Filomat 32:1 (2018), 71–85
https://doi.org/10.2298/FIL1801071B

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

Hamiltonian Properties on a Class of Circulant Interconnection Networks

Milan Bašić[a]

[a]*Faculty of Sciences and Mathematics, University of Niš, Serbia*

Abstract. Classes of circulant graphs play an important role in modeling interconnection networks in parallel and distributed computing. They also find applications in modeling quantum spin networks supporting the perfect state transfer. It has been noticed that unitary Cayley graphs as a class of circulant graphs possess many good properties such as small diameter, mirror symmetry, recursive structure, regularity, etc. and therefore can serve as a model for efficient interconnection networks. In this paper we go a step further and analyze some other characteristics of unitary Cayley graphs important for the modeling of a good interconnection network. We show that all unitary Cayley graphs are hamiltonian. More precisely, every unitary Cayley graph is hamiltonian-laceable (up to one exception for X_6) if it is bipartite, and hamiltonian-connected if it is not. We prove this by presenting an explicit construction of hamiltonian paths on X_{nm} using the hamiltonian paths on X_n and X_m for $\gcd(n,m) = 1$. Moreover, we also prove that every unitary Cayley graph is bipancyclic and every nonbipartite unitary Cayley graph is pancyclic.

1. Introduction

A good interconnection network topology permits many other network topologies (linear arrays, rings, meshes, tori, trees, stars) to be efficiently embedded in it. Embedding of linear arrays and rings in interconnection networks is one of the most desired properties, since both of these architectures are extensively applied in parallel and interconnection systems. An interconnection network is most often modeled by a graph in which vertices and edges correspond to nodes and communication links, respectively. Formally, the embedding is defined as an injective mapping g, which maps the vertices of a guest graph G to the vertices of a host graph H, such that for any two vertices u and v from G it holds that u and v are adjacent in G if and only if $g(u)$ and $g(v)$ are connected by a path in H. Thus, embedding of linear arrays and rings into interconnection networks can be modeled as finding paths and cycles in a graph. In the most important variant of the problem the longest paths or cycles are required; this is closely related to hamiltonian problems in graph theory.

Finding hamiltonian paths and cycles is widely studied in literature, most often on hypercube structures in a faulty setting (with certain number of faulty edges and vertices). In such case, the aim is to determine the maximal possible (tight) bound for the number of faulty vertices and/or faulty edges such that hamiltonian properties still hold through the fault-free elements of the network [9, 12, 25]. These papers also improve the

2010 *Mathematics Subject Classification*. 05C38, 68M10, 11A07, 68R05
Keywords. circulant networks, interconnection networks, hamiltonian graphs, pancyclicity
Received: 10 February 2017; Accepted: 15 August 2017
Communicated by Dragan S. Djordjević
The author gratefully acknowledge support from Research projects 174013 of the Serbian Ministry of Science.
Email address: basic_milan@yahoo.com (Milan Bašić)

numerous previously known results. Furthermore, hamiltonian properties together with the disjoint path cover problem of hypercube-like (HL) graphs attracted much attention in the literature [19–22]. The class of HL-graphs includes some well-known classes with good topological properties already proposed as a model of interconnection networks, such as twisted cubes [10], crossed cubes [8], multiply twisted cubes [7], Möbius cubes [6], and generalized twisted cubes [5]. These classes share several interesting properties with hypercubes of similar size such as logarithmic degree, regularity, hamiltonian connectedness, pancyclicity and connectivity; but lower diameter.

Circulant graphs are Cayley graphs over a cyclic group. The interest for circulant graphs in graph theory and applications has grown during the last two decades. They appeared in coding theory, VLSI design, Ramsey theory and other areas. Since they posses many interesting properties (such as vertex transitivity called mirror symmetry), circulants are applied in quantum information transmission and proposed as models for quantum spin networks that permit the quantum phenomenon called perfect state transfer [2, 24]. In the quantum communication scenario, the important feature of these graphs (especially those with integral spectrum) is the ability of faithfully transferring quantum states without modifying the network topology. Circulants and unitary Cayley graphs (as a subclass of circulants) have found important applications in molecular chemistry for modeling energy-like quantities such as the heat of formation of a hydrocarbon [3, 23].

Recently there has been a vast research on the interconnection schemes based on circulant topology – circulant graphs represent an important class of interconnection networks in parallel and distributed computing (see [11]). Recursive circulant, denoted by $G(n;d)$, is proposed as an interconnection structure for multicomputer networks [18]. $G(n;d)$ is a circulant graph with n vertices and set of symbols (jumps) which are powers of d, i.e. $d^0, d^1, \ldots, d^{\lceil \log_d n \rceil - 1}$. In literature, attention is mainly restricted to the class of recursive circulants $G(2^m;4)$ (or $G(cd^m;d)$ for some positive integers c, d and m), of the degree m, because it turns out that they have some nicer properties than the $m-$dimensional hypercube. While retaining the attractive properties of hypercubes such as node-symmetry, recursive structure, connectivity etc., these graphs achieve noticeable improvements in diameter [18] and possess a complete binary tree with $2^m - 1$ vertices as a subgraph [16]. $G(n;d)$ with degree three or higher is hamiltonian-connected [4] and $G(2^m;4)$ was shown to be almost pancyclic in [1] and also $m-2$-fault almost pancyclic later in [17].

In this paper, we propose unitary Cayley graphs (a class of circulants) as a model of interconnection structures for multicomputer networks. Unitary Cayley graphs are highly symmetric i.e, they are vertex and edge transitive, have integer eigenvalues which are indexed in symmetric palindromic order ($\lambda_i = \lambda_{n-i}$). Various properties of unitary Cayley graphs were investigated in some recent papers [13, 14]. It can be observed that unitary Cayley graphs represent very reliable networks, meaning that the vertex connectivity of the unitary Cayley graph X_n equals the degree of regularity which is $\varphi(n)$ (totient function of the order of X_n). For even orders they are bipartite – note that many of the proposed networks mainly derived from the hypercube structure by twisting some pairs of edges (twisted cube, crossed cub, multiply twisted cube, Möbius cube, generalized twisted cube) are nonbipartite. Furthermore, the fault diameter (the largest diameter obtained by deleting a set of certain number of vertices) related to the maximum path length among all vertex disjoint paths is constant in the case of this class of graphs. More precisely, the diameter of X_n is at most 3, which is important to estimate the degradation of performance of the network. Other important network metrics of X_n are analyzed as well, such as the chromatic number and the clique number which are both equal to p, and the cardinality of a maximal independent set which is equal to n/p, where p is the smallest prime number dividing n.

In this paper we go a step further and analyze some other characteristics of unitary Cayley graphs important for the modeling of a good interconnection network. In Section 4 we show that all unitary Cayley graphs are hamiltonian using some auxiliary results from Section 3. More precisely, every unitary Cayley graph is hamiltonian-laceable (up to one exception for X_6) if it is bipartite, and hamiltonian-connected if it is not. From the scope of network building, it is important to transfer such properties from a certain number of networks of lower dimension to a network of higher dimension, see [19]. Therefore, we prove this by presenting an explicit construction of hamiltonian paths for X_{nm} using the hamiltonian paths on X_n and X_m, for $\gcd(n,m) = 1$. Moreover, in Section 5 we also prove that every unitary Cayley graph is bipancyclic and every nonbipartite unitary Cayley graph is pancyclic. Our techniques in considering the mentioned problems relay heavily on some remarkable properties of these graphs built using the connection of the number theory and combinatorics. We conclude the paper by Section 6 giving directions for future research.

2. Preliminaries

Let Γ be a multiplicative group with identity e. For $S \subset \Gamma$, $e \notin S$ and $S^{-1} = \{s^{-1} \mid s \in S\} = S$, the Cayley graph $X = Cay(\Gamma, S)$ is the undirected graph having vertex set $V(X) = \Gamma$ and edge set $E(X) = \{\{a, b\} \mid ab^{-1} \in S\}$. For a positive integer $n > 1$ the unitary Cayley graph $X_n = Cay(Z_n,\ U_n)$ is defined by the additive group of the ring Z_n of integers modulo n and the multiplicative group $U_n = Z_n^*$ of its invertible elements. That is, $\{a, b\} \in E(X_n)$ if $a - b \in Z_n^*$ and $a - b$ is invertible element of Z_n if $\gcd(a - b, n) = 1$.

Let us recall that for a positive integer n and a subset $S \subseteq \{0, 1, 2, \ldots, n-1\}$, the circulant graph $G(n, S)$ is the graph with n vertices, labeled by integers modulo n, such that each vertex i is adjacent to $|S|$ other vertices $\{i + s \pmod n \mid s \in S\}$. The set S is called the *symbol* of $G(n, S)$. As we will consider only undirected graphs without loops, we assume that $0 \notin S$ and, that $s \in S$ if and only if $n - s \in S$, and therefore the vertex i is adjacent to vertices $i \pm s \pmod n$ for each $s \in S$. Unitary Cayley graphs are circulant graphs of the additive group of Z_n with respect to the Cayley set $S = \{k \mid \gcd(k, n) = 1,\ 1 \le k < n\}$.

