Journal of Sciences, Islamic Republic of Iran 20(3): 277-282 (2009) http://jsciences.ut.ac.ir
University of Tehran, ISSN 1016-1104

Non-Abelian Sequenceable Groups Involving α-Covers

A. Sadeghieh[1] and H. Doostie[2,*]

[1]*Mathematics Department, Faculty of Basic Sciences, Science and Research Branch, Islamic Azad University (IAU), Tehran, Islamic Republic of Iran*
[2]*Mathematics Department, Faculty of Mathematics and Computer Sciences, Tarbiat Moallem University, 49 Mofateh Ave., Tehran 15614, Islamic Republic of Iran*

Received: 1 August 2009 / Revised: 25 April 2009 / Accepted: 5 September 2009

Abstract

A non-abelian finite group G is called sequenceable if for some positive integer k, G is k-generated ($G =< a_1, a_2, ..., a_k >$) and there exist integers $\alpha_1, \alpha_2, ..., \alpha_k$ such that every element of G is a term of the k-step generalized Fibonacci sequence $x_i = a_i$, $i = 1, 2, \ldots, k$, $x_i = (x_{i-k})^{\alpha_1}(x_{i-k+1})^{\alpha_2} \ldots (x_{i-1})^{\alpha_k}$, $i \geq k+1$. A remarkable application of this definition may be find on the study of random covers in the cryptography. The 2-step generalized sequences for the dihedral groups studied for their periodicity in 2006 by H. Aydin and it is proved that in many cases for α_1 and α_2, they are not periodic. Aydin's work was in continuation of the research works of R. Dikici (1997) and E. Ozkan (2003) where they studied the ordinary Fibonacci sequences (sequences without the powers) of elements of groups. In this paper we consider 3-step generalized Fibonacci sequences and prove that the quaternion group Q_{2^n} (for every integer $n \geq 3$) and the dihedral group D_{2n} (for every integer $n \geq 3$) are sequenceable. The α-covers together with the Fibonacci lengths of the corresponding 3-step sequences have been calculated as well.

Keywords: Fibonacci length; Finite groups

Introduction

Let $G =< a, b >$ be a non-abelian finite group. The well known Fibonacci sequence of G with respect to the generating set $A = \{a, b\}$ is defined to be the sequence

$x_1 = a$, $x_2 = b$ and $x_n = x_{n-2}x_{n-1}$, $n \geq 3$

(one may see [1,3,4,6,13,14], for examples). It is obvious that each of the following subsets of G is also a generating set for G:

$$\{x_1, x_2, x_3\}, \{x_1, x_2, x_3, x_4\}, ..., \{x_1, x_2, ..., x_l\}$$

where, $l = LEN_A(G)$ is the least positive integer such that

* Corresponding author, Tel.: +98(21)77507772, Fax: +98(21)77602988, E-mail: doostih@saba.tmu.ac.ir

$x_{l+1} = x_1$ and $x_{l+2} = x_2$.

For every integer $k \geq 2$ we define the k-step generalized Fibonacci sequence as follows:

Definition 1.1. For every integer k where, $2 \leq k < LEN_A(G)$, the sequence $\{y_i\}_1^\infty$ of the elements of G defined by

$$\begin{cases} y_i = x_i, & i = 1,...,k, \\ y_i = (y_{i-k})^{\alpha_1}(y_{i-k+1})^{\alpha_2}...(y_{i-1})^{\alpha_k}, & i \geq k+1 \end{cases}$$

is called a k-step generalized Fibonacci sequence of G, for some positive integers $\alpha_1, \alpha_2, ..., \alpha_k$.

Definition 1.2. For an integer $k \geq 2$, a non-abelian finite group $G =< a,b >$ is called a k-sequenceable group if every element of G is a term of a periodic k-step generalized Fibonacci sequence where, $k \leq LEN_A(G)$ and $A = \{a,b\}$. Moreover, G is called sequenceable if G is k-sequenceable for some integer k.

