^2\rangle \simeq Z_2 \times Z_2$. Let $\Phi:Q_3 \to Q_3/\langle a^2\rangle$ denote the natural homomorphism of G onto the quotient group $Q_3/\langle a^2\rangle$. Let the members of $Z_2 \times Z_2$ be designeated by e,1,2,3 where e is the identity, each nonidentity element of $Z_2 \times Z_2$ is its own inverse and the product of any two distinct nonidentity elements is the remaining nonidentity element. So we can write $Q_3/\langle a^2\rangle = \{e,1,2,3\}$. Let $\overline{a}_i = \Phi(a_i)$, $a_i \in Q_3$, and $b_i = \overline{a}_1\overline{a}_2\ldots\overline{a}_i$. Then each $x \in Q_3/\langle a^2\rangle$ must occur two times in both of the sequences $\overline{a}_1,\overline{a}_2,\ldots,\overline{a}_n$ and $\overline{b}_1,\overline{b}_2,\ldots,\overline{b}_n$. Thus the sequence S must induce a sequence $\overline{S}$ on $Z_2 \times Z_2$ such that every element of $Z_2 \times Z_2$ occurs exactly twice in $\overline{S}$ and its associated partial product sequence $\overline{P}$. The sequence S force $\overline{S}$ to be in the form $\overline{S}$: 1,x,y,z,1,z,y,x. But then the associated partial product sequence is $\overline{P}$: 1,x,z,1,1, z,x,1. So Q_3 has no symmetric sequencing.

§4.2 Strong symmetric sequencings

If we put some more restrictions on symmetric sequencings, they can be used to construct families of Howell Designs which we will discuss in the next chapter. B.A. Anderson and P.A. Leonard showed that Z_{2p} had a strong symmetric sequencing if $p \geq 5$ and p prime. Also, B.A. Anderson showed that when $p>3$ is a prime and $p=5$ or $p \equiv \pm 3, \pm 13 \pmod{40}$, Z_{p-1} had a strong symmetric sequencing. We shall first take a look at the sequencings.

Definition 4.3 : Suppose G is an abelian group of order 2n and S is a symmetric sequencing of G. S is strong if and only if the associated partial product sequence P satisfies the following conditions:

(i) $1 \le i < j \le n-1$ implies $b_i b_{i+1} \neq b_j b_{j+1}$ and

(ii) $1 \le i \le n-1$ implies $b_i b_{i+1} \notin \{e, m^2\}$ where $m = b_n$ if n is even, $m = b_{n+1}$ if n is odd.

The sequencing of B. Gordon is symmetric but not strong because $b_{2j+1} b_{2j+2} = c_0 c_1 \ldots c_m$, $0 \le j < n$ for $n \ge 4$.

Up until now, the only known groups with strong symmetric sequencings are the cyclic groups Z_{2p}, where $p \ge 5$, p prime, and the cyclic groups Z_{p-1}, where $p > 3$ is a prime and $p = 5$, or $p \equiv \pm 3, \pm 13 \pmod{40}$.

Suppose $p \ge 3$ is a prime, Z_{2p} is the additive cyclic group of order 2p and $x = 2y \in Z_{2p}$. Note that x is even, the subgroup $\langle x \rangle$ generated by x has p elements and all elements of $\langle x \rangle$ are even. Also $\langle x \rangle + p \cup \langle x \rangle = Z_{2p}$.

We are going to define a sequence S and thus compute the partial sums P such that S and P have many of the properties required to be a strong symmetric sequencing. The sequencing S is as follows.

$$S : a_i \begin{cases} \equiv (i-1)x \pmod{2p} & \text{when } 1 \le i \le (p+1)/2 \\ = 2(i-1)-p & \text{when } (p+3)/2 \le i \le (3p+1)/2 \text{ and} \\ \equiv (i-1)x \pmod{2p} & \text{when } (3p+3)/2 \le i \le 2p. \end{cases}$$

When $1 \leq i \leq (p+1)/2$,

$$b_i \equiv a_1+a_2+\ldots+a_i$$

$$\equiv \frac{i}{2}(a_1+a_i)$$

$$\equiv \frac{i}{2}[0+(i-1)x]$$

$$\equiv [\frac{i(i-1)}{2}]x \pmod{2p}.$$

When $(p+3)/2 \leq i \leq (3p+1)/2$,

$$b_i \equiv a_1+a_2+\ldots+a_{(p+1)/2}+a_{(p+3)/2}+\ldots+a_i$$

$$\equiv[\frac{(p+1)/2}{2}][a_i+a_{(p+1)/2}]+[\frac{i-(p+3)/2+1}{2}][a_{(p+3)/2}+a_i]$$

$$\equiv (\frac{p+1}{4})(\frac{p-1}{4})x+[\frac{(2i-p-1)}{2}][2(\frac{p+3}{2}-1)-p+2(i-1)-p]x$$

$$\equiv (\frac{p^2-1}{8})x+(i-\frac{p+1}{2})^2 \pmod{2p}.$$

When $(3p+3)/2 \leq i \leq 2p$,

$$b_i \equiv a_1+\ldots+a_{(p+1)/2}+a_{(p+3)/2}+\ldots+a_{(3p+3)/2}$$

$$+a_{(3p+5)/2}+\ldots+a_i$$

$$\equiv [\frac{(p+1)/2}{2}][0+(\frac{p+1}{2}-1)]x+[\frac{(3p+1)/2-(p+3)/2+1}{2}]$$

$$[2(\frac{3p+1}{2}-1)-p+2(\frac{p+3}{2}-1)-p]+[\frac{i-(3p+3)/2+1}{2}]$$

$$[(i-1)x+(\frac{3p+3}{2}-1)x] \pmod{2p}.$$

$$\equiv (\frac{p^2-1}{8})x+p^2+(\frac{2i-3p-1}{4})(\frac{2i+3p-1}{2})x$$

$$\equiv (\frac{p^2-1}{8})x+p^2+(\frac{4i^2-4i+1-9p^2}{8})x$$

$$\equiv [\frac{i(i-1)}{2}]x+p \pmod{2p}.$$

Then the sequence of partial products is as follows:

$$P: b_i = \begin{cases} [\frac{i(i-1)}{2}]x \pmod{2p}, & 1 \le i \le \frac{p+1}{2}, \\ \beta_x + (i-\frac{p+1}{2})^2 \pmod{2p}, & \frac{p+3}{2} \le i \le \frac{3p+1}{2}, \\ [\frac{i(i-1)}{2}]x+p \pmod{2p}, & \frac{3p+3}{2} \le i \le 2p, \end{cases}$$

where $\beta_x = b_{(p+1)/2} = [(p^2-1)/8]x$.

Before going any further, we give two examples. In each case, S is the sequence of a_i's and P is the sequence of b_i's. The elements β_x are starred and the elements $m_x = b_{p+1}$ are underlined.

Example 1 We let $p = 11$, $x = 6$ and do the arithmetic modulo 22. We have

S: 0, 6, 12, 18, 2, 8, 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 14, 20, 4, 10, 16;

P: 0, 6, 18, 14, 16, 2^*, 3, 6, 11, 18, 5, $\underline{16}$, 7, 0, 17, 14, 13, 5, 3, 7, 17, 11=p;

C: $6=b_1b_2$, $2=b_2b_3$, $10=b_3b_4$, $8=b_4b_5$, $18=b_5b_6$, $5=b_6b_7$, $9=b_7b_8$, $17=b_8b_9$, $7=b_9b_{10}$, $1=b_{10}b_{11}$; $\beta_x=2$ and $m_x=16$.

Example 2 We let $p = 13$, $x = 4$ and do the arithmetic modulo 26. Then

S: 0, 4, 8, 12, 16, 20, 24, 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 2, 6, 10, 14, 18, 22;

P: 0, 4, 12, 24, 14, 8, 6^*, 7, 10, 15, 22, 5, 16, $\underline{3}$, 18, 9, 2, 23, 20, 19, 21, 1, 11, 25, 17, 13=p;

C: $4=b_1b_2$, $16=b_2b_3$, $10=b_3b_4$, $12=b_4b_5$, $22=b_5b_6$, $14=b_6b_7$, $13=b_7b_8$, $17=b_8b_9$, $25=b_9b_{10}$, $11=b_{10}b_{11}$, $1=b_{11}b_{12}$, $21=b_{12}b_{13}$; $\beta_x=6$ and $m_x=3$.

In the next theorem, we are going to give properties which the sequences S and P have.

Theorem 4.4[4] : Suppose $p\geq 3$ is a prime, $x = 2y\in Z_{2p}$ and S and P are defined as above. Then

(i) $\{a_i:1 \leq i \leq 2p\} = Z_{2p}$ (We will write this as $S = Z_{2p}$);

(ii) $a_1 = b_1 = 0$, $a_{p+1} = b_{2p} = p$;

(iii) $1 \leq k \leq p-1$ implies $a_{p+1+k} = -(a_{p+1-k})$;

(iv) $1 \leq j \leq 2p$ implies $b_j+p = b_{2p-(j-1)}$;

(v) $2 \leq i < j \leq p+1$ implies $b_{i-1}+b_i \not\equiv b_{j-1}+b_j$ (mod 2p) and

(vi) $2 \leq i \leq p+1$ implies $b_{i-1}+b_i \not\equiv 0$ (mod 2p).

Proof : The proofs of statements (i) to (iv) are based on calculations which are straightforward.

(1) In order to prove (i), we have to show that all the a_i's, $1 \leq i \leq 2p$, are distinct. Assume $a_i = a_j$.

For $1 \leq i, j \leq (p+1)/2$. This implies

$$(i-1)x-(j-1)x \equiv 0 \pmod{2p}$$

which implies $(i-1)x \equiv 0 \pmod{2p}$

which implies $(i-j) \equiv 0 \pmod{p}$

which implies $i = j$.

For $(p+3)/2 \leq i, j \leq (3p+1)/2$ we have

$$2(i-1)-p-[2(j-1)-p] \equiv 0 \pmod{2p}$$

which implies $2(i-j) \equiv 0 \pmod{2p}$

which implies $(i-j) \equiv 0 \pmod{p}$

which implies $i = j$.

For $(3p+3)/2 \le i, j \le 2p$ we have

$$(i-1)x-(j-1)x \equiv 0 \pmod{2p}$$

which implies $(i-j)x \equiv 0 \pmod{2p}$

which implies $(i-j) \equiv 0 \pmod{p}$

which implies $i = j$.

For $1 \le i \le (p+1)/2$, $(p+3)/2 \le j \le (3p+1)/2$ we have

$$(i-1)x-[2(j-1)-p] \equiv 0 \pmod{2p}$$

which implies $(i-1)x-2(j-1) \equiv -p \pmod{2p}$

which implies $(i-1)x-2(j-1) = 2kp-p$ (for some integer k)

$$= p(2k-1)$$

which is impossible because the left hand side is even while the right hand side is odd.

For $(p+3)/2 \le i \le (3p+1)/2$, $(3p+3)/2 \le j \le 2p$ we have

$$(j-1)x-[2(i-1)-p] \equiv 0 \pmod{2p}$$

which implies $(j-1)x-2(i-1) \equiv -p \pmod{2p}$

which implies $(j-1)x-2(i-1) = 2kp-p$ (for some integer k)

$$= p(2k-1)$$

which is also impossible because the left hand side is even while the right hand side is odd.

For $1 \le i \le (p+1)/2$, $(3p+3)/2 \le j \le 2p$ we have

$$(i-1)x-(j-1)x \equiv 0 \pmod{2p}$$

which implies $(i-j)x \equiv 0 \pmod{2p}$

which implies $(i-j) \equiv 0 \pmod{p}$

which is impossible because $p+1 \le j-i \le 2p-1$.

These cases finish the proof of (i).