We give the definition of the *tensor product* of two graphs since every unitary Cayley graph having non prime power order can be defined as a tensor product of a certain number of unitary Cayley graphs of lower dimensions. The tensor product $G \otimes H$ of graphs G and H is a graph the vertex set of which is the Cartesian product $V(G) \times V(H)$ where any two vertices (u, u') and (v, v') are adjacent if and only if u' is adjacent with v' and u is adjacent with v.

A *hamiltonian path (cycle)* is a path (cycle) in a graph that visits each vertex exactly once. If a graph contains a hamiltonian cycle, it is called *hamiltonian*. A graph G is *hamiltonian-connected* if every two vertices of G are connected by a hamiltonian path. All hamiltonian-connected graphs are hamiltonian and none of the bipartite graphs are hamiltonian-connected. A bipartite graph is called hamiltonian-laceable if there is a hamiltonian path for all pairs of vertices that belong to different sets of the bipartition.

A graph G of order n is called *pancyclic* if it contains a cycle of length l for every $3 \le l \le n$. Finally a graph is *bipancyclic* if it contains a cycle of even length l for every $4 \le l \le n$.

3. Auxiliary Results

Let R be a table of size $n \times m$. Each cell of R is labeled by an ordered pair of coordinates (i, j), where i and j denote the numbers of the row and the column of the cell, respectively, for $1 \le i \le n$ and $1 \le j \le m$. In addition, the upper-left cell of R has the coordinates $(1, 1)$ and the lower-right cell has the coordinates (n, m).

For a given table of size $n \times m$ define the (k, l)−pass through the table from the cell (x_1, y_1) to the cell (x_{mn}, y_{mn}), to be any sequence of cells

$$((x_1, y_1), (x_2, y_2), \ldots, (x_{mn}, y_{mn}))$$

such that $(x_i, y_i) \ne (x_j, y_j)$ for $1 \le i < j \le mn$, $1 \le |x_{i+1} - x_i| \le k$ and $1 \le |y_{i+1} - y_i| \le l$ for $1 \le i \le mn - 1$. In that case, we say that the pass $(x_1, y_1), (x_2, y_2), \ldots, (x_{mn}, y_{mn})$ covers the table R. For two consecutive pairs of coordinates (x_i, y_i) and (x_{i+1}, y_{i+1}) we also say that (x_{i+1}, y_{i+1}) is obtained from the pair (x_i, y_i) by the movement $(|x_{i+1} - x_i|, |y_{i+1} - y_i|)$.

Let $p_1 = ((x_1^1, y_1^1), (x_2^1, y_2^1), \ldots, (x_{nm}^1, y_{nm}^1))$ and $p_2 = ((x_1^2, y_1^2), (x_2^2, y_2^2), \ldots, (x_{nk}^2, y_{nk}^2))$ be two passes that cover the tables sharing its vertical edge of sizes $n \times m$ and $n \times k$, respectively. The concatenation of the passes p_1 and p_2, denoted by

$$p = p_1 \oplus p_2 = ((x_1^1, y_1^1), (x_2^1, y_2^1), \ldots, (x_{nm}^1, y_{nm}^1), (x_1^2, y_1^2 + m), (x_2^2, y_2^2 + m), \ldots, (x_{nk}^2, y_{nk}^2 + m)),$$

is defined as the pass which covers the table $n \times (m+k)$. In the rest of the paper, for the sake of clarity of notation we will omit the outer brackets in the notation of the pass.

In this section we examine the existence of different types of passes (mostly $(1,2)$ and $(2,2)$-passes) in tables of size $n \times m$, where m is odd. The construction of the passes will depend on the parity of n.

3.1. $(1,2)$*-passes for* $n \in 2\mathbb{N}$

Lemma 3.1. *The following statements are true*

- **(i)** *There is a* $(1,2)$*-pass through the table of size* 2×3 *from the upper-left cell to the lower-right cell.*
- **(ii)** *There is a* $(1,2)$*-pass through the table of size* 2×3 *from the cell with coordinates* $(1,2)$ *to the cell in the lower-right corner.*
- **(iii)** *There is a* $(1,2)$*-pass through the table of size* 2×4 *from the upper-left cell to the lower-right cell.*
- **(iv)** *There is a* $(1,2)$*-pass through the table of size* 2×5 *from the upper-left cell to the lower-right cell.*
- **(v)** *There is a* $(1,2)$*-pass through the table of size* 2×5 *from the upper-left cell to the lower-left cell.*
- **(vi)** *There is a* $(1,2)$*-pass through the table of size* 2×5 *from the cell with coordinates* $(1,2)$ *to the cell in the lower-right corner.*

Proof. The labels in the cells of the following tables represent the indices of the pairs of the coordinates of the passes that cover the tables from (*i*)-(*vi*), respectively.

1	5	3
4	2	6

5	1	3
2	4	6

1	7	5	3
6	4	2	8

1	5	7	9	3
6	8	2	4	10

1	9	5	3	7
10	2	8	6	4

7	1	3	9	5
2	8	6	4	10

.

□

Lemma 3.2. *For a given positive integer* $m \geq 3$*, there is a* $(1,2)$*-pass through the table of size* $2 \times m$ *from the cell in the upper-left corner to the cell in the lower-right corner.*

Proof. The proof will proceed by induction on m. For $m \in \{3,4,5\}$ the statement of the lemma is true, according to parts (i), (iii) and (iv) of Lemma 3.1. For $m \geq 6$, it is assumed by the induction hypothesis that there is a $(1,2)$-pass through the first $m-3$ columns of the table from the cell $(1,1)$ to the cell $(2, m-3)$. Now, by the first part of Lemma 3.1 there is a $(1,2)$-pass through the columns $m-2$, $m-1$ and m, starting from the cell $(1, m-2)$ and ending at the cell $(2, m)$. To obtain a $(1,2)-$pass through the whole table, it suffices to concatenate the two mentioned passes by joining the cells $(2, m-3)$ and $(1, m-2)$. The illustration of the proof is given by the following table.

1	...		$2m-5$		
		$2m-6$			$2m$

□

Lemma 3.3. *For a given odd number* $m \geq 5$*, there is a* $(1,2)$*-pass through the table of size* $2 \times m$ *from the cell in the upper-left corner to the cell in the lower-left corner.*

Proof. The proof will proceed by induction on m. For the base case for which $m = 5$ we use part (v) of Lemma 3.1. For $m \geq 7$, it is assumed by the induction hypothesis that there is a $(1, 2)$-pass through the last $m - 2$ columns of the table from the cell $(1, 3)$ to the cell $(2, 3)$. Denote this pass by p. Now, the pass

$$(1, 1), (2, 1), p(1), p(2), \dots, p(2m - 2), (1, 2), (2, 1)$$

represents a $(1, 2)-$pass through the whole table which is also shown by the table below.

1	$2m-1$	3	$\dots$	
$2m$	2	$2m-2$		

□

Remark 3.4. *Notice that there is no such* $(1, 2)-$*pass through the table of size* 2×3.

Lemma 3.5. *For a given odd number* $m \geq 3$*, there is a* $(1, 2)$*-pass through the table of size* $2 \times m$ *from the cell* $(1, 2)$ *to the cell in the lower-right corner.*

Proof. For $m = 5$ there is a $(1, 2)-$pass from the cell $(1, 2)$ to the cell $(2, 5)$, according to the part (vi) of Lemma 3.1. Suppose that $m = 3$ or $m \geq 7$. By the second part of Lemma 3.1 there is a $(1, 2)$-pass through the first three columns of the table, starting with the cell $(1, 2)$ and ending at the cell $(2, 3)$. Moreover, for $m \geq 7$ there is a $(1, 2)$-pass from the cell $(1, 4)$ to the cell $(2, m)$, according to Lemma 3.2. Finally, connecting the mentioned passes the assertion of the lemma immediately follows.

