Hamiltonian cycles in circulant digraphs with two stripes

Qi Fan Yang\(^a\), Rainer E. Burkard\(^b\,*\), Eranda Çela\(^b\),
Gerhard J. Woeginger\(^b\)

\(^a\)Mathematics Department, Zhejiang University, Hangzhou, China
\(^b\)Technische Universität Graz, Institut für Mathematik B, Steyrergasse 30, A-8010 Graz, Austria

Received 27 August 1992; revised 7 May 1996

Abstract

The circulant traveling salesman problem (CTSP) is the problem of finding a minimum weight Hamiltonian cycle in a weighted graph with circulant distance matrix. The computational complexity of this problem is not known. In fact, even the complexity of deciding Hamiltonicity of the underlying graph is unknown.

This paper provides a characterization of Hamiltonian digraphs with circulant distance matrix containing only two nonzero stripes. The corresponding conditions can be checked in polynomial time. Secondly, we show that all Hamiltonian cycles of a circulant 2-digraph are periodic. Based on these two results, a method for enumerating all Hamiltonian cycles in such digraphs is described. Moreover, two simple algorithms are derived for solving the sum and bottleneck versions of CTSP for circulant distance matrices with two nonzero stripes.

Keywords: Circulant digraph; Hamiltonian cycle; Traveling salesman problem

1. Introduction

For many years, the Hamiltonicity of certain classes of graphs has been studied. These investigations are closely related to the famous traveling salesman problem (TSP) with specially structured distance matrices. In this paper we study the Hamiltonicity and the TSP in digraphs with circulant distance matrices. For a given \(n \times n\) matrix \(C = (c_{ij})\), the \(k\)th stripe consists of all entries \(c_{ij}\) with \((i-j) \equiv k \pmod{n}\), \(i, j \in \{0, 1, \ldots, n-1\}\). A nonzero stripe is a stripe containing at least one nonzero element. A circulant matrix is an \((n \times n)\)-matrix \(C = (c_{ij})\) whose elements are constant in stripes, i.e. the value of \(c_{ij}\) depends only on \((i-j) \pmod{n}\) (cf. Fig. 1 for an illustration). A digraph with a circulant matrix as (weighted) adjacency matrix is called a circulant digraph.

* Corresponding author. E-mail: burkard@opt.math.tu-graz3.ac.at.

\(^1\)This research has been partially supported by the Spezialforschungsbereich F003 "Optimierung und Kontrolle"/Projektbereich Diskrete Optimierung.
the adjacency matrix of a circulant digraph has \( k \) nonzero stripes, the graph is called a \textit{circulant-}k \textit{digraph}.

The shortest Hamiltonian \textit{path} problem for circulant digraphs is polynomially solvable: Bach, Luby and Goldwasser proved that for such graphs the nearest neighbor rule yields a shortest Hamiltonian path (see [6]). The next important question, whether a shortest Hamiltonian \textit{cycle} can be found in polynomial time or not, is still open. However, a series of partial results on this problem has been derived. In 1977, Garfinkel [5] observed that the TSP on circulant-1 digraphs (with only one nonzero stripe) can be solved trivially. Boesch and Tindell (see [3]) studied the connectivity of circulant graphs. Their investigations were continued and extended to circulant digraphs by Van Doorn [4]. A characterization for Hamiltonian \textit{symmetric} circulant graphs has been derived by Burkard and Sandholzer in 1991 (see [2]). In [2] this characterization is used for solving efficiently the bottleneck TSP on symmetric circulant distance matrices. An exponential time algorithm for solving the sum TSP with nonsymmetric circulant distance matrices has been suggested by Medova-Dempster (see [8]). She comments also on complexity issues of this problem. Heuristics for the sum TSP on symmetric circulant distance matrices are suggested by Van der Veen (see [9]), who also reports computational results and analyzes these heuristics theoretically.

Two major results are derived in this paper. First, a necessary and sufficient condition for the Hamiltonicity of (nonsymmetric) circulant-2 digraphs is derived. It is shown that this necessary and sufficient condition can be checked in time that is polynomial in the logarithm of the number \( n \) of vertices of the given digraph. (Observe that a circulant-2 digraph with \( n \) vertices can be fully described by three numbers of length \( \log n \): by the number \( n \) and by two numbers that encode the position of the two nonzero stripes.) From an algorithmic point of view, this is the strongest possible result. The second major result concerns the structure of the Hamiltonian cycles of a circulant-2 digraph. Notice that in a circulant-2 digraph each arc can be associated to the nonzero stripe which contains the element of the adjacency matrix representing this arc. Considering this association there are two types of arcs in a circulant-2 digraph. We show that all Hamiltonian cycles possess a specific structure: the sequence of the types of arcs visited when moving along the cycle consists of a periodical repetition of a certain
pattern. Moreover, the length of this pattern, that is, the number of arcs represented by this pattern, is the same for all Hamiltonian cycles.

These results yield quite naturally two methods for the solution of the sum TSP and of the bottleneck TSP in circulant-2 digraphs, respectively. Once the problem of the existence of a Hamiltonian cycle in the given digraph has been solved, both bottleneck and sum optimal tours can be given in $O(n)$ time. Let us emphasize that all our results reporting time complexities are conformal to the unit cost model. Hence, we assume that any arithmetical operation (e.g. addition or division of two integers) can be carried out in constant time; see e.g. Aho et al. [1].

The paper is organized as follows. In Section 2, we introduce some definitions and preliminaries needed for deriving the necessary and sufficient conditions for a circulant-2 digraph to be Hamiltonian. In Section 3, we state the first major result, where we fully characterize Hamiltonian circulant-2 digraphs. Using this characterization we derive two algorithms for checking the Hamiltonicity and finding the Hamiltonian cycles of a circulant-2 digraph (if there are any), respectively. These algorithms and the analysis of their complexity are presented in Section 4. Then, in Section 5 we state and prove our second major result, describing the periodic structure of the Hamiltonian cycles of a circulant-2 digraph. In Section 6, the overall number of pairwise different Hamiltonian cycles in a circulant-2 digraph is given. Finally, the bottleneck and sum TSP on circulant-2 digraphs are discussed in Section 7. Section 8 completes the paper by presenting open problems, conclusions and remarks.

2. Definitions and preliminaries

**Definition 2.1.** Let $n, a_1, a_2, \ldots, a_m$ be arbitrary integers with $0 < a_1 < \cdots < a_m < n$ and let $V = \{0, 1, \ldots, n-1\}$. A digraph $G = (V, E)$ with vertex set $V$ and arc set $E$ is called a circulant digraph generated by $a_1, a_2, \ldots, a_m$ and denoted by $G(n, a_1, a_2, \ldots, a_m)$ if its arc set $E$ consists only of the arcs $(i, j)$ with $j-i \equiv a_t \pmod{n}$ for any $t \in \{1, 2, \ldots, m\}$. An arc $(i, j)$ of $G$ with $j-i \equiv a_t \pmod{n}$ is called an $a_t$-arc.

The circulant graph $G(6, 2, 3)$ with 6 vertices is depicted in Fig. 2.

Throughout this paper $\gcd(n_1, n_2, \ldots, n_m)$ denotes the greatest common divisor of the integers $n_1, n_2, \ldots, n_m$. Moreover, the notation $a \mid b$ means “$a$ divides $b$” for any two integers $a$ and $b$. We will make use of the following well-known results on circulant digraphs.

**Proposition 2.1.** Let $g = \gcd(n, a_1, a_2, \ldots, a_m)$. Then $G(n, a_1, a_2, \ldots, a_m)$ has exactly $g$ strongly connected components, which are induced by the sets $Z_i$:

$$Z_i = \{ j \in V \mid j = i + \lambda g \pmod{n}, \lambda \in \mathbb{N} \} \text{ for } i = 0, 1, \ldots, g-1.$$ 

The proof of Proposition 2.1 is elementary and can be found in [2]. To give an example, consider $G(12, 3, 6)$. In this case, we have $g = \gcd(12, 3, 6) = 3$ and therefore
Fig. 2. A strongly connected circulant digraph: $G(6, 3, 2)$.

Fig. 3. A circulant digraph with three strongly connected components: $G(12, 3, 6)$.

$G(12, 3, 6)$ has three strongly connected components. They are induced by the sets \{0, 3, 6, 9\}, \{1, 4, 7, 10\} and \{2, 5, 8, 11\}, respectively (see Fig. 3).

The two following properties of circulant digraphs can be derived as straightforward corollaries of Proposition 2.1.

**Corollary 2.2.** A circulant digraph $G(n, a_1, a_2, \ldots, a_m)$ is strongly connected if and only if $g = \gcd(n, a_1, a_2, \ldots, a_m) = 1$.

