Far East Journal of Mathematical Sciences (FJMS)

http://www.pphmj.com
http://dx.doi.org/10.17654/MS101112461
Volume 101, Number 11, 2017, Pages 2461-2474 **ISSN: 0972-0871**

HAMILTONICITY PROPERTIES OF CIRCULANT DIGRAPHS OF SEMIPRIME OR POWER OF PRIME ORDER

Zbigniew R. Bogdanowicz

Armament Research, Development and Engineering Center
Picatinny, New Jersey 07806
U. S. A.

Abstract

Let $G = G_n(a_1, a_2, ..., a_k)$ be a circulant digraph of order either $n = p_1p_2$ or $n = p^q$ for some positive integer q, primes p, p_1, p_2, and jumps $a_1, a_2, ..., a_k$. We give new necessary and sufficient conditions for G to be Hamiltonian if either $n = p^q$ or $k = 2$. Furthermore, we give new necessary and sufficient conditions for $G_{p^q}(a_1, a_2)$ to be decomposable into Hamilton cycles, and to be decomposable into cycles of equal lengths. Finally, we prove the necessary and sufficient conditions for any circulant digraph of even order to be decomposable into Hamilton paths, which also provide Hamilton path decompositions for two special cases of G.

1. Introduction

A *circulant* digraph $G_n(a_1, a_2, ..., a_k)$ on n vertices with k distinct

Received: January 10, 2017; Accepted: March 18, 2017
2010 Mathematics Subject Classification: 05C20, 05C38, 05C51.
Keywords and phrases: circulant digraph, Hamilton cycle, Hamiltonian digraph, graph decomposition.

jumps $a_1, a_2, ..., a_k$ has vertices $i + a_1, i + a_2, ..., i + a_k \pmod n$ adjacent to each vertex i, where for $k \geq j \geq 1$, each $a_j < n$. On one hand, it is well-known that all connected undirected circulants are Hamiltonian [1, 8]. On the other hand, not all connected circulant digraphs G are Hamiltonian [3, 12], and determining the necessary and sufficient conditions for G to be Hamiltonian remains an open hard problem. Furthermore, it is even less known about the decomposition of G into Hamilton cycles or cycles of equal lengths [4, 5]. These problems, however, are of great interest to some communities for potential applicability and relevance to cryptology, cryptography, etc. Hence, there has been extensive research done and published in the number of papers (e.g., [3-5, 11, 12]) focused on the Hamiltonicity and decomposition of subsets of circulant digraphs.

In this paper, we consider circulant digraphs G of order either $n = p_1^q$ or $n = p_1 p_2$ for some primes p_1 and p_2 and positive integer q. For the reason described above, we study the Hamiltonicity and decomposition of G. That is, we focus on the existence of Hamilton cycle in G and decomposition of G into: (1) Hamilton cycles, (2) cycles of equal lengths, and (3) Hamilton paths. The paper is organized as follows: After preliminary known results briefly recapped in Section 2, in Section 3, we prove that if $n = p_1^q$ and $G = G_n(a_1, a_2, ..., a_k)$ is connected, then G is Hamiltonian. Otherwise, if $n = p_1 p_2$, then for $k = 2$, we prove that $G = G_n(a_1, a_2)$ is Hamiltonian if and only if either $\gcd(n, a_1) = 1$ or $\gcd(n, a_2) = 1$. In Section 4, we give new simple necessary and sufficient conditions for decomposition into Hamilton cycles of $G_{p_1^q}(a_1, a_2)$ that cannot be extended to generic $G_n(a_1, a_2)$ (that is known [4]), and in particular cannot be extended to $G_{p_1 p_2}(a_1, a_2)$. In Section 5, we prove that $G_{p_1^q}(a_1, a_2)$ can be decomposed into directed cycles of equal lengths if and only if $\gcd(n, a_1) = \gcd(n, a_2)$. Finally, in Section 6, we prove that $G_{2m}(a_1, a_2, ..., a_k)$ can be decomposed into Hamilton paths if and only if $k = 2m - 1$.

2. Preliminary Results

There are two facts concerning circulants that will be useful in proving the results in the next sections. First, according to Boesch and Tindell [2]:

Theorem 2.1 [2]**.** *Circulant digraph* $G_n(a_1, a_2, ..., a_k)$ *is connected if and only if* $\gcd(n, a_1, a_2, ..., a_k) = 1$.