	1		7	$\dots$	
		6			$2m$

□

Theorem 3.6. *Let* $m \geq 3$ *be an odd positive integer and* $n \geq 2$ *an even positive integer. Then, if* $mn \neq 6$ *there is a* $(1, 2)$*-pass through the table of size* $n \times m$ *from the cell in the upper-left corner to the cell in the lower-right (lower-left) corner.*

Proof. Suppose that $n = 2k$, for some positive integer k. We prove that there is a $(1, 2)$-pass in the $2k \times m$ table from the upper-left to the lower-right (lower-left) cell. The proof will be carried out by induction on k. Suppose first that $m \geq 5$. For $k = 1$ the statement of the theorem is true, according to Lemmas 3.2 and 3.3. Using the induction hypothesis there is a $(1, 2)$-pass through the rows $\{1, 2, \dots, 2k - 2\}$ of the table from the cell $(1, 1)$ to the cell $(2k - 2, 1)$. Applying Lemma 3.5 there is a $(1, 2)-$pass from $(2k - 1, 2)$ to $(2k, m)$. Now, joining the cells $(2k - 2, 1)$ and $(2k - 1, 2)$ we obtain a $(1, 2)-$pass through whole table. The problem of the existence of a $(1, 2)$-pass in the $2k \times m$ table from the upper-left to the lower-left cell is symmetric to the one in the previous case and can be proven in the same way. The starting and the ending cells of the mentioned passes are shown in the following table.

<table>
<tr><td>1</td><td>2</td><td>3</td><td></td><td>...</td><td>m</td></tr>
<tr><td>1</td><td colspan="5" rowspan="3">...</td></tr>
<tr><td></td></tr>
<tr><td>(2k − 2)m</td></tr>
<tr><td></td><td>(2k − 2)m + 1</td><td></td><td></td><td>...</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>2km</td></tr>
</table>

Now assume that $m = 3$. For $k = 1$ the statement of the theorem is true, according to Lemma 3.1 part (i) and Remark 3.4 and the induction step can be similarly proven using Lemma 3.1 part (ii).

□

3.2. $(2,2)$*-passes for* $n \in 2\mathbb{N}+1$

Lemma 3.7. *There is a* $(2,2)$*-pass through the table of size* 3×3 *from the cell in the upper-left corner to the cell in the lower-right (lower-left) corner.*

Proof. The labels in the cells of the following tables represent the ordinal numbers of passes' elements in each of the above cases, respectively

1	8	5
4	6	2
7	3	9

1	8	5
4	6	2
9	3	7

.

□

Lemma 3.8. *For a given odd number* $m \geq 3$*, there is a* $(2,2)$*-pass through the table of size* $3 \times m$ *from the cell in the upper-left corner to the cell in the lower-right corner.*

Proof. The proof will proceed by induction on m. The base case for $m = 3$ holds according to Lemma 3.7. For $m \geq 5$, it is assumed by the induction hypothesis that there is a $(2,2)$-pass through the columns $\{1, 2, \ldots m-2\}$ of the table from the cell $(1,1)$ to the cell $(3, m-2)$. Furthermore, by the second part of Lemma 3.1 there is the $(2,1)$-pass through the columns $m-1$ and m, starting at the cell $(2, m-1)$ and ending at the cell $(3, m)$. To obtain a $(2,2)-$pass through the whole table, it suffices to concatenate the two mentioned passes joining the cells $(3, m-2)$ and $(2, m-1)$. The illustration of the proof is given by the following table.

1				
	$\ldots$		$3m-5$	
		$3m-6$		$3m$

□

Lemma 3.9. *For a given odd number* $m \geq 3$*, there is a* $(2,2)$*-pass through the table of size* $3 \times m$ *from the cell in the upper-left corner to the cell in the lower-left corner.*

Proof. The proof will proceed by induction on m. For the base case if $m = 3$ we use Lemma 3.7. For $m \geq 5$, it is assumed by the induction hypothesis that there is a $(2,2)$-pass through the columns $\{3, 4, \ldots, m\}$ of the table from the cell $(3,3)$ to the cell $(1,3)$. Denote this pass by p. Now the pass

$$(1,1), (2,2), p(1), p(2), \ldots, p(3m-6), (3,2), (2,1), (1,2), (3,1)$$

represents a $(2,2)-$pass through the whole table which is also shown by the table below.

<table>
<tr><td>1</td><td>$3m-1$</td><td>$3m-4$</td><td></td><td></td></tr>
<tr><td>$3m-2$</td><td>2</td><td colspan="2">$\ldots$</td><td></td></tr>
<tr><td>$3m$</td><td>$3m-3$</td><td>3</td><td></td><td></td></tr>
</table>

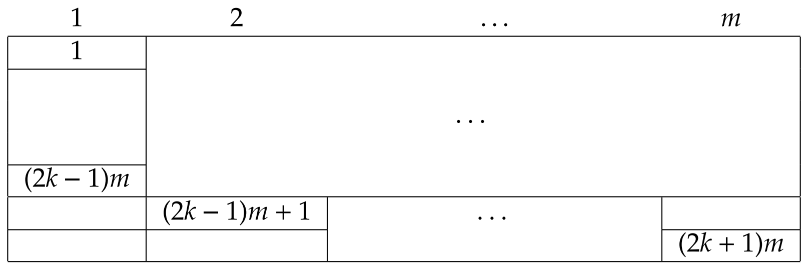
□

Theorem 3.10. *Let* $m, n \geq 3$ *be odd numbers. Then there is a* $(2,2)$*-pass through the table of size* $n \times m$ *from the cell in the upper-left corner to the cell in the lower-right (lower-left) corner.*

Proof. Let $n = 2k+1$ for some positive integer k. We prove that there is a $(2,2)$-pass in the $(2k+1) \times m$ table from the upper-left to the lower-right and lower-left cell, respectively. The proof will be carried out by induction on k. For $k = 1$ the statement of the theorem is true, according to Lemmas 3.8 and 3.9. Now, suppose that there is a $(2,2)$-pass through the first $2k-1$ rows of the table from the cell $(1,1)$ to the cell $(2k-2, 1)$ and $(2k-2, m)$, respectively.

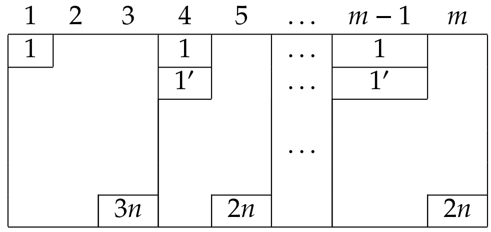
Applying Lemma 3.5 there are $(1,2)-$passes from $(2k, 2)$ to $(2k+1, m)$ and from $(2k, m-1)$ to $(2k+1, 1)$.

Now, joining the cells $(2k-1, 1)$ and $(2k, 2)$ ($(2k-1, m)$ and $(2k, m-1)$) we obtain a $(2,2)-$pass through the whole table from the cell in the upper-left corner to the cell in the lower-right (lower-left) corner.



□

Remark 3.11. *Let m, n be positive odd integers and $m = 2k+1$. Notice that there exists a cover of the table of size $m \times n$ by a sequence of the passes $p_1, p_2, \ldots, p_k$, where the pass p_1 starts at the cell $(1,1)$ and ends at $(n,3)$ and p_i starts at $(1,2i)$ and ends at $(n,2i+1)$ for $2 \le i \le k$. Similarly, the same table can be covered by a sequence of the passes $p_1, p'_2, \ldots, p'_k$, where the pass p'_i starts at the fleld $(2,2i)$ and ends at $(n,2i+1)$ for $2 \le i \le k$. The above observation holds according to Lemma 3.8, Lemma 3.2 and Lemma 3.5.*



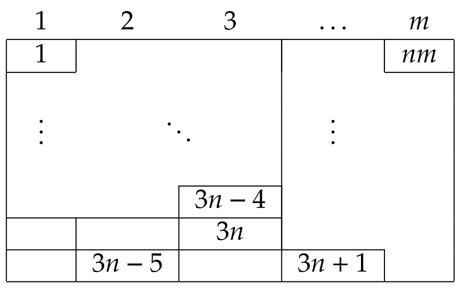
Theorem 3.12. *Let $n \ge 3$ and $m \ge 5$ be odd integers. Then, there is a $(2,2)$-pass through the table of the size $n \times m$ from the cell in the upper-left corner to the cell in the upper-right corner.*

Proof. Suppose that $n \ge 5$. According to Theorem 3.10 there is a $(2,2)-$path connecting the cells $(1,1)$ and $(n-2,3)$ through the columns 1 to 3 and the rows 1 to $n-2$. Moreover, there is a $(1,2)-$path from $(n,2)$ to $(n-1,3)$ through the columns 1 to 3 and the rows $n-1$ and n, by Lemma 3.1 part (ii). Now a $(2,2)-$pass p from the cell $(1,1)$ to the cell $(n-1,3)$ can be obtained by concatenating the above paths. The same $(2,2)$-pass, for $n = 3$, can be obtained by connecting the cells $(1,1)$ and $(2,3)$ in the following table

1	7	4
6	3	9
8	5	2

.

Now, using Theorem 3.6, there is a $(2,1)-$pass q connecting the cell $(n,4)$ with the cell $(1,m)$. Finally, concatenating the pass q to the pass p, we obtain a $(2,2)-$pass through the whole table.