(ii) Clearly, $a_1 = (1-1)x = 0$ and $b_1 = a_1 = 0$. Now

$$a_{p+1} = 2\,(p+1)-1\,-p = p \text{ and}$$

$$\begin{aligned} b_{2p} &\equiv [\tfrac{2p(2p-1)}{2}]x+p \pmod{2p} \\ &\equiv 2p(2p-1)y+p \pmod{2p} \text{ where } x = 2y \\ &\equiv p \pmod{2p}. \end{aligned}$$

(iii) Now $1 \le k \le p-1$ implies $p+2 \le p+1+k \le 2p$ and $2 \le p+1-k \le p$. If $1 \le k \le (p-1)/2$ then $p+2 \le p+1+k \le (3p+1)/2$ and $(p+3)/2 \le p+1-k \le p$. Therefore,

$$a_{p+1+k} = 2(p+1+k-1)-p = p+2k \text{ and}$$

$$a_{p+1-k} = 2(p+1-k-1)-p = p-2k. \text{ Then}$$

$$-a_{p+1-k} = p+2k. \text{ We have}$$

$$a_{p+1+k} = -a_{p+1-k}.$$

If $(p+1)/2 \le k \le p-1$, then $(3p+3)/2 \le p+1+k \le 2p$ and $2 \le p+1-k \le (p+1)/2$. Therefore,

$$a_{p+1+k} \equiv (p+1+k-1)x \equiv (p+k)x \equiv kx \pmod{2p} \text{ and}$$

$$a_{p+1-k} \equiv (p+1-k-1)x \equiv (p-k)x \pmod{2p}. \text{ We have}$$

$$a_{p+1-k} = -a_{p+1-k} \text{ since } -(p-k)x \equiv kx \pmod{2p}.$$

(iv) Suppose $1 \le j \le (p-1)/2$. Then $(3p+3)/2 \le 2p-(j-1) \le 2p$. We have

$$\begin{aligned} b_j+p &\equiv [\tfrac{j(j-1)}{2}]x \pmod{2p} + p \\ &\equiv j(j-1)y \pmod{2p} + p \text{ and} \end{aligned}$$

$$b_{2p-(j-1)} \equiv \{\frac{[2p-(j-1)][2p-(j-1)-1]}{2}\}x+p \pmod{2p}$$

$$\equiv [4p^2-2pj-2p(j-1)+j(j-1)]y+p \pmod{2p}$$

$$\equiv j(j-1)y+p \pmod{2p}$$

which is congruent to b_j+p.

Suppose $j = (p+1)/2$. Then $2p-(j-1) = (3p+1)/2$. We have

$$b_j+p \equiv \{\frac{[(p+1)/2][(p+1)/2-1]}{2}\}x \pmod{2p} + p$$

$$\equiv (\frac{p^2-1}{4})y \pmod{2p} + p \text{ and}$$

$$b_{2p-(j-1)} \equiv (\frac{p^2-1}{8})x+(\frac{3p+1}{2}-\frac{p+1}{2})^2 \pmod{2p}$$

$$\equiv (\frac{p^2-1}{4})y+p^2 \pmod{2p}$$

$$\equiv (\frac{p^2-1}{4})y+p \pmod{2p}$$

which is congruent to b_j+p.

Suppose $(p+3)/2 \le j \le (3p-1)/2$. Then $(p+3)/2 \le 2p-(j-1) \le (3p-1)/2$. We have

$$b_j+p \equiv (\frac{p^2-1}{8})x+(j-\frac{p+1}{2})^2+p \pmod{2p}$$

$$\equiv (\frac{p^2-1}{4})y+(\frac{2j-p-1}{2})^2+p \pmod{2p} \text{ and}$$

$$b_{2p-(j-1)} \equiv (\frac{p^2-1}{8})x+[2p-(j-1)-\frac{p+1}{2}]^2 \pmod{2p}$$

$$\equiv (\frac{p^2-1}{4})y+[2p-(j-1)-\frac{p+1}{2}]^2 \pmod{2p}$$

$$\equiv (\frac{p^2-1}{4})y+(\frac{2j-p-1}{2})^2+p \pmod{2p}$$

which is congruent to b_j+p.

Suppose $j = (3p+1)/2$. Then $2p-(j-1) = 2p-[(3p+1)-1] = (p+1)/2$. We have

$$b_j+p \equiv (\frac{p^2-1}{8})x+[\frac{3p+1}{2}-\frac{p+1}{2}]^2+p \pmod{2p}$$

$$\equiv (\frac{p^2-1}{8})x+p^2+p \pmod{2p}$$

$$\equiv\Box(\frac{p^2-1}{8})x \pmod{2p} \text{ and}$$

$$b_{2p-(j-1)} \equiv \{\frac{[(p+1)/2][(p+1)/2-1]}{2}\}x \pmod{2p}$$

$$\equiv (\frac{p^2-1}{8})x \pmod{2p}$$

which is congruent to b_j+p.

Suppose $(3p+3)/2 \le j \le 2p$. Then $2p-(2p-1) \le 2p-(j-1) \le 2p-(3p+3)/2-1$, that is, $1 \le 2p-(j-1) \le (p-1)/2$. We have

$$b_j+p \equiv [\frac{j(j-1)}{2}]x+p+p \pmod{2p}$$

$$\equiv [\frac{j(j-1)}{2}]x \pmod{2p} \text{ and}$$

$$b_{2p-(j-1)} \equiv \{\frac{[2p-(j-1)][2p-(j-1)-1]}{2}\}x \pmod{2p}$$

$$\equiv \{\frac{[2p-(j-1)](2p-j)}{2}\}x \pmod{2p}$$

$$\equiv [\frac{(j-1)j}{2}]x \pmod{2p}.$$

We see that (v) and (vi) are slightly stronger statements than those given in Definition 4.3 though one part of that definition is not covered by these statements.

(v) For $2 \le i \le p$, let $c_i = b_{i-1}+b_i$.

When $2 \le i \le (p+1)/2$

$$\begin{aligned}
b_{i-1}+b_i &\equiv [\frac{(i-1)(i-1-1)}{2}]x+[\frac{i(i-1)}{2}]x \pmod{2p} \\
&\equiv [\frac{i^2-3i+2+i^2-i}{2}]x \pmod{2p} \\
&\equiv [\frac{2i^2-4i+2}{2}]x \pmod{2p} \\
&\equiv (i-1)^2x \pmod{2p}.
\end{aligned}$$

When $(p+3)/2 \le i \le p+1$,

$$\begin{aligned}
b_{i-1}+b_i &\equiv \beta_x\ [(i-1)-\frac{(p+1)}{2}]^2+\beta_x+[i-\frac{(p+1)}{2}]^2 \pmod{2p} \\
&\equiv 2\beta_x+(i-\frac{p+3}{2})^2+(i-\frac{p+1}{2})^2 \pmod{2p}.
\end{aligned}$$

Thus

$$c_i = b_{i-1}+b_i \equiv \begin{cases} (i-1)^2x \pmod{2p} & 2 \le i \le (p+1)/2 \text{ and} \\ 2\beta_x+[(i-\frac{p+1}{2})^2+(i-\frac{p+1}{2})^2] \pmod{2p} & (p+3)/2 \le i \le p+1. \end{cases}$$

Since $x = 2y$, $(i-1)^2x \pmod{2p}$ is even. Therefore, c_i is even for $2 \le i \le (p+1)/2$. For $(p+3)/2 \le i \le p+1$,

$$\begin{aligned}
c_i &\equiv 2\beta_x+[(i-\frac{p+3}{2})^2+(i-\frac{p+1}{2})^2] \pmod{2p} \\
&\equiv 2\beta_x+i^2-i(p+3)+(\frac{p+3}{2})^2+i^2-i(p+1)+(\frac{p+1}{2})^2 \pmod{2p} \\
&\equiv 2\beta_x+2i^2-i(2p+4)+2p+2+\frac{p^2+1}{2} \pmod{2p}.
\end{aligned}$$

We see that $(p^2+1)/2$ is always odd. Therefore, c_i is odd if $(p+3)/2 \le i \le p+1$. Thus it will suffice to show that there is no duplication in either half above. Suppose there exist i, j where $2 \leq i < j \leq (p+1)/2$ such that

$$(i-1)^2x \equiv (j-1)^2x \pmod{2p}.$$

Then $[(i-1)^2-(j-1)^2]y \equiv 0 \pmod{p}$

$\quad$ iff $(i^2-2i-j^2+2j)y \equiv 0 \pmod{p}$

$\quad$ iff $(i-j)(i+j-2)y \equiv 0 \pmod{p}$

$\quad$ iff either $i \equiv j \pmod{p}$

$\qquad\quad$ or $i+j \equiv 2 \pmod{p}$ for $y \not\equiv 0 \pmod{p}$.

But neither of these cases is possible so that the even c_i's are all distinct.

Suppose there exist i and j where $(p+3)/2 \leq i < j \leq p+1$ such that

$$2\beta'_x+[(i-\frac{p+3}{2})^2+(i-\frac{p+1}{2})^2] \equiv 2\beta_x+[(j-\frac{p+3}{2})^2+(j-\frac{p+1}{2})^2] \pmod{2p}$$

and $$2i^2-4i \equiv 2j^2-4j \pmod{2p}.$$

Let $i = t+(p+3)/2$ and $j = s+(p+3)/2$. Then $0 \leq t < s \leq (p-1)/2$. The above then becomes

$$2(t+\frac{p+3}{2})^2-4(t+\frac{p+3}{2}) \equiv 2(s+\frac{p+3}{2})^2-4(s+\frac{p+3}{2}) \pmod{2p}$$

$\quad$ iff $2t^2+2t \equiv 2s^2+2s \pmod{2p}$

$\quad$ iff $t(t+1) \equiv s(s+1) \pmod{p}$.

Let $s = t+k$. The above reduces to

$$t(t+1) \equiv (t+k)(t+k+1) \pmod{p}$$

$\quad$ iff $k(2t+k+1) \equiv 0 \pmod{p}$

$\quad$ iff either $k \equiv 0 \pmod{p}$

$\qquad$ or $2t+k+1 \equiv 0 \pmod{p}$.

But since $k \leq (p-1)/2-t$, it follows that

$$2t+k+1 \le 2t+(p-1)/2-t+1 = (p-1)/2+t+1 \le (p-1)/2+(p-3)/2+1$$
$$= p-1.$$

Neither of these cases is possible so that the odd c_i's are distinct and (v) is verified.

(vi) For $(p+3)/2 \le i \le p+1$, the c_i's are odd numbers. Therefore, in order to show (vi), it suffices to show that

$$2 \le i \le (p+1)/2 \text{ implies } c_i \not\equiv 0 \pmod{2p}.$$

For $2 \le i \le (p+1)/2$, $c_i \equiv (i-1)^2 x \pmod{2p}$.

Thus, $c_i \equiv 0 \pmod{2p}$

iff $(i-1)^2 y \equiv 0 \pmod{p}$

iff $(i-1)^2 \equiv 0 \pmod{p}$ for $y \not\equiv 0 \pmod{p}$

iff $(i-1) \equiv 0 \pmod{p}$.

This is impossible. We have finished the proof. □

In example 1 and example 2, the rows labelled C show c_i's in each case. They are all different.

From Theorem 4.4, if S is a sequencing, it is symmetric and it has several of the properties of strong symmetric sequencings. Thus, we would like to find out when it is the case that S is a sequencing and when it is true that $2m \not\equiv c_i \pmod{2p}$, $2 \le i \le p+1$. Clearly S will be a sequencing precisely when $\{b_i : 1 \le i \le 2p\} = Z_{2p}$, that is, when $P = Z_{2p}$. We will determine exactly when this happens in the following. If we can choose x so that $P = Z_{2p}$ and 2m misses all the c_i's, then we will have a strong symmetric sequencing.

Theorem 4.5 : Let $\Sigma_x = \{(0+1+...+i)x \pmod{2p} : 0 \le i \le (p-1)/2\}$ and $W_x \equiv \{[\beta +(2k)^2] \pmod{2p} : 1 \le k \le (p-1)/2\}$ where $\beta_x = [(p^2-1)/8]x$. If $x = 2y \in Z_{2p}$, then $|\Sigma_x| = (p+1)/2$ and $|W_x| = (p-1)/2$.