Boesch and Tindell [2] stated the above Theorem 2.1 for undirected circulants, but the extension of their result to directed circulants is trivial.

Second, we prove the following:

Theorem 2.2 [3]**.** *Connected circulant digraph* $G_n(a_1, a_2)$ *has Hamilton cycle formed by both jumps if and only if* $\gcd(n, s_1 \cdot a_1 + s_2 \cdot a_2) = s_1 + s_2$ *and* $a_1 \equiv a_2 \pmod{s_1 + s_2}$ *for some positive integers* s_1 *and* s_2.

In particular, Theorem 2.2 will be useful in the next section in proving the necessary and sufficient conditions for the existence of Hamilton cycle in the circulant of semiprime order. Both Theorems 2.1 and 2.2 will be used in proofs concerning decomposition of G_{p^q} and $G_{p_1p_2}$ in Sections 4 and 5.

3. Existence of Hamilton Cycle in Circulant Digraphs G_{p^q} and $G_{p_1p_2}$

First, consider a circulant digraph $G_{p^q}(a_1, a_2, ..., a_k)$, where p is a prime and q is some positive integer.

Theorem 3.1. *Let* $n = p^q$ *for some prime* p *and positive integer* q. *Circulant digraph* $G = G_n(a_1, a_2, ..., a_k)$ *is Hamiltonian if and only if* $\gcd(n, a_1, a_2, ..., a_k) = 1$. *Furthermore, if* G *is Hamiltonian, then it has a Hamilton cycle formed by a single jump* a_i *for some* i, *where* $k \geq i \geq 1$.

Proof. If $\gcd(n, a_1, a_2, ..., a_k) \neq 1$, then by Theorem 2.1, G is not Hamiltonian, which proves the necessary condition. Consider now the sufficient condition for G being Hamiltonian. Suppose $\gcd(n, a_1, a_2, ..., a_k)$

$= 1$. Since n is a prime power, there is an i such that $\gcd(n, a_i) = 1$ and now, since a_i is a generator of the additive group of the integers module n, the digraph $G_n(a_i)$ is Hamiltonian, and hence also $G_n(a_1, a_2, ..., a_k)$ is Hamiltonian. □

Note that not every Hamilton cycle has to be formed by a single jump in $G_{p^q}(a_1, a_2, ..., a_k)$. For example, it is easy to check that $G_8(1, 5)$ contains a Hamilton cycle formed by both jumps with a sequence $(1, 5, 1, 5, 1, 5, 1, 5)$ and $G_9(1, 2, 3)$ contains a Hamilton cycle formed by all 3 jumps with a jump sequence $(1, 2, 3, 2, 3, 2, 1, 2, 2)$.

We now focus on circulant digraphs of semiprime order with two jumps only, i.e., results for a circulant digraph $G_{p_1p_2}(a_1, a_2)$, where p_1 and p_2 are primes. Note that the special case when $p_1 = p_2$ is a special case of Theorem 3.1 when $q = 2$.

Theorem 3.2. *Let $n = p_1p_2$ for some primes p_1 and p_2. Circulant digraph $G = G_n(a_1, a_2)$ is Hamiltonian if and only if $\gcd(n, a_i) = 1$ for either $i = 1$ or $i = 2$. Furthermore, if such a_i exists, then G has a Hamilton cycle formed by a_i.*

Proof. If $p_1 = p_2$, then by Theorem 3.1, G is Hamiltonian if and only if it contains a_i such that $\gcd(n, a_i) = 1$, $2 \geq i \geq 1$. So, the case when $p_1 = p_2$ is covered in Theorem 3.1. Hence, assume that $p_1 \neq p_2$. Clearly, if there exists a_i such that $\gcd(n, a_i) = 1$, then a_i is a generator of the additive group of integers module n, and $G_n(a_i)$ has a Hamilton cycle formed by jump a_i. This implies that $G_n(a_1, a_2)$ has a Hamilton cycle formed by a_i for either $i = 1$ or $i = 2$, which proves the sufficient condition. Consider now the necessary condition. Suppose that in this case, G is Hamiltonian and there is no a_i such that $\gcd(n, a_i) = 1$. If $\gcd(p_1, a_i) \geq 2$ and $\gcd(p_2, a_i) \geq 2$, then $a_i \geq p_1p_2$ - a contradiction. Then, for some positive integers k_1