□

Remark 3.13. *Notice that the $(2,2)-$pass from the proof of the previous theorem that covers the table contains $(1,2)$ and $(2,2)$ movements only in the covering of the first three columns. More precisely, in the pass $(x_1,y_1),(x_2,y_2),\ldots,(x_{mn},y_{mn})$, it holds that $|y_{i+1}-y_i| = 2$ if and only if $y_i, y_{i+1} \in \{1,3\}$ and $y_i \ne y_{i+1}$, $1 \le i \le mn-1$.*

4. Hamiltonicity of Unitary Cayley Graphs

In this section, we prove by induction that every bipartite unitary Cayley graph is hamiltonian-laceable and every nonbipartite unitary Cayley graph is hamiltonian-connected.

Let us briefly explain the motivation behind the idea of the proof. Namely, we have mentioned that hypercubes, recursive circulants and unitary Cayley graphs have recursive structures. For example the n-dimensional hypercubes can be obtained from the Cartesian product of n copies of 2-dimensional hypercubes, i.e. $Q_n = Q_{n-1} \times Q_2$. Similarly, recursive circulants can be constructed by a certain more complex operation (than the Cartesian product) starting from a certain number of recursive circulants of lower dimension. Also, unitary Cayley graphs X_N of a given order N can be represented as tensor products of graphs X_n and X_m, where $N = nm$ and $\gcd(n, m) = 1$. This decomposition allows us to list the vertices of X_N as functions of the vertices of X_n and X_m, which is shown by the table R in the comment after Proposition 4.2. We actually want to prove that there exists a hamiltonian path on X_N if there are hamiltonian paths on both X_n and X_m.

Notice that the unitary Cayley graph X_n is bipartite if and only if n is even. Indeed, it is clear that the bipartition classes are equivalent to the classes modulo 2.

4.1. *N is odd*

We show that unitary Cayley graphs of the odd order are hamiltonian-connected. Since the graphs in this class are vertex-transitive, it is sufficient to prove that there exists a hamiltonian path joining the vertex 0 to an arbitrary vertex $1 \le t \le n-1$. So, our task here is to find a permutation $p_0, p_1, \dots, p_{n-1}$ of vertices $\{0, 1, \dots, n-1\}$, such that $p_0 = 0$, $p_{n-1} = t$ and p_i is adjacent to p_{i+1} ($\gcd(p_{i+1} - p_i, n) = 1$), for $0 \le i \le n-2$.

In this section we will label the rows and columns of the table of size $n \times m$ by the numbers $0, 1, \dots, n-1$ and $0, 1, \dots, m-1$, respectively.

Lemma 4.1. *Let p be a prime number and n be a power of p.*

(i) For $p = 2$ the graph X_n is hamiltonian laceable.

(ii) For $p > 2$ the graph X_n is hamiltonian-connected. Moreover, for any two vertices there exists a hamiltonian path $a_0, a_1, \dots, a_{n-1}$ joining them such that a_i and a_{i+2} are adjacent, for $0 \le i \le n-3$.

Proof. We prove that there is hamiltonian path joining the vertex 0 to an arbitrary vertex $1 \le t \le n-1$.

Let $n = p^k$ and $C_0, C_1, \dots, C_{p-1}$ be the classes modulo p,

$$C_i = \{j \mid 0 \le j < p^k,\ j \equiv i \pmod{p}\}, \qquad 0 \le i \le p-1.$$

Two vertices a and b from X_n are adjacent if and only if $\gcd(a-b, n) = \gcd(a-b, p^k) = 1$ or, equivalently, if $p \nmid a-b$. This means that for each $0 \le i \le p-1$ all the vertices from C_i are adjacent to the vertices from $X_n \setminus C_i$, while there are no edges between any two vertices from C_i. In other words, X_n is a complete multipartite graph.

If $p \nmid t$ then $t \equiv i \pmod{p}$, for some $1 \le i \le p-1$. This implies that $t \in C_i$ and we can find the vertices $a_0, a_1, \dots, a_{n-1}$ of the desired hamiltonian path by choosing the vertices $a_{kp}, a_{kp+1}, \dots, a_{kp+(p-1)}$ from the sets $C_0, C_1, \dots, C_{i-1}, C_{i+1}, \dots, C_{p-1}, C_i$, respectively, for $0 \le k \le n/p - 1$.

For odd p, if $p \mid t$ we have $0, t \in C_0$. Now, we can choose the vertices of the hamiltonian path from the sets $\underbrace{C_0, C_1, \dots, C_{p-1}, C_0, C_1, \dots, C_{p-1}, \dots, C_0, C_1, \dots, C_{p-1}}_{n-p}, C_1, \dots, C_{p-1}, C_0$, respectively.

For odd p, in both of the two mentioned cases in the hamiltonian path $a_0, a_1, \dots, a_{n-1}$ the vertices a_i and a_{i+2} are adjacent, for every $0 \le i \le n-3$, since they belong to different classes C_j modulo $p \ge 3$. □

Proposition 4.2. *Let S be a complete (reduced) residue system modulo m, T be a complete (reduced) residue system modulo n and* $\gcd(m,n) = 1$. *Then the set*

$$R = \{an + bm \mid a \in S,\ b \in T\}$$

is a complete (reduced) residue system modulo mn.

Proof. We prove the first part of the statement. Let S and T be complete residue systems modulo m and n, respectively. Assume that there exist $a_1, a_2 \in S$ and $b_1, b_2 \in T$ such that $a_1n + b_1m \equiv a_2n + b_2m \mod mn$. From the last relation we have that $mn \mid (a_2 - a_1)n + (b_2 - b_1)m$ implying that $m \mid (a_2 - a_1)n$ and $n \mid (b_2 - b_1)m$. As $\gcd(m,n) = 1$ it holds that $m \mid a_2 - a_1$ and $n \mid b_2 - b_1$. This is a contradiction since S and T are complete residue systems modulo m and n, respectively.

Let S and T be reduced residue systems modulo m and n, respectively. Now, assume that $\gcd(am + bn, mn) \neq 1$ for $a \in S$ and $b \in T$. Without loss of generality, this means that there exists an odd prime $p \mid n$ such that $p \mid am + bn$. This further implies that $p \mid am$ and $p \mid a$, since $\gcd(m,n) = 1$. Finally, we obtain that $p \mid \gcd(a,n)$, which is a contradiction since $a \in S$. $\square$

If $S = \{a_0, a_2, \ldots a_{n-1}\}$ and $T = \{b_0, b_2, \ldots b_{m-1}\}$, in the rest of the section the elements of the set R in the previous lemma will be denoted by $c_{i,j} = a_im + b_jn$ for $0 \leq i \leq n-1$ and $0 \leq j \leq m-1$ and arranged in the following table

$$R = \begin{bmatrix} a_0m + b_0n & a_0m + b_1n & \ldots & a_0m + b_{m-1}n \\ a_1m + b_0n & a_1m + b_1n & \ldots & a_1m + b_{m-1}n \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1}m + b_0n & a_{n-1}m + b_1n & \ldots & a_{n-1}m + b_{m-1}n \end{bmatrix}$$

Now, we prove the following useful assertion concerning the elements c_{ij} of R.

Proposition 4.3. *Let m and n be positive relatively prime integers greater than* 1. *Then* $\gcd(c_{i,j} - c_{k,l}, nm) = 1$ *if and only if* $\gcd(a_i - a_k, n) = 1$ *and* $\gcd(b_j - b_l, m) = 1$.

Proof. Assume that $\gcd(c_{i,j} - c_{k,l}, nm) = 1$ and let p be an arbitrary prime divisor of n. From these assumptions we have that $p \nmid c_{i,j} - c_{k,l} = (a_i - a_k)m + (b_j - b_l)n$ and thus $p \nmid (a_i - a_k)m$. From the last conclusion it must be also $p \nmid a_i - a_k$. Since no prime divisor of n divides $a_i - a_k$, it follows that $\gcd(a_i - a_k, n) = 1$. The equation $\gcd(b_j - b_l, m) = 1$ can be established in the same way.