**Corollary 2.3.** If $G(n, a_1, a_2, \ldots, a_m)$ is Hamiltonian, then $g = \gcd(n, a_1, a_2, \ldots, a_m) = 1$.

Corollary 2.2 can be also derived as corollary from a stronger graph theoretical result of Van Doorn on the connectivity of circulant digraphs (see [4]). Note that Corollary 2.3 gives a necessary condition for the Hamiltonicity of a circulant digraph, but not a sufficient one. The circulant $G(6, 2, 3)$ represented by Fig. 2 is strongly connected but not Hamiltonian and $\gcd(6, 2, 3) = 1$. The following sufficient condition for $G(n, a_1, a_2, \ldots, a_m)$ being Hamiltonian was given by Garfinkel [5].
Proposition 2.4. A circulant digraph $G(n, a_1, a_2, \ldots, a_m)$ is Hamiltonian, if there is an $a_i$ with $\gcd(n, a_i) = 1$.

Under the assumptions in Proposition 2.4, there exists a Hamiltonian cycle which consist only of arcs $(i, j)$ with $j - i \equiv a_i \pmod{n}$. The circulant digraph $G(12, 5)$ with $\gcd(12, 5) = 1$ is Hamiltonian. It contains a Hamiltonian cycle which consists only of arcs $(i, j)$ with $j - i \equiv 5 \pmod{12}$ as shown by Fig. 4.

Definition 2.2. A circulant graph $G(n, a_1, a_2, \ldots, a_m)$ is called symmetric if for all $i \in \{1, 2, \ldots, m\}$, there exists a $j \in \{1, 2, \ldots, m\}$ with $a_i = n - a_j$.

In [2] it has been shown that the condition of Corollary 2.3 is necessary and sufficient for the Hamiltonicity of a symmetric circulant digraph. Therefore, the Hamiltonian symmetric circulant digraphs can be characterized as follows.

Proposition 2.5. A symmetric circulant graph $G(n, a_1, a_2, \ldots, a_m)$ is Hamiltonian if and only if $\gcd(n, a_1, a_2, \ldots, a_m) = 1$.

In Section 3 we derive necessary and sufficient conditions for the Hamiltonicity of nonsymmetric circulant-2 digraphs, i.e. for $G(n, a_1, a_2)$.

3. Necessary and sufficient conditions for $G(n, a_1, a_2)$ being Hamiltonian

In this section, we formulate and prove the first major result of this paper: the characterization of Hamiltonian circulant-2 digraphs. Below, Theorem 3.5 gives a necessary and sufficient condition for the Hamiltonicity of a circulant-2 digraph $G(n, a_1, a_2)$ in terms of $n, a_1, a_2$. This section is organized as follows. At first we formulate and prove
a technical lemma which is also interesting as an independent result. The next two lemmata give necessary and sufficient conditions for \( G(n, a_1, a_2) \) being Hamiltonian, respectively. Then, applying these lemmata, we derive a first characterization of Hamiltonian circulant-2 digraphs, which serves as an intermediate result. At last, we transform this characterization into the final one, formulating and proving Theorem 3.5. This theorem will be used in the next section for polynomially solving the Hamiltonicity problem on circulant-2 graphs.

The following lemma is a key result which will be essentially used for deriving the necessary conditions for \( G(n, a_1, a_2) \) to be Hamiltonian.

**Lemma 3.1.** Let \( \mathcal{C} \) be a Hamiltonian cycle in \( G(n, a_1, a_2) \) with \( k_1 \) \( a_1 \)-arcs and \( k_2 \) \( a_2 \)-arcs. Let \( p, q, l \) be nonnegative integers with \( pl = k_1, ql = k_2, l > 1 \). Then, for every \( t, 1 \leq t \leq l - 1 \), there exists a pair of vertices \((i, j)\) such that the path which joins them along \( \mathcal{C} \) has exactly \( tp \) \( a_1 \)-arcs and \( tq \) \( a_2 \)-arcs.

**Proof.** Let a Hamiltonian digraph \( G(n, a_1, a_2) \) and a Hamiltonian cycle \( \mathcal{C} \) in \( G \) be given. If \( \mathcal{C} \) contains only \( a_1 \)-arcs or only \( a_2 \)-arcs, the lemma is obviously correct. So, let us assume that \( \mathcal{C} \) contains \( a_1 \)-arcs as well as \( a_2 \)-arcs. Let \( p, q \) and \( l \) fulfill the assumptions of Lemma 3.1 and let us fix any \( t \) with \( 1 \leq t \leq l - 1 \).

We define a function \( f: V \to \mathbb{N} \) such that for all \( i \in V \), \( f(i) \) is the number of \( a_1 \)-arcs among the next \( t(p + q) \) arcs following vertex \( i \) along the cycle \( \mathcal{C} \). Obviously, \( |f(i) - f(i + 1)| \leq 1 \). If there is a vertex \( i_0 \) with \( f(i_0) = tp \), then there is a pair \((i_0, j_0)\) of vertices with the required property and we are done. So, let us assume that there is no vertex \( i_0 \) with \( f(i_0) = tp \). The case that some \( f(i) \) are greater than \( tp \) and some are smaller is impossible, since in this case there would exist a pair of neighbors \( i' \) and \( i' + 1 \) with \( |f(i') - f(i'+1)| \geq 2 \). Thus, either \( f(i) < tp \), for all \( i \in V \), or \( f(i) > tp \), for all \( i \in V \). W.l.o.g, let us assume the latter. Then

\[
\sum_{i=0}^{n-1} f(i) > n(tp) = l(p + q)tp. \tag{1}
\]

On the other hand, the cycle \( \mathcal{C} \) contains exactly \( k_1 \) \( a_1 \)-arcs and in the sum \( \sum_{i=0}^{n-1} f(i) \) every \( a_1 \)-arc of the cycle is counted exactly \( t(p + q) \) times. Therefore,

\[
\sum_{i=0}^{n-1} f(i) = k_1 t(p + q). \tag{2}
\]

Eqs. (1) and (2) imply \( k_1 > lp \), which is a contradiction. \( \square \)

Next let us give necessary conditions for the Hamiltonicity of \( G(n, a_1, a_2) \).

**Lemma 3.2.** If \( G(n, a_1, a_2) \) is Hamiltonian then there exist integers \( p, q \geq 0 \) such that

\[
\begin{align*}
(p + q) \mid (a_2 - a_1), \\
p + q &= \gcd(n, pa_1 + qa_2). \tag{3}
\end{align*}
\]
Proof. Let us suppose that the given $G(n, a_1, a_2)$ is Hamiltonian. If $\gcd(n, a_1) = 1$ or $\gcd(n, a_2) = 1$, we set $p = 1$, $q = 0$ or $p = 0$, $q = 1$, respectively. Obviously, in both cases $p$ and $q$ have the required properties. If neither $\gcd(n, a_1)$ nor $\gcd(n, a_2)$ equals 1, we proceed as follows. Consider a Hamiltonian cycle $\mathcal{C}$ in $G(n, a_1, a_2)$ with $k_1 a_1$-arcs and $k_2 a_2$-arcs and set $l := \gcd(k_1, k_2)$. Next, let $p = k_1/l$ and $q = k_2/l$. The following equalities hold:

$$0 = \sum_{(i,j) \in \mathcal{C}} (j - i) = k_1 a_1 + k_2 a_2 \pmod{n}. \quad (4)$$

Since $k_1 a_1 + k_2 a_2 > 0$, equality (4) yields $n \mid k_1 a_1 + k_2 a_2$. Thus,

$$n = k_1 + k_2 = l(p + q) \text{ divides } (k_1 a_1 + k_2 a_2) = l(pa_1 + qa_2).$$

The last equality implies

$$(p + q) \mid (pa_1 + qa_2). \quad (5)$$

Thus, $p + q$ divides $n$ and $pa_1 + qa_2$, which implies that $p + q$ divides $\gcd(n, pa_1 + qa_2)$. Assume $\gcd(n, pa_1 + qa_2) > p + q$. Then, there exist $r > 1$, $l'$ and $z$ such that $n = rl'(p + q)$ and $pa_1 + qa_2 = rz(p + q)$. Obviously, $1 \leq l' \leq l - 1$. By multiplying the last equality by $l'$ we get $l'(pa_1 + qa_2) = nz$, which implies $n \mid l'(pa_1 + qa_2)$ for some $l'$ with $1 \leq l' \leq l - 1$. Hence, $i \equiv i + l'(pa_1 + qa_2) \pmod{n}$ for any $i \in V$. Thus, the Hamiltonian cycle $\mathcal{C}$ does not contain a pair $(i, j)$ such that $l'pa_1$-arcs and $l'q a_2$-arcs lead from $i$ to $j$ along $\mathcal{C}$. Considering that the conditions of Lemma 3.1 are fulfilled, such a pair should exist. This contradiction shows that $\gcd(n, pa_1 + qa_2) = p + q$.