and k_2, there must exist $G_{p_1p_2}(k_1p_1, k_2p_2)$ that has a Hamilton cycle formed by both jumps k_1p_1 and k_2p_2. By Theorem 2.2, $G_{p_1p_2}(k_1p_1, k_2p_2)$ has a Hamilton cycle formed by both jumps if and only if $\gcd(p_1p_2, s_1k_1p_1 + s_2k_2p_2) = s_1 + s_2$ and $k_1p_1 \equiv k_2p_2 \pmod{s_1 + s_2}$ for some positive integers s_1 and s_2. We know that $\gcd(k_1, p_2) = 1$ and $\gcd(k_2, p_1) = 1$, because otherwise $\gcd(p_1p_2, k_1p_1, k_2p_2) > 1$ - a contradiction. Also, $\gcd(p_1p_2, s_1k_1p_1 + s_2k_2p_2) = s_1 + s_2$ implies either $s_1 + s_2 = p_1$ or $s_1 + s_2 = p_2$ or $s_1 + s_2 = p_1p_2$. On one hand, if for either $i = 1$ or $i = 2$, $p_i = s_1 + s_2$, then $k_ip_i \equiv 0 \pmod{s_1 + s_2}$ and $k_{3-i}p_{3-i} > 0 \pmod{s_1 + s_2}$, which imply $k_1p_1 \neq k_2p_2 \pmod{s_1 + s_2}$ - a contradiction. On the other hand, by definition of a_i in G, $k_1p_1 < p_1p_2$, $k_2p_2 < p_1p_2$ and $k_1p_1 \neq k_2p_2$ imply that if $s_1 + s_2 = p_1p_2$, then $k_1p_1 \neq k_2p_2 \pmod{s_1 + s_2}$ - a contradiction, which proves that G is Hamiltonian only if $\gcd(n, a_i) = 1$ for either $i = 1$ or $i = 2$. □

Again, as was the case with G_{p^q} a Hamilton cycle in $G = G_{p_1p_2}(a_1, a_2)$ does not have to be formed by a single jump, e.g., it is easy to check that $G_{10}(1, 3)$ contains a Hamilton cycle formed by both jumps with a jump sequence $(1, 3, 1, 3, 1, 3, 1, 3, 1, 3)$. Furthermore, for $k \geq 3$, there are the cases that any Hamilton cycle in $G_{p_1p_2}(a_1, a_2, ..., a_k)$ must be formed by multiple jumps. For example, it is easy to verify that $G_{2.5}(2, 4, 5)$ does not have a Hamilton cycle formed by a single jump, and yet it has a Hamilton cycle formed by the following jump sequence: $(2, 2, 2, 5, 4, 2, 2, 4, 5, 2)$. Similarly, $G_{3.5}(3, 5, 6)$ does not have a Hamilton cycle formed by a single jump but has the following Hamilton cycle formed by a jump sequence: $(3, 3, 5, 3, 6, 3, 5, 3, 3, 5, 3. 5, 5, 3, 5)$.

4. Decomposition of Circulant Digraph G_{p^q} into Hamilton Cycles

For any connected circulant digraph with two jumps, the following is

known:

Theorem 4.1 [4]**.** *Connected circulant digraph* $G_n(a_1, a_2)$ *has two arc-disjoint Hamilton cycles if and only if any of the following holds*:

(1) $\gcd(n, a_1) = \gcd(n, a_2) = 1$,

(2) $\gcd(n, s_1 \cdot a_1 + s_2 \cdot a_2) = \gcd(n, s_1 \cdot a_2 + s_2 \cdot a_1) = s_1 + s_2$ *and* $a_1 \equiv a_2 \pmod{s_1 + s_2}$ *for some positive integers* s_1 *and* s_2.

Furthermore, if (2) *is satisfied, then these Hamilton cycles are formed by both jumps each*.

In this section, we simplify the necessary and sufficient conditions of Theorem 4.1 for circulant digraphs of order equal power of prime. In addition, we will show that for the circulant digraph of order equal semiprime, such a simplification is not possible.