Note that there are differences between our definition of k-step generalized Fibonacci sequence and the k-nacci sequence of Aydin [2]. The article [2] is a nice generalization of the ordinary Fibonacci sequences of elements of a group and this article studies the 2-step generalized Fibonacci sequences by proving that the 2-step generalized Fibonacci sequences are not periodic in many cases. The article [2] is in continuation of the articles [5] and [9] which studying the ordinary 3-step Fibonacci sequences (as a notation of these articles the "ordinary" is used for the sequences without powers) in certain classes of finite groups. The basic difference between our results in this paper and the approaches of the articles [5] and [9] is the considering of 3-step generalized Fibonacci sequences and the notion of sequenceable groups which was posed firstly in [2], inspired us to give the Definition 1.2 and to pose two natural questions: which groups are sequenceable? And how applicable may be the sequenceability of finite groups?

To investigate these questions we follow Svaba [12] and recall the notion of a cover of a finite group:

Definition 1.3. Let G be a finite group and $\alpha = [A_1, A_2, ..., A_s]$ be a collection of ordered subsets $A_i = [a_{i1}, a_{i2}, ..., a_{ir_i}]$ of G. Then α is called a cover for G if for every element $g \in G$ there exist elements $a_{ij_i} \in A_i$ such that

$g = a_{1j_1}a_{2j_2}..a_{sj_s}$.

This cover is known as an α-cover for G.

The covers and α-covers are the interesting and important tools in generation of random covers which themselves are useful in the cryptography, specially when G is non-abelian (one may see [7,8,10,11,12], for examples).

As a result of finiteness of the group $G =< a,b >$, $LEN_A(G)$ is finite.

A k-step generalized Fibonacci sequence $\{y_i\}_1^\infty$ may be periodic and to distinguish this period with the Fibonacci length $LEN_A(G)$ we have to give the following definition.

Definition 1.4. For a finite non-abelian group $G =< a,b >$, the period of a k-step generalized Fibonacci sequence $\{x_i\}_1^\infty$ is called the k-step Fibonacci length of G and will be denoted by $LEN_A(G, x_1, ..., x_k)$.

This number depends on the fixed integers $\alpha_1, ..., \alpha_k$ of the Definition 1.1.

We are now ready to investigate the posed questions. Indeed, in what follows we prove that the quaternion group Q_{2^n} and dihedral group D_{2n} are 3-sequenceable for every integer $n \geq 3$.

Moreover, following the Definition 1.3, if we let A_i as singleton subsets, then by proving the sequenceability of a group G, we are able to give an α-cover for G. In this paper we will construct the appropriate α-covers for the considered groups.

Sequenceability of D_{2n}, ($n \geq 3$)

Let $D_{2n} =< x, y \mid x^2 = y^n = (xy)^2 = 1 >$. For every integer $n \geq 3$, we define the 3-step generalized Fibonacci sequence $\{a_m\}_1^\infty$ of the elements of D_{2n} as follow:

$$a_1 = x, \quad a_2 = y, \quad a_3 = xy,$$

$$a_m = a_{m-3}(a_{m-2})^\beta a_{m-1}, \quad m \geq 4$$

for a positive integer β.

Our main results in this section are the Propositions 2.1 and 2.4. These propositions identify the values of β for different values of the integer n.

Proposition 2.1. For every even value of $n \geq 4$ and $\beta = n-1$, $\{a_m\}_1^\infty$ is periodic. Moreover, For every

element $g \in D_{2n}$, there exists an integer $m \geq 1$ such that $g = a_m$.

To prove this proposition first we identify the elements of $\{a_m\}_1^\infty$ by the following lemma.

Lemma 2.2. Let n be even. Then, every element of $\{a_m\}_1^\infty$ where,

$$a_1 = x, \quad a_2 = y, \quad a_3 = xy,$$

$$a_m = a_{m-3}a_{m-2}^{\,n-1}a_{m-1}, \quad m \geq 4$$

may be represented by

$$a_m = \begin{cases} x\, y^{\frac{m-1}{2}}, & m \text{ is odd} \\ y^{\frac{m}{2}}, & m \text{ is even}. \end{cases}$$

Proof. We argue by induction on m. For $m = 1$, $m = 2$ and $m = 3$ it is true and by the induction hypothesis, if the assertion holds for $m-1$, $m-2$ and $m-3$, then we may consider two cases for m:

Case 1: m is even, then $m-1$ and $m-3$ are odd, so,

$$\begin{aligned} a_m &= a_{m-3}a_{m-2}^{\,n-1}a_{m-1} \\ &= xy^{(m-4)/2}(y^{(m-2)/2})^{n-1}xy^{(m-2)/2} \\ &= xy^{(m-4)/2+(n-1)(m-2)/2}xy^{(m-2)/2} \\ &= y^{-((m-4)/2+(n-1)(m-2)/2)}x^2y^{(m-2)/2}, \end{aligned}$$

(for, $(xy)^2 = 1$ yields $xy^k = y^{-k}x$)

$$\begin{aligned} a_m &= y^{(-m+4-(n-1)(m-2)+m-2)/2} \\ &= y^{-n(m-2)/2}y^{(-m+4+m-2+m-2)/2} \\ a_m &= y^{m/2}. \end{aligned}$$

Case 2: m is odd, then $m-1$ and $m-3$ are even and we proceed in the similar way as above to show that $a_m = xy^{(m-1)/2}$.

Proof of Proposition 2.1. Every element g of the group

$$D_{2n} = \langle x, y \mid x^2 = y^n = (xy)^2 = 1 \rangle$$

may be written in the form $g = x^i y^j$ where $i = 0,1$ and $j = 0,1,...,n-1$. If $i = 0$ then $g = a_{2j}$, and if $i = 1$ then $g = a_{2j+1}$ by using Lemma 2.2. To find the period of $\{a_m\}_1^\infty$ we show that

$$LEN_A(D_{2n}, a_1, a_2, a_3) = 2n \text{ where, } A = \{x, y\}.$$

Let $LEN_A(D_{2n}, a_1, a_2, a_3) = t$. Then the equations

$a_{t+1} = a_1$, $a_{t+2} = a_2$ and $a_{t+3} = a_3$ hold, or equivalently,

$$a_{t+1} = x, \quad a_{t+2} = y, \quad a_{t+3} = xy.$$

If t is even then using Lemma 2.2, gives us $xy^{t/2} = x$, $y^{(t+2)/2} = y$ and $xy^{(t+2)/2} = xy$, i.e.; $y^{t/2} = 1$. Since y is of order n then, $t = 2n$. However, t is not an odd integer, for, in this case the equation $a_{t+1} = x$ yields $y^{(t+1)/2} = x$ which shows that D_{2n} is an abelian group. Consequently,

$$LEN_A(D_{2n}, a_1, a_2, a_3) = 2n.$$

Lemma 2.3. For every odd value of n consider the group

$$D_{2n} = \langle x, y \mid x^2 = y^n = (xy)^2 = 1 \rangle,$$

And the sequence $\{c_m\}_1^\infty$ as follows:

$$c_1 = x, \quad c_2 = y, \quad c_3 = xy,$$

$$c_m = c_{m-3}c_{m-2}^{\,3}c_{m-1}, \quad m \geq 4.$$

Then for every $m \geq 1$,

$$c_m = \begin{cases} y^{-(\frac{m}{2})}, & m \equiv 0 (\mathrm{mod}\, 4) \\ xy^{-(\frac{m-1}{2})}, & m \equiv 1 (\mathrm{mod}\, 4) \\ y^{\frac{m}{2}}, & m \equiv 2 (\mathrm{mod}\, 4) \\ xy^{\frac{m-1}{2}}, & m \equiv 3 (\mathrm{mod}\, 4). \end{cases}$$

Proof. We argue by induction on m. The assertion holds for $m = 1$, $m = 2$ and $m = 3$. Let $m \geq 4$ and suppose that the assertion holds for all integers $k < m$. Consider four cases for m modulo 4.

If $m \equiv 0 (\mathrm{mod} 4)$, then $m-1 \equiv 3 (\mathrm{mod}\, 4)$, $m-2 \equiv 2 (\mathrm{mod}\, 4)$ and $m-3 \equiv 1 (\mathrm{mod}\, 4)$.