In order to show that the integers $p$ and $q$ defined as above fulfill also the first property stated by the lemma, note that $(pa_1 + qa_2)$ can be written as

$$(pa_1 + qa_2) = (p + q)a_1 + q(a_2 - a_1). \quad (6)$$

Considering equality (5), equality (6) implies $p + q \mid q(a_2 - a_1)$. But $l = \gcd(k_1, k_2)$ implies $\gcd(q, p + q) = 1$, hence $p + q \mid (a_2 - a_1)$. $\square$

Example 1. Does $G(10, 2, 5)$ admit a Hamiltonian cycle?

Notice that $\gcd(10, 2, 5) = 1$ and $\gcd(10, 2) \neq 1$, $\gcd(10, 5) \neq 1$. If a Hamiltonian cycle exists, then there would exist two natural numbers $p$ and $q$ such that $(p + q) \mid (a_2 - a_1)$, namely $(p + q) \mid 3$. Since also $(p + q) \mid 10$, we get $p + q = 1$. Thus, there are only two feasible pairs $(p, q)$: $p = 1$, $q = 0$ and $p = 0$, $q = 1$. Let us set $p = 1$, $q = 0$. We have $\gcd(n, pa_1 + qa_2) = \gcd(10, 2) = 2 \neq p + q$. Thus, this choice of $p$ and $q$ is not allowed. Similarly, the choice $p = 0$, $q = 1$ is not allowed, since $\gcd(10, 5) = 5 \neq 1$. Therefore, $G(10, 2, 5)$ is not Hamiltonian.

The next lemma gives sufficient conditions for $G(n, a_1, a_2)$ to be Hamiltonian.

Lemma 3.3. Let a circulant-2 digraph $G(n, a_1, a_2)$ be given. If $\gcd(n, a_1, a_2) = 1$ and there exist $p, q \geq 0$ which fulfill (3), then $G(n, a_1, a_2)$ is Hamiltonian.
Proof. If \( p + q = 1 \), either \( p = 1, q = 0 \) or \( p = 0, q = 1 \). These two choices imply \( \gcd(n, a_1) = 1 \) or \( \gcd(n, a_2) = 1 \), respectively. In each of these two cases \( G(n, a_1, a_2) \) is Hamiltonian according to Proposition 2.4.

Next, we analyze the case \( p + q > 1 \). We denote \( n' = n/(p + q) \), \( \kappa = pa_1 + qa_2 \) and define \( v(t, r, s) \in V \) by

\[
v(t, r, s) = (\kappa + ra_1 + sa_2) \mod n \quad 0 \leq t \leq n' - 1, \quad 0 \leq r \leq p, \quad 0 \leq s \leq q - 1.
\]

Let us denote by \( \mathcal{A}_t \) and \( \mathcal{B}_t \) the paths given as follows:

\[
\mathcal{A}_t = (v(t, 0, 0), v(t, 1, 0), \ldots, v(t, i, 0), v(t, i + 1, 0), \ldots, v(t, p, 0)),
\]

\[
\mathcal{B}_t = (v(t, p, 0), v(t, p, 1), \ldots, v(t, p, i), v(t, p, i + 1), \ldots, v(t, p, q)).
\]

It is easily seen that the right endpoint of path \( \mathcal{A}_t \) coincides with the left endpoint of \( \mathcal{B}_t \) for \( 0 \leq t \leq n' - 1 \) and the right endpoint of \( \mathcal{B}_t \) coincides with the left endpoint of \( \mathcal{A}_{t+1} \) for all \( 0 \leq t \leq n' - 2 \). Moreover, the right endpoint of \( \mathcal{B}_{n'-1} \) coincides with the left endpoint of \( \mathcal{A}_0 \). Therefore, the paths \( \mathcal{A}_t, \mathcal{B}_t \) can be concatenated as follows:

\[
\mathcal{C} = (\mathcal{A}_0, \mathcal{B}_0, \ldots, \mathcal{A}_t, \mathcal{B}_t, \ldots, \mathcal{A}_{n'-1}, \mathcal{B}_{n'-1})
\]

and the resulting path \( \mathcal{C} \) is a closed one. Each \( \mathcal{A}_t \) contains exactly \( p \) arcs and each \( \mathcal{B}_t \) contains exactly \( q \) arcs. Thus, the closed path \( \mathcal{C} \) contains \( n'(p + q) = n \) arcs. We show that each pair of these arcs have different left endpoints. This implies that \( \mathcal{C} \) is a cycle of length \( n \), thus a Hamiltonian cycle. Let us consider two vertices \( v(t, r, s) \) and \( v(t_1, r_1, s_1) \) of \( \mathcal{C} \) with \( (t, r, s) \neq (t_1, r_1, s_1) \). W.l.o.g., we can suppose \( 0 \leq t \leq t_1 \leq n' - 1, \quad 0 \leq r, r_1 \leq p, \quad 0 \leq s, s_1 \leq q - 1 \). Note that, for any vertex \( v(t, r, s) \) in \( \mathcal{C} \), if \( s > 0 \) then \( r = p \). We show that

\[
(t_1 - t)\kappa + (r_1 - r)a_1 + (s_1 - s)a_2 \neq 0 \mod n
\]

and this implies then \( v(t, r, s) \neq v(t_1, r_1, s_1) \). We prove (7) by distinguishing the following two cases.

**Case 1:** \( r = r_1 \) and \( s = s_1 \)

In this case \( t < t_1 \) and \( \gcd(n, pa_1 + qa_2) = \gcd(n, \kappa) = p + q \) implies \( v(t, r, s) - v(t_1, r_1, s_1) = (t_1 - t)\kappa \neq \lambda n \) for any integer number \( \lambda \).

**Case 2:** \( r \neq r_1 \) or \( s \neq s_1 \)

In this case \( v(t_1, r_1, s_1) - v(t, r, s) \) is of the form \( \tilde{t}\kappa + \tilde{r}a_1 + \tilde{s}a_2 \), where \( 0 < |\tilde{r} + \tilde{s}| < p + q \) and \( 0 \leq \tilde{t} \leq n' - 1 \). We suppose \( n \mid (\tilde{t}\kappa + \tilde{r}a_1 + \tilde{s}a_2) \) and derive a contradiction out of it. Notice that if \( n \) divides \( \tilde{t}\kappa + \tilde{r}a_1 + \tilde{s}a_2 \), then \( p + q \) divides it also. Thus,

\[
(p + q)\mid \tilde{t}\kappa + \tilde{r}a_1 + \tilde{s}a_2 = \tilde{r}a_1 + (\tilde{r} + \tilde{s})a_2 - a_1.
\]

Considering that \( (p + q)\mid \kappa \) and \( (p + q)\mid (a_2 - a_1) \), Eq. (8) implies that \( (p + q)\mid (\tilde{r} + \tilde{s})a_1 \).

On the other side, \( 0 < |\tilde{r} + \tilde{s}| < p + q \), hence there exists the natural numbers \( l, l' \).
\[ l > 1 \text{ such that } p + q = ll' \text{ and} \]
\[ l \mid a_1. \quad \text{(\textasteriskcentered{\textasteriskcentered}{\textasteriskcentered})} \]

On the other hand, \((p + q) \mid (a_2 - a_1)\) implies
\[ l \mid (a_2 - a_1). \quad \text{(**)} \]

Now, combining (\textasteriskcentered{\textasteriskcentered}{\textasteriskcentered}) and (\textasteriskcentered{\textasteriskcentered}{\textasteriskcentered}) we get
\[ l \mid a_2. \quad \text{(***)} \]

Considering (\textasteriskcentered{\textasteriskcentered}{\textasteriskcentered}), (\textasteriskcentered{\textasteriskcentered}{\textasteriskcentered}{\textasteriskcentered}) and taking into account that \((p + q) \mid n\) implies \(l \mid n\) one would get \(\gcd(n, a_1, a_2) \geq l > 1\), which contradicts the condition \(\gcd(n, a_1, a_2) = 1\). Thus, we have shown that, also in this case, \(v(t, r, s) - v(t', r, s) \neq 0 \pmod{n}\) and this completes the proof. \(\Box\)

Making use of the Lemmas 3.2 and 3.3 we obtain \textit{necessary and sufficient} conditions for the Hamiltonicity of \(G(n, a_1, a_2)\).

\textbf{Theorem 3.4.} The circulant-2 digraph \(G(n, a_1, a_2)\) is Hamiltonian if and only if \(\gcd(n, a_1, a_2) = 1\) and there exists a pair \(p, q\) of nonnegative numbers such that \(p + q = \gcd(n, a_2 - a_1)\) and \(p + q = \gcd(n, pa_1 + qa_2)\).

\textbf{Proof.} Let a circulant-2 digraph \(G(n, a_1, a_2)\) be given. We suppose that \(\gcd(n, a_1, a_2) = 1\) and that there exist \(p, q \geq 0\) which fulfill the conditions of the theorem. In this case Lemma 3.3 can be applied in order to state that \(G(n, a_1, a_2)\) is Hamiltonian.