Proof : Suppose $x = 2y \in Z_{2p}$. In order to show $|\Sigma_x| = (p+1)/2$, it is sufficient to show that all elements of Σ_x are distinct. If we assume the contrary, then there are i_1, i_2 within the specified limits and $i_1 > i_2$ such that

$(0+1+...+i_1)x \equiv (0+1+...+i_2)x \pmod{2p}$

iff $i_1(i_1+1)y \equiv i_2(i_2+1)y \pmod{2p}$.

Let $i_1 = i_2+t$. The above reduces to

$i_2(i_2+1)y \equiv (i\ +t)(i_2+t+1)y \pmod{2p}$

iff $t(2i_2+t+1)y \equiv 0 \pmod{2p}$.

But $0 < t \le (p-1)/2-i_2$ and it follows that

$2i_2+t+1 \le 2i_2+(p-1)/2-i_2+1 = i_2+(p-1)/2+1 \le p-1$ and $y<p$, $t<p$. Therefore, $t(2i_2+t+1)y \equiv 0 \pmod{2p}$ is impossible. Then all elements of Σ_x are distinct. We have $|\Sigma_x| = (p+1)/2$.

Similarly, suppose not all elements of W_x are distinct. There exist k_1 and k_2 with $1 \le k_2 < k_1 \le (p-1)/2$ such that

$\beta_x+(2k_1)^2 \equiv \beta_x+(2k_2)^2 \pmod{2p}$

iff $2(k_1-k_2)(k_1+k_2) \equiv 0 \pmod{2p}$

iff $(k_1-k_2)(k_1+k_2) \equiv 0 \pmod{p}$.

This is impossible and therefore $|W_x| = (p-1)/2$. □

In the next theorem, we are going to see under what conditions S is a sequencing. That is, under what conditions $P = \{b_i : 1 \le i \le 2p\} = Z_{2p}$.

Theorem 4.6 : If $\Sigma_x \cap W_x = \phi$, then $P = Z_{2p}$.

Proof : Let $N = \{1,2,\ldots,2p\}$ and $Q = \{\{j,2p-(j-1)\} : 1 \le j \le p\}$. Suppose $D = \{1,2,\ldots,(p+1)/2\}$ and $E = \{(p+1)/2+2k : 1 \le k \le (p-1)/2\}$. Let $V = D \cup E$. We see that if x_1, x_2 belong to $D \cup E$, then $x_1+x_2 \ne 2p+1$. Hence $V = D \cup E$ contains exactly one element of each member of Q. By the definitions of Σ_x and W_x, $\Sigma_x = \{b_r : r \in D\}$ and $W_x = \{b_r : r \in E\}$. Then $\Sigma_x \cup W_x = \{b_r : r \in V\}$. Also all elements of Σ_x and W_x are even. So $\Sigma_x \cup W_x \subset \langle x \rangle$.

If $\Sigma_x \cap W_x = \phi$, then by the last theorem $|\Sigma_x \cup W_x| = p$. We have $\Sigma_x \cup W_x = \langle x \rangle$. It implies $\{b_r : r \in V\} = \langle x \rangle$. By Theorem 4.4(iv), $\{b_t : t \in N \setminus V\} = \langle x \rangle + p$. Then $P = \{b_t : t \in N\} = \langle x \rangle + p \cup \langle x \rangle = Z_{2p}$. □

Theorem 4.7[4] : Suppose $p \ge 3$ is a prime, $x = 2y \in Z_{2p}$ and S and P are defined as usual. Then

(1) $(y|p) = -1$ if and only if $\Sigma_x \cup W_x = \langle x \rangle$ if and only if S is a symmetric sequencing.

(2) $(y|p) = 1$ if and only if $\Sigma_x \setminus \{\beta_x\} = W_x$.

Proof : $\Sigma_x \cap W_x \ne \phi$ means that there exist i, $0 \le i \le (p-1)/2$, and k, $1 \le k \le (p-1)/2$, such that

$$(0+1+\ldots+i)x \equiv [\beta_x+(2k)^2] \pmod{2p}$$

$$\text{iff } [i(i+1)/2]2y \equiv [(p^2-1)/8]2y+4k^2 \pmod{2p}$$

$$\text{iff } 4i(i+1)y \equiv [(p^2-1)y+16k^2] \pmod{2p}$$

$$\text{iff } 16k^2 \equiv (2i+1)^2y \pmod{p}. \qquad (*)$$

Also, we notice that $16k^2 \not\equiv 0 \pmod{p}$ for $1 \le k \le (p-1)/2$ and $i \ne (p-1)/2$.

(1) If $(y|p) = -1$, then $(y(2i+1)^2|p) = -1((2i+1)^2|p) = -1$. Therefore, (*) does not hold. Hence $\Sigma_x \cap W_x = \phi$ which implies $\Sigma_x \cup W_x = \langle x \rangle$.

Now, suppose $\Sigma_x \cup W_x = \langle x \rangle$ so that $\Sigma_x \cap W_x = \phi$. If $(y|p) = 1$, then $((2i+1)^2y|p) = 1$. This means that for any given i there exists a k such that $16k^2 \equiv (2i+1)^2y \pmod{p}$. Thus $(y|p) = -1$. It is obvious that $\Sigma_x \cup W_x = \langle x \rangle$ if and only if S is a symmetric sequencing.

(2) Suppose $(y|p) = 1$. For a given i, there exists an unique k such that (*) holds. The existence is as above. For uniqueness, suppose that for a given i there exist k_1 and k_2, $k_1 \ne k_2$ such that

$16k_1^2 \equiv (2i+1)^2y \pmod{p}$ and

$16k_2^2 \equiv (2i+1)^2y \pmod{p}$. Then

$16k_1^2-16k_2^2 \equiv 0 \pmod{p}$.

This is equivalent to $16(k_1-k_2)(k_1+k_2) \equiv 0 \pmod{p}$ which is impossible for any k in the allowed range. Thus there are $(p-1)/2$ solutions to (*). Since $i = (p-1)/2$ is eliminated at the beginning, it follows that $\Sigma_x \backslash \{\beta_x\} = W_x$.

Suppose $W_x = \Sigma_x \backslash \{\beta_x\}$, then $\Sigma_x \cap W_x \neq \phi$, which implies $16k^2 \equiv (2i+1)^2 y \pmod{p}$ for some i, k. Then $((2i+1)^2 y|p) = ((2i+1)^2|p)(y|p) = (y|p) = 1$. The proof if finished. □

From the above theorem, we know that for a prime $p \geq 3$, if we can choose a y such that $(y|p) = -1$, then S is a symmetric sequencing. We are going to show such a sequencing S is a strong symmetric sequencing if $p \geq 5$. In the following, let

$$\begin{aligned} C &= \{b_{i-1}+b_i : 2\leq i\leq p+1\} \\ &= \{c_i : 2\leq i\leq p+1\}. \end{aligned}$$

<u>Theorem 4.8</u>[4] : Suppose $p \geq 3$ is a prime, $x = 2y \in Z_{2p}$ and S and P are constructed as usual. We have that

(1) if $p \equiv 1 \pmod{4}$, then $2m \notin C$ iff $(y|p) = (y-1|p)$ and

(2) if $p \equiv 3 \pmod{4}$, then $2m \notin C$ iff $(y|p) = (y-1|p)$.

<u>Proof</u> : If $2m \in C$, then there exists an i, $2\leq i\leq p+1$, such that $b_{i-1}+b_i \equiv 2m \pmod{2p}$.

However, 2m is always even so that we only have to consider the i's such that $2\leq i\leq (p+1)/2$ as c_i is even only when $2\leq i\leq (p+1)/2$. We have only to consider

$(i-1)^2x \equiv [(p^2-1)/4]x+[(p+1)^2]/2 \pmod{2p}$ for $2\le i\le(p+1)/2$.

This is equivalent to

$$(i-1)^2y \equiv [(p^2-1)/4]y+[(p+1)^2]/4 \pmod{p}$$

and $4(i-1)^2y \equiv (-1)(y-1) \pmod{p}$.

Hence $(4(i-1)^2y|p) = ((-1)(y-1)|p)$ and then

$$(y|p) = (-1|p)(y-1|p).$$

Therefore, $2m \in C$ if and only if $(y|p) = (-1|p)(y-1|p)$.

Now $(-1|p) = (-1)^{(p-1)/2} = \begin{cases} 1 \text{ if } p \equiv 1 \pmod{4} \text{ and} \\ -1 \text{ if } p \equiv 3 \pmod{4}. \end{cases}$

If $p \equiv 1 \pmod{4}$, then $2m \notin C$

iff $(y|p) \ne (-1|p)(y-1|p)$

iff $(y|p) \ne (y-1|p)$.

If $p \equiv 3 \pmod{4}$, then $2m \notin C$

iff $(y|p) \ne (-1|p)(y-1|p)$

iff $(y|p) \ne -(y-1|p)$

iff $(y|p) = (y-1|p)$. □

<u>Theorem 4.9</u>[4] : Suppose $p \ge 3$ is a prime, $x = 2y \in Z_{2p}$ and S and P are constructed as usual. We have that

(1) if $p \equiv 1 \pmod{4}$, then S is a strong symmetric sequencing if and only if $(y|p) = -1$ and $(y-1|p) = 1$ and

(2) if $p \equiv 3 \pmod{4}$, then S is a strong symmetric sequencing if and only if $(y|p) = -1$ and $(y-1|p) = -1$.

<u>Proof</u> : Let $P \equiv 1 \pmod{4}$ for case (1). If S is a strong symmetric sequencing, then from Theorem 4.7 $(y|p) = -1$ and

from Theorem 4.8 $(y|p) \neq (y-1|p)$, that is, $(y-1|p) = 1$. If $(y|p) -1$ and $(y-1|p) = 1$, then from Theorem 4.7 S is a symmetric sequencing and from Theorem 4.8 $2m \notin C$. That is, S is a strong symmetric sequencing.

Case (2) is similar to (1). □

If we use the process given above for Z_6, we get a sequencing S: 0,4,1,3,5,2 which is a symmetric sequencing but not strong. The only other symmetric sequencings for Z_6 are

S_1: 0,5,2,3,4,1; P_1: 0,5,1,4,2,3; C_1: 5,0,5; $2m_1 = 3$;
S_2: 0,2,5,3,1,4; P_2: 0,2,1,4,5,3; C_2: 2,3,5; $2m_2 = 3$;
S_3: 0,1,4,3,2,5; P_3: 0,1,5,2,4,3; C_3: 1,0,1; $2m_3 = 4$;
S_4: 0,4,1,3,5,2; P_4: 0,4,5,2,1,3; C_4: 4,3,1; $2m_4 = 4$.

None of them is strong. Therefore, no strong symmetric sequencing exists from Z_6.

Now we come to one of our main theorems.

<u>Theorem 4.10</u>[4] : If $p \geq 5$ is a prime, then Z_{2p} has a strong symmetric sequencing.

<u>Proof</u> : According to the previous theorems, what we have to prove is to show that when $p \equiv 1 \pmod 4$, there exists $y \in Z_{2p}$ such that $(y|p) = -1$ and $(y-1|p) = 1$ and when $p \equiv 3 \pmod 4$, there exists $y \in Z_{2p}$ such that $(y|p) = (y-1|p) = -1$.

We know that the number of pairs of consecutive integers in [1,p-1] in which the first is a quadratic residue and the second is a quadratic nonresidue modulo p is $N_1(p) = (1/4)[p-(-1)^{(p-1)/2}]$ and the number of pairs of consecutive integers in [1,p-1] in which the first is a quadratic nonresidue and the second is a quadratic nonresidue modulo p is $N_2(p) = (1/4)[(p-2)+(-1)^{(p-1)/2}]$ see [5]. Then when $p \geq 5$ and $p \equiv 1 \pmod 4$ $N_1(p) \geq 1$ and when $p \geq 5$ and $p \equiv 3 \pmod 4$, $N_2(p) \geq 1$. That is, when $p \geq 5$, $p \equiv 1 \pmod 4$, there exists $y \in Z_{2p}$ such that $(y|p) = -1$ and $(y-1|p) = 1$ and when $p \geq 5$, $p \equiv 3 \pmod 4$, there exists $y \in Z_{2p}$ such that $(y|p) = -1$ and $(y-1|p) = -1$. Thus a strong symmetric sequencing always exists for Z_{2p} when $p \geq 3$. □

<u>Example</u> : Let $p = 5$, $x = 4$ and $y = 7$. Then $p \equiv 1 \pmod 4$, $(y-1|p) = (6|5) = 1$, and $(y|p) = (7|5) = -1$. Also,

$S = 0,4,8,1,3,5,7,9,2,6;$

$P = 0,4,2,3,6,1,8,7,9,5;$

$C = 4,6,5,9,7;$

$m_x = b_6 = 1$; and $2m_x = 2$.

