The Hamiltonian Property of the Consecutive-3 Digraph

G. J. Chang, F. K. Hwang and Li-Da Tong
Department of Applied Mathematics
National Chiao Tung University
Hsinchu 30050, Taiwan
(Received February 1997; accepted March 1997)

Abstract—A consecutive-d digraph is a digraph \( G(d, n, q, r) \) whose \( n \) nodes are labeled by the residues modulo \( n \) and a link from node \( i \) to node \( j \) exists if and only if \( j \equiv q + k \mod n \) for some \( k \) with \( r \leq k \leq r + d - 1 \). Consecutive-d digraphs are used as models for many computer networks and multiprocessor systems, in which the existence of a Hamiltonian circuit is important. Conditions for a consecutive-d graph to have a Hamiltonian circuit were known except for \( \gcd(n, d) = 1 \) and \( d = 3 \) or \( 4 \). It was conjectured by Du, Hsu, and Hwang that a consecutive-3 digraph is Hamiltonian. This paper produces several infinite classes of consecutive-3 digraphs which are not (respectively, are) Hamiltonian, thus suggesting that the conjecture needs modification.

Keywords—Hamiltonian circuit, Consecutive-d digraph, Network, Loop.

1. INTRODUCTION

Define \( G(d, n, q, r) \), also known as a consecutive-d digraph, to be a digraph whose \( n \) nodes are labeled by the residues modulo \( n \), and a link \( i \rightarrow j \) from node \( i \) to node \( j \) exists if and only if \( j \in \{ q_i + k \mod n : r \leq k \leq r + d - 1 \} \) where \( 1 \leq q, d \leq n - 1 \) and \( 0 \leq r \leq n - 1 \) given. Many computer networks and multiprocessor systems use consecutive-d digraphs as the topology of their interconnection networks. For example, \( q = 1 \) yields the multiloop networks \([1]\), also known as circulant digraphs \([2]\), with the skip set \( \{ r, r + 1, \ldots, r + d - 1 \} \). \( q = d \) and \( r = 0 \) yields the generalized de Bruijn digraphs \([3,4]\), and \( q = r = n - d \) yields the Imase-Itoh digraphs \([5]\). In some applications, it is important to know whether a Hamiltonian circuit (of length \( n \)) is embedded in a consecutive-d digraph. Hwang \([6]\) gave a necessary and sufficient condition for \( G(1, n, q, r) \) to be Hamiltonian. This is also equivalent to the existence of a linear congruential sequence of full period \( n \) in the theory of random number generators (see \([7,8]\)). Du and Hsu \([9]\) observed that \( G(2, n, q, r) \) is Hamiltonian if and only if \( G(1, n, q, r) \) or \( G(1, n, q, r + 1) \) is. Du, Hsu, and Hwang \([10]\) proved that a consecutive-d digraph is always Hamiltonian for \( d \geq 5 \). They also conjectured that consecutive-3 digraphs are Hamiltonian. Some partial support of this conjecture was given in \([9,11]\). In this paper, we produce several infinite classes of consecutive-3 digraphs which are not Hamiltonian, thus suggesting that the conjecture needs modification. We also construct several infinite classes of consecutive-3 digraph which are Hamiltonian.

After this paper was submitted, we proved that all consecutive-4 digraphs are Hamiltonian, and thus completely settled the conjecture, see \([12]\).
2. SOME PRELIMINARY RESULTS

We first state some results obtained in [6] which will be used in this paper.

**THEOREM 1.** (See [6-8].) $G(1, n, q, r)$ is Hamiltonian if and only if it satisfies the following three conditions.

(i) $\gcd(n, q) = 1$.

(ii) Any prime $p$ dividing $n$ divides $q - 1$.

(iii) If 4 divides $n$, then 4 divides $q - 1$.

A node $i$ in $G(1, n, q, r)$ is called a loop if $i \rightarrow i$ is a link, or equivalently, $i \equiv qi + r \pmod{n}$.

**THEOREM 2.** (See [6].) $G(1, n, q, r)$ contains a loop if and only if $\gcd(n, q - 1) = \gcd(n, q - 1, r)$.

Furthermore, if $G(1, n, q, r)$ contains a loop, then the number of loops it contains is $\gcd(n, q - 1)$.

The following result is in [10].

**THEOREM 3.** (See [10].) Suppose $\gcd(n, q) \geq 2$. Then, $G(d, n, q, r)$ is Hamiltonian if and only if $d \geq \gcd(n, q)$.