Now, let us suppose that the given digraph is Hamiltonian. Corollary 2.3 guarantees that \(\gcd(n, a_1, a_2) = 1\). Lemma 3.2 states the existence of \(p_1, q_1 \geq 0\) which fulfill (3). Let us denote \(u = \gcd(n, a_2 - a_1)\). Then, obviously \((p_1 + q_1)\) divides \(u\). Let us denote \(l = u/(p_1 + q_1)\), \(l' = n/u\), \(p = lp_1\) and \(q = lq_1\). Obviously, \(p + q = u = \gcd(n, a_2 - a_1)\).

On the other side, the following equalities hold:

\[ \gcd(n, pa_1 + qa_2) = \gcd(l'(p_1 + q_1), l(p_1a_1 + q_1a_2)) \]
\[ = l \gcd(l'(p_1 + q_1), p_1a_1 + q_1a_2). \quad (9) \]

Obviously, \(\gcd(l'(p_1 + q_1), p_1a_1 + q_1a_2) | \gcd(n, p_1a_1 + q_1a_2) = p_1 + q_1\). On the other side, \(p_1 + q_1\) divides both \(l'(p_1 + q_1)\) and \(p_1a_1 + q_1a_2\). The two last statements imply \(p_1 + q_1 = \gcd(l'(p_1 + q_1), p_1a_1 + q_1a_2)\). Therefore, equality (9) implies \(\gcd(n, pa_1 + qa_2) = l(p_1 + q_1) = p + q\). Thus, \((p, q)\) is the required pair of numbers. \(\Box\)

Next, let us reformulate the necessary and sufficient conditions given by Theorem 3.4 in order to get our final characterization for the Hamiltonicity of a circulant-2 digraph.
Theorem 3.5. Let a circulant-2 digraph $G(n,a_1,a_2)$ be given and let $t = \gcd(n, a_2 - a_1)$, $n' = n/t$, $a' = (a_2 - a_1)/t$. The digraph $G(n,a_1,a_2)$ is Hamiltonian if and only if $\gcd(n,a_1,a_2) = 1$ and there exists a number $0 \leq h \leq t$ such that

$$\gcd(n',a_1 + a'h) = 1.$$  \hfill (10)

Proof. We show that the existence of a pair of nonnegative integers $(p,q)$ which fulfill the equalities

$$p + q = \gcd(n,a_2 - a_1),$$
$$p + q = \gcd(n, pa_1 + qa_2)$$ \hfill (11)

is equivalent to the existence of a number $0 \leq h \leq t$ which fulfills (10). If such a pair $(p,q)$ exists, we have $p + q = t$ and

$$pa_1 + qa_2 = (t - q)a_1 + qa_2 = ta_1 + qta'.$$ \hfill (12)

Hence, $\gcd(n, pa_1 + qa_2) = p + q$ can be rewritten as $\gcd(n't, t(a_1 + a'q)) = t$, which is equivalent to (10). So, setting $h := q$ yields the required number.

On the other hand, if a number $0 \leq h \leq t$ fulfilling (10) exists, we set $q := h$ and $p := t - q$. Considering equalities (12), it is easily seen that the pair $(p,q)$ fulfills (11). \quad \square

Throughout the remaining sections of this paper we will use the notations $t,n',a'$ as defined in Theorem 3.5.

4. Checking the Hamiltonicity of $G(n,a_1,a_2)$

In this section, we describe the algorithms ‘Check’ and ‘Find’ for checking the Hamiltonicity of a given $G(n,a_1,a_2)$ and for finding a Hamiltonian cycle in it, respectively. ‘Check’ is based on Theorem 3.5 as a characterization of Hamiltonian circulant-2 digraphs. This algorithm answers the question for the existence of a number $0 \leq h \leq t$ such that Eq. (10) holds, where $t = \gcd(n,a_1 - a_1)$. In order to outline the algorithm we need two more notations:

Definition 4.1. Let a circulant-2 digraph $G(n,a_1,a_2)$ be given. Let $t = \gcd(n,a_2 - a_1)$ and $t^* = c^* \log^3(n/t)$, where $c^*$ is a certain constant specified below and where $\log n$ denotes the base two logarithm of $n$. Then, $S(G)$ and $S'(G)$ are defined as follows:

$$S(G) := \{0 \leq h \leq t | \gcd(n',a_1 + ha') = 1\},$$
$$S'(G) := \{0 \leq h \leq \min(t,t^*) | \gcd(n',a_1 + ha') = 1\},$$

where $n'$ and $a'$ are defined as in Theorem 3.5.

The algorithm ‘Check’ decides whether the set $S(G)$ is empty or not. Actually, ‘Check’ computes the subset $S'(G) \subseteq S(G)$, but $S'(G)$ is empty if and only if $S(G)$ is empty,
as it will be shown in Theorem 4.3. Computing \( S'(G) \) instead of \( S(G) \) makes sense as \( |S(G)| = O(n) \), whereas \( |S'(G)| = O(\log n) \). For showing that \( S'(G) = \emptyset \) if and only if \( S(G) = \emptyset \), we make use of the following result due to Iwaniec [7].

**Proposition 4.1.** There exists a constant \( c^* > 0 \), such that for any set \( P \) of \( k \) pairwise distinct primes, any sequence consisting of \( c^*k^2 \log^2 k \) consecutive integers contains at least one element that is not divisible by any prime in \( P \).

**Corollary 4.2.** There exists a constant \( c^* > 0 \), such that the following holds. For any set \( P \) of \( k \) pairwise distinct primes and for any integers \( a \) and \( b \) for which \( \gcd(a,b) \) is relatively prime to the elements in \( P \), the set

\[
\{a + jb | 1 \leq j \leq c^*k^2 \log^2 k \}
\]

contains at least one element that is not divisible by any prime in \( P \).

**Proof.** For \( 1 \leq j \leq c^*k^2 \log^2 k \), set \( x_j = a + jb \). Let \( P = \{p_1, \ldots, p_k\} \). Without loss of generality, one may assume that \( b \) is not divisible by any \( p_i \) (otherwise, none of the numbers \( x_j \) is divisible by \( p_i \), and \( p_i \) may as well be removed from \( P \)).

For \( p_i \in P \), let \( k(i) < p_i \) denote the smallest index \( j \) for which \( x_j \) is divisible by \( p_i \). Clearly, exactly the numbers \( x_j \) with index \( j = k(i) + \ell p_i \) are divisible by \( p_i \). By the Chinese remainder theorem, we can find a positive integer \( N \) such that

\[
N \equiv p_i - k(i) \mod p_i \quad \text{for all } p_i \in P
\]

holds. Then by construction, \( N + j \) is divisible by \( p_i \) if and only if \( x_j \) is divisible by \( p_i \). Hence, the sequence \( \langle N + 1, N + 2, \ldots, N + c^*k^2 \log^2 k \rangle \) has the same divisibility properties with respect to \( P \) as the numbers \( x_j \) and Proposition 4.1 applies. 

**Theorem 4.3.** Consider a circulant-2 digraph \( G(n, a_1, a_2) \). The set \( S(G) \) is empty if and only if the set \( S'(G) \) is empty.

**Proof.** Denote \( u = \min(t, t^*) \), where \( t^* \) is as in Definition 4.1. In the case that \( u = t \) then \( S(G) = S'(G) \) and we are done. In the case that \( u = t^* < t \) we show that \( S'(G) \neq \emptyset \). Indeed, \( S'(G) = \emptyset \) implies that none of the numbers

\[
a_1, a_1 + a', a_1 + 2a', \ldots, a_1 + t^*a'
\]

is relatively prime to \( n' \). But, now Corollary 4.2 yields that \( n' \) has more than \( \log n' \) pairwise distinct prime divisors. Since every prime divisor is at least two, \( n' > 2\log n' \) must hold; a contradiction. Thus, \( S' \neq \emptyset \). The last statement implies \( S(G) \neq \emptyset \) and this completes the proof. 

**Algorithm 4.4 (Check).** Checking whether a given \( G(n, a_1, a_2) \) is Hamiltonian or not.

**Input:** Three numbers \( n, a_1, a_2 \) with \( a_1 < a_2 < n \) in binary representation.
Output: \( S'(G) \) for \( G := G(n, a_1, a_2) \) and a boolean variable \( HC \) which equals one if \( G(n, a_1, a_2) \) is Hamiltonian and 0 otherwise.

Initialize

Set \( S'(G) = \emptyset \), \( h = 0 \).

GCD Check

If \( \gcd(n, a_1, a_2) \neq 1 \) then go to Stop.

GCD Calculate

Calculate \( t := \gcd(n, a_2 - a_1) \), \( t^* = c^* \log^3(n/t) \) and \( u = \min(t, t^*) \).

Repeat

Set \( n' := n/t \), \( a' := (a_2 - a_1)/t \). Repeat Loop until \( h > u \):

Loop

If \( \gcd(n', a_1 + a'h) = 1 \) then \( S'(G) := S'(G) \cup \{h\} \). Set \( h := h + 1 \).