Thus S is a strong symmetric sequencing.

In the following we are going to show that strong symmetric sequencings occur for the cyclic groups Z_{p-1}, when $p \geq 3$ is a prime and $p = 5$ or $p \equiv \pm 3, \pm 13 \pmod{40}$.[10] In order to show this, we begin by defining the definition of starter first.

Definition 4.4 : Suppose n is a positive integer and G is an abelian group of order 2n written additively. Suppose that G has exactly one element g^* of order 2. Then E is an even starter for G if and only if $E = \{\{x_i, y_i : 1 \le i \le n-1\}$ such that

(1) Every nonzero element of G except one, denoted by m, occurs as an element in some pair of E and

(2) Every nonzero element of G except g^* occurs as a difference of some pair of G.

If $1 \le i < j \le n-1$ implies $x_i + y_i \ne x_j + y_j$, $x_i + y_i \notin \{0, 2m\}$, and $m \ne g^*$ we call E a strong even starter. Strong even starters can be used to construct Howell designs and even starters induce 1-factorizations of K_{2n+2} which we will discuss in the next chapter. At this time we are only interested in the construction of strong symmetric sequences.

Theorem 4.11 : If G has a strong even starter, then G has a strong symmetric sequencing where $G = Z_{2n}$.

Proof : Suppose G has a strong even starter $E = \{\{x_i, y_i\} : 1 \le i \le n-1\}$. Let $E^* = E \cup \{0, m\}$ and $Q^* = \{\{x, x+g^*\} : x \in G\}$. Then every element of G occurs as an element in some pair of Q^* and $Q^* \cap E^* = \phi$. Therefore, $E^* = \{0, h_1\} \cup \{\{h_i + g^*, h_{i+1}\} : 1 \le i \le n-1\}$ where $h_1 = m$.

Let us define H to be a sequencing in the form

H: $0,h_1,h_1+g^*,h_2,h_2+g^*,\ldots,h_{n-1},h_{n-1}+g^*,h_n = g^*$. According to H, we construct the sequence P of partial products. If n is even, we start $h_1 = m$ in the middle at b_n. If n is odd, we start $h_1 = m$ in the middle at b_{n+1}. Then we work to the ends of P alternating from side to side. We have P_{even}: $0, h_{n-1}, h_{n-2}+g^*, \ldots, h_3, h_2+g^*, h_1,$

$h_1+g^*, h_2, h_3+g^*, \ldots, h_{n-1}+g^*, h_n$, and

P_{odd} : $0, h_{n-1}, h_{n-2}+g^*, \ldots, h_4, h_3+g^*, h_2,$

$h_1+g^*, h_1, h_2+g^*, h_3, h_4+g^*, \ldots, h_{n-1}+g^*, h_n$.

For n even, $b_n = h_1 = m$, $b_{2n} = h_n = g^*$ and for n odd, $b_{n+1} = h_1$ and $b_{2n} = h_n$. We construct the sequencing $S = \{a_i : a_i=b_i-b_{i-1}, 2\le i\le 2n\}$ and $a_1 = 0$. We have $a_{n+1} = g^*$ for $-g^* = g^*$, and $a_{n+1+i} = -h_{i+1}+h_i+g^*$, $a_{n+1+i} = h_{i+1}-h_i-g^*$, $1\le i\le n-1$. So $a_{n+1+i} = -(a_{n+1-1})$ and each a_{n+1-i} is a difference of a pair $\{h_i+g^*, h_{i+1}\}$ of the starter E. Therefore, S induces every element of G and is a symmetric sequencing.

Since E is a strong even starter, then for $1\le i<j\le n-1$, we have $b_i+b_{i+1} \ne b_j+b_{j+1}$ and $b_i+b_{i+1} \notin \{0,2m\}$. So S is a strong symmetric sequencing. □

<u>Example</u> : For n = 5, E = {{4,2}, {3,6}, {8,7}, {9,5}} with $m = 1$, $g^* = 5$ is a strong even starter of Z_{10} because $4+2 = 6$, $3+6 = 9$, $8+7 = 5$, $9+5 = 4$ are all distinct and not equal to $2m = 2$. Now $Q^* = \{\{x,x+g^*\} : x\in G\}$

$= \{\{0,5\}, \{1,6\}, \{2,7\}, \{3,8\}, \{4,9\}\}$;

H: 0,1,6,3,8,7,2,4,9,5;

P: 0,4,2,3,6,1,8,7,9,5; and

S: 0,4,8,1,3,5,7,9,2,6.

Thus S is a strong symmetric sequencing.

In order to show that there exists a strong symmetric sequencing in Z_{p-1}, we have to show that there exists a strong even starter in Z_{p-1}.

Let $f: (Z_p \setminus \{0\}) \to Z_{p-1}$ be the function defined by $f(r^i) = i$ where r is a primitive root of GF[p]. Obviously f is a 1-1, onto function.

Example : For p = 11, 2 is a primitive root of GF[11] because $2^0 \equiv 1$, $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 5$, $2^5 \equiv 10$, $2^6 \equiv 9$, $2^7 \equiv 7$, $2^8 \equiv 3$, $2^9 \equiv 6$ (mod 11). Therefore, f(1)=0, f(2)=1, f(3)=8, f(4)=2, f(5)=4, f(6)=9, f(7)=7, f(8)=3, f(9)=6, f(10)=5. Evidently it is 1-1 and onto.

Note that $p-1 = 2^n t$, t odd and $r^{(p-1)/2} \equiv -1 \pmod p$. Therefore, $r^{2^{n-1}t} \equiv -1 \pmod p$. If $x = r^i$, $x \neq 0$, then

$$f(\{x,-x\}) = f(\{r^i,-r^i\}) = f(\{r^i,-1\cdot r^i\})$$

$$= f(\{r^i,r^{i+2^{n-1}t}\}) = \{i,i+2^{n-1}t\} = \{i,i+(p-1)/2\}.$$

Let us consider the sequence T: $\{a_i\}_{i=0}^{p-1} = \{1,3,5,\ldots$ $\ldots,p-4,p-2,0,2,4,6,\ldots,p-5,p-3,p-1\}$.

Let $E = \{\{a_i,a_{i+1}\} : i = 1,3,5,\ldots,p-2\}$
$\setminus$ {the pair with 0 as one of the elements}.

Note that the element in T paired with 0 is either 2 or -2.

Theorem 4.12 : If $p > 3$ and $p = 5$ or $p \equiv \pm 3, \pm 13 \pmod{40}$, then $f(E)$ is a strong even starter.

Proof : Let $K = \{\{a_i, a_{i+1}\} : i = 0,1,\ldots,p-2$, minus the two pairs with zero$\}$. We see that if $\{a_i, a_{i+1}\} \in K$, then $\{-a_i, -a_{i+1}\} \in K$ and $f(a_i)-f(a_{i+1}) = f(-a_i)-f(-a_{i+1})$. For if $a_i = r^s$ and $a_{i+1} = r^t$, then $f(a_i)-f(a_{i+1}) = s-t$ and $f(-a_i)-f(-a_{i+1}) = [s+(p-1)/2]-[t+(p-1)/2] = s-t$. And, if $\{a_i, a_{i+1}\} \in E$, then $\{-a_i, -a_{i+1}\} \notin E$. Since $f(\{x,-x\}) = \{i, i+(p-1)/2\}$ where $r^i = x$ and none of the pairs in E have one entry that is the inverse of the other, then there exists no pair $\{i,j\}$ in E such that $f(i)-f(j) = (p-1)/2 = g^*$ in Z_{p-1}. Also $f(i)-f(j) \neq 0$ for any pair $\{i,j\} \in E$ because f is one-one and onto. Thus $f(E)$ will be an even starter for Z_{p-1}, if we can show that $1 \leq i < j \leq (p-3)/2$ implies $[f(2i)-f(2i+2)] \not\equiv \pm[f(2j)-f(2j+2)] \pmod{p-1}$.

Suppose $2 = r^k$, $i = r^s$ and $j = r^t$. Then $i \neq j$, $r^k(r^s+1) = r^m$ and $r^k(r^t+1) = r^n$.

To the contrary, assume that for some i,j, we have $[f(2i)-f(2i+2)] \equiv [f(2j)-f(2j+2)] \pmod{p-1}$. Then

$$(k+s)-f(r^k r^s+r^k) \equiv (k+t)-f(r^k r^t+r^k) \pmod{p-1}$$

or $(k+s-m) \equiv (k+t-n) \pmod{p-1}$

or $\quad s+n \equiv t+m \pmod{p-1}$.

Therefore, $r^{s+n} \equiv r^{t+m} \pmod{p}$ or

$$r^s r^k(r^t+1) \equiv r^t r^k(r^s+1) \pmod p \text{ or}$$
$$r^s r^k \equiv r^t r^k \pmod p \text{ or}$$
$$r^s \equiv r^t \pmod p.$$

This is a contradiction.

Assume $[f(2i-f(2i+2)] \equiv -[f(2j-f(2j+2)] \pmod{p-1}$.

Then $(k+s-m) \equiv -(k+t-n) \pmod{p-1}$ or

$$s+t \equiv m+n-2k \pmod{p-1}.$$

Therefore, $r^{s+t} \equiv r^{m+n-2k} \pmod p$ or

$$r^{s+t} \equiv r^k(r^s+1)r^k(r^t+t)r^{-2k} \pmod p \text{ or}$$
$$r^{s+t} \equiv (r^s+1)(r^t+1) \pmod p \text{ or}$$
$$r^s+r^t \equiv -1 \pmod p \text{ or}$$
$$i+j \equiv -1 \pmod p.$$

This is impossible for the range of i,j. It follows that $f(E)$ is an even starter for Z_{p-1}.

To show $f(E)$ is a strong even starter, we still have to show $m \neq g^*$ in $f(E)$, the sum of the pairs of $f(E)$ are distinct and they are neither 0 nor $2m$.

We know that $m = f(2)$ or $m = f(-2)$ and $g^* = (p-1)/2$. Suppose $2 = r^k$. Then $f(2) = k$ and $f(-2) = k+(p-1)/2$. If $k = (p-1)/2$, then $-2 = r^{(p-1)/2+(p-1)/2} = 1$ and $p = 3$. If $k = 0$, then $2 = r^{(p-1)/2} = 1$. Both cases are impossible so that $m \neq g^*$.

Consider the pairs in K. It is clear that $f(a_i)+f(a_{i+1}) \equiv f(-a_i)+f(-a_{i+1}) \pmod{p-1}$. The sums of the pairs of $f(E)$ are distinct if we can show

$f(2i)+f(2i+2)] \not\equiv [f(2j)+f(2j+2)] \pmod{p-1}$

for $1 \leq i < j \leq (p-3)/2$.

To the contrary, assume for some i,j, we have

$[f(2i)+f(2i+2)] \equiv [f(2j)+f(2j+2)] \pmod{p-1}$.

Then $k+s+m \equiv k+t+n \pmod{p-1}$ or

$s+m \equiv t+n \pmod{p-1}$ or

$r^{s+m} \equiv r^{t+n} \pmod{p}$ or

$r^s(r^s+1) \equiv r^t(r^t+1) \pmod{p}$ or

$r^s r^s - r^t r^t \equiv -(r^s - r^t) \pmod{p}$ or

$(r^s+r^t) \equiv -1 \pmod{p}$.