According to Theorem 3, we may assume that $\gcd(n, q) = 1$. In this case, for any $i \in \{0, 1, \ldots, n - 1\}$, there is a unique $j$ such that $j \rightarrow i$ is a type-$r$ (respectively, type-$(r + 2)$) link; we use $i'$ (respectively, $i''$) to denote this $j$.

Call $i \rightarrow j$ an odd link if $i$ is odd and an even link if $i$ is even. Let $G_0(1, n, q, r)$ and $G_E(1, n, q, r)$ denote the set of odd links and even links, respectively, of $G(1, n, q, r)$.

**LEMMA 4.** Suppose $\gcd(n, q) = 1$. If $H$ is a Hamiltonian circuit of $G(1, n, q, r) \cup G(1, n, q, r + 2)$ using both type-$r$ links and type-$(r + 2)$ links, then $n$ is even and $H$ is either $G_0(1, n, q, r) \cup G_E(1, n, q, r + 2)$ or $G_E(1, n, q, r) \cup G_0(1, n, q, r + 2)$.

**PROOF.** Suppose $H$ contains a type-$r$ link $i' \rightarrow i$. Then, the type-$(r + 2)$ link $i' \rightarrow i + 2$ is not in $H$, which forces the type-$r$ link $(i + 2)' \rightarrow i + 2$ to be in $H$. Hence, $i' \rightarrow i$ in $H$ implies $(i + 2)' \rightarrow i + 2$ in $H$. If $n$ was odd, then $H$ contained all the $n$ type-$r$ links $j' \rightarrow j$, which contradicts the assumption. Thus, $n$ is even. Also, note that if $i$ and $j$ have the same parity, then so does $i'$ and $j'$. Hence, $H$ contains either all links of $G(1, n, q, r)$ of the same parity or none. Lemma 4 follows immediately.

**LEMMA 5.** Suppose $\gcd(n, q - 1) = \gcd(n, q - 1, r + 1) = n/k$ and $q^2 \equiv 1 \pmod{n}$.

(i) Consider a node $u = i + x(qr + r + 2)$ (mod $n$) for some $x \in \{0, 1, \ldots, n - 1\}$. If $u \rightarrow v$ in $G(1, n, q, r)$ and $v \rightarrow w$ in $G(1, n, q, r + 2)$, then $w \equiv i + (x + 1)(qr + r + 2)$ (mod $n$).

(ii) Consider a node $u = i + x(qr + 2q + r)$ (mod $n$) for some $x \in \{0, 1, \ldots, n - 1\}$. If $u \rightarrow v$ in $G(1, n, q, r + 2)$ and $v \rightarrow w$ in $G(1, n, q, r)$, then $w \equiv i + (x + 1)(qr + 2q + r)$ (mod $n$).

**PROOF.**

(i) $w \equiv q(qu + r + r + 2) \equiv u + qr + r + 2 \equiv i + (x + 1)(qr + r + 2)$ (mod $n$).

(ii) $w \equiv q(qu + r + 2) + r \equiv u + qr + 2q + r \equiv i + (x + 1)(qr + 2q + r)$ (mod $n$).

**LEMMA 6.** Suppose $\gcd(n, q - 1) = \gcd(n, q - 1, r + 1) = n/k$ and $q + 1 \equiv 0 \pmod{k}$. Then, $i \rightarrow j$ in $G(1, n, q, r + 1)$ implies $j \rightarrow i$ in $G(1, n, q, r + 1)$.

**PROOF.** Note that $(q + 1)(r + 1) \equiv (q + 1)(q - 1) \equiv 0 \pmod{n}$. Thus, in $G(1, n, q, r + 1)$, $i \rightarrow j$ implies $j = qi + r + 1 \rightarrow q(qi + r + 1) + r + 1 = i + (q + 1)(r + 1) \equiv i \pmod{n}$.

**LEMMA 7.** Let $H$ be a Hamiltonian circuit in $G(3, n, q, r)$. If $H$ contains two type-$r$ (respectively, two type-$(r + 2)$) links $i' \rightarrow i$ and $(i + 1)' \rightarrow i + 1$ (respectively, links $i'' \rightarrow i$ and $(i + 1)'' \rightarrow i + 1$) for some $i \in \{0, 1, \ldots, n - 1\}$, then $H = G(1, n, q, r)$ (respectively, $G(1, n, q, r + 2)$).