Now let $\gcd(a_i - a_k, n) = 1$ and $\gcd(b_j - b_l, m) = 1$ and assume that there exists a prime number p such that $p \mid nm$ and $p \mid c_{i,j} - c_{k,l} = (a_i - a_k)m + (b_j - b_l)n$. Without loss of generality we may assume that $p \mid n$ and thus, since $\gcd(m,n) = 1$, we have that $p \mid a_i - a_k$, which is a contradiction with $\gcd(a_i - a_k, n) = 1$. $\square$

Lemma 4.4. *Let N be an odd positive integer other than a power of prime and m a divisor of N such that $N = p^\alpha m$ for some positive integer α and prime number p not dividing m. For any $1 \leq t \leq N-1$ such that m divides t, there exists a permutation $(p_0, p_1, \ldots, p_{N-1})$ of the numbers $\{0, 1, \ldots, N-1\}$ such that $p_0 = 0$, $p_{N-1} = t$,* $\gcd(p_{i+1} - p_i, N) = 1$ *and* $\gcd(p_2, N) = 1$, *for $0 \leq i \leq N-2$.*

Proof. Let $n = p^\alpha$, $t = mq$ and $b_i = i$ for $0 \leq i \leq m-1$. According to Lemma 4.1 there exists a permutation a of the numbers $\{0, 1, \ldots, n-1\}$, such that $a_0 = 0$, $a_{n-1} = q$ and $\gcd(a_{i+1} - a_i, n) = 1$ for $1 \leq i \leq n-1$. Now, we see that the sets $\{a_0, a_1, \ldots a_{n-1}\}$ and $\{b_0, b_1, \ldots, b_{m-1}\}$ are the permutations of the numeber $\{0, .., n-1\}$ and $\{0, .., m-1\}$ and therefore form complete residue systems modulo n and m, respectively whence we conclude that the set $\{c_{i,j} = a_im + b_jn \mid 0 \leq i \leq n-1,\ 0 \leq j \leq m-1\}$ is a complete residue system modulo N (according to Proposition 4.2).

Furthermore, according to Theorem 3.10 there is a $(2,2)-$pass

$$(x_0, y_0) = (0,0), (x_1, y_1), \ldots, (x_{nm-1}, y_{nm-1}) = (n-1, 0)$$

from the upper-left cell to the lower-left cell through some table of size $n \times m$. If we define $p_i = c_{x_i,y_i}$ for $0 \le i \le nm-1$, then we have that

$$\begin{aligned} p_0 &= c_{x_0,y_0} = c_{0,0} = a_0 m + b_0 n = 0 \\ p_{nm-1} &= c_{x_{nm-1},y_{nm-1}} = c_{n-1,0} = a_{n-1}m + b_0 n = qm = t. \end{aligned}$$

Moreover, for any $0 \le i \le N-2$ it holds that $\gcd(p_{i+1}-p_i, N) = 1$ if and only if $\gcd(c_{x_{i+1},y_{i+1}} - c_{x_i,y_i}, N) = 1$. Using Proposition 4.3, the last equation holds if and only if $\gcd(a_{x_{i+1}} - a_{x_i}, n) = 1$ and $\gcd(b_{y_{i+1}} - b_{y_i}, m) = 1$. Since, $\{(x_i, y_i) \mid 0 \le i \le N-1\}$ is a $(2,2)-$pass, we conclude that $|x_{i+1}-x_i|, |y_{i+1}-y_i| \in \{1,2\}$. From the last observation and the definition of the sequence b we have $|b_{y_{i+1}} - b_{y_i}| \in \{1,2\}$ and thus $\gcd(b_{y_{i+1}} - b_{y_i}, m) = 1$ trivially holds. Furthermore, from the proof of Lemma 4.1 we conclude that the p consecutive numbers $a_{i+1}, a_{i+2}, \ldots a_{i+p}$ $(0 \le i \le n-p-1)$ belong to different classes modulo p, given that $p \ge 3$, and that consequently a_{x_i} and $a_{x_{i+1}}$ belong to different classes modulo p. Finally, $p \nmid a_{x_{i+1}} - a_{x_i}$ and $\gcd(a_{x_{i+1}} - a_{x_i}, n) = 1$ hold.

Furthermore, since $p_2 = c_{x_2,y_2}$, according to the proof of Theorem 3.10 we conclude that either $x_2 = y_2 = 2$ or $x_2 = 2$ and $y_2 = 1$ and thus either $p_2 = c_{2,2}$ or $p_2 = c_{2,1}$. Notice that $p_2 = c_{2,2}$ and N are relatively prime if and only if $\gcd(a_2, n) = 1$ and $\gcd(b_2, m) = 1$. Since, a_0 and a_2 belong to different classes modulo $p \ge 3$ and $p \mid a_0$, we have that $p \nmid a_2$ and therefore $\gcd(a_2, n) = 1$. As $b_2 = 2$ and m is odd, the fact $\gcd(b_2, m) = 1$ clearly holds. In the same fashion we conclude that $\gcd(p_2, N) = 1$ for $p_2 = c_{2,1}$. □

Theorem 4.5. *Let N be an odd positive number and* $1 \le t \le N-1$*. Then there exists a permutation p of the numbers* $\{0, 1, \ldots, N-1\}$ *, such that* $p_0 = 0$*,* $p_{N-1} = t$*,* $\gcd(p_{i+1} - p_i, N) = 1$ *and* $\gcd(p_2, N) = 1$*, for* $0 \le i \le N-2$*.*

Proof. If N is a power of prime then the assertion holds by Lemma 4.1. Now, let $N = q_1^{\alpha_1} q_2^{\alpha_2} \cdot \ldots \cdot q_k^{\alpha_k}$ be the prime factorization of N, where $q_1 < q_2 < \ldots < q_k$ are distinct primes, $\alpha_i \ge 1$, and let $n = q_1^{\alpha_1}$ and $m = N/n$. Using Bezout's identity, since $\gcd(m, n) = 1$ we can find two positive integers $0 \le q \le n-1$ and $0 \le s \le m-1$ such that $qm + sn \equiv t \pmod N$. If $s = 0$ then $m \mid t$ and using Lemma 4.4 the assertion of the theorem immediately follows. Now suppose that $s \ne 0$.

We prove the assertion using induction on N. The base case, when N is a power of prime, holds according to Lemma 4.1 (part (ii)). Suppose that the assertion of the theorem holds for any $l < N$. Thus, applying the induction hypothesis to m we conclude that there exists a permutation $b_0, b_1, \ldots, b_{m-1}$ such that $b_0 = 0$, $b_{m-1} = s$, $\gcd(b_{i+1} - b_i, m) = 1$ and $\gcd(b_2, m) = 1$, for $0 \le i \le m-2$. We distinguish two cases depending on whether q is equal to zero or not.

Case 1 $q = 0$. Let $a_i = i$ for $0 \le i \le n-1$. Now, since the sets $\{a_0, a_1, \ldots a_{n-1}\}$ and $\{b_0, b_1, \ldots, b_{m-1}\}$ are complete residue systems modulo n and m, respectively, the set $\{c_{i,j} = a_i m + b_j n \mid 0 \le i \le n-1,\ 0 \le j \le m-1\}$ is also a complete residue system modulo N, according to Proposition 4.2.

Furthermore, according to Theorem 3.12 there is a $(2,2)-$pass

$$(x_0, y_0) = (0,0), (x_1, y_1), \ldots, (x_{nm-1}, y_{nm-1}) = (0, m-1)$$

from the upper-left cell to the upper-right cell through some table of size $n \times m$. If we define $p_i = c_{x_i,y_i}$ for $0 \le i \le nm-1$, then we have that

$$\begin{aligned} p_0 &= c_{x_0,y_0} = c_{0,0} = a_0 m + b_0 n = 0 \\ p_{nm-1} &= c_{x_{nm-1},y_{nm-1}} = c_{0,m-1} = a_0 m + b_{m-1} n = sn = t. \end{aligned}$$

For any $0 \le i \le N-2$ it holds that $\gcd(p_{i+1} - p_i, N) = 1$ if and only if $\gcd(c_{x_{i+1},y_{i+1}} - c_{x_i,y_i}, N) = 1$. Using Proposition 4.3, the last equation holds if and only if $\gcd(a_{x_{i+1}} - a_{x_i}, n) = 1$ and $\gcd(b_{y_{i+1}} - b_{y_i}, m) = 1$. Since, $\{(x_i, y_i) \mid 0 \le i \le N-1\}$ is a $(2,2)-$pass we conclude that $|x_{i+1} - x_i|, |y_{i+1} - y_i| \in \{1,2\}$. From the last observation and the definition of the sequence a we have $|a_{x_{i+1}} - a_{x_i}| \in \{1,2\}$ and thus $\gcd(a_{x_{i+1}} - a_{x_i}, n) = 1$ trivially holds. Moreover, from Remark 3.13 we see that $|y_{i+1} - y_i| = 2$ if and only if $y_i, y_{i+1} \in \{0,2\}$ and $y_i \ne y_{i+1}$, which further implies that in this case $|b_{y_{i+1}} - b_{y_i}| = b_2$ and $\gcd(b_{y_{i+1}} - b_{y_i}, m) = 1$, according to the induction hypothesis. If $|y_{i+1} - y_i| = 1$ we obtain that b_{y_i} and $b_{y_{i+1}}$ are consecutive elements of the sequence $b_0, b_1, \ldots b_{m-1}$ and by the induction hypothesis we have that $\gcd(b_{y_{i+1}} - b_{y_i}, m) = 1$ holds in this case, also.