This is a contradiction. All sums of pairs of $f(E)$ are distinct modulo $p-1$. We can show the sums of the pairs in $f(E)$ are not equal to 0 or $2m$, similar to the above. The prime p will have the required properties if and only if for $1 \leq i \leq (p-3)/2$ neither

$[f(2i)+f(2i+2)] \equiv 0 \pmod{p-1}$ nor

$[f(2i)+f(2i+2)] \equiv 2f(2) \pmod{p-1}$ has a solution.

Now $f(2i)+f(2i-2) \equiv 0 \pmod{p-1}$

iff $(k+s+m) \equiv 0 \pmod{p-1}$

iff $r^{k+s+m} \equiv 1 \pmod{p}$

iff $r^s r^k (r^s+1) r^k \equiv 1 \pmod{p}$

iff $4i(i+1) \equiv 1 \pmod{p}$. (a)

Also, $[f(2i)+f(2i+2)] \equiv 2f(2) \pmod{p-1}$

iff $s+m \equiv k \pmod{p-1}$

iff $r^{s+m} \equiv r^k \pmod{p}$

iff $r^s(r^s+1) \equiv 1 \pmod{p}$

iff $i(i+1) \equiv 1 \pmod{p}$. (b)

If $p = 5$, obviously (a), (b) do not both hold. Since $(-n-1)(-n-1+1) = n(n+1)$, if n is a solution to either (a) or (b) so is $-n-1$. This means that if we have integer n_1 where $1 \le n_1 \le (p-3)/2$ which is a solution to either (a) or (b), then there exists n_2 which has the same properties as n_1 and $p/2 \le n_2 \le p-2$ as $n_2 = -1-n_1$. If $p > 5$, $(p-1)/2$ is not a solution of either (a) or (b), and $(p+1)/2$ has the same properties as $(p-1)/2$. This reduces the problem to looking for the primes p such that there are no solutions at all to (a) and (b). Since

$$n(n+1) \equiv 1 \pmod{p}$$

$$\text{iff } 4n(n+1) \equiv 4 \pmod{p}$$

$$\text{iff } 4n^2+4n+1 \equiv 5 \pmod{p}$$

$$\text{iff } (2n+1)^2 \equiv 5 \pmod{p}.$$

Then (a) has no solution if and only if $(5|p) = -1$. Now

$$4n(n+1) \equiv 1 \pmod{p}$$

$$\text{iff } 4n^2+4n+1 \equiv 2 \pmod{p}$$

$$\text{iff } (2n+1)^2 \equiv 2 \pmod{p}.$$

Therefore, (b) has no solution if and only if $(2|p) = -1$. We know that $(5|p) \equiv -1$ iff $p \equiv \pm 3 \pmod{5}$ and

$$(2|p) \equiv -1 \text{ iff } p \equiv \pm 3 \pmod{8}$$

which implies that $p \equiv \pm 3, \pm 13 \pmod{40}$. Therefore, $f(E)$ is a strong even starter if and only if $p \equiv 5$ or $p \equiv \pm 3, \pm 13 \pmod{40}$. □

CHAPTER FIVE

Applications of Sequenceable Group

In this cahpter, we will discuss some applications of sequenceable groups to Latin Squares, Howell Designs and Graphy Theory.

§5.1 Applications to Latin Squares

Definition 5.1 : A Latin square L of order n is an n×n matrix with n^2 elements based on a set X with n distinct elements such that none of them occurs twice in any row or column of the matrix.

Definition 5.2 : A Latin square L of order n on a set X with n distinct elements is called row (column) complete if for every ordered pair (a,b) where $a \neq b$, $a,b \in X$, there exists exactly one row (column) of the Latin square in which a and b appear as adjacent elements.

If a Latin square is both row and column complete, we call it a complete Latin square.

Let $[m_{st}]$ denote a Latin square of order n on X. Then it is row (column) complete if for any ordered pair (a,b), where $a,b \in X$, there exists exactly one pair of integers s, t where $1 \leq s \leq n$, $1 \leq t \leq n$ such that

$$m_{st} = a \qquad m_{s,t+1} = b$$

$$(m_{st} = a \qquad m_{s+1,t} = b).$$

Examples :

The Latin square $\begin{matrix} 0 & 1 & 3 & 2 \\ 1 & 2 & 0 & 3 \\ 2 & 3 & 1 & 0 \\ 3 & 0 & 2 & 1 \end{matrix}$ is row complete.

The Latin square $\begin{matrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 3 & 0 & 1 & 2 \\ 2 & 3 & 0 & 1 \end{matrix}$ is column complete.

Finally, the Latin square $\begin{matrix} 0 & 2 & 1 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 1 & 2 & 0 \end{matrix}$ is complete.

B. Gordon found a sufficient condition for the existence of a complete Latin square.

Theorem 5.1 : If G is a sequenceable group of order n, then there exists a complete Latin square of order n.

Proof : Let $S:a_1,a_2,\ldots,a_n$ be a sequencing of G and $P:b_1,b_2,\ldots,b_n$ be the sequence of partial products of S. We are going to verify that the matrix $[m_{st}]$ with $m_{st} = b_s^{-1}b_t = a_{s+1}a_{s+2}\ldots a_t$ is a complete Latin square.

Since S is a sequencing, then $a_{s+1}a_{s+2}\ldots a_t \neq a_{r+1}a_{r+2}\ldots a_t$ if $s \neq r$. That is, $m_{st} \neq m_{rt}$ if $r \neq s$.

Therefore, each row of $[m_{st}]$ contains each element of G exactly once. Furthermore, $m_{rt} \neq m_{ru}$ if $t \neq u$, as $a_{r+1}a_{r+2}\cdots a_t \neq a_{r+1}a_{r+2}\cdots a_u$. Therefore, each column of $[m_{st}]$ contains each element of G exactly once. Thus $[m_{st}]$ is a Latin square.

To show $[m_{st}]$ is row complete, suppose

$$m_{st} = m_{uv} \text{ and } m_{s,t+1} = m_{u,v+1}.$$

We have to show $s = u$ and $t = v$. By the definition of m_{st},

$$b_s^{-1}b_t = b_u^{-1}b_v \qquad (i)$$

and $$b_s^{-1}b_{t+1} = b_u^{-1}b_{v+1}. \qquad (ii)$$

From (i), $(b_s^{-1}b_t)^{-1} = (b_u^{-1}b_v)^{-1}$ which implies

$$b_t^{-1}b_s = b_v^{-1}b_u. \quad (iii)$$

The product of (ii) and (iii) yields

$$(b_t^{-1}b_s)(b_s^{-1}b_{t+1}) = (b_v^{-1}b_u)(b_v^{-1}b_{v+1})$$

which implies $b_t^{-1}b_{t+1} = b_v^{-1}b_{v+1}$.

That is, $a_{t+1} = a_{v+1}$, and we have $t = v$.

Put $t = v$ into (i) which produces $b_s^{-1} = b_u^{-1}$ and implies $s = u$. Therefore, $[m_{st}]$ is row complete. Similarly, $[m_{st}]$ is also column complete. Then the matrix $[m_{st}]$ which is based on the sequenceable group G is a complete Latin square. □

Using the proof of the preceeding theorem, we can construct a complete Latin square of order n if a sequenceable group of order n exists.

<u>Example</u> : Let us consider the group Z_8. S: 0,1,6,3,4,5,2,7 is a sequencing and P: 0,1,7,2,6,3,5,4 is the sequence of partial products. Then the Latin square

$$[m_{st}] = \begin{array}{cccccccc} 0 & 1 & 7 & 2 & 6 & 3 & 5 & 4 \\ 7 & 0 & 6 & 1 & 5 & 2 & 4 & 3 \\ 1 & 2 & 0 & 3 & 7 & 4 & 6 & 5 \\ 6 & 7 & 5 & 0 & 4 & 1 & 3 & 2 \\ 2 & 3 & 1 & 4 & 0 & 5 & 7 & 6 \\ 5 & 6 & 4 & 7 & 3 & 0 & 2 & 1 \\ 3 & 4 & 2 & 5 & 1 & 6 & 0 & 7 \\ 4 & 5 & 3 & 6 & 2 & 7 & 1 & 0 \end{array}$$

is complete.

We notice that for a comple Latin square, if we interchange some rows (columns), this complete square will become a row (column) complete but not column (row) complete.

<u>Example</u> : Let us consider Z_6. Now S: 0,1,4,3,2,5 is a sequencing and P: 0,1,5,2,4,3 is the partial product sequence. Then the Latin square

$$\begin{array}{cccccc} 0 & 1 & 5 & 2 & 4 & 3 \\ 1 & 2 & 0 & 3 & 5 & 4 \\ 5 & 0 & 4 & 1 & 3 & 2 \\ 2 & 3 & 1 & 4 & 0 & 5 \\ 4 & 5 & 3 & 0 & 2 & 1 \\ 3 & 4 & 2 & 5 & 1 & 0 \end{array}$$

is complete.

The Latin square

$$\begin{array}{cccccc}
0 & 1 & 5 & 2 & 4 & 3 \\
1 & 2 & 0 & 3 & 5 & 4 \\
4 & 5 & 3 & 0 & 2 & 1 \\
3 & 4 & 2 & 5 & 1 & 0 \\
2 & 3 & 1 & 4 & 0 & 5 \\
5 & 0 & 4 & 1 & 3 & 2
\end{array}$$

is row complete.

We now consider some relations between sequenceable groups and orthogonal Latin squares.

Definition 5.3 : Two Latin squares $[k_{ij}]$ and $[t_{ij}]$ of order n on the n-sets R and S respectively, are orthogonal if every ordered pair of symbols occurs exactly once among the n^2 pairs $[k_{ij}, t_{ij}]$, $i = 1,\dots,n$, $j = 1,\dots,n$.

For example, let

$$[k_{ij}] = \begin{array}{ccc} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 1 & 2 \end{array} \quad \text{and} \quad [t_{ij}] = \begin{array}{ccc} 2 & 1 & 3 \\ 1 & 3 & 2. \\ 3 & 2 & 1 \end{array}$$

Superimposing one upon the other yields

$$\begin{array}{ccc}
2,2 & 3,1 & 1,3 \\
1,1 & 2,3 & 3,2 \\
3,3 & 1,2 & 2,1.
\end{array}$$

We see that the Latin squares $[k_{ij}]$ and $[t_{ij}]$ are othogonal. The following theorems were proven by K. Heinrich.

Theorem 5.2 : If G is a sequenceable group of order n and if there are two orderings of G, say $h_1, h_2, \ldots, h_n$ and h_1', $h_2', \ldots, h_n'$, with the property that $h_1(h_1')^{-1}, h_2(h_2')^{-1}, \ldots$ $\ldots, h_n(h_n')^{-1}$ is also an ordering of G, then we can construct a pair of orthogonal Latin squares of order n with the property that one is row complete and the other is complete.

Proof : Let $a_1, a_2, \ldots, a_n$ be a sequencing of G. Choose $h_1 = a_1, h_2 = a_1a_2, \ldots, h_n = a_1a_2\ldots a_n$. Construct the Latin square $[t_{ij}]$ with the first row being $a_1, a_1a_2, \ldots$ $\ldots, a_1a_2\ldots a_n$. Row i is obtained by multipling each element of row one on the left by h_i. Construct the Latin square $[k_{ij}]$ with the first row being $a_1, a_1a_2, \ldots, a_1a_2\ldots a_n$. Row i is again obtained by multipling each element of row one on the left by h_i'. Then by Theorem 5.2, Latin square $[t_{ij}]$ is complete and $[k_{ij}]$ is row complete.

In order to show $[t_{ij}]$ and $[k_{ij}]$ are orthogonal, assume that there exist ordered pairs (r,s) and (u,v) such that the ordered pairs (t_{rs}, k_{rs}) and (t_{uv}, k_{uv}) are equal. We have to show $r = u$, $s = v$. From our construction we have $h_ra_1a_2\ldots a_s = h_ua_1a_2\ldots a_v$

and $h_r'a_1a_2\ldots a_s = h_u'a_1a_2\ldots a_v$.

Then $(h_ra_1a_2\ldots a_s)(h_r'a_1a_2\ldots a_s)^{-1} = (h_ua_1a_2\ldots a_v)(h_u'a_1a_2\ldots a_v)^{-1}$

which implies $h_r(h_r')^{-1} = h_u(h_u')^{-1}$.