Stop

If \( S'(G) = \emptyset \) then \( HC = 0 \) otherwise \( HC = 1 \). Output \( HC \) and \( S'(G) \).

The next theorem states the correctness of Algorithm ‘Check’ and analyzes its complexity.

**Theorem 4.5.** For three numbers \( n \), \( a_1 \) and \( a_2 \) in binary representation, algorithm ‘Check’ decides whether the circulant-2 digraph \( G(n, a_1, a_2) \) is Hamiltonian. This decision takes \( O(\log^4 n) \) arithmetical operations in the unit cost model.

**Proof.** According to Theorem 3.5, if \( \gcd(n, a_1, a_2) = 1 \) holds, then \( G(n, a_1, a_2) \) is Hamiltonian iff the corresponding set \( S(G) \) is not empty. On the other side, Theorem 4.3 shows that \( S(G) = \emptyset \) if and only if \( S'(G) = \emptyset \). After having computed \( \gcd(n, a_1, a_2) \), ‘Check’ computes \( S'(G) \) and decides whether it is empty or not, i.e. it decides whether \( G(n, a_1, a_2) \) is Hamiltonian. This completes the correctness argument for algorithm ‘Check’. To see the claimed complexity, observe that ‘Check’ essentially consists of \( u = O(\log^3 n) \) greatest common divisor computations. A common divisor computation takes \( O(\log n) \) arithmetical operations in the unit cost model (applying for example the Euclidean algorithm). \( \square \)

**Remark.** The constant \( c^* \) in Definition 4.1 is huge (see [7]). Moreover, notice that the algorithm ‘Check’ would work and Theorem 4.5 would hold all the same, when using some \( l^* \geq c^* \) instead of \( c^* \). Under these conditions, for values of \( n \) of practical interest, we can assume that \( t \leq t^* \), and hence \( S(G) = S(G') \). Concluding, the existence of the constant \( c^* \) is essential for the correctness of our complexity result, but its value is irrelevant for practical applications of the algorithm ‘Check’.

The next algorithm ‘Find’ explicitly computes a Hamiltonian cycle in a given \( G(n, a_1, a_2) \). We assume that we have already applied ‘Check’ and may use its output. We select a number \( h \in S'(G) \) and find a Hamiltonian cycle \( \mathcal{C} \) consisting of \( n'(t - h) \) \( a_1 \)-arcs and \( n'h \) \( a_2 \)-arcs.

**Algorithm 4.6 (Find).** Finding a Hamiltonian cycle in \( G(n, a_1, a_2) \) consisting of \( n' \) \( (t - h) \) \( a_1 \)-arcs and \( n'h \) \( a_2 \)-arcs, for a given \( h \in S'(G) \)

**Input:** Four numbers \( n, a_1, a_2, h \) with \( a_1 < a_2 < n \) and \( h \in S'(G) \).

**Output:** A Hamiltonian cycle \( \mathcal{C} \) in \( G(n, a_1, a_2) \) with \( n'h \) \( a_2 \)-arcs.

**Initialize**

Set \( j = 0 \), \( t = \gcd(n, a_2 - a_1) \), \( l = n' \), \( v[i] = 0 \), for \( 0 \leq i \leq n - 1 \).

**While** \( l > 0 \):

...
Repeat for $a_1$  
Set $j = 0$. Repeat Loop for $a_1$ until $j = t - h - 1$

Loop for $a_1$  
Set $v[j+1] := v[j] + a_1 \pmod{n}$, $j := j + 1$

Repeat for $a_2$  
Set $j = 0$. Repeat Loop for $a_2$ until $j = h - 1$

Loop for $a_2$  

End-while  
Set $l := l - 1$.

Stop  
Set $\mathcal{C} = (v[0], v[1], \ldots, v[i], v[i+1], \ldots, v[n-1], v[0])$. Output $\mathcal{C}$.

The correctness of algorithm ‘Find’ follows immediately from Lemma 3.3. Obviously, ‘Find’ runs in $O(n)$ time. Summarizing, finding a Hamiltonian cycle in a Hamiltonian circulant-2 digraph takes $O(n)$ arithmetical operations in the unit cost model.

We conclude this section with an example illustrating the algorithms ‘Check’ and ‘Find’.

Example 2. Check whether the circulant-2 digraph $G(30, 3, 8)$ is Hamiltonian and find a Hamiltonian cycle in it if there exist any.

Let us first apply algorithm ‘Check’ to the given digraph $G(30, 3, 8)$. After having applied steps ‘GCD Check’ and ‘GCD Calculate’ and according to the remark following Theorem 4.5, we have: $S'(G) = \emptyset$, $\gcd(n, a_1, a_2) = \gcd(30, 3, 8) = 1$, $t = \gcd(n, a_2 - a_1) = \gcd(30, 5) = 5$ and $u = t = 5$. Further, $n' = n/t = 6$ and $t' = (a_2 - a_1)/t = 1$.

For $h \in \{0, 1, 2, 3, 4, 5\}$, compute $\gcd(n', a_1 + a'h) = \gcd(6, 3 + h)$. If $\gcd(6, 3 + h) = 1$, add $h$ to $S'(G)$. Since $\gcd(6, 3 + 2) = 1$, $\gcd(6, 3 + 4) = 1$ and $\gcd(6, 3 + h) \neq 1$ for $h \in \{0, 1, 3, 5\}$, we have $S'(G) = S(G) = \{2, 4\}$ (consider again the remark following Theorem 4.5). Thus, $S'(G) \neq \emptyset$ and hence $G(30, 3, 8)$ is Hamiltonian.

Next, we select a $h \in S'(G)$ and apply algorithm ‘Find’ to derive a Hamiltonian cycle $\mathcal{C}$ in $G(30, 3, 8)$ with $n'(t - h) = 6(5 - h)$ $a_1$-arcs and $n'h = 6h$ $a_2$-arcs. For $h := 2 \in S'(G)$ the cycle $\mathcal{C}$ will have 18 $a_1$-arcs and 12 $a_2$-arcs. After the initializing step we have $l = n' = 6$ and $v[i] = 0$, $0 \leq i \leq 29$. The execution of step ‘Repeat for $a_1$’ yields:


Similarly, the execution of step ‘Repeat for $a_2$’ yields


Then, $l$ is decreased by 1, that is $l = 5$. We get the required Hamiltonian cycle by repeating steps ‘Repeat for $a_1$’ and ‘Repeat for $a_2$’ five other times consecutively (until $l = 0$):

$$\mathcal{C} = (0, 3, 6, 9, 17, 25, 28, 1, 4, 12, 20, 23, 26, 29, 7, 15, 18, 21, 24, 2, 10, 13, 16, 19, 27, 5, 8, 11, 14, 22, 0).$$
5. The Hamiltonian cycles of a circulant-2 digraph are periodic

In this section, we formulate and prove the second major result of our paper: the periodicity of the Hamiltonian cycles in a circulant-2 digraph, if there are any. Notice, moreover, that all circulant-2 digraphs $G(n, a_1, a_2)$ considered in this section are assumed to be Hamiltonian.

First of all, let us explain the notion of a periodic Hamiltonian cycle. It is related to the pattern of a path in a circulant-2 digraph. Consider a path in a circulant-2 digraph. Each of its arcs is either an $a_1$-arc or an $a_2$-arc.

**Definition 5.1.** The pattern of the path $P = (v_1, v_2, \ldots, v_k)$ in $G(n, a_1, a_2)$ is the sequence of numbers $(a^1, a^2, \ldots, a^{k-1})$ where $a^i = a_1$ if $(v_i, v_{i+1})$ is an $a_1$-arc and $a^i = a_2$ otherwise.

**Definition 5.2.** A Hamiltonian cycle in a circulant-2 digraph is called periodic if and only if it is the concatenation of $\ell \geq 2$ paths having the same pattern. The maximum possible number $\ell$ of such paths is called the period of the Hamiltonian cycle. The pattern of the path $(v_0 = 0, v_1, \ldots, v_{n/\ell})$ is called the pattern of the Hamiltonian cycle, whereas the length of this path is called the length of the pattern of the Hamiltonian cycle.

Notice that the Hamiltonian cycle produced by algorithm ‘Find’ is periodic with period $n'$, by construction. The length of the pattern of such a cycle equals $t$, where $n'$ and $t$ are as defined in the previous section.

**Example 3.** The periodicity and the pattern of a Hamiltonian cycle in $G(6, 2, 5)$.

Consider the digraph $G(6, 2, 5)$ and the path $(0, 2, 4, 3)$ in it. The corresponding pattern is $(2, 2, 5)$. Now consider the Hamiltonian cycle $(0, 2, 4, 3, 5, 1, 0)$. This cycle is a concatenation of the paths $(0, 2, 4, 3)$ and $(3, 5, 1, 0)$ which have the same pattern: $(2, 2, 5)$. Thus, this Hamiltonian cycle is periodic. Moreover, it is easily seen that this cycle cannot be derived as a concatenation of more than 2 paths having the same pattern. Hence, the period of this cycle is 2 and its pattern is $(2, 2, 5)$.