We now use the induction hypothesis and get:

$$c_m = c_{m-3}c_{m-2}^{\,3}c_{m-1} = xy^{-(m-4)/2}(y^{(m-2)/2})^3 xy^{(m-2)/2}$$
$$= xy^{-m/2+2}y^{3m/2-3}xy^{m/2-1} = xy^{m-1}xy^{m/2-1}$$
$$= x^2y^{-m+1}y^{m/2-1} = y^{-m/2}.$$

Proofs in other cases are similar.

Proposition 2.4. For every odd values of $n \geq 3$, the sequence $\{c_m\}_1^\infty$ defined as above, is periodic. Moreover, for every element $g \in D_{2n}$, there exists an integer $m \geq 1$ such that $g = c_m$.

Proof. Since n is odd then by Lemma 2.3, we get:

$$c_1 = x, \quad c_2 = y, \quad c_3 = xy, \quad c_4 = y^{-2},$$
$$c_5 = xy^{-2}, \quad c_6 = y^3, \quad c_7 = xy^3, \quad c_8 = y^{-4},$$
$$c_9 = xy^{-4}, \quad c_{10} = y^5, \quad c_{11} = xy^5, ..., c_{2n-2} = y,$$
$$c_{2n-1} = xy, \quad c_{2n} = 1, \quad c_{2n+1} = x, \quad c_{2n+2} = y^{-1},$$
$$c_{2n+3} = xy^{-1}, \quad c_{2n+4} = y^2, \quad c_{2n+5} = xy^2,$$
$$c_{2n+6} = y^{-3}, \quad c_{2n+7} = xy^{-3}, \quad c_{2n+8} = y^4,$$
$$c_{2n+9} = xy^4, ..., c_{4n-2} = y^{-1}, \quad c_{4n-1} = xy^{-1},$$
$$c_{4n} = 1, \quad c_{4n+1} = x, \quad c_{4n+2} = y, \quad c_{4n+3} = xy, ...$$

Every element of D_{2n} appears exactly twice in the set $\{c_1, c_2, ..., c_{4n}\}$ and

$LEN_A(D_{2n}, c_1, c_2, c_3) = 4n$, (where, $A = \{x, y\}$) for, if $LEN_A(D_{2n}, c_1, c_2, c_3) = t$, then the equations, $c_{t+1} = c_1 = x$, $c_{t+2} = c_2 = y$, and $c_{t+3} = c_3 = xy$ hold. The integer t is even, for, otherwise $c_{t+1} = y^{-(t+1)/2}$ or $c_{t+1} = y^{(t+1)/2}$ thus $x = y^{-(t+1)/2}$ or $x = y^{(t+1)/2}$. That is, D_{2n} is abelian. Also, if $t \equiv 2 (\mathrm{mod}\, 4)$, then we get $c_{t+2} = y^{-(t+2)/2}$. So, $xy = y^{-t/2-1}$ which yields the contradiction $x = y^{-t/2-2}$. Hence $t \equiv 0 (\mathrm{mod}\, 4)$, and then $c_{t+1} = xy^{-t/2}$, $c_{t+2} = y^{(t+2)/2}$ and $c_{t+3} = xy^{(t+2)/2}$. Thus $xy^{-t/2} = x$, $y^{(t+2)/2} = y$ and $xy^{(t+2)/2} = xy$, i.e.; $y^{t/2} = 1$ holds and the least value of t is indeed $4n$.

Sequenceability of $Q_{2^n}, n \geq 3$

For every integer $n \geq 3$ the generalized quaternion group Q_{2^n} is defined by the presentation

$$Q_{2^n} = < x, y \mid x^{2^{n-1}} = 1, y^2 = x^{2^{n-2}}, y^{-1}xy = x^{-1} >$$

which is finite of order 2^n. The main result of this section is:

Proposition 3.1. For every integer $n \geq 3$ the group Q_{2^n} is 3-sequenceable.

