Isomorphism testing for circulant graphs $C_n(a, b)$

Sara Nicoloso * Ugo Pietropaoli †

March 10, 2010

Abstract

In this paper we focus on connected directed/undirected circulant graphs $C_n(a, b)$. We investigate some topological characteristics, and define a simple combinatorial model, which is new for the topic. Building on such a model, we derive a necessary and sufficient condition to test whether two circulant graphs $C_n(a, b)$ and $C_n(a', b')$ are isomorphic or not. The method is entirely elementary and consists of comparing two suitably computed integers in $\{1, \ldots, \frac{n}{\gcd(n,a)\gcd(n,b)} - 1\}$, and of verifying if $\{\gcd(n, a), \gcd(n, b)\} = \{\gcd(n, a'), \gcd(n, b')\}$. It also allows for building the mapping function in linear time. In addition, properties of the classes of mutually isomorphic graphs are analyzed.

KEYWORDS: isomorphism, circulant graph, Ádám's conjecture.

1 Introduction

Consider three integers n, a, b such that $n > 0$ and, w.l.o.g., $a, b \in \{1, \ldots, n-1\}$. The (simple) graph $C_n(a, b) = (V, E)$ where $V = \{v_0, v_1, \ldots, v_{n-1}\}$ and $E = \{(v_i, v_{(i+a) \bmod n}), (v_i, v_{(i+b) \bmod n}), \text{for } i = 0, \ldots, n-1\}$ is called *circulant graph* (see Fig. 1). By *directed circulant graph* we shall denote a circulant graph where edges $(v_i, v_{(i+a) \bmod n})$ are directed from v_i to $v_{(i+a) \bmod n}$, and edges $(v_i, v_{(i+b) \bmod n})$ are directed from v_i to $v_{(i+b) \bmod n}$. If no direction is defined on the edges, we get an *undirected circulant graph*. In the paper, we shall deal with both directed and undirected circulant graphs (when no specified it means that we are referring to both of them), and we shall assume that all arithmetic is done modulo n.

*IASI - CNR, Viale Manzoni 30, 00185 Roma, Italy. - nicoloso@disp.uniroma2.it

†Università di Roma Tor Vergata, Dipartimento di Ingegneria dell'Impresa, Via del Politecnico 1, 00133 Roma, Italia - pietropaoli@disp.uniroma2.it

W.l.o.g. we shall assume that $a+b \neq n$ in the undirected case, and that $a \neq b$, in both directed and undirected case, otherwise $C_n(a,b)$ degenerates into $C_n(a) = C_n(b)$. Under these conditions, the vertices of a directed $C_n(a,b)$ do always have two outgoing and two incoming edges, and an undirected $C_n(a,b)$ is 3-regular iff either a or b are equal to $\frac{n}{2}$, and is 4-regular in all other cases.

The circulant graphs we deal with, are a subclass of the more general class of circulant graphs $C_n(a_1, a_2, \ldots, a_k)$ for $k = 2$ (where $a_1 = a$ and $a_2 = b$). Circulant graphs $C_n(a_1, a_2, \ldots, a_k)$ are defined on n vertices, and each vertex v_i is adjacent to vertices $v_{(i+a_j) \bmod n}$, for $j = 1, \ldots, k$. The set $\{a_1, a_2, \ldots, a_k\}$ is called the *connection set* of the graph [12, 27, 28]. Circulant graphs $C_n(a_1, a_2, \ldots, a_k)$ are Cayley graphs over the cyclic group $\mathbb{Z}_n$. In the literature, they are also called chordal rings or multiple-loops iff $a_1 = 1$ [19, 26, 30]. Circulant graphs $C_n(1, b)$ are called double loops [17, 21, 22], cyclic graphs [17], or 2-jumps [5].

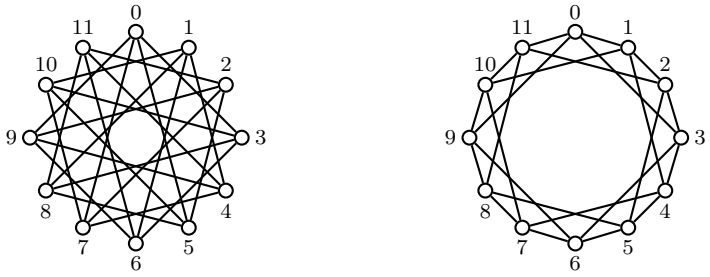

Figure 1: The isomorphic undirected graphs $C_{12}(3,5)$ and $C_{12}(1,3)$.

In this paper we investigate the ISOMORPHISM TESTING problem for both directed and undirected circulant graphs $C_n(a,b)$:

ISOMORPHISM TESTING

Given	two connected circulant graphs $C_n(a,b) = (V,E)$ and $C_n(a',b') = (V',E')$
Test	whether they are isomorphic or not.

We propose an elementary method to solve ISOMORPHISM TESTING, which is purely combinatorial and new for the problem. The method derives from basic topological properties of circulant graphs $C_n(a,b)$'s: the necessary and sufficient condition (Theorem 4.1) for two circulant graphs $C_n(a,b)$, $C_n(a',b')$ to be isomorphic consists of evaluating if $\{\gcd(n,a), \gcd(n,b)\} = \{\gcd(n,a'), \gcd(n,b')\}$ and if two suitably computed integers in $\{1, \ldots, \frac{n}{\gcd(n,a)\gcd(n,b)} - 1\}$ are equal. Our method requires $O(\log n)$ elementary operations and compares favorably with the known results on the $C_n(a_1,$

$a_2, \ldots, a_k$)'s [7, 13, 14, 25, 29] (see Section 1.1). Furthermore, it allows for building the mapping function in linear time.

We also analyze the structure of the class of mutually isomorphic graphs.

The paper is organized as follows: the literature is reviewed in Section 1.1; in Section 2 preliminary conditions for connectedness and isomorphism are discussed; in Section 3 the structure of peculiar cycles and a matrix model for the graphs are described; Section 4 is devoted to prove the main isomorphism theorem, which solves ISOMORPHISM TESTING; in Section 5 we study the structure of the classes of mutually isomorphic graphs.

1.1 State of the art

The problem of testing isomorphism of two given circulant graphs $C_n(a_1, a_2, \ldots, a_k)$ and $C_n(a'_1, a'_2, \ldots, a'_k)$ is polynomial-time solved in [7, 29] for n prime, while, for arbitrary n, it is shown to be polynomial-time solvable in [13, 14] and solved in $O(n^2)$ in [25].

The isomorphism of circulant graphs is closely related to Ádám's isomorphism: two directed (undirected, resp.) graphs $C_n(a_1, a_2, \ldots, a_k)$ and $C_n(a'_1, a'_2, \ldots, a'_k)$ are *Ádám-isomorphic* if there exists a $\mu \in \{1, \ldots, n-1\}$ coprime with n such that $\{a'_1, a'_2, \ldots, a'_k\} = \{\mu a_1, \mu a_2, \ldots, \mu a_k\}$ ($\{a'_1, a'_2, \ldots, a'_k\} = \{\pm\mu a_1, \pm\mu a_2, \ldots, \pm\mu a_k\}$, resp.). The integer μ will be called *Ádám's multiplier*. The problem of testing Ádám's isomorphism has been completely solved in $O(k \log n(\log(k \log n) + 2)^c)$ for some absolute constant c, see [8]. It has also been proved to be equivalent to testing for a *color-preserving isomorphism* on circulant graphs whose arbitrary edge $(v_i, v_{(i+a_t) \bmod n})$ has color a_t [3].