Finally, according to the proof of Theorem 3.12 we have that $p_2 = c_{2,1} = a_2m + b_1n$, for $n \geq 5$. p_2 and N are relatively prime if and only if $\gcd(a_2, n) = 1$ and $\gcd(b_1, m) = 1$. This is clearly true, since $a_2 = 2$ and $\gcd(b_1 - b_0, m) = 1$. If $n = 3$, we have $p_2 = c_{2,2} = a_2m + b_2n$ and for the same reason $\gcd(a_2, n) = 1$ and $\gcd(b_2, m) = 1$ trivially follows from the induction hypothesis.

Case 2. $q \neq 0$. As $n = q_1^{\alpha}$, by Lemma 4.1 there exists a permutation a of the numbers $\{0, 1, \ldots, n-1\}$, such that $a_0 = 0$, $a_{n-1} = q$ and $\gcd(a_{i+1} - a_i, n) = 1$ for $1 \leq i \leq n-1$. Similarly, as in the previous case we have that the set $\{c_{i,j} = a_im + b_jn \mid 0 \leq i \leq n-1,\ 0 \leq j \leq m-1\}$ is also a complete residue system modulo N, according to Proposition 4.2.

Assume that $\gcd(q, n) = 1$. Let $m = 2l + 1$. According to Remark 3.11 there is a sequence of passes $r_1, r_2, \ldots, r_l$, where the pass r_1 starts at the cell $(0, 0)$ and ends at $(n-1, 2)$ and r_i starts at $(0, 2i-1)$ and ends at $(n-1, 2i)$ for $2 \leq i \leq l$. Now, consider the pass

$$r = r_1 \oplus r_2 \oplus \ldots \oplus r_l = (x_0, y_0), (x_1, y_1), \ldots, (x_{nm-1}, y_{nm-1})$$

($(x_0, y_0) = (0, 0)$ and $(x_{nm-1}, y_{nm-1}) = (n-1, m-1)$) from the upper-left cell to the lower-right cell through some table of size $n \times m$. If we define $p_i = c_{x_i, y_i}$ for $0 \leq i \leq nm-1$, then we have that

$$\begin{aligned} p_0 &= c_{x_0, y_0} = c_{0,0} = a_0m + b_0n = 0 \\ p_{nm-1} &= c_{x_{nm-1}, y_{nm-1}} = c_{n-1, m-1} = a_{n-1}m + b_{m-1}n = qm + sn = t. \end{aligned}$$

We prove that $\gcd(p_{i+1} - p_i, N) = 1$ for $0 \leq i \leq N-2$, which is true if and only if $\gcd(a_{x_{i+1}} - a_{x_i}, n) = 1$ and $\gcd(b_{y_{i+1}} - b_{y_i}, m) = 1$, according Proposition 4.3. We consider three cases depending on which part of the pass r the pairs (x_i, y_i) and (x_{i+1}, y_{i+1}) belong to for $0 \leq i \leq mn-2$. If both (x_i, y_i) and (x_{i+1}, y_{i+1}) are from r_1 then it must be that $|x_{i+1} - x_i|, |y_{i+1} - y_i| \in \{1, 2\}$, since r_1 is a $(2, 2)$–pass. On the other hand, if $|y_{i+1} - y_i| = 2$, then as r_1 covers the first three columns of the table it holds that $y_i = 0$ and $y_{i+1} = 2$ and thus, using the induction hypothesis, $\gcd(b_{y_{i+1}} - b_{y_i}, m) = \gcd(b_2, m) = 1$. If $|y_{i+1} - y_i| = 1$, $\gcd(b_{y_{i+1}} - b_{y_i}, m) = 1$ holds by the induction hypothesis. From the proof of Lemma 4.1 we conclude that the q_1 consecutive numbers $a_{i+1}, a_{i+2}, \ldots a_{i+q_1}$ $(0 \leq i \leq n-1-q_1)$ belong to different classes modulo q_1 and since $q_1 \geq 3$, that a_{x_i} and $a_{x_{i+1}}$ belong to different classes modulo q_1. Thus, $q_1 \nmid a_{x_{i+1}} - a_{x_i}$ and $\gcd(a_{x_{i+1}} - a_{x_i}, n) = 1$. Assume that (x_i, y_i) and (x_{i+1}, y_{i+1}) are elements of the sequence r_j for some $2 \leq j \leq l$. Since r_j is a $(2, 1)$–pass, for the same reason as in the previous case we conclude that $\gcd(a_{x_{i+1}} - a_{x_i}, n) = 1$ and by the induction hypothesis $\gcd(b_{y_{i+1}} - b_{y_i}, m) = 1$ holds, since $|y_{i+1} - y_i| = 1$. Finally, assume that (x_i, y_i) is an element of the pass r_j and (x_{i+1}, y_{i+1}) is an element of r_{j+1} for some $2 \leq j \leq l-1$. According to Remark 3.11 $x_i = n-1$, $y_i = 2j$, $x_{i+1} = 0$ and $y_{i+1} = 2j+1$. Furthermore, we see that $|a_{x_{i+1}} - a_{x_i}| = q$ which is relatively prime with n. As $y_{i+1} - y_i = 1$, by the induction hypothesis now directly implies that $\gcd(b_{y_{i+1}} - b_{y_i}, m) = 1$. The same conclusion holds if (x_i, y_i) belongs to r_1 and (x_{i+1}, y_{i+1}) belongs to r_2.

If $\gcd(q, n) \neq 1$ then $q_1 \mid q$ implying that $a_0 = 0$ and $a_{n-1} = q$ belong to the same class modulo q_1. Since $\gcd(a_1 - a_0, n) = \gcd(a_1, n) = 1$, which means that $q_1 \nmid a_1$, it holds that $q_1 \nmid a_{n-1} - a_1$. Now, we can use a similar construction of the pass as in the previous case. In fact, the construction of the pass is given in Remark 3.11. So, we can repeat the above proof in the same manner considering the pass

$$r' = r'_1 \oplus r'_2 \oplus \ldots \oplus r'_l$$

where the pass r'_1 starts at the filed $(0, 0)$ and ends at $(n-1, 2)$ and r'_i starts at $(1, 2i-1)$ and ends at $(n-1, 2i)$ for $2 \leq i \leq l$ where $m = 2l + 1$.

Finally, according to Remark 3.11 and the proof of Lemma 3.8 we have that $p_2 = c_{2,1} = a_2m + b_1n$. By the induction hypothesis it trivially holds that $\gcd(b_1, m) = 1$. According to the definition of the sequence $a_0, a_1, \ldots, a_{n-1}$ we conclude that $q_1 \nmid a_2$, since $q_1 \geq 3$, and thus $\gcd(a_2, n) = 1$. Now, it is clear that $\gcd(p_2, N) = 1$, according to Proposition 4.3.

□

Notice that, following the proof of the above theorem we can find numbers $p(i)$, for $0 \leq i \leq N-1$, which form a complete residue system modulo N, but they are not necessarily nonnegative and less than N. It is clear that if we replace $p(i)$ by $p_1(i)$ so that $p_1(i) \equiv p(i) \pmod{N}$ and $0 \leq p_1(i) \leq N-1$, the assertion of the theorem still holds. From this fact and the previous theorem we conclude that unitary Cayley graphs of the odd order are hamiltonian-connected.

4.2. N is even

Now, we show that unitary Cayley graphs of even order $N \neq 6$ are hamiltonian-laceable.

Theorem 4.6. *Let $N \neq 6$ be an even positive integer and $1 \leq t \leq N-1$ be an odd number. Then there exists a permutation p of the numbers $\{0, 1, \dots N-1\}$, such that $p_0 = 0$, $p_{N-1} = t$ and $\gcd(p_{i+1} - p_i, N) = 1$, for $0 \leq i \leq N-2$.*

Proof. If N is a power of two then the assertion holds by Lemma 4.1. Let $N = 2^{\alpha_1} q_2^{\alpha_2} \cdot \ldots \cdot q_k^{\alpha_k}$ be the prime factorization of N, where $2 < q_2 < \ldots < q_k$ are distinct primes, $\alpha_i \geq 1$. Let q_r be an arbitrary odd prime divisor of N, $n = {q_r}^{\alpha_r}$ and $m = N/n$, for some $2 \leq r \leq k$. According to Bezout's identity, since $\gcd(m, n) = 1$ we can find two nonegative integers $0 \leq q \leq n-1$ and $0 \leq s \leq m-1$ such that $qm + sn \equiv t \pmod{N}$. As t is odd and m is even, then s must also be odd (and thus $s \neq 0$). Therefore we distinguish two cases, $q = 0$ and $q \neq 0$. For the sake of simplicity of notation we set $p = q_r$ and $\alpha = \alpha_r$.

We prove the assertion using induction on N. The base case holds according to the first part of Lemma 4.1. Suppose that the assertion of the theorem holds for any $l < N$. Thus, applying the induction hypothesis to m we conclude that there exists a permutation $b_0, b_1, \dots, b_{m-1}$ such that $b_0 = 0$, $b_{m-1} = s$ and $\gcd(b_{i+1} - b_i, m) = 1$, for $0 \leq i \leq m-2$.