Proof. Consider the sequence $\{b_i\}_1^\infty$ of the elements of Q_{2^n} as follows:

$$b_1 = x, \quad b_2 = y, \quad b_3 = xy,$$
$$b_k = b_{k-3}(b_{k-2})^7 b_{k-1}, \quad (k \geq 4).$$

This is a generalized 3-step Fibonacci sequence and we show that for every $k \geq 1$, b_k may be represented by: if $k \equiv 1 (\mathrm{mod}\, 8)$ then,

$$b_k = \begin{cases} x^{\frac{3k+1}{2}+(\frac{(k-1)(k-9)}{2})'}, (\frac{(k-1)(k-9)}{2})' \geq 2^{n-2}, \\ x^{\frac{3k+1}{2}+(\frac{(k-1)(k-9)}{2})'+((k-1)(k-9))'+...+2^{n-2}}, (\frac{(k-1)(k-9)}{2})' < 2^{n-2}, \end{cases}$$

where, $1 \leq k \leq 2^n - 7$,
if $k \equiv 2 (\mathrm{mod}\, 8)$ then,

$$b_k = \begin{cases} x^{\frac{k-2}{2}+(\frac{(k-2)^4}{2^5})'} y, (\frac{(k-2)^4}{2^5})' \geq 2^{n-2}, \\ x^{\frac{k-2}{2}+(\frac{(k-2)^4}{2^5})'+(\frac{(k-2)^4}{2^4})'+...+2^{n-2}} y, (\frac{(k-2)^4}{2^5})' < 2^{n-2}, \end{cases}$$

where, $2 \leq k \leq 2^n - 6$,
if $k \equiv 3 (\mathrm{mod}\, 8)$ then,

$$b_k = \begin{cases} x^{\frac{9k-25}{2}+(\frac{(k-3)(k-11)}{2})'} y, (\frac{(k-3)(k-11)}{2})' \geq 2^{n-2}, \\ x^{\frac{9k-25}{2}+(\frac{(k-3)(k-11)}{2})'+((k-3)(k-11))'+...+2^{n-2}} y, (\frac{(k-3)(k-11)}{2})' < 2^{n-2}, \end{cases}$$

where, $3 \leq k \leq 2^n - 5$,
if $k \equiv 4 (\mathrm{mod}\, 8)$ then,

$$b_k = \begin{cases} x^{\frac{-5k+20}{2}+(\frac{(k-4)^4}{2^5})'}, (\frac{(k-4)^4}{2^5})' \geq 2^{n-2}, \\ x^{\frac{-5k+20}{2}+(\frac{(k-4)^4}{2^5})'+(\frac{(k-4)^4}{2^4})'+...+2^{n-2}}, (\frac{(k-4)^4}{2^5})' < 2^{n-2}, \end{cases}$$

where, $4 \leq k \leq 2^n - 4$,
if $k \equiv 5 (\mathrm{mod}\, 8)$ then,

$$b_k = \begin{cases} x^{\frac{-13k+63}{2}-(\frac{(k-5)(k-13)}{2})'}, (\frac{(k-5)(k-13)}{2})' \geq 2^{n-2}, \\ x^{\frac{-13k+63}{2}-(\frac{(k-5)(k-13)}{2})'+((k-5)(k-13))'+...+2^{n-2}}, (\frac{(k-5)(k-13)}{2})' < 2^{n-2}, \end{cases}$$

where, $5 \le k \le 2^n - 3$,
if $k \equiv 6 (\mathrm{mod}\, 8)$ then,

$$b_k = \begin{cases} x^{\frac{9k-50}{2}+(\frac{(k-6)(k-14)}{2})'-(\frac{(k-6)^4}{2^5})'} y, (\frac{(k-6)^4}{2^5})' \ge 2^{n-2}, \\ x^{\frac{9k-50}{2}+(\frac{(k-6)(k-14)}{2})'-(\frac{(k-6)^4}{2^5})'+(\frac{(k-6)^4}{2^4})'+\ldots+2^{n-2}} y, (\frac{(k-6)^4}{2^5})' < 2^{n-2}, \end{cases}$$

where, $6 \le k \le 2^n - 2$,
if $k \equiv 7 (\mathrm{mod}\, 8)$ then,

$$b_k = \begin{cases} x^{\frac{9k-73}{2}+(\frac{(k-7)(k-15)}{2})'} y, (\frac{(k-7)(k-15)}{2})' \ge 2^{n-2}, \\ x^{\frac{9k-73}{2}+(\frac{(k-7)(k-15)}{2})'+((k-7)(k-15))'+\ldots+2^{n-2}} y, (\frac{(k-7)(k-15)}{2})' < 2^{n-2}, \end{cases}$$