Theorem 4.2. *Let* $n = p^q$ *for some prime* p *and positive integer* q. *Circulant digraph* $G = G_n(a_1, a_2)$ *can be decomposed into Hamilton cycles if and only if* $\gcd(n, a_1) = \gcd(n, a_2) = 1$. *Furthermore, if* G *can be decomposed into Hamilton cycles, then every Hamilton cycle in decomposition can be formed by a single jump* a_i, *where* $2 \geq i \geq 1$.

Proof. If $G = G_{p^q}(a_1, a_2)$ can be decomposed into Hamilton cycles, then either $\gcd(p^q, a_1) = 1$ or $\gcd(p^q, a_2) = 1$, otherwise $\gcd(p^q, a_1, a_2) > 1$ implying by Theorem 2.1 a disconnected G - a contradiction. Without loss of generality, assume $\gcd(p^q, a_1) = 1$. If $\gcd(p^q, a_1) = 1$ and $\gcd(p^q, a_2) > 1$, then $a_1 \equiv a_2 \pmod{s_1 + s_2 = p^x}$ cannot be satisfied for any positive integers s_1, s_2, x and by Theorem 4.1, G cannot be decomposed into Hamilton cycles, which proves the necessary conditions. On the other hand, if $\gcd(p^q, a_1) = 1$ and $\gcd(p^q, a_2) = 1$, then by Theorem 2.1, both Hamilton cycles can be formed by single jumps, which proves the sufficient conditions. □

Even though $\gcd(n, a_1) = \gcd(n, a_2) = 1$ must be satisfied based on Theorem 4.2 for decomposition of $G = G_{p^q}(a_1, a_2)$, it does not mean that both Hamilton cycles must be formed by single jumps. For example, for $G_{3^3}(4, 13)$, we have $\gcd(27, 4) = \gcd(27, 13) = 1$, and we also have (2) satisfied in Theorem 4.1 for $s_1 = 1$ and $s_2 = 2$. So, by Theorem 4.1, $G_{27}(4, 13)$ can easily be decomposed into Hamilton cycles formed by both jumps.

Based on Theorem 4.2, we conjecture the following:

Conjecture 4.3. Let $n = p^q$ for some prime p and positive integer q. Circulant digraph $G = G_n(a_1, a_2, ..., a_k)$ can be decomposed into Hamilton cycles if and only if $\gcd(n, a_i) = 1$ for every a_i, $k \geq i \geq 1$. Furthermore, if G can be decomposed into Hamilton cycles, then every Hamilton cycle can be formed by a single jump a_i, where $k \geq i \geq 1$.

There is no similar simplification for $G_{p_1p_2}$. Consider $G_{3\cdot5}(2, 5)$ that does not satisfy $\gcd(n, a_2) = 1$. So,

$$\gcd(15, 2 \cdot 2 + 1 \cdot 5) = \gcd(15, 2 \cdot 5 + 1 \cdot 2) = 3$$

and $2 \equiv 5 \pmod{2 + 1}$, implying by Theorem 4.1 a decomposition of $G_{3\cdot5}(2, 5)$ into Hamilton cycles. Another counterexample is $G_{10}(1, 3, 5)$ that does not satisfy $\gcd(n, a_3) = 1$ (i.e., $\gcd(10, 5) = 5$) and yet it can be decomposed into three Hamilton cycles with the following jump sequences: $(1, 5, 1, 5, 1, 5, 1, 5, 1, 5)$, $(1, 5, 1, 5, 1, 5, 1, 5, 1, 5)$ and $(3, 3, 3, 3, 3, 3, 3, 3, 3, 3)$.

5. Decomposition of Circulant Digraph G_{p^q} into Cycles of Equal Lengths

Decomposition of circulant digraphs into cycles of equal lengths generalizes the Hamiltonian cycle decomposition in these graphs but in general, it is more difficult problem. For example, for $G_n(a_1, a_2)$, we know

the necessary and sufficient conditions for decomposition into Hamilton cycles, recall Theorem 4.1, but only sufficient conditions have been determined for decomposition of $G_n(a_1, a_2)$ into cycles of equal lengths [5]. In this section, we allow circulant digraphs to be disconnected as opposed to the previous two sections. The following lemma derived from Theorem 2.1 will be useful in the proof of decompositions of G_{p^q} into directed cycles of equal lengths.

Lemma 5.1. *Circulant* $G_n(a_1, a_2, ..., a_k)$ *consists of* r *connected components if and only if* $\gcd(n, a_1, a_2, ..., a_k) = r$.