Case 1 $q = 0$. Let $a_i = i$ for $0 \leq i \leq n-1$. Now, since $\gcd(m, n) = 1$, it is clear that the set $\{c_{i,j} = a_i m + b_j n \mid 0 \leq i \leq n-1,\ 0 \leq j \leq m-1\}$ is a complete residue system modulo N.

Assume that $N \neq 6$. According to Theorem 3.6 there is a $(2, 1)-$pass

$$(x_0, y_0) = (0, 0), (x_1, y_1), \dots, (x_{nm-1}, y_{nm-1}) = (0, m-1)$$

from the upper-left cell to the upper-right cell through some table of size $n \times m$. If we define $p_i = c_{x_i, y_i}$ for $0 \leq i \leq nm-1$, then we have that

$$\begin{aligned} p_0 &= c_{x_0,y_0} = c_{0,0} = a_0 m + b_0 n = 0 \\ p_{nm-1} &= c_{x_{nm-1},y_{nm-1}} = c_{0,m-1} = a_0 m + b_{m-1} n = sn = t. \end{aligned}$$

Since $\{(x_i, y_i) \mid 0 \leq i \leq N-1\}$ is a $(2, 1)-$pass we conclude that $|x_{i+1} - x_i| \in \{1, 2\}$ and $|y_{i+1} - y_i| = 1$. From the definition of the sequence a it is clear that $1 \leq |a_{x_{i+1}} - a_{x_i}| \leq 2$ and therefore $\gcd(a_{x_{i+1}} - a_{x_i}, n) = 1$ trivially holds. On the other hand, since $|y_{i+1} - y_i| = 1$ by the induction hypothesis we have $\gcd(b_{y_{i+1}} - b_{y_i}, m) = 1$. Using Proposition 4.3, $\gcd(p_{i+1} - p_i, N) = 1$ holds for all $0 \leq i \leq N-2$.

Case 2 $q \neq 0$. According to Lemma 4.1 there exists a permutation a of the numbers $\{0, 1, \dots, n-1\}$, such that $a_0 = 0$, $a_{n-1} = q$ and $\gcd(a_{i+1} - a_i, n) = 1$ for $1 \leq i \leq n-1$. Again, we conclude that $\{c_{i,j} = a_i m + b_j n \mid 0 \leq i \leq n-1,\ 0 \leq j \leq m-1\}$ is a residue system modulo N, according to Proposition 4.2.

Assume that $N \neq 6$. According to Theorem 3.6 there is a $(2, 1)-$pass

$$(x_0, y_0) = (0, 0), (x_1, y_1), \dots, (x_{nm-1}, y_{nm-1}) = (n-1, m-1)$$

from the upper-left cell to the lower-right cell through some table of size $n \times m$. If we define $p_i = c_{x_i, y_i}$ for $0 \leq i \leq nm-1$, then we have that

$$\begin{aligned} p_0 &= c_{x_0,y_0} = c_{0,0} = a_0 m + b_0 n = 0 \\ p_{nm-1} &= c_{x_{nm-1},y_{nm-1}} = c_{n-1,m-1} = a_{n-1} m + b_{m-1} n = qm + sn = t. \end{aligned}$$

Since $\{(x_i, y_i) \mid 0 \le i \le N-1\}$ is a $(2,1)$−pass we conclude that $|x_{i+1} - x_i| \in \{1, 2\}$ and $|y_{i+1} - y_i| = 1$. From the proof of Lemma 4.1 we conclude that any p consecutive numbers from $a_{i+1}, a_{i+2}, \ldots a_{i+p}$ belong to different classes modulo $p \ge 3$ $(0 \le i \le n-p-1)$, which implies that $\gcd(a_{x_{i+1}} - a_{x_i}, n) = 1$. On the other hand, since $|y_{i+1} - y_i| = 1$ by the induction hypothesis we have $\gcd(b_{y_{i+1}} - b_{y_i}, m) = 1$. Using Proposition 4.3, $\gcd(p_{i+1} - p_i, N) = 1$ holds for all $0 \le i \le N-2$.

□

By Theorem 4.5, we have actually shown that there is a hamiltonian path between the vertex 0 and each vertex of unitary Cayley graph X_n. As X_n is vertex-transitive, there is a hamiltonian path between any two vertices of X_n, i.e. X_n is hamiltonian-connected. Similarly, according to Theorem 4.6, there is a hamiltonian path between the vertex 0 and each odd vertex t of X_n (with the exception for $n = 6$). Since 0 and t belong to different classes of the bipartition of X_n, we conclude that X_n is hamiltonian-laceable. These results imply that every unitary Cayley graph X_n is hamiltonian, for $n \ne 6$.

5. Pancyclicity of Unitary Cayley Graphs

In this section, we give a method for embedding cycles of arbitrary even length into unitary Cayley graphs. Throughout this section we let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ be the prime factorization of n, where $p_1 < p_2 < \ldots < p_k$ are distinct primes, $\alpha_i \ge 1$.

Theorem 5.1. *Every unitary Cayley graph X_n is bipancyclic for $n \ge 4$.*

Proof. Let $4 \le l \le n$ be even. We want to prove that there exists a cycle of length l in X_n. We will find the cycle as the sequence of the vertices in the following form

$$v_0 = 0, v_1 = l_1, v_2 = l_1 + 1, \ldots, v_{l-2} = l_1 + l - 3, v_{l-1} = l_1 + l - 2, v_l = 0,$$

where $0 < l_1 \le n-1$, (the addition in the above formulas is taken modulo n). It is clear that the vertex v_i is adjacent to v_{i+1} for $1 \le i \le l-2$. We prove that there exists l_1 such that v_0 is adjacent to v_1 and v_{l-1} is adjacent to v_l, for every l. Such l_1 must satisfy $\gcd(l_1, n) = 1$ and $\gcd(l_1 + l - 2, n) = 1$ and thus we could conclude that $p_i \nmid l_1$ and $p_i \nmid l_1 + l - 2$. The last relation can be rewritten in the following form $l_1 \not\equiv 0 \pmod{p_i}$ and $l_1 \not\equiv 2 - l \pmod{p_i}$ for $1 \le i \le k$. Since l is even the system of congruences $l_1 \not\equiv \{0, 2-l\} \pmod{p_i}$ has a solution modulo p_i, for $1 \le i \le k$. Thus, according to the Chinese remainder theorem, it follows that there exists a solution s of the above system of congruences such that $0 \le s < M$ and $l_1 \equiv s \pmod{M}$ where $M = p_1 p_2 \ldots p_k$.

If $l = n$ then we can choose $l_1 = 1$ and thus $v_i = i$ for $1 \le i \le n-1$. Assume that $l < n$. If $v_j \ne 0$, for $2 \le j \le l-1$ then the sequence $v_0, \ldots, v_l$ indeed forms a cycle. If there is a vertex v_j, for $2 \le j \le l-1$ such that $v_j = 0$, we conclude that the vertices of the sequence $v_0, v_1, \ldots, v_{l-1}, v_l$ do not form a cycle, in fact form a closed walk, and $l_1 + l - n - 1, l_1 + l - n, \ldots, l_1 - 1$ are not included in the walk. Therefore, we distinguish two cases depending on the different values of l modulo 3.

Suppose that $l \not\equiv 1 \pmod 3$. Putting $u = l_1 + l - n - 1$ we have already concluded that $u \ne v_j$ for $0 \le j \le l$. The vertex u is adjacent to the vertex $v_{j-1} = n - 1$ if and only if $\gcd(v_{j-1} - u, n) = 1$ and the last relation is satisfied if and only if $l_1 \not\equiv -l \pmod{p_i}$ for $1 \le i \le k$. Since l is even and $l \not\equiv 1 \pmod 3$ we conclude that the system $l_1 \not\equiv \{0, 2-l, -l\} \pmod{p_i}$ $(1 \le i \le k)$ has a solution modulo M. The vertices $v_0, v_1, \ldots, v_{j-1}, u, v_{l-1}, v_{l-2}, \ldots, v_1, v_0$ are mutually distinct and thus form a cycle.

Suppose that $l \equiv 1 \pmod 3$. According to the previous case we can form a cycle of length $l - 2 \equiv 2 \pmod 3$.

First, it can be assumed that the cycle contains the sequence of the vertices $v_0 = 0, v_1, \ldots, v_{j-1}$, $u, v_{l-3}, v_{l-4}, \ldots, v_1, v_0 = 0$, where $u = l_1 + l - n - 3$. The number of vertices that do not belong to the cycle is equal to $n - l + 2 \ge 3$, whence we conclude that the vertices $u + 1$ and $u + 2$ do not belong to the cycle. Since u is adjacent to $v_{j-1} = n - 1$, $u + 1$ is also adjacent to $v_0 = 0$ and $u + 2$ is adjacent to $v_{j+1} = 1$. Therefore, the sequence $v_0, v_1, \ldots, v_{j-1}, u, v_{l-3}, v_{l-4} \ldots, v_{j+1}, u + 2, u + 1, v_0$ forms a cycle of length l.