where, $7 \le k \le 2^n - 1$,
if $k \equiv 0 (\mathrm{mod}\, 8)$ then,

$$b_k = \begin{cases} x^{\frac{-13k+116}{2}-(\frac{(k-8)(k-16)}{2})'-(\frac{(k-8)^4}{2^5})'}, (\frac{(k-8)^4}{2^5})' \ge 2^{n-2}, \\ x^{\frac{-13k+116}{2}-(\frac{(k-8)(k-16)}{2})'-(\frac{(k-8)^4}{2^5})'+(\frac{(k-8)^4}{2^4})'+\ldots+2^{n-2}}, (\frac{(k-8)^4}{2^5})' < 2^{n-2}, \end{cases}$$

where, $8 \le k \le 2^n$, in which, $(a)' = \frac{a}{q}$ where q is the largest odd integer such that q dividing a.

Proof is easy by using the induction on k by considering 32 cases. For example, let $k \equiv 0 (\mathrm{mod}\, 8)$.

The assertion holds for $k = 1, 2, ..., 8$. Let $k > 8$ and let the assertion holds for every $t < k$. Suppose $k - 8 = 2^s q$, for some positive integer s, where q is an odd integer, i.e.;

$(k-8)' = \frac{k-8}{q}$, similarly, let $(k-16)' = \frac{k-16}{q'}$.

Let $\frac{(k-8)^4}{2^5} \ge 2^{n-2}$ and $\frac{(k-8)(k-16)}{2} \ge 2^{n-2}$. Observe that $k-1 \equiv 7, k-2 \equiv 6$ and $k-3 \equiv 5$. So, $b_k = b_{k-3}(b_{k-2})^7 b_{k-1}$

$$= x^{-13(k-3)+63-(\frac{(k-8)(k-16)}{2})'}$$

$$. x^{\frac{9(k-2)-50}{2}+(\frac{(k-8)(k-16)}{2})'-(\frac{(k-8)^4}{2^5})'} y^7$$

$$. x^{\frac{9(k-1)-73}{2}+(\frac{(k-8)(k-16)}{2})'} y$$

$$= x^{\frac{-13k+102}{2}-(\frac{(k-8)(k-16)}{2})'+\frac{9k-68}{2}+(\frac{(k-8)(k-16)}{2})'-(\frac{(k-8)^4}{2^5})'}$$

$$. x^{-\frac{9k-82}{2}-(\frac{(k-8)(k-16)}{2})'}$$

$$= x^{\frac{-13k+116}{2}-\frac{(k-8)(k-16)}{2qq'}-\frac{(k-8)^4}{2^5 q^4}}$$

$$= x^{\frac{-13k+116}{2}-(\frac{(k-8)(k-16)}{2})'-(\frac{(k-8)^4}{2^5})'},$$

As required.

To prove the sequenceability of Q_{2^n}, we consider its relations. By the relations $y^{-1}xy = x^{-1}$ and $y^2 = x^{2^{n-2}}$, we deduce that every element $g \in Q_{2^n}$ may be written in the form

$$g = x^i y^j, \quad 0 \le i \le 2^{n-2}, \quad 0 \le j \le 1.$$

The rest of proof is similar to that of the Proposition 2.1 by considering two cases : $j = 0$ and $j = 1$. This proves that $g = b_k$, for some integer $k \ge 1$.

Note that the defined sequence $\{b_k\}$ as above, is periodic. Moreover, $LEN_A(Q_{2^n}, b_1, b_2, b_3) = 2^n$, for, if $t = LEN_A(Q_{2^n}, b_1, b_2, b_3)$ then the equations $b_{t+1} = b_1$, $b_{t+2} = b_2$ and $b_{t+3} = b_3$ hold. Suppose $t \ne 2^n$. Since $n \ge 3$ then $t \equiv a (\mathrm{mod}\, 8)$ where, $a \in \{\pm 1, \pm 2, \pm 3, 4\}$. In each case we get a contradiction. For example, if $t \equiv 1 (\mathrm{mod}\, 8)$ then $t + 1 \equiv 2 (\mathrm{mod}\, 8)$. So,

If $(\frac{(t-1)^4}{2^5})' \ge 2^{n-2}$ then $x^{\frac{t-1}{2}+(\frac{(t-1)^4}{2^5})'} y = x$ which shows that Q_{2^n} is abelian, and if

$$(\frac{(t-1)^4}{2^5})' < 2^{n-2}$$

Then, $x^{\frac{t-1}{2}+(\frac{(t-1)^4}{2^5})'+(\frac{(t-1)^4}{2^4})'+\ldots+2^{n-2}} y = x$ which also proves the abelianity of Q_{2^n}.