**PROOF.** Consider the node $(i - 1)'$ such that $q(i - 1)' + r = i - 1 \pmod{n}$. Then, $(i - 1)'$ also has links to $i$ and $i + 1$. But $i$ and $i + 1$ are already reached in $H$; hence, $(i - 1)' \rightarrow i - 1$, which
is in \(G(1, n, q, r)\), must be in \(H\). Iterate this argument, we have \(H = G(1, n, q, r)\). The case for \(H = G(1, n, q, r + 2)\) is analogous.

### 3. THE MAIN RESULTS

**Theorem 8.** Let \(I\) be an independent set of edges of the (undirected) cycle 0, 1, \ldots, \(n - 1, 0\). If \(I \cup G(1, n, q, r + 1)\) is connected (not necessarily strongly), then \(G(3, n, q, r)\) is Hamiltonian.

**Proof.** We use a link-interchange method first introduced in [10]. Suppose that \(G(1, n, q, r + 1)\) consists of \(m\) disjoint cycles \(C_1, C_2, \ldots, C_m\). If \(m = 1\), then there is nothing to prove. So assume \(m > 1\). Let \(e_{ij} = (k, k + 1) \in I\) be the edge connecting \(k \in C_i\) and \(k + 1 \in C_j\). Let \(x \rightarrow k\) be in \(C_i\) and \(y \rightarrow k + 1\) in \(C_j\). Replace the two links \(x \rightarrow k\) and \(y \rightarrow k + 1\) by the two links \(x \rightarrow k + 1\) and \(y \rightarrow k\). Then, \(C_i\) and \(C_j\) are connected into one cycle \(C_{ij}\). Note that \(x \rightarrow k + 1\) is a type-\((r + 2)\) link and \(y \rightarrow k\) is a type-\(r\) link. Now do the same for the set of \(m - 1\) cycles with \(C_{ij}\) replacing \(C_i\) and \(C_j\). Since \(I \cup C_1 \cup \cdots \cup C_m\) is connected, \(e_{ij}\) as described above always exists. Furthermore, since \(I\) is an independent set, the \(e_{ij} = (k, k + 1)\) chosen each time induces the interchange of two type-\((r + 1)\) links with a type-\((r + 2)\) and a type-\(r\) link.

For even \(n\), let \(I_0\) denote the independent set \(\{(2i - 1, 2i) : i = 1, 2, \ldots, n/2\}\).

**Theorem 9.** Suppose \(gcd(n, q) = 1\) and \(n\) is even. Then, \(g(3, n, q, r)\) is Hamiltonian if either \(gcd(n, q - 1) = 2\) and \(r\) is odd, or \(gcd(n, q + 1) = 2\) and \(r\) is even.

**Proof.** By Theorem 8, it suffices to show that \(G^0 = I^0 \cup G(1, n, q, r + 1)\) is connected. Since \(2i - 1 \rightarrow 2i, 2i - 1 \rightarrow (2i - 1)q + r + 1, 2i \rightarrow 2iq + r + 1\) are all in \(G^0\), \(2i - 1 \rightarrow (2i - 1)q + r + 1\) and \(2i \rightarrow 2iq + r + 1\) are connected in \(G^0\). If we replace all links \(2i - 1 \rightarrow (2i - 1)q + r + 1\) and \(2i \rightarrow 2iq + r + 1\) for \(i = 1, 2, \ldots, n/2\) by links \(2i - 1 \rightarrow 2iq + r + 1\) for \(i = 1, 2, \ldots, n/2, 2\), and call the new graph \(G^*\), then \(G^0\) must be connected if \(G^*\) is.

For even \(n\), let \(I^0\) denote the independent set \(\{(2i - 1, 2i) : i = 1, 2, \ldots, n/2\}\).

**Theorem 10.** Suppose \(gcd(n, q) = 1\) and \(gcd(n, q - 1) = gcd(n, q - 1, r + 1) = n/k\). If \(q + 1 \equiv 0 \pmod{k}\) for \(k > 3\) and \(q + 1 \equiv 0 \pmod{4}\) for \(k = 2\), then \(G(3, n, q, r)\) is not Hamiltonian for \(n > 2k\).
Figure 2. $G(1,12,11,1)$ and various independent sets.

**Proof.** First note that $\text{gcd}(n, q - 1, r + 1) = n/k$ and $q + 1 \equiv 0 \mod k$ imply $q^2 \equiv 1 \mod n$ and $(q + 1)(r + 1) \equiv 0 \mod n$.