Next, we give a rather technical lemma which provides an auxiliary result.

**Lemma 5.1.** Let a triple $(n, a_1, a_2)$ of natural numbers be given, with $a_1 < a_2 < n$. If the pair of natural numbers $(t, h)$ fulfills $\gcd(n', a_1 + a'h) = 1$, where $t$, $h$, $n'$ and $a'$ are defined as in Theorem 3.5, then there exists a number $k_0 \in \{1, 2, \ldots, n' - 1\}$ such that $k_0(a_1 + a'h) + a' \equiv 0 \pmod{n}$ and $\gcd(n', k_0) = 1$.

**Proof.** From the assumptions of the lemma we have $\gcd(n', a_1 + a'h) = 1$. Therefore, any pair of integers in the set $\{k(a_1 + a'h) + a' | k = 0, 1, \ldots, n' - 1\}$ are different modulo $n'$. Obviously, $n'$ is not a divisor of $a'$, otherwise $n = n't$ would divide $a't = \ldots$
Thus, if \( k = 0 \), \( k(a_1 + a'h) + a' \not\equiv 0 \pmod{n'} \). So, there exists a \( k_0 \in \{1,2,\ldots,n'-1\} \) such that
\[
k_0(a_1 + a'h) + a' \equiv 0 \pmod{n'}.
\]
(13)

Moreover, we have \( \gcd(n',k_0) = 1 \). Indeed, if \( \gcd(n',k_0) > 1 \), Eq. (13) would imply \( \gcd(n',a') > 1 \) which contradicts the definition of \( t, a' \) and \( n' \).

The following theorem fully describes the structure of Hamiltonian cycles of a circulant-2 digraph. In particular, it is shown that all Hamiltonian cycles of a circulant-2 digraph \( G(n,a_1,a_2) \) are periodic and have the same period, namely \( n' \), where \( n' \) is defined as in the previous section.

**Theorem 5.2.** Let a Hamiltonian circulant-2 digraph \( G(n,a_1,a_2) \) be given. Each Hamiltonian cycle of \( G(n,a_1,a_2) \) is periodic with period \( n' \) and its pattern consists of \( (t - h) a_1 \)-arcs and \( h a_2 \)-arcs, for some \( h \) with \( \gcd(n',a_1 + a'h) = 1 \) and \( t, n', a' \) defined as in Theorem 3.5.

**Proof.** Let us consider a Hamiltonian cycle \( \mathcal{H} \) in \( G(n,a_1,a_2) \) with \( k_1 a_1 \)-arcs and \( k_2 a_2 \)-arcs. As in the proof of Theorem 3.4, there exist natural numbers \( p \) and \( q \) such that \( \gcd(n,a_2 - a_1) = p + q \) and \( \gcd(n, pa_1 + qa_2) = p + q \). Now, from the way how these numbers are derived follows that \( k_1 = n'(t - h) \) and \( k_2 = n'h \), where \( t = p + q \) and \( h = q \) and \( n' \) is as defined in Theorem 3.5. Moreover, as in the proof of Theorem 3.5 we have \( t = \gcd(n,a_2 - a_1) \) and \( \gcd(n',a_1 + a'h) = 1 \), where \( a' = (a_2 - a_1)/t \). From now on, we work with the pair \( (t,h) \) throughout the proof.

According to Lemma 5.1, there exists a \( k_0 \in \{1,2,\ldots,n'-1\} \) such that Eq. (13) holds and \( \gcd(k_0,n') = 1 \). We construct two functions defined on the vertex set \( V \) of \( G(n,a_1,a_2) \) as follows. For all \( i \in V \) consider the path \( \mathcal{P}(i) \) along \( \mathcal{H} \) which starts at \( i \) and contains \( k_0t \) arcs. The value of \( f_1(i) \) is the number of \( a_2 \)-arcs in \( \mathcal{P}(i) \) and \( f_2(i) = f_1(i) - k_0h \). We distinguish two cases.

Case 1: For all \( i \in V \), \( f_2(i) = 0 \).

We show that in this case \( \mathcal{H} \) is periodic and consists of a concatenation of \( n' \) paths with a common pattern of \( h a_2 \)-arcs and \( t - h a_1 \)-arcs. To do so let us construct another function \( f'_1 \). For \( i \in V \), consider the path \( \mathcal{P}'(i) \) along \( \mathcal{H} \) which starts at \( i \) and contains \( t \) arcs. \( f'_1(i) \) is the number of \( a_2 \)-arcs in \( \mathcal{P}'(i) \). We begin with \( \mathcal{P}'(0) \) and denote it by \( \mathcal{P}'_0 \). Then, continue with the path of length \( t \) following \( \mathcal{P}'_0 \) along \( \mathcal{H} \), denote it by \( \mathcal{P}'_1 \) and so on, up to the path \( \mathcal{P}'_{n'-1} \) whose right endpoint is the vertex 0. Now, we construct an auxiliary digraph \( \mathcal{G}' \) with vertex set \( V' = \{0,1,\ldots,n'-1\} \) and arc set
\[
E' = \{(j,k) \mid k - j \equiv 0 \pmod{k_0}\}.
\]

Obviously, this is the circulant-1 digraph \( G(n',k_0) \). As \( \gcd(n',k_0) = 1 \), \( G(n',k_0) \) is Hamiltonian due to Proposition 2.4. Every vertex \( i \) of \( V' \) can be identified with the path \( \mathcal{P}'_i \). Let us denote by \( v_i \) the left endpoint of path \( \mathcal{P}'_i \) for \( i = 0,1,\ldots,n'-1 \). It is easily seen that \( f_2(i) = 0, \forall i \in V \) implies
• $f'_1(v_j) = f'_1(v_k)$ for all pairs $(v_j, v_k)$ such that $(j, k) \in E'$.
• If $(j, k) \in E'$, the paths $P'_2$, $P'_k$ have the same pattern of $a_1$-arcs and $a_2$-arcs.

The Hamiltonicity of $G'$ implies now that $f'_1(v_i)$ is constant, say equal to $R$ for $i = 0, 1, \ldots, n' - 1$. Since

$P(0) = (P'_0, P'_1, \ldots, P'_{k_0-1})$,

we obtain $f_1(0) = \sum_{i=0}^{k_0-1} f'_1(v_i)) = k_0 R = k_0 h$, which implies $h = R$. Thus, we have shown that all the paths $P'_i$, $i = 0, 1, \ldots, n' - 1$, have a common pattern consisting of $t - h$ $a_1$-arcs and $h$ $a_2$-arcs. This completes the proof in Case 1.

Case 2: There exists a point $i \in V$ such that $f'_2(i) < 0$. Let us suppose $f'_2(i) > 0$. (The proof for the case $f'_2(i) < 0$ is analogous.) We will derive a contradiction and consequently conclude that this case can never happen. Let us suppose that

$\mathcal{H} = (i_0, i_1, \ldots, i_{n-1}, i_0)$.

We will assume that $i_n = i_0$, throughout the rest of the proof. It is easily seen that the function $f'_2$ has the following properties:

\begin{align}
|f'_2(i_{r+1}) - f'_2(i_r)| & \leq 1 & \forall r & \in \{0, 1, \ldots, n - 1\}, \\
\sum_{r=0}^{n-1} f'_2(i_r) &= 0. & \quad (15)
\end{align}

From (15) and $f'_2(i) > 0$ it follows that there exists a $j \in V$ such that $f'_2(j) < 0$. Then, due to (14), there exists a vertex $i_r$ between $i$ and $j$ in $\mathcal{H}$ such that

$f'_2(i_r) = 0 \quad \text{and} \quad f'_2(i_{r+1}) < 0. \quad (16)$

Let $s := i + k_0 t \pmod{n}$ and $s' := i + 1 + k_0 t \pmod{n}$. We make the following notations:

$i = i_r, \quad j = i_s, \quad i' = i_{r+1}, \quad j' = i_{s'}$.