Proof. If $r = 1$, then by Theorem 2.1, $G = G_n(a_1, a_2, ..., a_k)$ consists of a single connected component if and only if $\gcd(n, a_1, a_2, ..., a_k) = r = 1$, and we are done. Otherwise, G is a disconnected circulant. Let in this case, G^i be an ith connected component in G. Let q be the smallest number such that a connected component G^i contains vertices 1 and $1 + q$ of G. By isomorphism $i \to i + 1$ of G, each G^i is a connected circulant of form $G^i = G^i_{n/q}(a_1/q, a_2/q, ..., a_k/q)$. So, $q = r$. Therefore, by Theorem 2.1,

$$\gcd\left(\frac{n}{r}, \frac{a_1}{r}, \frac{a_2}{r}, ..., \frac{a_k}{r}\right) = 1,$$

which means that

$$r = \gcd\left(\frac{n}{r}, \frac{a_1}{r}, \frac{a_2}{r}, ..., \frac{a_k}{r}\right) r = \gcd(n, a_1, a_2, ..., a_k). \qquad \square$$

As in previous section, let us consider the circulant digraph of order equal power of prime.

Theorem 5.2. *Let* $n = p^q$ *for some prime* p *and positive integer* q. *Circulant digraph* $G = G_n(a_1, a_2)$ *can be decomposed into directed cycles of equal lengths if and only if* $\gcd(n, a_1) = \gcd(n, a_2)$.

Proof. Consider first a decomposition of G into the cycles formed by single jumps. By Lemma 5.1, the size of a cycle formed by a single jump a_i in G is $\frac{n}{\gcd(n, a_i)}$. Therefore, in this case, G can be decomposed into the cycles of equal lengths and each formed by a single jump if and only if $\gcd(n, a_1) = \gcd(n, a_2)$.

Consider now a case when any decomposition of G into the cycles of equal lengths must contain a cycle formed by both jumps, i.e., a cycle with r_1 arcs induced by a_1 and with r_2 arcs induced by a_2, for some positive integers r_1 and r_2. Let $\gcd(n, a_1, a_2) = 1$, i.e., G is connected. Then, for some positive integer $t < q$, either $\gcd(n, a_1) = 1$ and $\gcd(n, a_2) = p^t$ or $\gcd(n, a_1) = p^t$ and $\gcd(n, a_2) = 1$. Without loss of generality, assume $\gcd(n, a_1) = 1$ and $\gcd(n, a_2) = p^t$, implying $a_2 = rp$ for some positive integer $r < p^{q-1}$. Since there are $2p^q$ arcs in G, either $r_1 + r_2 = p^{q_1}$ or $r_1 + r_2 = 2p^{q_1}$ for some nonnegative $q_1 < q$. So, for such a cycle, one of the following relations must be satisfied:

$$r_1 a_1 + (p^{q_1} - r_1) a_2 \equiv 0 \pmod{p^q}, \tag{1}$$

$$r_1 a_1 + (2p^{q_1} - r_1) a_2 \equiv 0 \pmod{p^q}. \tag{2}$$

First, suppose (1) is satisfied. Then

$$r_1 a_1 + (p^{q_1} - r_1) a_2 = kp^q,$$

for some positive integer k. By substituting $a_1 - a_2$ with a_3, we obtain

$$r_1 a_3 + p^{q_1} a_2 = kp^q$$

$$\Rightarrow r_3 p^{q_3} a_3 + p^{q_1} a_2 = kp^q,$$

where $r_1 = r_3 p^{q_3}$ for some positive integers a_3, q_3 and r_3 satisfying $\gcd(n, a_3) = \gcd(n, r_3) = 1$.

Since $p^q > p^{q_1} > r_1$, we obtain the following:

$$r_3 a_3 + p^{q_1-q_3} a_2 = k p^{q-q_3}$$

$$\Rightarrow r_3 a_3 + p^{q_1-q_3} a_2 = k p^{q-q_1} p^{q_1-q_3}$$

$$\Rightarrow r_3 a_3 + p^{q_1-q_3} a_2 = k_1 p^{q_1-q_3}$$

$$\Rightarrow r_3 a_3 = (k_1 - a_2) p^{q_1-q_3},$$

for some positive integer k_1 - a contradiction, because $\gcd(r_3 a_3, p) = 1$. On the other hand, based on the above substitutions, we can evaluate (2) as follows:

$$r_3 p^{q_3} a_3 + 2 p^{q_1} a_2 = k p^q$$

$$\Rightarrow r_3 a_3 + 2 p^{q_1-q_3} a_2 = k p^{q-q_3}$$

$$\Rightarrow r_3 a_3 + 2 p^{q_1-q_3} a_2 = k p^{q-q_1} p^{q_1-q_3}$$

$$\Rightarrow r_3 a_3 + 2 p^{q_1-q_3} a_2 = k_1 p^{q_1-q_3}$$

$$\Rightarrow r_3 a_3 = (k_1 - 2a_2) p^{q_1-q_3},$$

which again results in a contradiction because $\gcd(r_3 a_3, p) = 1$. This proves Theorem 5.2. □

Note that the result for $G = G_{p^q}(a_1, a_2)$ cannot be extended to $G_{p^q}(a_1, a_2, ..., a_k)$ for $k \geq 3$ (as opposed to extension to Hamilton decomposition by Conjecture 4.3 in previous section). For example, $G_8(1, 2, 3)$ does not satisfy $\gcd(n, a_2) = 1$ (i.e., $\gcd(8, 2) = 2$) and yet it can be decomposed into squares of the following two jump sequence forms: $(1, 3, 1, 3)$ and $(2, 2, 2, 2)$.

Finally, we note that the necessary and sufficient conditions cannot be

carried over from $G_{p^q}(a_1, a_2)$ to $G = G_{p_1p_2}(a_1, a_2)$ because of the counterexamples (i.e., $G_{3\cdot5}(2, 5)$ and $G_{10}(1, 3, 5)$) from the previous section for the decomposition of G into Hamilton cycles, which was a special case of decomposition into cycles of equal lengths.

6. Decomposition of Circulant Digraph G_{2m} into Hamilton Paths

In this section, we consider a circulant digraph $G_{2m}(a_1, a_2, ..., a_k)$ for any positive integers k and m. By a Hamilton path in G, we mean in this section a simple directed path that visits each vertex in G exactly once and that is not a Hamilton cycle in G - a standard definition.

A row complete Latin square is a Latin square that has every distinct pair of treatments in adjacent cells in a row exactly once. Row complete $n \times n$ squares are known to exist for all even n [6]. In particular, the following is known:

Theorem 6.1 [7]**.** *If there exists a permutation of integers* $0, 1, 2, ..., n-1$ *with the property that the differences* $(\mathrm{mod}\, n)$ *between pairs of adjacent integers are all distinct, then there exists a row complete Latin square of order n.*

The complete digraph K_n^* on n vertices has decomposition into Hamilton paths if a row complete Latin square of order n exists [10]. For example, for $K_6^* = G_6(1, 2, 3, 4, 5)$, a jump sequence $(1, 4, 3, 2, 5)$ can generate the first row $(0, 1, 5, 2, 4, 3)$ in a row complete Latin square. Furthermore, for every last generated row, the next row can be generated by adding one $(\mathrm{mod}\, 6)$ to each element of the last generated row, until completing 6×6 Latin square. Consequently, we have

Lemma 6.2. K_n^* *can be decomposed into Hamilton paths if n is even.*

Proof. It is a direct consequence of conclusions of [6] and [10] above. □

We first give the necessary conditions for arbitrary circulant diagraph G to have Hamilton path decomposition as follows:

Theorem 6.3. *Circulant digraph* $G_n(a_1, a_2, ..., a_k)$ *has decomposition into Hamilton paths only if* $k = n - 1$.

Proof. Suppose $k < n-1$ and $G = G_n(a_1, a_2, ..., a_k)$ can be decomposed into Hamilton paths. Then G has $m = n \cdot k$ arcs and by the Hamilton decomposition of G, we have $n-1 | n \cdot k$ - a contradiction. □

Consider now the circulant digraphs of even order.