By Lemma 6, if $i \rightarrow j$ is in $G(1, n, q, r + 1)$, then so is $j \rightarrow i$. Let $i$ be a loop in $G(1, n, q, r + 1)$. Then, $i \rightarrow i - 1$ in $G(1, n, q, r)$ and $i \rightarrow i + 1$ in $G(1, n, q, r + 2)$. Furthermore, $i' \rightarrow i$ in $G(1, n, q, r)$ implies $i' \rightarrow i + 1$ in $G(1, n, q, r + 1)$ and $i + 1 \rightarrow i'$ is also in $G(1, n, q, r + 1)$. This in turns implies $i + 1 \rightarrow i' + 1$ is in $G(1, n, q, r + 2)$. In fact,

$$i' + 1 \equiv q(i + 1) + r + 2 = q(yi + r + 2) + r + 2 \equiv i + (q + 1)(r + 2) \equiv i + q + 1 \mod n.$$ 

Since $q + 1 \equiv 0 \mod k$, $i' + 1$ has the same residue as $i \mod k$; hence, $i' + 1$ is also a loop in $G(1, n, q, r + 1)$ by Theorem 2. It follows that $i' + 1 \rightarrow i'$ is in $G(1, n, q, r)$ and $i' + 1 \rightarrow i' + 2$ is in $G(1, n, q, r + 2)$. Similarly, we have $i - 1 \rightarrow i'' - 1 = i - q - 1$, which is a loop, in $G(1, n, q, r + 1)$ and $i'' - 1 \rightarrow i''$ in $G(1, n, q, r + 2)$. We show these relations in Figure 3, where $\rightarrow$ denotes a type-$r$ link, $\rightarrow$ a type-$(r + 1)$ and $\rightarrow$ a type-$(r + 2)$. We call the two loops $i - q - 1$ and $i + q + 1$ *neighbors* of loop $i$. By Lemma 7, there are only two paths through a loop $i$, either a type-$r$ link followed by a type-$(r + 2)$ link, or a type-$(r + 2)$ link followed by a type-$r$ link. Each path blocks a path of one if its two neighbor loops which has the same end points. For example, the path $i + q \rightarrow i \rightarrow i + 1$ blocks the path $i + 1 \rightarrow i + q + 1 \rightarrow i + q$ because the union of both paths creates a 4-cycle. Let $L$ be the graph whose vertices are the loops and whose edges are pairs of end points of paths. Furthermore, an edge is incident to a vertex only if that loop has a path with that pair of end points. Then, $L$ is a cycle. Note that each edge can only be assigned to one of its incident vertices.

![Figure 3. Relations between a loop and its neighbor loops.](image-url)

Let $H$ be a Hamiltonian circuit of $G(3, n, q, r)$. Suppose $H$ contains a type-$(r + 1)$ link, say, $i + q \rightarrow i + 1$. Then, this link blocks the path with $(i + q, i + 1)$ as end points. So there are only $n/k - 1$ paths left to cover for the $n/k$ loops; one of the loops has no path passing it. Therefore, $H$ contains no type-$(r + 1)$ link.
Note that $q + 1 \equiv 0 \pmod{4}$ implies $q$ does not divide $q - 1$ for $k \geq 3$, and $q + 1 \equiv 0 \pmod{4}$ implies 4 divides $n$, but not $q - 1$. By Theorem 1, neither $G(1, n, q, r)$ nor $G(1, n, q, r + 2)$ is Hamiltonian. By Lemma 4, we only need to look into $G_E(1, n, q, r) \cup G_O(1, n, q, r + 2)$ and $G_E(1, n, q, r) \cup G_E(1, n, q, r + 2)$ for a Hamiltonian circuit. We show that a $(2k)$-cycle exists in either case. Hence, $G(3, n, q, r)$ is not Hamiltonian for $n > 2k$.

For $G_E(1, m, q, r) \cup G_O(1, m, q, r + 2)$, we have $0 \rightarrow r \rightarrow qr + r + 2$. By Lemma 5 (i), after $2k$ moves, we reach the node

$$k(qr + r + 2) = k(q - 1)r + 2k(r + 1) \equiv 0 \pmod{n}.$$ 

For $G_O(1, m, q, r) \cup G_E(1, m, q, r + 2)$, we have $0 \rightarrow r \rightarrow qr + q + r$. By Lemma 5 (ii), after $2k$ moves, we reach the node

$$k(qr + 2q + r) - k(q + 1)(r + 1) + k(q - 1) \equiv 0 \pmod{n}.$$ 

Note that for each $k \geq 2$, the set $NH_k(n, q, r)$ of $(n, q, r)$ satisfying the conditions of Theorem 10 is not empty. For example, $(k(2k - 2), 2k - 1, 2k - 3)$, $k(2k - 2), 2k - 1, 2k - 3 \equiv 0 \pmod{n}$. We now apply Theorem 10 to obtain more specific results for various $k$.