In 1967 Ádám [1] stated the so-called *Ádám's conjecture*: two circulant graphs $C_n(a_1, a_2, \ldots, a_k)$ and $C_n(a'_1, a'_2, \ldots, a'_k)$ are isomorphic if and only if they are Ádám-isomorphic. This conjecture is not generally true: Elspas and Turner [12] showed that directed $C_8(1, 2, 5)$ and $C_8(1, 5, 6)$ as well as undirected $C_{16}(1, 2, 7)$ and $C_{16}(2, 3, 5)$ are isomorphic, but not Ádám-isomorphic (in fact, both isomorphisms are not color-preserving). The conjecture also fails, among the other cases, when n is divisible by 8 or by an odd square [23], or when $n = p^2$ where p is a prime number [2]. However, there are cases where the conjecture holds, for example: when n is prime [12, 29]; when the adjacency matrix has non-repeated eigenvalues [12]; when $n = pq$, for p and q distinct primes [2, 20]; when n is square-free [23] or twice square-free [24]; when $a_1, a_2, \ldots, a_k$ are all coprime with n [11, 28]. Other cases are reported in [5, 23, 27].

When the connection set has two elements, all the above results apply. Ádám's conjecture is true also on the following undirected (connected) circulants: (3-regular) $C_n(a, \frac{n}{2})$ with n even [28]; (4-regular) $C_n(1, b)$ with

$n = p^c$, where p is a prime number and c is a positive integer [28]; (4-regular) $C_n(1, b)$ with $b < \min\{\frac{n}{4}; \frac{\phi(n)}{2}\}$ where $\phi(n)$ is the Euler totient function (in other words, for $a = 1$ and "small" b) [21]; on all the $C_n(1, b)$'s [17]; and, finally, on all the (4-regular) graphs $C_n(a, b)$'s [15, 22]. The results by [15, 17, 21, 22], however, were proved for the first time in [10] both for directed and undirected 4-regular $C_n(a, b)$'s.

It is interesting to notice that different methods have been used to approach the isomorphism of circulant graphs: group theory and algebraic-combinatorial theory [2, 14, 15, 20, 23, 24, 25], and the study of the eigenvalues [7, 12, 21, 22, 26]. Even though Ádám's conjecture is false for arbitrary $C_n(a_1, a_2, \ldots, a_k)$'s, we believe that the topological approach introduced in this paper can be extended to characterize isomorphic graphs $C_n(a_1, a_2, \ldots, a_k)$'s, and to identify subclasses of them on which Ádám's conjecture is valid.

2 Preliminary conditions

This section is devoted to describe the condition for $C_n(a, b)$ to be connected, and to review some isomorphism conditions.

Proposition 2.1. [5] *$C_n(a, b)$ is connected if and only if* $\gcd(n, a, b) = 1$.

Notice that the graph $C_n(a, b)$ has $\gcd(n, a, b)$ connected components, each of which is isomorphic to $C_{n'}(a', b')$, where $n' = \frac{n}{\gcd(n,a,b)}$, $a' = \frac{a}{\gcd(n,a,b)}$, and $b' = \frac{b}{\gcd(n,a,b)}$ [5]. It is worth noticing that each connected component of a directed $C_n(a, b)$ is strongly connected.

Given two graphs $C_n(a, b) = (V, E)$ and $C_n(a', b') = (V', E')$ we shall say that they are *isomorphic* if there exists a mapping function $f : V \to V'$ such that $(f(u), f(v)) \in E'$ if and only if $(u, v) \in E$ (of course, $n = |V| = |V'| = n'$ and $|E| = |E'|$). For example, $C_n(a, b)$ and $C_n(b, a)$ are (trivially) isomorphic, both in the directed and in the undirected case; while $C_n(a, b)$, $C_n(-a, b)$, $C_n(a, -b)$, $C_n(-a, -b)$, $C_n(b, a)$, $C_n(b, -a)$, $C_n(-b, a)$, $C_n(-b, -a)$ are (trivially) isomorphic in the undirected case, only.

We shall also say that two directed (undirected, resp.) graphs $C_n(a, b)$ and $C_n(a', b')$ are *Ádám-isomorphic* if there exists a $\mu \in \{1, \ldots, n-1\}$ coprime with n such that $\{a', b'\} = \{\mu a, \mu b\}$ ($\{a', b'\} = \{\pm\mu a, \pm\mu b\}$, resp.). That is to say, a-edges are mapped onto either a'-edges or b'-edges (thus, b-edges are mapped onto either b'- or a'-edges). For example consider $C_{175}(7, 15)$. If it is undirected, then $\mu = 3$ transforms it into the 8 Ádám-isomorphic circulants $C_n(a', b')$ with $\{a', b'\} = \{\pm 21, \pm 45\}$. If it is directed, then $\mu = 3$ transforms it into the 2 Ádám-isomorphic circulants $C_{175}(21, 45)$ and $C_{175}(45, 21)$.

The following two propositions are examples of Ádám-isomorphism.

Proposition 2.2. [18] *Let n, a verify $\gcd(n,a) = 1$, and let t be an integer s.t. $(ta) \bmod n = 1$. Then, $C_n(a,b)$ and $C_n(1,(tb) \bmod n)$ are isomorphic.*

The proposition is an application of Ádám's isomorphism with $\mu = t$, since the two conditions $\gcd(n,a) = 1$ and $(ta) \bmod n = 1$ imply $\gcd(n,t) = 1$ (we remark that, assuming $\gcd(n,a) = 1$, a t as required does always exist). Thus $C_n(a,b)$ and $C_n(1,(tb) \bmod n)$ are Ádám-isomorphic.

If both $\gcd(n,a) = 1$ and $\gcd(n,b) = 1$ hold, the above proposition applies twice, yielding two graphs $C_n(1,x)$ and $C_n(y,1)$, with suitable x and y, both isomorphic to $C_n(a,b)$.

Proposition 2.2 can be easily generalized into the following one:

Proposition 2.3. *Let n, a verify $\gcd\left(n, \frac{a}{\gcd(n,a)}\right) = 1$, and let t be an integer s.t. $(ta) \bmod n = \gcd(n,a)$. Then, $C_n(a,b)$ and $C_n(\gcd(n,a),(tb) \bmod n)$ are isomorphic.*

This proposition, too, is an application of Ádám's isomorphism with $\mu = t$, as $\gcd\left(n, \frac{a}{\gcd(n,a)}\right) = 1$ and $(ta) \bmod n = \gcd(n,a)$ imply $\gcd(n,t) = 1$. Like above, we notice that $\gcd\left(n, \frac{a}{\gcd(n,a)}\right) = 1$ implies that such a t does always exist, and $C_n(a,b)$ and $C_n(\gcd(n,a),(tb) \bmod n)$ turn out to be Ádám-isomorphic.

Many authors [10, 15, 22, 28] contributed to prove Ádám's conjecture for two circulant graphs $C_n(a,b)$ and $C_n(a',b')$ (see Section 1.1):

Theorem 2.4. [10, 15, 22, 28] *Two (directed or undirected, 3- or 4-regular) circulant graphs $C_n(a,b)$ and $C_n(a',b')$ are isomorphic if and only if they are Ádám-isomorphic.*

From now on, we shall limit ourselves to consider connected circulant graphs, that is $C_n(a,b)$'s verifying $\gcd(n,a,b) = 1$. This hypothesis allows us for writing $n = H \gcd(n,a) \gcd(n,b)$, where $H \in \mathbb{Z}^+$.