Inequalities (16) show that there exist exactly $k_0(t - h)$ $a_1$-arcs and $k_0 h$ $a_2$-arcs in path $P(i)$, but there exist less than $k_0 h$ $a_2$-arcs in $P(i')$. This can happen if and only if $(i, i')$ is an $a_2$-arc and $(j, j')$ is an $a_1$-arc. Thus, due to Lemma 5.1, we have

\begin{align}
\quad j' - i' = k_0[(h - t)a_1 + ha_2] + (a_2 - a_1) &= h[k_0(a_1 + ha') + a'] \equiv 0 \pmod{n}.
\quad (17)
\end{align}

Meanwhile, there are $k_0 t \leq (n' - 1)t \leq n - 1$ arcs between $i'$ and $j'$. Since $\mathcal{H}$ is a Hamiltonian cycle, these last inequalities and Eq. (17) are contradictory. \square

6. How many Hamiltonian cycles has $G(n, a_1, a_2)$?

First, notice that all circulant-2 digraphs $G(n, a_1, a_2)$ considered in this section are assumed to be Hamiltonian. Theorem 5.2 shows that any Hamiltonian cycle in a
circulant-2 digraph $G(n, a_1, a_2)$ is periodic with period $n' = n/t$ and its pattern consists of $t - h$ $a_1$-arcs and $h$ $a_2$-arcs, where $t = \gcd(n, a_2 - a_1)$, $a' = (a_2 - a_1)/t$ and $0 \leq h \leq t$ such that $\gcd(n', a_1 + ha') = 1$. For the circulant-2 digraph $G(n, a_1, a_2)$, the values of $t$, $n'$ and $a'$ are unique, whereas $h$ may take different values. Thus, the patterns corresponding to two different Hamiltonian cycles of $G(n, a_1, a_2)$ have the same length but different structure. This difference in the structure of the patterns may either concern the number of $a_1$-arcs and $a_2$-arcs, or the distribution of the $a_1$ and $a_2$ elements in the pattern. In the first case the values of $h$ corresponding to these cycles are different. In the second case the same value of $h$ corresponds to each of the cycles but the corresponding patterns are different. In this section we first count the Hamiltonian cycles having the same number of $a_1$-arcs and $a_2$-arcs in their patterns and then give the overall number of the Hamiltonian cycles in $G(n, a_1, a_2)$. These results are stated in the following two theorems.

**Theorem 6.1.** Consider the circulant-2 digraph $G(n, a_1, a_2)$. Let $t$, $n'$, $a'$ be defined as in Theorem 3.5 and let $h$ be an integer, $0 \leq h \leq t$, which fulfills $\gcd(n', a_1 + ha') = 1$. Then, the number of pairwise different Hamiltonian cycles whose patterns contain exactly $h$ $a_2$-arcs is $\binom{t}{h}$.

**Proof.** First notice that for any sequence of length $t$ consisting of $t - h$ $a_1$'s and $h$ $a_2$'s, there exist a Hamiltonian cycle whose corresponding pattern is the given sequence. Indeed, the numbers $t - h$ and $h$ fulfill the conditions of Lemma 3.3. Thus, a Hamiltonian cycle with period $n'$ and pattern

$$\underbrace{a_1, a_1, \ldots, a_1}_{t-h}, \underbrace{a_2, a_2, \ldots, a_2}_{h}$$

can be constructed as in the proof of this lemma. Now, the key observation is that this construction works for any pattern consisting of $t - h$ $a_1$-arcs and $h$ $a_2$-arcs. Moreover, it is obvious that by applying the above construction with different patterns different Hamiltonian cycles are produced. Thus, there exist $\binom{t}{h}$ pairwise different Hamiltonian cycles fulfilling the conditions of the theorem, corresponding to $\binom{t}{h}$ patterns with $t - h$ $a_1$-arcs and $h$ $a_2$-arcs each. Finally, it is obvious that there are no other Hamiltonian cycles whose corresponding patterns contain $h$ $a_2$-arcs.

The next theorem gives the overall number of the pairwise different Hamiltonian cycles in a circulant-2 digraph $G(n, a_1, a_2)$.

**Theorem 6.2.** The overall number of pairwise different Hamiltonian cycles in a circulant-2 digraph $G(n, a_1, a_2)$, is given by $\sum_{h \in S(G)} \binom{t}{h}$, where

$$S(G) = \{0 \leq h \leq t \mid \gcd(n', a_1 + ha') = 1\}$$

and $n'$, $a'$ and $t$ are defined as in Theorem 3.5.
Proof. Theorem 5.2 states that every Hamiltonian cycle of $G(n, a_1, a_2)$ is periodic with period $n'$ and a pattern consisting of $t - h$ $a_1$-arcs and $h$ $a_2$-arcs for some $h \in S(G)$. Moreover, Theorem 6.1 states that for each $h \in S(G)$ there exist $\binom{n'}{h}$ pairwise different Hamiltonian cycles with corresponding patterns consisting of $t - h$ $a_1$-arcs and $h$ $a_2$-arcs. These two results imply that the overall number of pairwise different Hamiltonian cycles is $\sum_{h \in S(G)} \binom{n'}{h}$.

Next, we give an example of finding all Hamiltonian cycles in a given circulant-2 digraph.

Example 4. Find all Hamiltonian cycles in $G(30, 3, 8)$.

We have shown in Example 2 that the circulant digraph $G(30, 3, 8)$ is Hamiltonian with $S'(G) = S(G) = \{2, 4\}$ and $t = \gcd(n, a_2 - a_1) = \gcd(30, 5) = 5$. Then, according to Theorem 6.2 we have two groups of Hamiltonian cycles in $G(30, 3, 8)$, each group containing cycles with the same number of $a_1$-arcs and $a_2$-arcs.

(a) $h = 2$. According to Theorem 6.1 there are $\binom{5}{2} = 10$ different Hamiltonian cycles whose patterns consist of 2 8-arcs and 3 3-arcs, namely

1. (0, 3, 6, 9, 17, 25, 28, 1, 4, 12, 20, 23, 26, 29, 7, 15, 18, 21, 24, 2, 10, 13, 16, 19, 27, 5, 8, 11, 14, 22); pattern (3, 3, 8, 8).
2. (0, 3, 6, 14, 17, 25, 28, 1, 9, 12, 20, 23, 26, 4, 7, 15, 18, 21, 29, 2, 10, 13, 16, 24, 27, 5, 8, 11, 19, 22); pattern (3, 3, 8, 3, 8).
3. (0, 3, 6, 14, 22, 25, 28, 1, 9, 17, 20, 23, 26, 4, 12, 15, 18, 21, 29, 7, 10, 13, 16, 24, 2, 5, 8, 11, 19, 27); pattern (3, 3, 8, 8, 3).
4. (0, 3, 11, 14, 22, 25, 28, 6, 9, 17, 20, 23, 1, 4, 12, 15, 18, 26, 29, 7, 10, 13, 21, 24, 2, 5, 8, 16, 19, 27); pattern (3, 8, 3, 8, 3).
5. (0, 3, 11, 14, 17, 25, 28, 6, 9, 12, 20, 23, 1, 4, 7, 15, 18, 26, 29, 2, 10, 13, 21, 24, 27, 5, 8, 16, 19, 22); pattern (3, 8, 3, 3, 8).
6. (0, 3, 11, 19, 22, 25, 28, 6, 14, 17, 20, 23, 1, 9, 12, 15, 18, 26, 4, 7, 10, 13, 21, 29, 2, 5, 8, 16, 24, 27); pattern (3, 8, 8, 3, 3).
7. (0, 8, 11, 14, 17, 25, 3, 6, 9, 12, 20, 28, 1, 4, 7, 15, 23, 26, 29, 2, 10, 18, 21, 24, 27, 5, 13, 16, 19, 22); pattern (8, 3, 3, 3, 8).
8. (0, 8, 11, 14, 22, 25, 3, 6, 9, 17, 20, 28, 1, 4, 12, 15, 23, 26, 29, 7, 10, 18, 21, 24, 2, 5, 13, 16, 19, 27); pattern (8, 3, 3, 8, 3).
9. (0, 8, 11, 19, 22, 25, 3, 6, 14, 17, 20, 28, 1, 9, 12, 15, 23, 26, 4, 7, 10, 18, 21, 29, 2, 5, 13, 16, 24, 27); pattern (8, 3, 8, 3, 3).
10. (0, 8, 16, 19, 22, 25, 3, 11, 14, 17, 20, 28, 6, 9, 12, 15, 23, 1, 4, 7, 10, 18, 26, 29, 2, 5, 13, 21, 24, 27); pattern (8, 3, 8, 3, 3).

(b) $h = 4$. According to Theorem 6.1 there are $\binom{5}{4} = 5$ different Hamiltonian cycles whose patterns consist of 4 8-arcs and 1 3-arcs, namely

1. (0, 3, 11, 19, 27, 5, 8, 16, 24, 2, 10, 13, 21, 29, 7, 15, 18, 26, 4, 12, 20, 23, 1, 9, 17, 25, 28, 6, 14, 22); pattern (3, 8, 8, 8, 8).
2. (0, 8, 11, 19, 27, 5, 13, 16, 24, 2, 10, 18, 21, 29, 7, 15, 23, 26, 4, 12, 20,
    28, 1, 9, 17, 25, 3, 6, 14, 22); pattern (8,3,8,8).
3. (0, 8, 16, 19, 27, 5, 13, 21, 24, 2, 10, 18, 26, 29, 7, 15, 23, 1, 4, 12, 20, 28,
    6, 9, 17, 25, 3, 11, 14, 22); pattern (8,8,3,8).
4. (0, 8, 16, 24, 27, 5, 13, 21, 29, 2, 10, 18, 26, 4, 7, 15, 23, 1, 9, 12, 20, 28,
    6, 14, 17, 25, 3, 11, 19, 22); pattern (8,8,8,3).
5. (0, 8, 16, 24, 2, 5, 13, 21, 29, 7, 10, 18, 26, 4, 12, 15, 23, 1, 9, 17, 20, 28,
    6, 14, 22, 25, 3, 11, 19, 27); pattern (8,8,8,3).