**Theorem 11.** Suppose that $\gcd(n, q) = 1$ and $\gcd(n, q - 1) = \gcd(n, q - 1, r + 1) = n/2$. Then $G(3, n, q, r)$ is not Hamiltonian if and only if $n = 8t + 4$ for some $t \geq 1$.

**Proof.** Since $\gcd(n, q - 1) = \gcd(n, q - 1, r + 1) = n/2$, necessarily $n = 2k$, $q = k + 1$, $r = k - 1$ or $2k - 1$. $\gcd(n, q) = 1$ implies $k = 2m$ and so $n = 4m, q = 2m + 1, r = 2m - 1$ or $4m - 1$.

For odd $m = 2t + 1$ with $t \geq 1$, $q + 1 \equiv 0 \pmod{4}$ and $n = 8t + 4 > 4$. By Theorem 10, $G(3, n, q, r)$ is not Hamiltonian. For odd $m = 2t + 1$ with $t = 0$, $\gcd(n, q - 1) = 2m = 2$ and $r$ is odd. By Theorem 9, $G(3, n, q, r)$ is Hamiltonian.

For even $m = 2t$, $n = 8t$. It is easily verified that $\gcd(n, q) = 1$ implies that every $p > 2$ dividing $n$ divides $q - 1$ and $n = 8t$ implies 4 divides both $n$ and $q - 1$. By Theorem 1, both $G(1, n, q, r)$ and $G(1, n, q, r + 2)$ are Hamiltonian.

**Theorem 12.** Suppose that $\gcd(n, q) = 1$ and $\gcd(n, q - 1) = \gcd(n, q - 1, r + 1) = n/3$. Then, $G(3, n, q, r)$ is not Hamiltonian if and only if $n = 9t + 3$ or $9t - 6$ for some $t \geq 1$.

**Proof.** There are six classes of $(n, q, r)$ satisfying $\gcd(n, q - 1) = \gcd(n, q - 1, r + 1) = n/3$: $n = 3m$, $q = m + 1$ or $2m + 1$, $r = m - 1$, $2m - 1$ or $3m - 1$. Since $\gcd(n, q) = 1$, $q = m + 1$ implies $m \not\equiv 2 \pmod{3}$ and $q = 2m + 1$ implies $m \not\equiv 1 \pmod{3}$.

For the case when $q = m + 1$ with $m = 3t + 1$ or $q = 2m + 1$ with $m = 3t + 2$, where $t \geq 1$, $q + 1 \equiv 0 \pmod{3}$ and $n > 6$. By Theorem 10, $G(3, n, q, r)$ is not Hamiltonian. It is easily verified that $G(3, 3, 2, r)$ and $G(3, 6, 5, r)$ with odd $r$ are Hamiltonian.

Furthermore, if $m = 3t$, then every prime $p$ or 4 dividing $n$ divides $q - 1$. It is also easily verified that $\gcd(n, r) = \gcd(n, r + 2) = 1$. Hence, both $G(1, n, q, r)$ and $G(1, n, q, r + 2)$ are Hamiltonian by Theorem 1.

**Theorem 13.** Suppose that $\gcd(n, q) = 1$ and $\gcd(n, q - 1) = \gcd(n, q - 1, r + 1) = n/4$. Then, $G(3, n, q, r)$ is not Hamiltonian if and only if $n = 16t + 8$ for some $t \geq 1$.

**Proof.** To satisfy the conditions of the theorem, necessarily $n = 8m$, $q = 2m + 1$ or $6m + 1$, and $r = 2m - 1$, $4m - 1$, $6m - 1$ or $8m - 1$.

For odd $m = 2t + 1$ with $t \geq 1$, $q + 1 \equiv 0 \pmod{4}$ and $n = 16t + 8 > 8$. By Theorem 10, $G(3, n, q, r)$ is not Hamiltonian. For odd $m = 2t + 1$ with $t = 0$, $\gcd(n, q - 1) = 2m = 2$ and $r$ is odd. By Theorem 9, $G(3, n, q, r)$ is Hamiltonian.

For even $m = 2t$, every prime $p$ and 4 dividing $n$ divides $q - 1$, and $\gcd(n, r) = 1$. By Theorem 1, $G(1, n, q, r)$ is Hamiltonian.
REFERENCES