3 Cycles and matrices

In the present section we first describe the infinite matrix $M_n^*(a,b)$ associated to graph $C_n(a,b)$, then we focus on a submatrix of it, the representative matrix $M_n(a,b)$, which will be used to prove the isomorphism condition. To this extent, it is important to preliminarily investigate the structure of some peculiar cycles of a connected $C_n(a,b)$.

3.1 Cycles on $C_n(a,b)$

Consider an arbitrary $C_n(a,b) = (V,E)$. We say that $v_x, v_y \in V$ are *a-adjacent* and that $(v_x, v_y) \in E$ is an *a-edge* if $(x \pm a) \bmod n = y$; similarly,

we say that v_x, v_y are *b-adjacent* and that $(v_x, v_y) \in E$ is a *b-edge* if $(x \pm b) \bmod n = y$.

Let us focus on parameter a only (similar results will hold for b). The graph $C_n(a)$ induced by the whole set of a-edges has $\gcd(n, a)$ connected components, each of which is an *a-cycle* on $\frac{n}{\gcd(n,a)}$ vertices. This means that if $\gcd(n, a) = 1$, there is a unique a-cycle which visits all the vertices of $C_n(a, b)$. The a-cycles of $C_n(a, b)$ have the following property.

Lemma 3.1. *Consider an arbitrary a-cycle of $C_n(a, b)$, say A. Then each pair of vertices $v_x, v_y \in A$ verifies $x \equiv y \pmod{\gcd(n, a)}$.*

Proof. Since $v_x, v_y \in A$, there is a path from v_x to v_y with k a-edges. Thus, $y \equiv x + ka \pmod{n}$. Therefore, $y \bmod \gcd(n, a) = \big(x \bmod \gcd(n, a) + (ka) \bmod \gcd(n, a)\big) \bmod \gcd(n, a) = x \bmod \gcd(n, a)$, that is to say, $x \equiv y \pmod{\gcd(n, a)}$, as claimed. □

For example: consider $C_{42}(9, 10)$ and one of its $\gcd(42, 9) = 3$ a-cycles, whose vertices are $v_1, v_{10}, v_{19}, \ldots, v_{25}, v_{34}$, then $1 \equiv 10 \equiv 19 \equiv \cdots \equiv 34 \pmod 3$.

By what above, we define A_t as the (unique) a-cycle such that every vertex v_x in it verifies $x \equiv t \pmod{\gcd(n, a)}$, for $t = 0, \ldots, \gcd(n, a) - 1$. Clearly, $v_0 \in A_0$, $v_1 \in A_1$, $\ldots$, $v_{\gcd(n,a)-1} \in A_{\gcd(n,a)-1}$, and the indices of all the vertices in A_0 are multiples of $\gcd(n, a)$, and vice versa. As an example, consider $C_{42}(9, 10)$, which has $\gcd(42, 9) = 3$ a-cycles; the vertex set of A_0 is $\{v_0, v_9, v_{18}, \ldots, v_{24}, v_{33}\}$, the vertex set of A_1 is $\{v_1, v_{10}, v_{19}, \ldots, v_{25}, v_{34}\}$, and the vertex set of A_2 is $\{v_2, v_{11}, v_{20}, \ldots, v_{26}, v_{35}\}$.

Similar results hold if we substitute a with b in all the above conditions: in the sequel, B_t will denote the b-cycle whose arbitrary vertex v_x verifies $x \equiv t \pmod{\gcd(n, b)}$, for $t = 0, \ldots, \gcd(n, b) - 1$.

3.2 Matrix $M_n^*(a, b)$

$M_n^*(a, b)$ is a matrix with an infinite number of rows and columns, and can be correctly defined for any connected circulant graph $C_n(a, b)$: the value of an element is the index of the corresponding vertex (see Fig. 2). Every vertex of the graph is represented by infinitely many (regularly placed) elements of $M_n^*(a, b)$. Consider element $m_{i,j}^*$ corresponding to vertex v_x. Then, elements $m_{i,j-1}^*$, $m_{i,j+1}^*$ correspond to vertices $v_{(x-a) \bmod n}$, $v_{(x+a) \bmod n}$, respectively, which are both a-adjacent to v_x, and elements $m_{i-1,j}^*$, $m_{i+1,j}^*$ correspond to vertices $v_{(x-b) \bmod n}$, $v_{(x+b) \bmod n}$, respectively, which are both b-adjacent to v_x. The definition of a- and b-adjacency is extended to matrix elements. A similar structure is defined in [4, 6, 16, 30].

Consider $M_n^*(x, y)$ and notice that parameter x, the first into brackets, is associated by definition to the rows of $M_n^*(x, y)$, while y, the second one, is associated to the columns of $M_n^*(x, y)$. Thus the representative matrices $M_n^*(a, b)$ and $M_n^*(b, a)$ of two isomorphic graphs $C_n(a, b)$ and $C_n(b, a)$ are the transposes of each other.

34	1	4	7	10	13	16	19	22	25	28	31	34	1	4	7
6	9	12	15	18	21	24	27	30	33	0	3	6	9	12	15
14	17	20	23	26	29	32	35	2	5	8	11	14	17	20	23
22	25	28	31	34	1	4	7	10	13	16	19	22	25	28	31
30	33	0	3	6	9	12	15	18	21	24	27	30	33	0	3
2	5	8	11	14	17	20	23	26	29	32	35	2	5	8	11
10	13	16	19	22	25	28	31	34	1	4	7	10	13	16	19
18	21	24	27	30	33	0	3	6	9	12	15	18	21	24	27
26	29	32	35	2	5	8	11	14	17	20	23	26	29	32	35
34	1	4	7	10	13	16	19	22	25	28	31	34	1	4	7
6	9	12	15	18	21	24	27	30	33	0	3	6	9	12	15

Figure 2: Part of the infinite matrix $M_{36}^*(3, 8)$.

3.3 Matrix $M_n(a, b)$

The *representative matrix* $M_n(a, b)$ is a rectangular submatrix of consecutive rows and columns of $M_n^*(a, b)$, with the property that all the vertices are represented exactly once (thus it has n elements). It is defined on $R = \gcd(n, a)$ rows and $C = \frac{n}{R}$ columns. The elements $m_{i,j}$ of $M_n(a, b)$ are in one-to-one correspondence with the vertices of $C_n(a, b)$. Without loss of generality, vertex v_0 matches to element $m_{0,0}$ in the upper left corner of $M_n(a, b)$. Thus an arbitrary element $m_{i,j}$ corresponds to vertex v_x where $x = (ib + ja) \bmod n$ for $i = 0, \ldots, R - 1$, and $j = 0, \ldots, C - 1$ (see matrix $M_{36}(3, 8)$ in Fig. 3). Observe that $M_n(a, b)$ repeats itself periodically in the infinite matrix $M_n^*(a, b)$.

Since $M_n(a, b)$ is a submatrix of $M_n^*(a, b)$, two consecutive elements of a row are a-adjacent, and two consecutive elements of a column are b-adjacent. Clearly, also the first and last elements of a same row correspond to a-adjacent vertices. This property allows for saying that there is a one-to-one correspondence between rows of $M_n(a, b)$ and a-cycles. Precisely, the i-th row of the matrix, for $i = 0, \ldots, R - 1$, corresponds to a-cycle A_{ρ_i} with $\rho_i = (ib) \bmod R$.