Theorem 6.4. *Circulant digraph* $G_{2m}(a_1, a_2, ..., a_k)$ *has decomposition into Hamilton paths if and only if* $k = 2m - 1$. *Furthermore, if* $a_j = j$ *for every* $j \leq 2m-1$, *then each Hamilton path in decomposition of* $G_{2m}(a_1, a_2, ..., a_{2m-1})$ *can be formed by jump sequence*

$$((a_1, a_{2m-2}), (a_3, a_{2m-4}), ..., (a_{2m-5}, a_4), (a_{2m-3}, a_2), a_{2m-1}).$$

Proof. The necessity follows from Theorem 6.3, so we consider the sufficiency. If $k = 2m-1$, then $G = G_{2m}(a_1, a_2, ..., a_{2m-1})$ represents a complete digraph of order $2m$, which means that $G \simeq K^*_{2m}$. Hence, by Lemma 6.2, G can be decomposed into Hamilton paths. Furthermore, if $k = 2m-1$ and $a_j = j$ for every $j \leq 2m-1$, then jump sequence

$$((a_1, a_{2m-2}), (a_3, a_{2m-4}), ..., (a_{2m-5}, a_4), (a_{2m-3}, a_2), a_{2m-1})$$

represents a sequence of pairwise distinct integers exhausting all jumps in G that induces a sequence of vertices

$$(i, (i+1, i+2m-1), (i+2, i+2m-2), ..., (i+m-1, i+m+1), i+m) \pmod{2m}$$

that are also pairwise distinct, and by Theorem 6.1 represent the ith Hamilton path in decomposition of G, where $2m \geq i \geq 1$. □

Clearly, G_{p^q} and $G_{p_1p_2}$ for $p = p_1 = 2$ represent special cases of G_{2m}. Hence, we can state the following two results:

Corollary 6.5. *Circulant digraph* $G_{2^q}(a_1, a_2, ..., a_k)$ *with positive integer q has decomposition into Hamilton paths if and only if* $k = 2^q - 1$.

Corollary 6.6. *Circulant digraph* $G_{2p_2}(a_1, a_2, ..., a_k)$ *with some prime* p_2 *has decomposition into Hamilton paths if and only if* $k = 2p_2 - 1$.

Finally, we note that the generalization of Hamilton path decomposition to all circulant digraphs is directly related to the Hamilton path decomposition of directed complete graphs, which is an open hard problem since long time [9]. Hence, the generalization of Hamilton path decomposition to $G_{p^q}(a_1, a_2, ..., a_k)$ and $G_{p_1p_2}(a_1, a_2, ..., a_k)$ for p, p_1, p_2 odd, even though they represent the small subset of circulant digraphs, might turn out to be a hard problem as well.

References

[1] B. Alspach, D. Bryant and D. L. Kreher, Vertex-transitive graphs of prime-squared order are Hamilton-decomposable, J. Combin. Des. 22 (2014), 12-25.

[2] F. T. Boesch and R. Tindell, Circulants and their connectivities, J. Graph Theory 8 (1984), 129-138.

[3] Z. R. Bogdanowicz, Hamilton cycles in circulant digraphs with prescribed number of distinct jumps, Discrete Math. 309 (2009), 2100-2107.

[4] Z. R. Bogdanowicz, Arc-disjoint and edge-disjoint Hamilton cycles in circulants with two jumps, Graphs Combin. 29 (2013), 165-171.

[5] Z. R. Bogdanowicz, Decomposition of circulant digraphs with two jumps into cycles of equal lengths, Discrete Appl. Math. 180 (2015), 45-51.

[6] F. G. Giesbrecht and M. L. Gumpertz, Planning, Construction, and Statistical Analysis of Comparative Experiments, John Wiley & Sons, Hoboken, NJ, 2004, pp. 118-145.

[7] A. D. Keedwell and J. Dénes, Latin Squares and their Applications, North-Holland Publishing Company, Amsterdam, 2015.

[8] L. Lovász, Combinatorial Problems and Exercises, North-Holland Publishing Company, Amsterdam, 1979.

[9] T. P. McDonough and V. C. Mavron, Combinatorics, London Mathematical Society Lecture Note Series, Cambridge University Press, Vol. 13, 1974, pp. 91-92.

[10] N. S. Mendelsohn, Hamiltonian decomposition of the complete directed *n*-graph, Theory of Graphs (Proc. Colloquium Tihany, 1966), Academic Press, New York, 1968, pp. 237-241.

[11] J. Turner, Point-symmetric graphs with a prime number of points, J. Comb. Theory 3 (1967), 136-145.

[12] Q. Yang, R. Burkard, E. Cela and G. Woginger, Hamiltonian cycles in circulant digraphs with two stripes, Discrete Math. 176 (1997), 233-254.