Since $h_1(h_1')^{-1}$, $h_2(h_2')^{-1}, \dots, h_n(h_n')^{-1}$ is an ordering of G, then $r = u$. Substituting $r = u$ in the above, we obtain $s = v$. The proof is finished. □

<u>Theorem 5.3</u> : If the non-abelian group G of order $n = pq$, where p and q are distinct odd primes and $p|q-1$, is sequenceable, then there exists a set of p-1 pair wise orthogonal Latin squares of order n all of which are row complete.

<u>Proof</u> : Suppose G is the group described in the above. Then $G = \langle a,b\rangle$ and is defined by $a^q = b^p = 1$ and $ab = ba^r$ where $r^p \equiv 1 \pmod q$, $r \not\equiv 1 \pmod q$ and $p|q-1$.

Let us consider

$G_k = \{1,(b^i)^k,(a^i)^k,(b^ia^j)^k : 1\le i\le p-1,\ 1\le j\le q-1\}$ for a fixed k, $1\le k\le p-1$. Since $(b^i)^k = b^{ik}$ and all $(b^1)^k,(b^2)^k,\dots,(b^{q-1})^k$ are distinct given the range of i, then $\{(b^i)^k : 1\le i\le p-1\}$ is equal to $\{b^i : 1\le i\le p-1\}$. Similarly, $\{(a^j)^k : 1\le i\le q-1\} = \{a^j : 1\le j\le q-1\}$. Let us consider the set $\{(b^ia^j)^k : 1\le i\le p-1,\ 1\le j\le q-1\}$ for a fixed k. We have

$(b^ia^j)^k = b^{ik}a^{j[r^{(k-1)i}+r^{(k-2)i}+\dots+r^{2i}+r^i+1]}$ for $ab = ba^r$.

Suppose there exist (i_1,j_1) and (i_2,j_2) such that $(b^{i_1}a^{j_1})^k = (a^{i_2}a^{j_2})^k$. From what we have shown above, we know that i_1 must be equal to i_2 and j_1 may not be equal to j_2 only when $r^{(k-1)i}+r^{(k-2)i}+\dots+r^{2i}+r^i+1 \equiv 0 \pmod q$. That is, $(r^{ki}-1)/(r^i-1) \equiv 0 \pmod q$ and hence $r^{ki} \equiv 1 \pmod q$.

Assume $k_i = \alpha q+s$ where α is a positive integer and $0 \le s < p$. Since $r^p \equiv 1 \pmod p$, then $r^{ki} \equiv r^{\alpha p+s} \equiv r^s \equiv 1 \pmod q$. But p is a prime and $r \not\equiv 1 \pmod q$ so that $s = 0$ which implies $k_i = \alpha p$. This is impossible for the ranges of i and k. Therefore, $r^{(k-1)i}+r^{(k-2)i}+\ldots+r^{2i}+r^i+1 \not\equiv 0 \pmod q$. Hence $G_k = G$ for $1 \le k \le p-1$.

If we have an ordering of G, let us say $h_1, h_2, \ldots, h_n$ then $h_1^i, h_2^i, \ldots, h_n^i$ is also an ordering of G where $1 \le i \le p-1$. Also, if we choose any two orderings $h_1^i, h_2^i, \ldots, h_n^i$ and $h_1^j, h_2^j, \ldots, h_n^j$ where $1 \le i < j \le p-1$, then

$h_1^j(h_1^i)^{-1}$, $h_2^j(h_2^i)^{-1}$, ..., $h_n^j(h_n^i)^{-1}$ is also an ordering of G. By Theorem 5.2, we can construct a set of p-1 pairwise orthogonal Latin squares of order n all of which are row complete. □

<u>Theorem 5.4</u> : If the non-abelian group of order $n = p^3$ on two generators is sequenceable, then there exists a set of p-1 pairwise orthogonal Latin squares of order n all of which are row complete.

<u>Proof</u> : If G is the group described as above, then there exist a and b such $a^{p^2} = b^p = 1$ and $ab = ba^{p+1}$. We can use the method of the last theorem to construct p-1 pairwise orthogonal Latin squares of order n all of which are row complete. □

§5.2 Applications to Howell Designs

Definition 5.4 : Suppose X is a set such that $|X| = 2n$. A Howell design on X of type H(s,2n) consists of a square array of side s such that

(i) each cell is either empty or contains an unordered pair of elements taken from X,

(ii) each element of X appears exactly once in each row and each column of the array and

(iii) every unordered pair appears at most once in a cell of the array.

We can see that the range of possible values of s is $n \leq s \leq 2n-1$ for if $s < n$ condition (ii) is violated and if $s > 2n-1$, condition (iii) is not satisfied.

Definition 5.5 : Consider a Howell design on X of type H(s,2n) such that there is a set $Y \subset X$ with order $2n-s$ and no pair of elements of Y occupy a cell of the design of type H(s,2n). We denote such a Howell design by $H^*(s,2n)$ and say it satisfies the *-condition.

In this section we are only interested in the relationship between sequencing groups and Howell designs. By using the characteristics of strong symmetric sequencings, we will show that the Howell designs of types $H^*(2p,2p+2)$ exist for all primes p.

Example : The array

1,6	ϕ	4,5	2,3
3,4	2,6	ϕ	1,5
2,5	4,1	3,6	ϕ
ϕ	3,5	1,2	4,6

is a $H^*(4,6)$ Howell design with $Y = \{1,3\}$ and

ϕ	ϕ	1,2	3,4	5,6	7,8
ϕ	ϕ	5,7	6,8	1,3	2,4
4,5	1,8	ϕ	ϕ	2,7	3,6
3,7	2,6	ϕ	ϕ	4,8	1,5
2,8	3,5	4,6	1,7	ϕ	ϕ
1,6	4.7	3,8	2,5	ϕ	ϕ

is a $H^*(6,8)$ Howell design with $Y = \{1,4\}$.

In fact, all designs of type $H(2n-2,2n)$ satisfy the *-condition. This follows because an element x is paired with 2n-2 other elements so there remains an element y with which x is not paired in a cell.

We are going to show that a strong symmetric sequencing on an abelian group of order 2n will induce a Howell design of type $H^*(2n,2n+2)$. In Chapter four we showed that when $p \geq 5$ with p a prime, Z_{2p} has a strong symmetric sequencing and when $p > 3$ is a prime and $p = 5$ or $p \equiv \pm 3, \pm 13 \pmod{40}$, Z_{p-1} has a strong symmetric sequencing. This means that for such a prime, p, $H^*(2p,2p+2)$ exists. Together with the example above, $H^*(2p,2p+2)$ exists for all primes if we can prove our first statement in this paragraph.

Suppose an Abelian group Z_{2n} has a strong symmetric sequencing S: $a_1,a_2,\dots,a_{2n}$ associated with the partial product sequence P: $b_1,b_2,\dots,b_{2n}$.

$$\text{Let } E = \{\{b_{2j+2},b_{2(j+1)+1}\} : 0\le j<n/2-1\} \cup \{\{b_{2n-(2j+1)},b_{2n-2j}\} : 0\le j<n/2-1\}.$$

By Theorem 4.4, E is an even starter.

$$\text{Let } A = \{-(b_{2j+2}+b_{2(j+1)+1}) : 0\le j<n/2-1\} \cup \{-(b_{2n-(2j+1)}+b_{2n-2j}) : 0\le j\le n/2-1\} \cup \{-2m,0\}.$$

Then all elements in A are distinct because S is a strong symmetric sequencing. Also we notice that

$-(b_{2j+1}+b_{2(j+1)+1})+b_{2j+2}$, $-(b_{2j+1}+b_{2(j+1)+1})+b_{2(j+1)+1}$

for $0\le j<n/2-1$; $-(b_{2n-(2j+1)}+b_{2n-2j})+b_{2n-(2j+1)}$,

$-(b_{2n-(2j+1)}+b_{2n-2j})+b_{2n-2j}$ for $0\le j<n/2-1$; $0+0$, $-2m+m$

are all distinct elements of Z_{2n}. We call A an adder of the group Z_{2n}.

Theorem 5.5[11] : A strong symmetric sequencing on an Abelian group Z_{2n} with an unique element of order 2, induces a Howell design of type $H^*(2n,2n+2)$.

Proof : Consider the integers modulo 2n with two additional elements ∞_n, ∞_{n+1} such that $\infty_n+1 = \infty_n$, $\infty_{n+1}+1 = \infty_{n+1}$. From the above discussion, we know that there exists an even starter and adder which satisfy the properties in above. Let the set $E = \{\{x_i, y_i\} : 1 \le i \le n-1\}$ be a starter of Z_{2n}. Let $\{\infty_n, z_n\}$, $\{\infty_{n+1}, z_{n+1}\}$ be the pairs such that $z_n = 0$, $z_{n+1} = m$ where m is a nonzero element of G which does not occur as an element of some pairs of the starter. Also let $A = \{c_i : 1 \le i \le n+1\}$ be the adder. Then $x_i + c_i$, $y_i + c_i$ where $i = 1, 2, \ldots, n-1$ and $z_j + c_j$, $j = n, n+1$ are all distinct.

Now, we can construct a Howell design of type $H^*(2n, 2n+2)$ as follows. First we place $\{x_i, y_i\}$ in the first row, $(2n-c_i)^{th}$ column; $\{z_n, \infty_n\}$ in the first row, $(2n-c_n)^{th}$ column; and $\{z_{n+1}, \infty_{n+1}\}$ in the first row, $(2n-c_{n+1})^{th}$ column. Then if the pair $\{x, y\}$ occupies the cell in the i^{th} and j^{th} column, the pair $\{x+1, y+1\}$ occupies the cell in the $(i+1)^{th}$ row and $(j+1)^{th}$ column (row and column indices are taken modulo 2n).

If the cell in the i^{th} row and j^{th} column is empty, then so is the cell in $(i+1)^{th}$ row and $(j+1)^{th}$ column. Then the above construction produces a Howell design of type $H^*(2n, 2n+2)$. □

Now we can conclude that the designs of all types $H^*(2p, 2p+2)$ exist for p a prime.

Example : Consider the symmetric sequencing of Z_{10} with $n = 5$

S: 0,4,8,1,3,5,7,9,2,6 with partial product sequence

P: 0,4,2,3,6,1,8,7,9,5 where m = 1 and

$\{b_i + b_{i+1} = 1 \le i \le n-1\} = \{4,6,5,9\}$.

Then S satisfies all conditions of strong symmetric sequencings. The associated even starter is

E = {{4,2},{3,6},{8,7},{9,5}} and its associated adder

A = {-(4+2),-(3+6),-(8+7),-(9+5),-2,0}

= {4,1,5,6,8,0}

can be applied to the pairs {4,2}, {3,6}, {8,7}, {9,5}, $\{\infty_6,0\}$ and $\{\infty_5,1\}$ to get a starter-adder construction of $H^*(10,12)$. We have $H^*(10,12)$

ϕ	$\infty_5,1$	ϕ	9,5	8,7	4,2	ϕ	ϕ	3,6	$\infty_6,0$
$\infty_6,1$	ϕ	$\infty_5,2$	ϕ	0,6	9,8	5,3	ϕ	ϕ	4,7
5,8	$\infty_6,2$	ϕ	$\infty_5,3$	ϕ	1,7	0,9	6,4	ϕ	ϕ
ϕ	6,9	$\infty_6,3$	ϕ	$\infty_5,4$	ϕ	2,8	1,0	7,5	ϕ
ϕ	ϕ	7,0	$\infty_6,4$	ϕ	$\infty_5,5$	ϕ	3,9	2,1	8,6
9,7	ϕ	ϕ	8,1	$\infty_6,5$	ϕ	$\infty_5,6$	ϕ	4,0	3,2
4,3	0,8	ϕ	ϕ	9,2	$\infty_6,6$	ϕ	$\infty_5,7$	ϕ	5,1
6,2	5,4	1,9	ϕ	ϕ	0,3	$\infty_6,7$	ϕ	$\infty_5,8$	ϕ
ϕ	7,3	6,5	2,0	ϕ	ϕ	1,4	$\infty_6,8$	ϕ	$\infty_5,9$
$\infty_5,0$	ϕ	8,4	7,6	3,1	ϕ	ϕ	3,5	$\infty_6,9$	ϕ

§5.3 Applications to Graph Theory

We will discuss the relationship of decompositions of a complete graphs and sequencing groups. We give some definitions first.