On the contrary, no one-to-one correspondence can be set between the columns of $M_n(a, b)$ and the b-cycles, generally speaking. It depends on the number R of rows of $M_n(a, b)$ and on the number $\frac{n}{\gcd(n,b)}$ of vertices in a b-cycle, respectively. Two cases arise: $R = \frac{n}{\gcd(n,b)}$, or $R < \frac{n}{\gcd(n,b)}$ (it

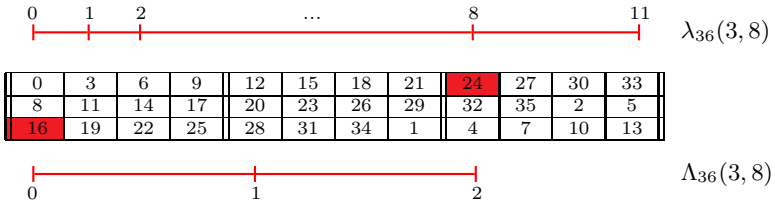

Figure 3: Matrix $M_{36}(3,8)$; highlighted the elements $m_{R-1,h} = m_{2,0}$ and $m_{0,(h+\lambda_{36}(3,8)) \bmod C} = m_{0,8}$, showing that $\lambda_{36}(3,8) = 8$. The blocks are separated by double lines, resulting in $\Lambda_{36}(3,8) = \frac{\lambda_{36}(3,8)}{\gcd(n,b)} = \frac{8}{4} = 2$.

clearly never happens that $R > \frac{n}{\gcd(n,b)}$). In the first case such a one-to-one correspondence exists: reasoning as above we can prove that the first and last elements of a same column correspond to b-adjacent vertices, that the j-th column of the matrix, for $j = 0, \ldots, C-1$, corresponds to b-cycle $B_{(ja) \bmod C}$. In the second case, that is when $R < \frac{n}{\gcd(n,b)}$, the number R of elements in a column of $M_n(a,b)$ is not sufficient to contain all the $\frac{n}{\gcd(n,b)}$ vertices of a b-cycle. However, it can be proved that

Lemma 3.2. *Consider an arbitrary element $m_{R-1,h}$ in the last row of $M_n(a,b)$ and let v_x be the corresponding vertex. Then, the graph $C_n(a,b)$ admits a unique integer constant $0 \leq \lambda_n(a,b) \leq C-1$, called* column-jump*, satisfying*

$$\gcd(n,a)b \equiv \lambda_n(a,b)a \pmod{n} \tag{1}$$

such that v_{x+b} corresponds to element $m_{0,(h+\lambda_n(a,b)) \bmod C}$ of $M_n(a,b)$.

Proof. Recalling that the last row of $M_n(a,b)$ corresponds to a-cycle A_t where $t = \big((R-1)b\big) \bmod R$, x verifies $x \equiv (R-1)b \pmod{R}$. Two are the vertices b-adjacent to v_x, namely, $v_{(x-b) \bmod n}$ and $v_{(x+b) \bmod n}$. The first one corresponds to element $m_{R-2,h}$, by definition. We claim that the other one belongs to row zero of $M_n(a,b)$. Since the vertices corresponding to the elements in row zero of $M_n(a,b)$ are all and only those belonging to a-cycle A_0, their indices are multiples of R (0 included). Thus, we have to show that $x + b \equiv 0 \pmod{R}$. The following equalities hold: $x + b \equiv x \bmod R + b \bmod R \equiv \big((R-1)b\big) \bmod R + b \bmod R \equiv (-b) \bmod R + b \bmod R \equiv 0 \pmod{R}$, as claimed.

It remains to show that v_{x+b} is found in column $h + \lambda_n(a,b)$. Consider the path $P = \{v_x, v_{x-b}, v_{x-2b}, \ldots, v_{x-(R-1)b}, v_{x-(R-1)b+a}, v_{x-(R-1)b+2a}, \ldots, v_{x-(R-1)b+\lambda_n(a,b)a}\}$ (all arithmetic is done modulo n) connecting v_x and v_{x+b} (thus $P \not\ni (v_x, v_{x+b})$), which contains $R-1$ b-edges and $\lambda_n(a,b)$ a-edges. The endpoints of P are b-adjacent iff $x-(R-1)b+\lambda_n(a,b)a \equiv x+b$

(mod n), that is iff $\gcd(n,a)b \equiv \lambda_n(a,b)a \pmod{n}$. Since this congruence does not depend on x and a, b are coprime, there exists a unique solution $0 \leq \lambda_n(a,b) \leq C-1$, and the thesis follows. □

Generally speaking, $\lambda_n(a,b) \neq \lambda_n(b,a)$. Moreover, it is easy to see that $\lambda_n(-a,b) = C - \lambda_n(a,b)$, and that $\lambda_n(a,-b) = C - \lambda_n(a,b)$, while, clearly, $\lambda_n(-a,-b) = \lambda_n(a,b)$. In other words, considering either $-a$ or $-b$, that is, complementing either one among a or b w.r.t. n, has the effect of complementing the column-jump w.r.t. C.

Equivalence (1) (also defined in [4, 6, 16, 30]) can be interpreted on the graph as follows. Refer to path P defined in the proof above. Vertices $v_{x-(R-1)b}$ and v_{x+b} are connected, among the others, by a path made of $\lambda_n(a,b)$ a-edges and by a path made of $\gcd(n,a)$ b-edges. Thus, Equivalence (1) describes the way a-cycles and b-cycles are "linked", in a topological sense (see Fig. 4).

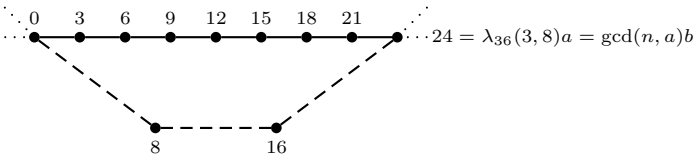

Figure 4: The parameter $\lambda_{36}(3,8)$: a measure of the way a- and b-cycles are linked in $C_{36}(3,8)$. Solid lines represent a-edges, while dashed lines represent b-edges.

The above lemma also shows that the $\frac{n}{\gcd(n,b)}$ vertices of each b-cycle are split onto $\frac{n/\gcd(n,b)}{R} = \frac{n}{\gcd(n,a)\gcd(n,b)} = H$ columns. Example: consider $C_{36}(3,8)$ and one of its four b-cycles, say B_0, whose vertices are v_0, v_8, v_{16}, v_{24}, v_{32}, v_4, v_{12}, v_{20}, v_{28}, the first three of which are found in the first column of $M_{36}(3,8)$, the second three of which are in the ninth column, and the remaining three of which are in the fifth column, as $H = 3$ (see Fig. 3). Notice that $\lambda_n(a,b) = 0$ if and only if the b-cycles are in one-to-one correspondence with the columns of $M_n(a,b)$ (this is to say, if and only if $n = \gcd(n,a)\gcd(n,b)$, or equivalently if and only if $H = 1$).