Now, suppose that the cycle of length $l - 2$ consists of the consecutive vertices $v_0 = 0, v_1, \ldots, v_{l-3}$, $v_0 = 0$. Since $n - l + 2 \ge 3$ vertices are not in the cycle, we conclude that the vertices $1, 2 \notin \{v_0, v_1, \ldots, v_{l-3}\}$

or $n-2, n-1 \notin \{v_0, v_1, \ldots, v_{l-3}\}$. If $1, 2 \notin \{v_0, v_1, \ldots, v_{l-3}\}$, since $v_0 = 0$ is adjacent to v_1, it holds that 1 is adjacent to v_2 and 2 is adjacent to v_3, as well. Therefore, the sequence of the vertices $v_0, v_1, v_2, 1, 2, v_3, \ldots, v_{l-3}$ forms a cycle of size l. Similarly, if $n-2, n-1 \notin \{v_0, v_1, \ldots, v_{l-3}\}$, since $v_0 = 0$ is adjacent to v_{l-3} it holds that $n-1$ is adjacent to v_{l-4} and $n-2$ is adjacent to v_{l-5}, as well. Therefore, the sequence of the vertices $v_0, v_1, \ldots, v_{l-5}, n-2, n-1, v_{l-4}, v_{l-3}$ forms a cycle of size l.
□

In the same way, following the proof of Theorem 5.1 the next result can be immediately obtained

Theorem 5.2. *Every nonbipartite unitary Cayley graph X_n (for odd $n \geq 3$) is pancyclic.*

Remark 5.3. *Note that no unitary Cayley graph X_n, for n even, contains a cycle of odd length, since X_n is bipartite.*

6. Concluding Remarks

We propose the class of unitary Cayley graphs as a subclass of circulant graphs for efficient interconnection networks, since they possess many good properties such as small diameter, mirror symmetry, recursive structure and regularity. In this paper we examine the hamiltonian properties as they are one of the most important requirements in designing network topologies since the embedding problem can be modeled by finding the longest paths and cycles. Furthermore, it is well known that hamiltonian paths and cycles can efficiently simulate many algorithms designed on linear arrays or rings.

First we show that every bipartite unitary Cayley graph is hamiltonian-laceable and every nonbipartite unitary Cayley graph is hamiltonian-connected. We actually prove this by transferring these propertiess from two networks of lower dimensions n and m to a network of higher dimension nm, $\gcd(n, m) = 1$. It is worthwhile to carry out further investigation on this topic in a faulty setting, since fault-tolerant ability is a highly desirable property in the interconnection networks that have high probability of failure. Namely, it is well known that for a graph G such that $G \setminus F$ has a hamiltonian cycle (resp. is hamiltonian connected) for any set F of faulty elements with $|F| \leq f$, it is necessary that $f \leq \delta(G) - 2$ (resp. $f \leq \delta(G) - 3$), where $\delta(G)$ is the minimum degree of G. Testing the low-order graphs X_n suggests that the above upper bound can be achieved as is the case for the class of restricted HL graphs [20].

The same authors in [21] also show that there exists a cycle of every length from 4 to $|V(G \setminus F)|$ for any faulty set F with $|F| \leq m-2$ and restricted $m-$dimensional HL-graph G with $m \geq 3$. Since we prove that every unitary Cayley graph X_n ($n \geq 4$) is bipanciclic and every unitary nonbipartite Cayley graph X_n ($n \geq 3$) is panciclic, it is natural to extend our future research to the problem of examining pancyclity on the graphs X_n with faulty elements. The examples for smaller values of n indicate that every graph $X_n \setminus F$ is bipancyclic ($X_n \setminus F$ is pancyclic for odd n) for any faulty set F with $|F| \leq \delta(X_n) - 2$.

Another possible direction in research would be the examination of the property of edge-pancyclity or vertex-pancyclity which is an extension of pancyclity. More precisely, a graph G is edge-pancyclic (resp. vertex-pancyclity) if every edge (resp. vertex) lies on a cycle of every length from 3 to $|V(G)|$. This concept can again be studied in a faulty setting as it is done in [15].

References

[1] T. Araki and Y. Shibata, *Pancyclicity of recursive circulant graphs*, Inform. Process. Lett. 81 (2002) 187–190.
[2] M. Bašić, *Which weighted circulant networks have perfect state transfer?*, Inform. Sci., Volume 257, (2014) 193–209.
[3] S. Blackburn, I. Shparlinski, *On the average energy of circulant graphs*, Linear Algebra Appl. 428 (2008), 1956–1963.
[4] C.C. Chen, N.F. Quimpo, *On strongly hamiltonian abelian group graphs*, Lecture Notes in Mathematics 884 (Springer, Berlin), Australian Conference on Combinatorial Mathematics (1980) 23–34.
[5] F.B. Chedid, *On the generalized twisted cube*, Inform. Process. Lett. 55 (1995), 49–52.
[6] P. Cull, S. Larson, *The Möbius cubes* in Proc. of the 6th IEEE Distributed Memory Computing Conf. (1991), 699– 702.
[7] K. Efe, *A variation on the hypercube with lower diameter*, IEEE Trans. Comput. 40(11) (1991), 1312–1316.
[8] K. Efe, *The crossed cube architecture for parallel computation*, IEEE Trans. Parallel Distrib. Syst. 3(5), (1992) 513–524.
[9] J. Fink, P. Gregor, *Long paths and cycles in hypercubes with faulty vertices*, Inform. Sci. 179(20) (2009), 3634–3644.
[10] P.A.J. Hilbers, M.R.J. Koopman, J.L.A. van de Snepscheut, *The Twisted Cube*, in J. Bakker, A. Nijman, P. Treleaven, eds., PARLE: Parallel Architectures and Languages Europe, Vol. I: Parallel Architectures, Springer, (1987) 152–159.

[11] F. K. Hwang, *A survey on multi-loop networks*, Theor. Comput. Sci. 299 (2003) 107–121.
[12] T.L. Kueng, T. Liang, L.H. Hsu, J. J. M. Tan, *Long paths in hypercubes with conditional node-faults*, Inform. Sci. 179(5) (2009) 667–681.
[13] W. Klotz, T. Sander, *Some properties of unitary Cayley graphs*, Electron. J. Combin. 14 (2007) #R45.
[14] W. Klotz, T. Sander, *Integral Cayley graphs over abelian groups*, Electron. J. Combin. 17 (2010) #R81.
[15] T.K. Li, C.H. Tsai, J.J.M. Tan, L.H. Hsu *Bipanconnectivity and edge–fault–tolerant bipancyclicity of hypercubes*, Inform. Process. Lett. 87 (2003), 107–110.
[16] H.S. Lim, J.H. Park, K.Y. Chwa, *Embedding trees into recursive circulants*, Discrete Appl. Math. 69 (1996) 83–99.
[17] J.H. Park, *Cycle embedding of faulty recursive circulants*, Journal of KISS 31(2) (2004), 86–94.
[18] J.H. Park, K.Y. Chwa, *Recursive circulants and their embeddings among hypercubes*, Theor. Comput. Sci. 244 (2000) 35–62.
[19] C.D. Park, K.Y. Chwa, *Hamiltonian properties on the class of hypercube-like networks*, Inform. Process. Lett. 91 (2004), 11–17.
[20] J.H. Park, H.C. Kim, H.S. Lim, *Fault-hamiltonicity of hypercube-like interconnection networks*, in Proc. IEEE International Parallel and Distributed Processing Symposium IPDPS 2005, Denver, Apr. 2005.
[21] J.H. Park, H.S. Lim, H.C. Kim, *Panconnectivity and pancyclicity of hypercube-like interconnection networks with faulty elements*, Theor. Comput. Sci. 377(1-3) (2007), 170–180.
[22] J.H. Park, H.C. Kim, H.S. Lim, *Many-to-many disjoint path covers in the presence of faulty elements*, IEEE Trans. Comput. 58(4) (2009) 528–540.
[23] H. N. Ramaswamy, C. R. Veena, *On the Energy of Unitary Cayley Graphs*, Electron. J. Combin. 16 (2007) #N24.
[24] N. Saxena, S. Severini, I. Shparlinski, *Parameters of integral circulant graphs and periodic quantum dynamics*, Int. J. Quantum Inf. 5 (2007), 417–430.
[25] A. Szepietowski, *Hamiltonian cycles in hypercubes with 2n-4 faulty edges*, Inform. Sci. 215 (2012), 75–82.