Definition 5.6 : An undirected (directed) graph G is a set V of vertices together with a set E of edges where E is a subset of the set of all unordered (ordered) pairs of elements of V.

Definition 5.7 : An undirected (directed) complete graph is a graph such that the set E consists of all the unordered (ordered) pairs of elements of V. It is an n-graph when $|V| = n$.

Definition 5.8 : If G_1 and G_2 are graphs with vertex-sets V_1, V_2 and edge-sets E_1, E_2 respectively, then their union and intersection are defined as follows:

$G_1 \cup G_2$ has vertex-set $V_1 \cup V_2$ and edge-set $E_1 \cup E_2$ and
$G_1 \cap G_2$ has vertex-set $V_1 \cap V_2$ and edge-set $E_1 \cap E_2$.

Definition 5.9 : A set $E_1 \subset E$ of edges of the graph G is called a matching of G if any two distinct edges of E_1 have no common endvertices.

Definition 5.10 : A matching of a graph G is called a 1-factor if every vertex of G appears as an endvertex of some edge in the matching.

Definition 5.11 : If $M_1, M_2, \ldots, M_n$ are mutually edge-disjoint 1-factors of a graph G containing all edges of G, then these 1-factors are said to form a 1-factorization of G.

Definition 5.12 : A Hamiltonian path (circuit) is a path (circuit) that passes through each of the vertices in a graph exactly once.

Definition 5.13 : An Eulerian circuit is a circuit that traverses each edge in a graph exactly once.

Suppose, we have a complete directed n-graph and we want to see whether it can be decomposed into n directed Hamiltonian paths. N.S. Mendelsohn found a relationship between sequenceable groups and decompositions of a complete directed n-graph into n directed Hamiltonian paths. Let us take a look at the theorem in the following.

Theorem 5.6 : If G is a sequenceable group, then the complete directed graph with vertex set G can be decomposed into n Hamiltonian paths.

Proof : It is clear that the length of each Hamiltonian path is equal to n-1. The total number of edges is equal to n(n-1).

Let us consider the Latin square such that the square is the multiplication table of the group G of order n.

Each row of the Latin square has n-pairs of consecutive letters, the total numbers of pairs in all the rows of the Latin square is equal to n(n-1) and the total number of ordered pairs amongst n letters is also n(n-1). This means that each pair appearing exactly once in the rows is equivalent to no pair of letters repeated in the rows. So, if we can construct a row complete Latin square of order n, we can decompose a complete directed graph of order n into n Hamiltonian paths. Since G is a sequenceable group of order n, there exists a row complete Latin square of order n. The proof is finished. □

The above theorem tells us that if a sequenceable group of order n exists, then we can decompose a complete directed n graph into n Hamiltonian directed paths.

Example : Let us consider the complete-directed n-graph where n = 6. Then

$$\begin{array}{cccccc}
0 & 1 & 5 & 2 & 4 & 3 \\
1 & 2 & 0 & 3 & 5 & 4 \\
4 & 5 & 3 & 0 & 2 & 1 \\
3 & 4 & 2 & 5 & 1 & 0 \\
2 & 3 & 1 & 4 & 0 & 5 \\
5 & 0 & 4 & 1 & 3 & 2
\end{array}$$

is a row complete Latin square of order 6.

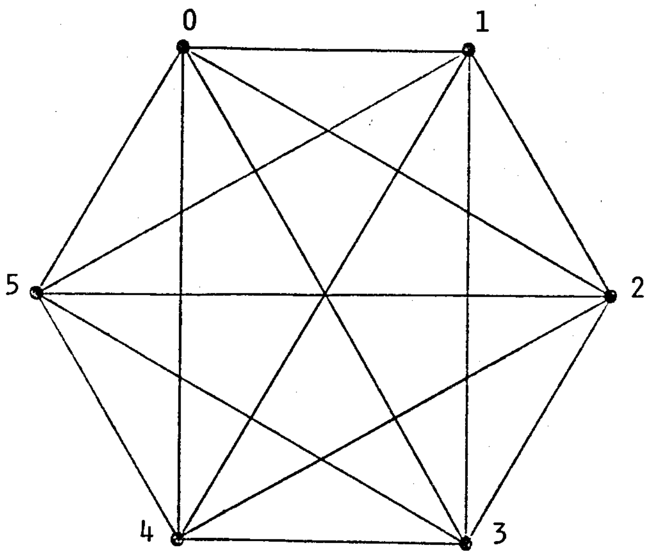


Figure 1.

A complete directed 6-graph is shown to the left.

The decomposition is shown below.

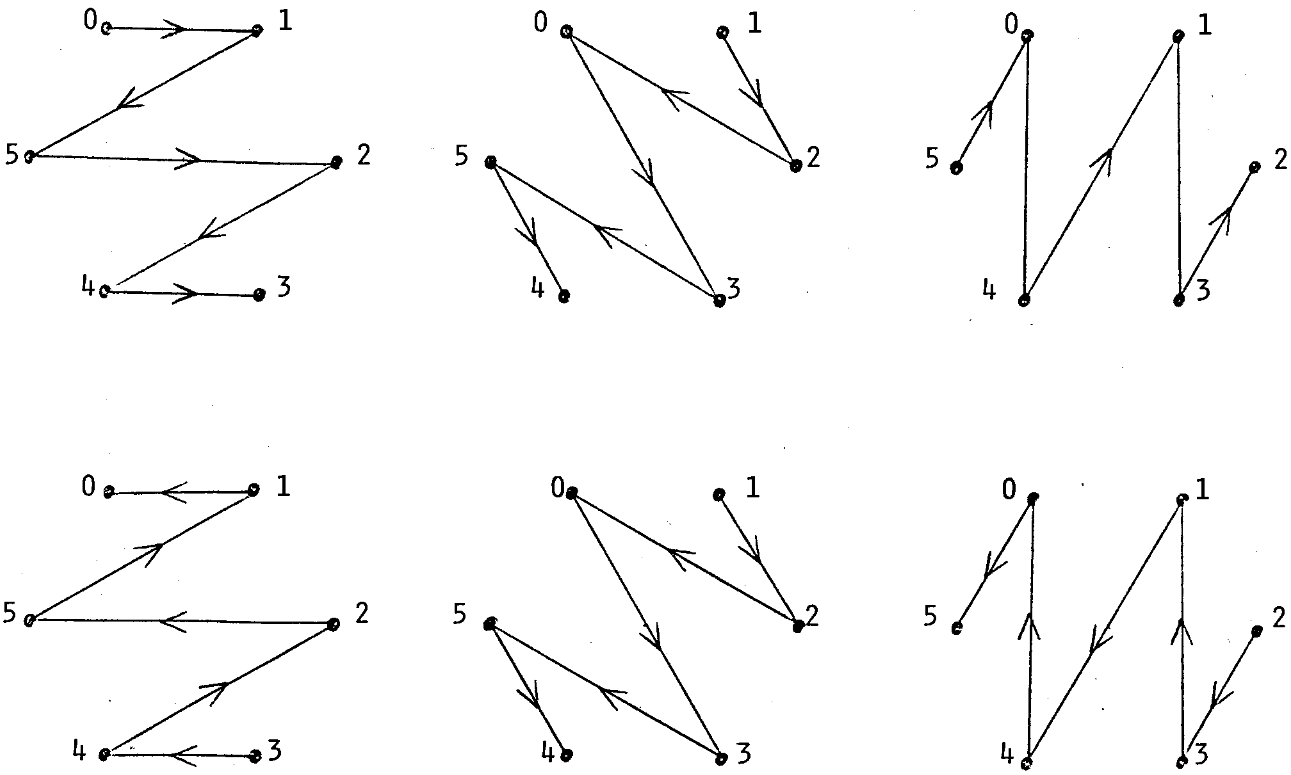


Figure 2.

Sequenceable groups also help us to deocmpose a complete undirected graph into Hamiltonian paths. Now S: $0,1,2m-2,3,2m-4,5,2m-6,\ldots,4,2m-3,2,2m-1$ is a sequencing of Z_{2m}. Let us construct a row complete Latin square by taking P as the first row and row i by adding i (modulo 2m) to the sequencing P. Then

0	1	2m-1	2	2m-2	...	m+2	m-1	m+1	m
1	2	0	3	2m-1	...	m+3	m	m+2	m+1
.	.	.	.	.	...	.	.	.	.
.	.	.	.	.	...	.	.	.	.
.	.	.	.	.	...	.	.	.	.
.	.	.	.	.	...	.	.	.	.
m-1	m	m-2	m+1	m-3	...	1	2m-2	0	2m-1
m	m+1	m-1	m+2	m-2	...	2	2m-1	1	0
.	.	.	.	.	...	.	.	.	.
.	.	.	.	.	...	.	.	.	.
.	.	.	.	.	...	.	.	.	.
.	.	.	.	.	...	.	.	.	.
2m-1	0	2m-2	1	2m-3	...	m+1	m-2	m	m-1

is row complete Latin square. Note that the last m rows are the same as the first but in reverse order. Thus, the first m rows of the Latin square exhaust all the possible unordered pairs i,j where $i,j \in Z_{2m}$. This leads to the following theorem.

<u>Theorem 5.7</u> : For every positive integer m,

(i) the complete undirected graph on 2m vertices has a decomposition into m disjoint Hamiltonian paths;

(ii) the complete undirected graph on 2m+1 vertices has a decomposition into m disjoint Hamiltonian circuits each of length 2m+1; and

(iii) every complete undirected graph on an odd number 2m+1 of vertices has an Eulerian circuit with the property that, when a certain vertex and all the edges through it are deleted, the remaining portions of the Eulerian circuit are Hamiltonian paths of the residual graph on 2m vertices.

<u>Proof</u> : Consider the Latin square above. Then the first m rows define the required Hamiltonian decomposition of the undirected graph on 2m vertices.

Now let us add two columns at the beginning and the ending of the Latin square where all the elements of these two columns are equal to 2m. We only consider the first m rows. We have,

2m	0	1	2m-1	2	...	m-1	m+1	m	2m
2m	1	2	0	3	...	m	m+2	m+1	2m
.	.	.	.	.	...	.	.	.	.
.	.	.	.	.	...	.	.	.	.
.	.	.	.	.	...	.	.	.	.
.	.	.	.	.	...	.	.	.	.
2m	m-1	m	m-2	m+1	...	2m-2	0	2m-1	2m.

Obviously, each row of the above defines a Hamiltonian circuit of length 2m+1 and they are all disjoint. The complete undirected graph on 2m+1 vertices is decomposed into m disjoint Hamiltonian circuits each of length 2m+1. Moreover, the union of all the above disjoint circuits forms an Eulerian circuit. Also this Eulerian circuit has the property that when a certain vertex and all the edges through it are deleted, the remaining portions of the Eulerian circuit are Hamiltonian paths of the residual graph on 2m vertices. □

A sequencing of a group G can be used to construct a decomposition of a completed graph into Hamiltonian paths. In the following, we are going to show that a symmetric sequencing can be used to construct a 1-factorization of a complete graph.

As in Chapter four, we use g^* to denote the unique element of order 2 in the appropriate group G of order 2n. E is used to denote the even starter induced by the symmetric sequencing of G and m is an element which is not in E.

Theorem 5.8 : If E is the even starter induced by a symmetric sequencing of the group, then $E^* \cup Q^*$ is a Hamiltonian circuit of a complete graph $K_{|G|}$ where $E^* = E \cup \{e,m\}$ and $Q^* = \{\{x, xg^*\} : x \in G\}$.