As a consequence, $M_n(a,b)$ can be partitioned into $H = \frac{n}{\gcd(n,a)\gcd(n,b)}$ equally sized submatrices, the *blocks*, denoted by $\beta_0, \beta_1, \ldots, \beta_{h-1}$, where block β_k is defined on all the $R = \gcd(n,a)$ rows and the $(k-1)$-th set of $\gcd(n,b)$ consecutive columns. Consider the first set of $\gcd(n,b)$ consecutive columns, that is columns 1 to $\gcd(n,b)$. Each of them contains R consecutive vertices of b-cycles $B_{\gamma_1}, \ldots, B_{\gamma_{\gcd(n,b)}}$, respectively. The

b-cycles $B_{\gamma_1}, \ldots, B_{\gamma_{\gcd(n,b)}}$ then continue in columns $(1+\lambda) \bmod C, \ldots,$ $(\gcd(n,b)+\lambda) \bmod C$, respectively, then in columns $(1+2\lambda) \bmod C, \ldots,$ $(\gcd(n,b)+2\lambda) \bmod C$, respectively, and so on, the last portion of each b-cycle being in columns $\big(1+(H-1)\lambda\big) \bmod C, \ldots, \big(\gcd(n,b)+(H-1)\lambda\big) \bmod C$. After that, b-cycle B_{γ_j} starts again from column j, for $j = 1, \ldots, \gcd(n,b)$, that is $\big(j+(H-1)\lambda+\lambda\big) \bmod C = (j+H\lambda) \bmod C = j$. Hence, $(H\lambda) \bmod C = 0$. Recalling that $H = \frac{n}{\gcd(n,a)\gcd(n,b)}$ and that $C = \frac{n}{\gcd(n,b)}$, we get that λ has to be a multiple of $\gcd(n,b)$. For this reason it is convenient to introduce the definition of block-jump:

Definition 3.3. *The* block-jump *of* $M_n(a,b)$ *is* $\Lambda_n(a,b) = \frac{\lambda_n(a,b)}{\gcd(n,b)}$.

Notice that $\Lambda_n(a,b) \in \{0, \ldots, H-1\}$, by definition, and that Equivalence (1) becomes

$$\gcd(n,a)b \equiv \Lambda_n(a,b)\gcd(n,b)a \pmod{n}. \tag{2}$$

Generally speaking $\Lambda_n(a,b) \neq \Lambda_n(b,a)$. In addition, $\Lambda_n(-a,b) = H - \Lambda_n(a,b)$ and $\Lambda_n(a,-b) = H - \Lambda_n(a,b)$, as $\frac{C}{\gcd(n,b)} = H$, while $\Lambda_n(-a,-b) = \Lambda_n(a,b)$.

4 Isomorphism testing

This section is devoted to describe an easy-to-evaluate necessary and sufficient condition (Theorem 4.1) to solve ISOMORPHISM TESTING, that is to say, to recognize if two given connected circulant graphs $C_n(a,b)$ and $C_n(a',b')$ are isomorphic. In the affirmative, the mapping function is immediately obtained.

Recalling that $\Lambda_n(a,b), \Lambda_n(a',b') \in \{0, \ldots, H-1\}$, and that, if $C_n(x,y)$ is connected, then $\gcd(n,x) = \gcd(n,y)$ implies $\gcd(n,x) = \gcd(n,y) = 1$, we have that:

Theorem 4.1. *Let* $C_n(a,b)$, $C_n(a',b')$ *be two directed* (*undirected, resp.*) *connected graphs, and assume w.l.o.g.* $\gcd(n,a) \leq \gcd(n,b)$ *and* $\gcd(n,a') \leq \gcd(n,b')$. *Then* $C_n(a,b)$, $C_n(a',b')$ *are isomorphic if and only if either one of the following two conditions holds:*

1. $\gcd(n,a) = \gcd(n,a') < \gcd(n,b) = \gcd(n,b')$ *and* $\Lambda_n(a,b) = \Lambda_n(a',b')$ $\big(\Lambda_n(a,b) \equiv \pm\Lambda_n(a',b') \pmod{H}$, *resp.*$\big)$;
2. $\gcd(n,a) = \gcd(n,a') = \gcd(n,b) = \gcd(n,b')$ *and either* $\Lambda_n(a,b) = \Lambda_n(a',b')$ *or* $\Lambda_n(a,b) = \Lambda_n(b',a')$ $\big($*either* $\Lambda_n(a,b) \equiv \pm\Lambda_n(a',b') \pmod{H}$, *or* $\Lambda_n(a,b) \equiv \pm\Lambda_n(b',a') \pmod{H}$, *resp.*$\big)$.

Proof. If part. Consider the matrix $M_n(a,b) = [m_{i,j}]$ defined for the graph $C_n(a,b)$ on $R = \gcd(n,a)$ rows and $C = \frac{n}{\gcd(n,a)}$ columns, and the matrix $M_n(a',b') = [m'_{i,j}]$ defined for the graph $C_n(a',b')$ on $R' = \gcd(n,a')$ rows and $C' = \frac{n}{\gcd(n,a')}$ columns. By hypothesis, it follows that the two matrices have the same size, being defined on the same number of rows and columns, and that, clearly, $H' = H$. In order to prove the claim, it suffices to show that there exists a one-to-one mapping which matches the vertices of $C_n(a,b)$ into those of $C_n(a',b')$.

Let us first consider the case $\Lambda_n(a,b) = \Lambda_n(a',b')$, which holds for both directed and undirected graphs and for both conditions *(1)* and *(2)*. Let $v(m_{i,j})$ denote the vertex associated to element $m_{i,j}$ of $M_n(a,b)$, and $v(m'_{h,k})$ the vertex associated to element $m'_{h,k}$ of $M_n(a',b')$. The required mapping is the one which maps $v(m_{i,j}) = v_{(ib+ja) \bmod n}$ onto the homologous $v(m'_{i,j}) = v_{(ib'+ja') \bmod n}$. It is easy to see that the correct adjacencies are preserved, in the sense that a-edges are biunivocally mapped onto a'-edges, as well as b-edges are biunivocally mapped onto b'-edges. In fact a-edge $\big(v(m_{i,j}), v(m_{i,(j+1) \bmod C})\big)$ is mapped onto the homologous a'-edge $\big(v(m'_{i,j}),\ v(m'_{i,(j+1) \bmod C})\big)$, for all $i = 0, \ldots, R-1$ and for all $j = 0, \ldots, C-1$. As for the b-edges, we distinguish two types: the b-edges connecting an element of the last row with an element of the first row of $M_n(a,b)$, and the other b-edges. A b-edge of the first type, say $\big(v(m_{R-1,j}), v(m_{0,(j+\Lambda_n(a,b)\gcd(n,b)) \bmod C})\big)$, is mapped onto the homologous b'-edge $\big(v(m'_{R-1,j}), v(m'_{0,(j+\Lambda_n(a',b')\gcd(n,b')) \bmod C})\big)$, for $j = 0, \ldots, C-1$, while a b-edge of the second type, say $\big(v(m_{i,j}), v(m_{i+1,j})\big)$, is mapped onto the homologous b'-edge $\big(v(m'_{i,j}), v(m'_{i+1,j})\big)$, for $i = 0, \ldots, R-2$ and $j = 0, \ldots, C-1$.

Now consider $\Lambda_n(a,b) = \Lambda_n(b',a')$, which holds for both directed and undirected graphs, for condition *(2)*, only. In this case it suffices to swap a' and b', and the above proof applies.

Now consider $\Lambda_n(a,b) \equiv -\Lambda_n(a',b') \pmod H$, which applies to the undirected case, only, for both conditions *(1)* and *(2)*. Consider either one among $C_n(-a',b')$ and $C_n(a',-b')$, say $C_n(-a',b')$: its block-jump has value $\Lambda_n(-a',b') = H - \Lambda_n(a',b') = \Lambda_n(a,b)$, as observed after Definition 3.3. Since $\Lambda_n(-a',b') = \Lambda_n(a,b)$, we are back to the previous case and $C_n(-a',b')$ and $C_n(a,b)$ are isomorphic. Since $C_n(-a',b')$ and $C_n(a',b')$ identify the same undirected graph, $C_n(a,b)$ and $C_n(a',b')$ are isomorphic too, as claimed.