7. The TSP on circulant-2 digraphs

Given a digraph with weights on its edges, the traveling salesman problem (TSP) consists of finding a minimum weight Hamiltonian cycle. A minimum weight Hamiltonian cycle is called an optimal cycle and its weight is termed as cost of the corresponding TSP. If the given digraph is circulant, the corresponding TSP is called the circulant traveling salesman problem (CTSP). In the sum TSP the weight of a Hamiltonian cycle is given as sum of the weights of its edges, whereas in the bottleneck TSP the weight of a Hamiltonian cycle equals the maximum of the weight over all edges of the cycle.

Let \( G(n,a_1,a_2) \) be a circulant-2 digraph and let \( c(a_1) \) and \( c(a_2) \) be the cost of \( a_1 \)-arcs and \( a_2 \)-arcs, respectively. Thus, we assume that the weighted adjacency matrix of the given digraph is a circulant matrix with two nonzero stripes. For circulant-2 digraphs the bottleneck CTSP is closely related to the existence of a Hamiltonian cycle. If \( c(a_i) = c(a_2) \) the problem is trivial: all Hamiltonian cycles have the same cost. If \( c(a_i) < c(a_j) \) the bottleneck CTSP has cost \( c(a_i) \) if and only if \( \gcd(n,a_i) = 1 \), \( i \neq j \), \( i, j \in \{1,2\} \). It has cost \( c(a_j) \), if and only if \( \gcd(n,a_i) > 1 \) and the conditions of Theorem 3.5 are fulfilled. In this case any Hamiltonian cycle produced by Algorithm 4.6 is optimal. Obviously, once we know that \( G(n,a_1,a_2) \) is Hamiltonian we can find the weight of a bottleneck optimal Hamiltonian cycle by performing \( O(\log n) \) arithmetical operations in the unit cost model (by checking whether \( \gcd(n,a_i) = 1 \) or not). The computation of a bottleneck optimal Hamiltonian cycle takes \( O(n) \) arithmetical operations in the unit cost model. Thus, this problem is pseudopolynomially solvable, by applying ‘Find’ for a certain \( h \in \mathcal{S}(G) \). If \( \gcd(n,a_i) = 1 \) we choose \( h = 0 \). Otherwise, all Hamiltonian cycles have the same weight and therefore we can choose any \( h \in \mathcal{S}(G) \).

The analysis of the circulant TSP with sum objective function is more subtle. Theorem 5.2 states that all Hamiltonian cycles of \( G(n,a_1,a_2) \) are periodic and the corresponding patterns consists of \( t-h \) \( a_1 \)-arcs and \( h \) \( a_2 \)-arcs for \( t = \gcd(n,a_2-a_1) \) and \( h \in \mathcal{S}(G) \). For a fixed \( h \in \mathcal{S}(G) \), all Hamiltonian cycles with the above described structure have the same weight:

\[
n'(t-h)c(a_1) + hc(a_2).
\] (18)
Again, if \( c(a_1) = c(a_2) \) the problem is trivial: all Hamiltonian cycles (i.e. for all \( h \in S(G) \)) have the same weight equal to \( nc(a_1) \). In the case that \( c(a_1) \neq c(a_2) \), we wish to minimize the coefficient of the largest cost among \( c(a_1) \) and \( c(a_2) \). Thus, in the case that \( c(a_1) < c(a_2) \), we try to minimize \( h \), whereas in the other case, \( c(a_1) > c(a_2) \), we try to minimize \( t - h \), that is to maximize \( h \). Obviously, we might generate the set \( S(G) \) for the given \( G(n,a_1,a_2) \) and then find either the smallest or the largest element in it, depending on the sign of the difference \( c(a_1) - c(a_2) \). This takes \( O(n) \) arithmetical operations (in the unit cost model), as \( |S(G)| = O(n) \). We show that we can do better. Namely, we can compute the needed \( h \) by performing only \( O(\log^4 n) \) operations. In the case that \( c(a_1) < c(a_2) \) the cost in (18) is minimized by \( h_0 = \min\{h \in S(G)\} \). From the definition of \( S'(G) \) and Theorem 4.3 it follows that \( h_0 \in S'(G) \). In the case that \( c(a_1) > c(a_2) \), the cost in (18) is minimized by \( h_0 = \max\{h \in S(G)\} \). We make use of the set \( S''(G) \) defined as

\[
S''(G) = \{t - \min(t^*, t) \leq h \leq t | l = \gcd(n', a_1 + ha')\},
\]

where \( t^* \) is defined as in Section 4. So, if we denote \( u = \min(t^*, t) \), \( S'(G) \) consists of the \( u \) smallest elements of \( S(G) \), whereas \( S''(G) \) consists of the \( u \) largest elements of \( S(G) \). Analogously to Theorem 4.3, it can be shown that \( S''(G) = \emptyset \) if and only if \( S(G) = \emptyset \). Then, ‘Check’ can be modified to compute \( S''(G) \) by starting with \( h = t \) and recursively decreasing it by 1, until it reaches the value \( t - \min(t^*, t) \). Obviously, a run of this version of ‘Check’ takes again \( O(\log^4 n) \) arithmetical operations in the unit cost model. Thus, we get:

**Theorem 7.1.** Let \( G(n,a_1,a_2) \) be Hamiltonian. An optimal solution of the sum CTSP is given by any periodic Hamiltonian cycle whose pattern consists of \( t - h \) \( a_1 \)-arcs and \( h \) \( a_2 \)-arcs, where \( h \) is the solution of

\[
\min h \ | h \in S'(G) \quad \text{or} \quad \max h \ | h \in S''(G)
\]

in the case that \( c(a_1) \leq c(a_2) \) or \( c(a_1) > c(a_2) \), respectively. Computing the value of the optimal solution by applying algorithm ‘Check’ takes \( O(\log^4 n) \) arithmetical operations in the unit cost model. The computation of an optimal tour by applying algorithm ‘Find’ takes \( O(n) \) arithmetical operations.

**Example 5.** Solving the sum CTSP in \( G(90,2,65) \) with \( c(2) = 3 \) and \( c(65) = 4 \).

In this case we have \( t = \gcd(90,65-2) = 9, n' = 10 \) and \( a' = 7 \). Since \( c(2) < c(65) \), we have to find a cycle with as few \( a_2 \)-arcs as possible. The choice \( h = 0 \) is infeasible, since \( \gcd(10,2) = 5 \neq 1 \). The choice \( h = 1 \) leads to \( \gcd(10,2+7) = 1 \) and is therefore possible. Thus, any cycle whose pattern has length 9 and consists of 8 \( a_1 \)-arcs and 1 \( a_2 \)-arc leads to an optimal solution.
8. Conclusions and remarks

In this paper, we identified conditions that fully characterize Hamiltonian circulant-2 digraphs \( G(n, a_1, a_2) \). The conditions are ‘simple’ from an algorithmic point of view, since their verification takes only \( O(\log^4 n) \) arithmetical operations in the unit cost model, that is a polynomial number of elementary operations in the length of the representation of \( n, a_1 \) and \( a_2 \). The study of the structure of Hamiltonian cycles in a circulant-2 digraph yields an interesting result: They all have a periodic structure, repeating the same pattern of \( a_1 \)-arcs and \( a_2 \)-arcs. We have also discussed both versions of TSP (sum and bottleneck) on such digraphs. For general circulant digraphs, there remains the open question of efficiently characterizing their Hamiltonicity. Even for circulant-3 digraphs this question seems to be difficult. In this case we were not able to derive conditions similar to those of this paper. We remark only that in a circulant-3 digraph there exist Hamiltonian cycles which are not periodic. The following example illustrates this.


Let the circulant-3 digraph \( G(12, 2, 3, 4) \) be given. \( G(12, 2, 3, 4) \) admits the following nonperiodic Hamiltonian cycle \( \mathcal{C} \):

\[
\mathcal{C} = (0, 4, 7, 10, 1, 3, 6, 9, 11, 2, 5, 8, 0)
\]

\((4, 3, 3, 3, 2, 3, 3, 2, 3, 3, 3, 4)\) is the sequence of 2-arcs, 3-arcs and 4-arcs in \( \mathcal{C} \). \( \mathcal{C} \) cannot be periodic with a period smaller than 6, because there are only two 4-arcs in it. But \( \mathcal{C} \) is not periodic with period 6 as well, because the 4-arcs in it are consecutive.

Acknowledgements

We would like to thank Andrew Odlyzko for pointing out Ref. [7] to us. We would also like to thank anonymous referees for reading the previous versions of this paper very carefully and for useful remarks and suggestions.

References