Results

For every even value of n, an α-cover for D_{2n}, may be given by using the sequence $\{a_n\}$ as follows:

$$\alpha = [A_1, A_2, ..., A_{2n}], \quad A_i = \{1, a_i\}.$$

Also for the odd values of n we use the sequence $\{c_n\}$ and define

$$\alpha = [A_1, A_2, ..., A_{4n}], \quad A_i = \{1, c_i\}.$$

Similarly, an α-cover for Q_{2^n} may be defined by using the sequence $\{b_n\}$ as

$$\alpha = [B_1, B_2, ..., B_{2n}], \quad B_i = \{1, b_i\}.$$

Each of these covers are indeed logarithmic signatures (i.e., representing every element of the groups in terms of A_i or B_i, is unique, see [12] for the definition and for the properties). To prove this property it is sufficient to consider the following obtained results:

$$\begin{cases} LEN_A(D_{2n}) = 2n, & n \text{ even}, \\ LEN_A(D_{2n}) = 4n, & n \text{ odd}, \\ LEN_A(Q_{2^n}) = 2^n, & n \geq 3. \end{cases}$$

Acknowledgements

Authors would like to offer their thanks to the referees for their useful comments and careful reading of the manuscripts of this paper.

References

1. Aydin H. and Smith G.C. Finite p-quotients of some cyclically presented groups. *J. London Math. Soc.*, **49**(2): 83-92 (1994).
2. Aydin H. and Karaduman E. On the periodic 2-step general Fibonacci sequences in dihedral groups. *МАТЕМАТИЧКИ ВЕСНИК* , **58**: 47-56 (2006).
3. Aydin H. and Dikici R. General Fibonacci sequences in finite groups. *Fibonacci Quarterly*, **36**(3): 216-221 (1998).
4. Campbell C. M., Doostie H. and Robertson E. F. Fibonacci length of generating pairs in groups. In: Bergum G.E., et al (Eds.), *Applications of Fibonacci numbers*, 3rd Ed., Kluwer Academic Publishers, pp. 27-35 (1990).
5. Dikici R. and Smith G. C. Fibonacci Sequences in Finite Nilpotent Groups. *Turkish J. Math*, **21**: 133-142 (1997).
6. Knox S. W. Fibonacci sequences in finite groups. *Fibonacci Quarterly*, **30** (2): 116-120 (1992).
7. Maliveras S. S. and Memon N. D. Algebraic properties of cryptosystem PGH. *J. of Cryptography*, **5**: 176-183 (1992).
8. Maliveras S. S., Stinson D. R. and Trung T. Van. New approaches to designing public Key Cryptosystems using one-way functions and trap-doors in finite groups. *J. of Cryptography*, **15**: 285-297 (2002).
9. Ozkan E., Aydin H. and Dikici R. Applications of Fibonacci sequences in a finite nilpotent group. *J. Applied Mathematics and Computations*, **141**(2-3): 565-578 (2003).
10. Sun Z. W. Finite coverings of groups. *Fund. Math. Soc.*, **134**: 37-53 (1990).
11. Sun Z. W. On covering multiplicity. *Proc. Amer. Math. Soc.,* **127**: 1293-1300 (1999).
12. Svaba P. and Trung T. Van. On generation of random covers for finite groups. *Tatra Mountains Mathematical Publications*, **37**: 105-112 (2007).
13. Wall D. D. Fibonacci series modulo n. *Amer. Math. Monthly*, **67**: 525-532 (1969).
14. Wilcox H. J. Fibonacci sequences of period *n* in groups. *Fibonacci Quarterly*, **24**: 351-361 (1986).