Finally consider $\Lambda_n(a,b) \equiv -\Lambda_n(b',a') \pmod H$, which holds in the undirected case of condition *(2)*, only. Again, swap a' and b', and the above proof applies.

Only if part. Assume that $C_n(a,b)$ and $C_n(a',b')$ are isomorphic. Consider the subgraphs $C_n(a)$, $C_n(b)$, $C_n(a')$, and $C_n(b')$ induced by all the a-edges,

all the b-edges, all the a'-edges, and all the b'-edges, respectively. By Theorem 2.4 since $C_n(a,b)$ and $C_n(a',b')$ are isomorphic, $C_n(a)$ and $C_n(a')$ also are, as well as $C_n(b)$ and $C_n(b')$. Recall that $C_n(a)$ consists of $\gcd(n,a)$ cycles of $\frac{n}{\gcd(n,a)}$ vertices, $C_n(b)$ consists of $\gcd(n,b)$ cycles of $\frac{n}{\gcd(n,b)}$ vertices, $C_n(a')$ consists of $\gcd(n,a')$ cycles of $\frac{n}{\gcd(n,a')}$ vertices, and $C_n(b')$ of $\gcd(n,b')$ cycles of $\frac{n}{\gcd(n,b')}$ vertices. Since we assumed w.l.o.g. that $\gcd(n,a) \leq \gcd(n,b)$ and $\gcd(n,a') \leq \gcd(n,b')$, two cases may happen: either $\gcd(n,a) = \gcd(n,a') < \gcd(n,b) = \gcd(n,b')$ or $\gcd(n,a) = \gcd(n,a') = \gcd(n,b) = \gcd(n,b')$.

If $\gcd(n,a) = \gcd(n,a') < \gcd(n,b) = \gcd(n,b')$, it remains to show that $\Lambda_n(a',b') = \Lambda_n(a,b)$ in the directed case, and that $\Lambda_n(a',b') \equiv \pm\Lambda_n(a,b) \pmod H$ in the undirected case. Since $C_n(a,b)$ and $C_n(a',b')$ are isomorphic, there exists a one-to-one mapping f which associates vertex v_i of $C_n(a,b)$ to vertex $v_{f(i)}$ of $C_n(a',b')$. The mapping f must verify $f(i+a) \equiv f(i) + a' \pmod n$ and $f(i+b) \equiv f(i) + b' \pmod n$ in the directed case, while it must verify either $f(i+a) \equiv f(i)+a' \pmod n$ or $f(i+a) \equiv f(i)-a' \pmod n$, as well as either $f(i+b) \equiv f(i)+b' \pmod n$ or $f(i+b) \equiv f(i)-b' \pmod n$ in the undirected case. For the sake of shortness, we resume these conditions by improperly writing $f(i+a) \equiv f(i) \pm a' \pmod n$ and $f(i+b) \equiv f(i) \pm b' \pmod n$, meaning that the "minus" applies to the undirected case, only. By definition of $\Lambda_n(a,b)$, $b\gcd(n,a) \equiv \Lambda_n(a,b)a\gcd(n,b) \pmod n$. Thus $f(b\gcd(n,a)) \equiv f(\Lambda_n(a,b)a\gcd(n,b)) \pmod n$. By repeatedly applying $f(i+a) \equiv f(i) \pm a' \pmod n$ and $f(i+b) \equiv f(i) \pm b' \pmod n$, we get $f(b\gcd(n,a)) \equiv \pm b'\gcd(n,a) \pmod n$ and $f(\Lambda_n(a,b)a\gcd(n,b)) \equiv \pm\Lambda_n(a,b)a'\gcd(n,b) \pmod n$. Recalling the definition of $\Lambda_n(a',b')$ we can write $\Lambda_n(a',b')a'\gcd(n,b') \equiv b'\gcd(n,a') \equiv b'\gcd(n,a) \equiv \pm f(b\gcd(n,a)) \equiv \pm f(\Lambda_n(a,b)a\gcd(n,b)) \equiv \pm\Lambda_n(a,b)a'\gcd(n,b) \equiv \pm\Lambda_n(a,b)a'\gcd(n,b')$, all the equivalences being modulo n. Since $\frac{a'}{\gcd(n,a')}$ is coprime with H and $n = H\gcd(n,a')\gcd(n,b')$, this finally shows that $\Lambda_n(a',b') \equiv \pm\Lambda_n(a,b) \pmod H$, which reduces to $\Lambda_n(a',b') = \Lambda_n(a,b)$ in the directed case.

If $\gcd(n,a) = \gcd(n,a') = \gcd(n,b) = \gcd(n,b')$ (hence all equal to 1), it remains to show that $\Lambda_n(a',b') = \Lambda_n(a,b)$ or $\Lambda_n(b',a') = \Lambda_n(a,b)$ in the directed case, and that $\Lambda_n(a',b') \equiv \pm\Lambda_n(a,b) \pmod H$ or $\Lambda_n(b',a') \equiv \pm\Lambda_n(a,b) \pmod H$ in the undirected case. The assumptions $\gcd(n,a) \leq \gcd(n,b)$ and $\gcd(n,a') \leq \gcd(n,b')$ do not help, in this case, to associate a with a' and b with b' because $\gcd(n,a)$, $\gcd(n,a')$, $\gcd(n,b)$ and $\gcd(n,b')$ are all equal to 1. That is to say, since $C_n(a)$, $C_n(b)$ are both hamiltonian cycles, as $C_n(a')$, $C_n(b')$ are, two cases may happen: $C_n(a)$ corresponds to $C_n(a')$ (hence $C_n(b)$ to $C_n(b')$) or $C_n(a)$ corresponds to $C_n(b')$ (hence $C_n(b)$ to $C_n(a')$). Therefore we possibly have to swap a' and b'. Having in mind these facts, we can basically apply the proof above, obtaining $\Lambda_n(a',b')a'\gcd(n,b') \equiv \pm\Lambda_n(a,b)a'\gcd(n,b')$, or $\Lambda_n(b',a')b'\gcd(n,a')$

$\equiv \pm\Lambda_n(a,b)b' \gcd(n,a')$, all the equivalences being modulo n. This finally shows that $\Lambda_n(a',b') \equiv \pm\Lambda_n(a,b) \pmod H$ or $\Lambda_n(b',a') \equiv \pm\Lambda_n(a,b) \pmod H$, which reduces to $\Lambda_n(a',b') = \Lambda_n(a,b)$ or $\Lambda_n(b',a') = \Lambda_n(a,b)$ in the directed case, only. □

The computational complexity of applying this theorem depends on the complexity of computing the four gcd's and that of twice solving the linear congruence (2) to determine the two block-jumps. This can be done in $O(\log n)$ elementary operations, by Euclid's algorithm [9] (in an arithmetic complexity model).

The mapping function between two isomorphic $C_n(a,b)$ and $C_n(a',b')$ can be constructed in linear time as follows. We shall build a one-to-one correspondence between homologous elements of the matrices associated to $C_n(a,b)$ and $C_n(a',b')$. The matrix associated to $C_n(a,b)$ is always $M_n(a,b)$, while the matrix associated to $C_n(a',b')$ is either one among $M_n(a',b')$, $M_n(-a',b')$, $M_n(b',a')$, $M_n(-b',a')$, depending on the value of the gcd's and of the block-jumps, as in the proof of the above theorem.

Consider the case $\gcd(n,a) = \gcd(n,a') < \gcd(n,b) = \gcd(n,b')$ first.