Proof : As in Theorem 4.4,

$$E = \{\{b_{2j+2}, b_{2(j+1)+1}\} : 0 \le j < n/2-1\}$$
$$\cup \{\{b_{2n-(2j+1)}, b_{2n-2}\} : 0 \le j \le n/2-1\}$$

which is an even starter of G and note that $g^* = a_{n+1} = b_{2n}$, $g^* \ne m$.

Obviously, there is no element in the intersection of E^* and Q^*. Let the vertex set of $K_{|G|}$ be G. Then Q^* and E^* are disjoint 1-factors of $K_{|G|}$.

When n is odd,

$$m = b_{n+1},\ E^* = \{\{b_2, b_3\}, \{b_4, b_5\}, \ldots, \{b_{n-1}, b_n\}\}$$
$$\cup \{\{b_{2n}, b_{2n-1}\}, \{b_{2n-2}, b_{2n-3}\}, \ldots, \{b_{n+3}, b_{n+2}\}\}$$
$$\cup \{\{e, b_{n+1}\}\}.$$

When n is even,

$$m = b_n,\ E^* = \{\{b_2, b_3\}, \{b_4, b_5\}, \ldots, \{b_{n-2}, b_{n-1}\}\}$$
$$\cup \{\{b_{2n}, b_{2n-1}\}, \{b_{2n-2}, b_{2n-3}\}, \ldots, \{b_{n+2}, b_{n+1}\}\}$$
$$\cup \{\{e, b_n\}\}$$

and

$$Q^* = \{\{x, xg^*\} : x \in G\}$$
$$= \{\{b_i, b_i g^*\} : 1 \le i \le 2n\}$$
$$= \{\{e, b_{2n}\}, \{b_2, b_{2n-1}\}, \ldots, \{b_n, b_{n+1}\}\}$$

In each of the two cases, n even and odd, we can see that $E^* \cup Q^*$ is a Hamiltonian circuit of $K_{|G|}$. □

Theorem 5.9 : If G is a group of order 2n with a symmetric sequencing, then the even starter E, as described above, induces a 1-factorization F(E) on K_{2n+2}.

<u>Proof</u> : Let the vertex set of $K_{2n+2} = G\cup\{\infty_1,\infty_2\}$. Extend the group operation by defining

$$x\cdot\infty_1 = \infty_1\cdot x = \infty_1 \text{ and } x\cdot\infty_2 = \infty_2\cdot x = \infty_2 \text{ for every } x\in G.$$

Let $E^\# = E\cup\{e,\infty_1\} \cup \{m,\infty_2\}$ and $Q^\# = \{\{x,g^*x\}:x\in G\} \cup \{\infty_1,\infty_2\}$. Let $F(E) = \{xE^\#:x\in G\} \cup Q^\#$. Since $E^\#$ and $Q^\#$ are both 1-factors of K_{2n+2}, then each element of $F(E)$ is a 1-factor of K_{2n+2}. The order of $F(E)$ is $2n+1$. It will suffice to show that every edge of K_{2n+2} occurs in some element of $F(E)$. It is obvious that all $\{x,\infty_1\}$ and $\{x,\infty_2\}$ belong to a 1-factor of $F(E)$ and $\{\infty_1,\infty_2\} \in Q^\#$. We need to show that $\{g,h\}$ belongs to some element of $F(E)$ for any $g,h\in G$ and $g \neq h$.

Suppose $g^{-1}h = g^*$. Then $h = g^*g$ which implies $\{g,h\} = \{g,g^*g\}$ which belongs to $Q^\#$.

Suppose $g^{-1}h \neq g^{*1}$ Then there exists a pair $\{x,y\}\in E$ such that $g^{-1}h = x^{-1}y$. Thus, $gx^{-1} = hy^{-1}$. Let us say they are equal to k. Then $gx^{-1} = k$ which implies $g = kx$ and $hy^{-1} = k$ so that $h = ky$. We have $k\{x,y\} = \{g,h\}$ which belongs to $kE^\#$. Thus, $F(E)$ is a 1-factorization of K_{2n+2}. □

<u>Example</u> : Let us consider Z_6.

Now S: 0,1,4,3,2,5 is a symmetric sequencing of Z

and P: 0,1,5,2,4,3 is the partial product sequence of S.

$$\begin{aligned} \text{Then } E &= \{\{b_2,b_3\}, \{b_5,b_4\}\} \\ &= \{\{1,5\}, \{3,4\}\} \end{aligned}$$

and $m = 2$, $e = 0$ and $g^* = 3$.

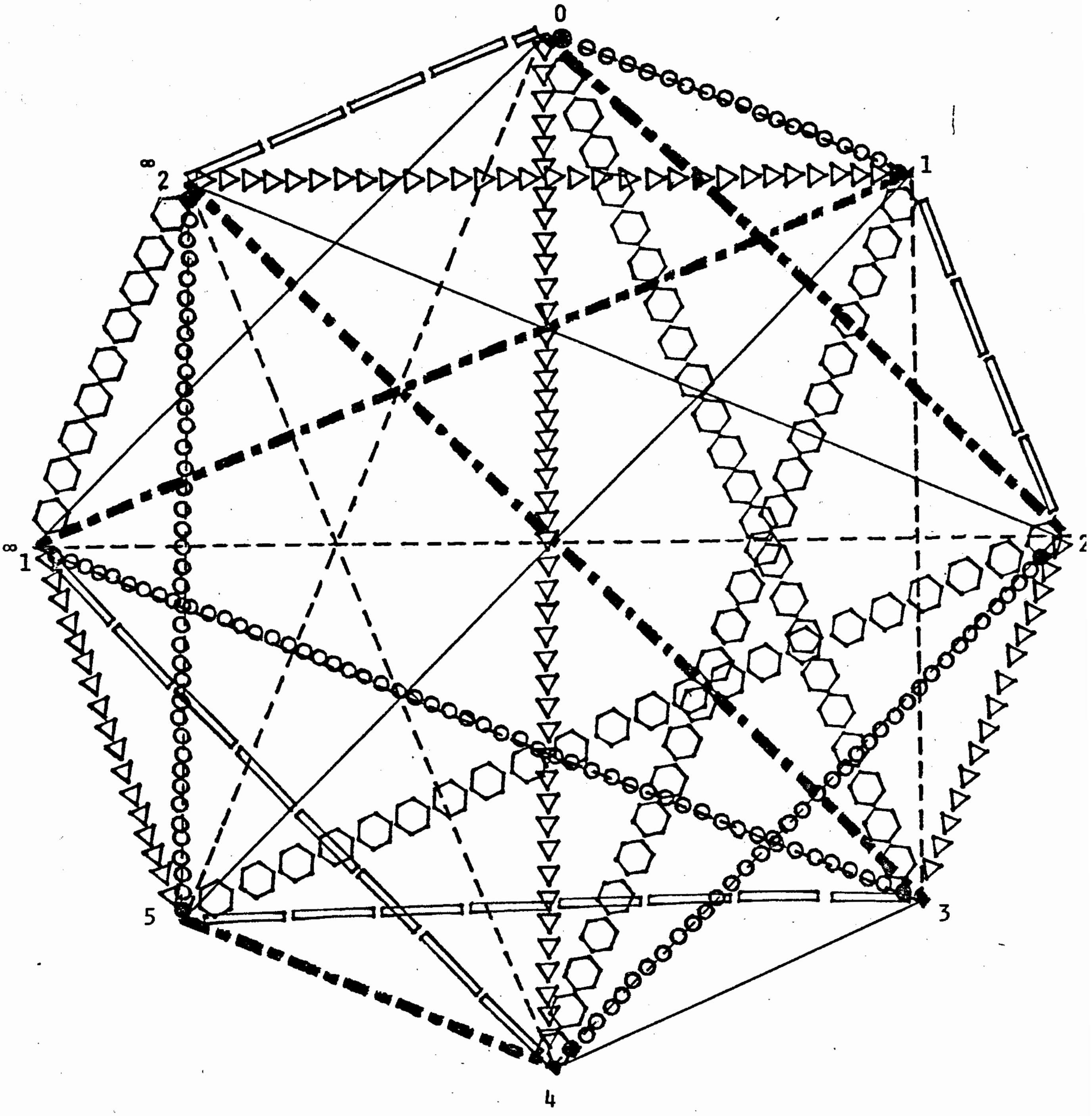
Also, $E^{\#} = \{\{1,5\}, \{3,4\}\{0,\infty_1\}, \{2,\infty_2\}\}$

and $\quad Q^{\#} = \{\{x,g^*+x\} : x\in G\} \cup \{\infty_1,\infty_2\}$

$\qquad\quad = \{\{0,3\}, \{1,4\}, \{2,5\}, \{\infty_1,\infty_2\}\}.$

Then $F(E) = \{xE^{\#} : x\in G\} \cup Q^{\#}$

$$
\begin{aligned}
&= \{\{1,5\}, \{3,4\}, \{0,\infty_1\}, \{2,\infty_2\}\} \cup \\
&\quad \{\{2,0\}, \{4,5\}, \{1,\infty_1\}, \{3,\infty_2\}\} \cup \\
&\quad \{\{3,1\}, \{5,0\}, \{2,\infty_1\}, \{4,\infty_2\}\} \cup \\
&\quad \{\{4,2\}, \{0,1\}, \{3,\infty_1\}, \{5,\infty_2\}\} \cup \\
&\quad \{\{5,3\}, \{1,2\}, \{4,\infty_1\}, \{0,\infty_2\}\} \cup \\
&\quad \{\{0,4\}, \{2,3\}, \{5,\infty_1\}, \{1,\infty_2\}\} \cup \\
&\quad \{\{0,3\}, \{1,4\}, \{2,5\} , \{\infty_1,\infty_2\}\}.
\end{aligned}
$$



The above diagram is a 1-factorization of K_8.

Figure 3.

BIBLIOGRAPHY

[1] Anderson, B.A., Sequencings of certain dihedral groups, *Proc. Sixth Southeastern Conf. on Combinatorics, Graph Theory and Computing*, Winnipeg, 1975, p. 65-76.

[2] Anderson, B.A., Sequencings and Starters, Pacific J. Math., 64, 1976, p. 17-24.

[3] Anderson, B.A., A class of starter-induced 1-factorizations, *Lecture Notes in Mathematics No. 406*, Springer-Veriag, 1974, p. 180-185.

[4] Anderson, B.A. and Leonard, P.A., Sequencings and Howe Howell Designs, Technical Report, No. 25.

[5] Andrews, G.E., *Number Theory*, Saunders, 1971, p. 132.

[6] Dénes, J. and Keedwell, A.D., *Latin Squares and Their Applications*, Akademiai Kiado, Budapest, 1974.

[7] Dénes, J. and Török, E., Groups and graphs, *Combinatorial Theory and Its Applications*, North Holland, Amsterdam, 1970, p. 257-289.

[8] Friedlander, R., Sequences in non-abelian groups with distinct partial products, *Aequationes Math. 14*, 1976, p. 59-66.

[9] Gordon, B., Sequence in groups with distinct partial products, *Pacific J. Math. 11*, 1961, p. 1309-1313.

[10] Heinrich, K., Pairwise orthogonal row-complete latin square, *Proc. Tenth Southeastern Conf. on Combinatorics*, Graph Theory and Computing, Florida, 1979, p. 501-510.

[11] Hung, S.H.Y. and Mendelson, N.S., On Howell Designs, *J. Comb. Theory Ser.* A16, 1974, p. 174-198.

[12] Keewdell, A.D., On the sequenceability of non-abelian groups of order p,q, Unpublished.

[13] Keewdell, A.D., Some problems concerning complete latin squares, *Proc. Fifth British Combinatorial Conf.*, 1975, p. 383-393.

[14] Mendelson, N.S., Hamiltonian decomposition of the complete directed n-graph, Theory of Graph, Proc. Colloq., Tihany, 1966, p. 237-241.

[15] Paige, L.J., A note on finite abelain group, Bull, Amer. Math. Soc. 53, 1947, p. 590-593.

[16] Paige, L.J., Complete mappings of finite groups, Pacific J. Math. 1, 1951, p. 111-116.

[17] Wang, L.L., A test for the sequencing of a class of finite groups with two generators, Amer. Math. Soc. Notices 20, 1973, p. 73T-A275.