If $\Lambda_n(a,b) = \Lambda'_n(a',b')$, vertex $v(m_{i,j}) = v_{(jb+ia) \bmod n}$, associated to element $m_{i,j}$ of $M_n(a,b)$, is mapped onto the homologous vertex $v(m'_{i,j}) = v_{(jb'+ia') \bmod n}$, associated to element $m'_{i,j}$ of $M_n(a',b')$. As an example consider $C_{36}(3,8)$ and $C_{36}(15,4)$, which verify $\Lambda_{36}(3,8) = \Lambda_{36}(15,4) = 2$, depicted in Fig. 5. The mapping function, for example, maps vertex $v(m_{2,1}) = 19$ of $M_{36}(3,8)$ onto vertex $v(m'_{2,1}) = 23$ of $M_{36}(15,4)$.

On the contrary, if $\Lambda_n(a,b) = H - \Lambda_n(a',b')$, the theorem states that two directed graphs are not isomorphic, while two undirected ones are. In the latter case, the mapping function can be obtained by associating vertex $v(m_{i,j})$, corresponding to element $m_{i,j}$ of $M_n(a,b)$, to vertex $v(\overline{m}_{i,j}) = v_{(jb'-ia') \bmod n}$, corresponding to element $\overline{m}_{i,j}$ of $M_n(-a',b')$, as $\Lambda_n(-a',b') = \Lambda_n(a,b)$. As an example, consider the undirected $C_{36}(3,8)$ and the undirected $C_{36}(21,4)$, which verify $\Lambda_{36}(21,4) = H - \Lambda_{36}(3,8)$. Since $C_{36}(-21,4) = C_{36}(15,4)$, $\Lambda_{36}(3,8) = \Lambda_{36}(15,4)$. Thus the mapping function between $C_{36}(3,8)$ and $C_{36}(21,4)$ is the same which maps elements of $M_{36}(3,8)$ onto homologous elements of $M_{36}(15,4)$.

Now consider the remaining case $\gcd(n,a) = \gcd(n,a') = \gcd(n,b) = \gcd(n,b')$ (thus all equal to 1), observing that the representative matrices have one row, only.

If $\Lambda_n(a,b) = \Lambda_n(a',b')$, vertex $v(m_{0,j})$ of $M_n(a,b)$ is mapped onto the homologous vertex $v(m'_{0,j})$ of $M_n(a',b')$, while if $\Lambda_n(a,b) = \Lambda_n(b',a')$, vertex $v(m_{0,j})$ of $M_n(a,b)$ is mapped onto the vertex associated to the (homologous) element in column j of $M_n(b',a')$.

If $\Lambda_n(a,b) = H - \Lambda_n(a',b')$, the theorem states that two directed graphs are not isomorphic, while two undirected ones are. In the lat-

ter case, the mapping function can be obtained by associating vertices corresponding to homologous elements of $M_n(-a', b')$ and $M_n(a, b)$, as $\Lambda_n(-a', b') = \Lambda_n(a, b)$. Finally, if $\Lambda_n(a, b) = H - \Lambda_n(b', a')$, only undirected graphs can be considered, and the mapping function can be obtained by associating vertices corresponding to homologous elements of $M_n(-b', a')$ and $M_n(a, b)$, as $\Lambda_n(-b', a') = \Lambda_n(a, b)$.

$\lambda_{36}(3, 8) = \lambda_{36}(15, 4)$

0	3	6	9	12	15	18	21	24	27	30	33
8	11	14	17	20	23	26	29	32	35	2	5
16	19	22	25	28	31	34	1	4	7	10	13

0	15	30	9	24	3	18	33	12	27	6	21
4	19	34	13	28	7	22	1	16	31	10	25
8	23	2	17	32	11	26	5	20	35	14	29

Figure 5: The representative matrices of the two isomorphic graphs $C_{36}(3, 8)$ and $C_{36}(15, 4)$.

5 Mutually isomorphic graphs

In this section we study the properties of the family of mutually isomorphic graphs.

Consider a directed circulant graph $C_n(a, b)$ such that $\gcd(n, a) < \gcd(n, b)$, and let Λ denote $\Lambda_n(a, b)$ throughout the present section. According to Theorem 4.1, any $C_n(a', b')$ isomorphic to $C_n(a, b)$ verifies $\gcd(n, a') = \gcd(n, a)$, $\gcd(n, b') = \gcd(n, b)$, and $\Lambda = \Lambda_n(a', b')$.

The first two conditions show that a' has to be a multiple of $\gcd(n, a)$ and b' a multiple of $\gcd(n, b')$. Recalling that $n = H \gcd(n, a) \gcd(n, b)$, these conditions also show that a' must not be a multiple of H nor of $\gcd(n, b)$, as well as b' must not be a multiple of H nor of $\gcd(n, a)$. Define $\mathcal{A} = \{\bar{a} = \bar{k}_a \gcd(n, a) : \bar{k}_a = 1, \ldots, \frac{n}{\gcd(n,a)} \text{ and } \gcd(\bar{k}_a, H \gcd(n, b)) = 1\}$ and

$\mathcal{B} = \{\bar{b} = \bar{k}_b \gcd(n, b) : \bar{k}_b = 1, \ldots, \frac{n}{\gcd(n,b)} \text{ and } \gcd(\bar{k}_b, H \gcd(n, a)) = 1\}$.

A necessary condition for $C_n(a', b')$ to be isomorphic to $C_n(a, b)$ is that $(a', b') \in \mathcal{A} \times \mathcal{B}$.

Now consider the partition of $\mathcal{A}$ into $H-1$ subsets $\mathcal{A}^h$, for $h = 1, \ldots, H-1$, where $\mathcal{A}^h$ is defined as follows

$$\begin{aligned} \mathcal{A}^h &= \{\bar{a} \in \mathcal{A} : \tfrac{\bar{a}}{\gcd(n,a)} \bmod H = c\} = \\ &= \{\bar{a} \in \mathcal{A} : \bar{k}_a = \bar{k}'_a H + h, \bar{k}'_a = 0, \ldots, \gcd(n, b) - 1\}. \end{aligned}$$

We do the same with $\mathcal{B}$ obtaining, a partition into the following subsets $\mathcal{B}^h$ for $h = 1, \ldots, H-1$

$$\begin{aligned}\mathcal{B}^h &= \{\bar{b} \in \mathcal{B} : \tfrac{\bar{b}}{\gcd(n,\bar{b})} \bmod H = c\} = \\ &= \{\bar{b} \in \mathcal{B} : \bar{k}_b = \bar{k}'_b H + h, \bar{k}'_b = 0, \ldots, \gcd(n,a) - 1\}.\end{aligned}$$

The interest in these subsets is justified by the following reasoning. Consider an arbitrary $\bar{a} = (\bar{k}'_a H + h)\gcd(n,a) \in \mathcal{A}^h$ and call

$$N(\bar{a}) = \{\bar{b} : C_n(\bar{a}, \bar{b}) \text{ is isomorphic to } C_n(a,b)\} \subseteq \mathcal{B}.$$

In application of Theorem 4.1, recalling the definition of Λ, and recalling that $n = H\gcd(n,a)\gcd(n,b)$, $\gcd(n,\bar{a}) = \gcd(n,a)$, and $\gcd(n,\bar{b}) = \gcd(n,b)$, we get

$$\begin{aligned}N(\bar{a}) &= \{\bar{b} : \gcd(n,\bar{a})\bar{b} = \Lambda\gcd(n,\bar{b})\bar{a} \pmod n\} = \\ &= \{\bar{b} : \tfrac{\bar{b}}{\gcd(n,\bar{b})} = \Lambda(\bar{k}'_a H + h) \pmod H\} = \\ &= \{\bar{b} : \bar{b} = h\Lambda \pmod H\} = \\ &= \mathcal{B}^{h\Lambda}\end{aligned}$$

which shows that $N(\bar{a})$ depends on h, that is on the fact that $\bar{a} \in \mathcal{A}^h$, and not on the value of $\bar{a}$ itself. Thus we better write $N(\mathcal{A}^h)$ instead of $N(\bar{a})$, obtaining

$$N(\mathcal{A}^h) = \mathcal{B}^{h\Lambda} \quad \text{for } h = 1, \ldots, H-1.$$

Similarly, it can be proved that

$$N(\mathcal{B}^{h\Lambda}) = \mathcal{A}^h, \text{ for } h = 1, \ldots, H-1.$$

Define $\mathcal{A}^s \times \mathcal{B}^t = \{(\bar{a}, \bar{b}) : \bar{a} \in \mathcal{A}^s, \bar{b} \in \mathcal{B}^t\}$, we conclude stating that $C_n(a',b')$ is isomorphic to a directed $C_n(a,b)$ with $\gcd(n,a) < \gcd(n,b)$ if and only if

$$(a',b') \in \bigcup_{h=1}^{H-1} \mathcal{A}^h \times \mathcal{B}^{h\Lambda \bmod H}.$$

The "h" in this formula highlights the role of Theorem 2.4, while "Λ" highlights the role of Theorem 4.1.

Similar results can be derived for directed circulant graphs $C_n(a,b)$ with $\gcd(n,a) = \gcd(n,b)$, and for undirected graphs with $\gcd(n,a) < \gcd(n,b)$ or $\gcd(n,a) = \gcd(n,b)$. We get:

Theorem 5.1. *A directed $C_n(a',b')$ is isomorphic to a directed $C_n(a,b)$ with $\gcd(n,a) < \gcd(n,b)$ ($\gcd(n,a) = \gcd(n,b)$, resp.) if and only if*

$$(a',b') \in \textstyle\bigcup_{h=1}^{H-1} \mathcal{A}^h \times \mathcal{B}^{h\Lambda \bmod H}$$

$$\left((a',b') \in \bigcup_{h=1}^{H-1} \left(\mathcal{A}^h \times \mathcal{B}^{h\Lambda \bmod H} \cup \mathcal{A}^h \times \mathcal{B}^{h\Lambda_n(b,a) \bmod H} \right),\ resp. \right)$$

An undirected $C_n(a',b')$ *is isomorphic to an undirected* $C_n(a,b)$ *with* $\gcd(n,a) < \gcd(n,b)$ $\left(\ \gcd(n,a) = \gcd(n,b),\ resp.\ \right)$ *if and only if*

$$(a',b') \in \bigcup_{h=1}^{H-1} \left(\mathcal{A}^h \times \mathcal{B}^{h\Lambda \bmod H} \cup \mathcal{A}^h \times \mathcal{B}^{(-h\Lambda) \bmod H} \right)$$

$$\left((a',b') \in \begin{array}{l} \bigcup_{h=1}^{H-1} \left(\mathcal{A}^h \times \mathcal{B}^{h\Lambda \bmod H} \cup \mathcal{A}^h \times \mathcal{B}^{(-h\Lambda) \bmod H} \right) \bigcup \\ \bigcup_{h=1}^{H-1} \left(\mathcal{A}^h \times \mathcal{B}^{h\Lambda_n(b,a) \bmod H} \cup \mathcal{A}^h \times \mathcal{B}^{(-h\Lambda_n(b,a)) \bmod H} \right), resp. \end{array} \right)$$

As a final remark on the structure of mutually isomorphic graphs, we observe what follows.

The sets $\mathcal{A}^h$'s and $\mathcal{B}^h$'s depend on $\gcd(n,a)$, $\gcd(n,b)$ and H, therefore, two graphs with pairwise equal gcd's have identical $\mathcal{A}^h$'s and $\mathcal{B}^h$'s, even if they are not isomorphic.

The value of Λ gives a matching of the sets $\mathcal{A}^h$'s to the sets $\mathcal{B}^h$'s: precisely $\mathcal{A}^h$ is matched to $\mathcal{B}^{h\Lambda \bmod H}$. Such a matching is clearly perfect because Λ is coprime with H.

Thus Theorem 4.1 states that two graphs are isomorphic iff they have identical $\mathcal{A}^h$'s and $\mathcal{B}^h$'s, and these sets are matched "in the same way".

As an example, the directed graphs $C_{42}(2,9)$ and $C_{42}(2,15)$ have the same $\mathcal{A}^h$'s and $\mathcal{B}^h$'s: precisely $\mathcal{A}^1 = \{2,16\}$, $\mathcal{A}^2 = \{4,32\}$, $\mathcal{A}^3 = \{20,34\}$, $\mathcal{A}^4 = \{8,22\}$, $\mathcal{A}^5 = \{10,38\}$, $\mathcal{A}^6 = \{26,40\}$, and $\mathcal{B}^1 = \{3\}$, $\mathcal{B}^2 = \{27\}$, $\mathcal{B}^3 = \{9\}$, $\mathcal{B}^4 = \{33\}$, $\mathcal{B}^5 = \{15\}$, $\mathcal{B}^6 = \{39\}$. Since $\Lambda_{42}(2,9) = 3$, an arbitrary $C_n(a',b')$ is isomorphic to $C_{42}(2,9)$ if and only if $(a',b') \in \bigcup_{h=1}^{6} \mathcal{A}^h \times \mathcal{B}^{3h \bmod 7} = \{(2,9),\ (16,9),\ (4,39),\ (32,39),\ (20,27),\ (34,27),\ (8,15),\ (22,15),\ (10,3),\ (38,3),\ (26,33),\ (40,33)\}$. This shows that $C_{42}(2,15)$ is not isomorphic to $C_{42}(2,9)$. In fact, for $C_{42}(2,9)$, $\mathcal{A}^h$ is matched to $\mathcal{B}^{3h \bmod 7}$ as $\Lambda_{42}(2,9) = 3$, while for $C_{42}(2,15)$, $\mathcal{A}^h$ is matched to $\mathcal{B}^{5h \bmod 7}$ as $\Lambda_{42}(2,15) = 5$.

References

[1] A. Ádám. Research problem 2-10. *J. Combinatorial Theory*, 2:393, 1967.

[2] B. Alspach and T. D. Parsons. Isomorphism of circulant graphs and digraphs. *Discrete Mathematics*, 25:97–108, 1979.

[3] L. Barrière, P. Fraigniaud, C. Gavollile, B. Mans, and J.M. Robson. On recognizing Cayley graphs. In *Proceedings of the 8th European Symposium on Algorithms, ESA '00*, volume 1879 of *Lecture Notes in Computer Science*, pages 76–87. Springer-Verlag, Berlin, 2000.

[4] J.C. Bermond, O. Favaron, and M. Maheo. Hamiltonian decomposition of Cayley graphs of degree 4. *J. Combinatorial Theory B*, 46:142–153, 1989.

[5] F. Boesch and R. Tindell. Circulants and their connectivities. *J. Graph Theory*, 8:487–499, 1984.

[6] Y. Chen, F.K. Hwang, I.F. Akyildiz, and D.F. Hsu. Routing algorithms for double loop networks. *Int. J. Foundations Comput. Sci.*, 3:323–331, 1992.

[7] B. Codenotti, I. Gerace, and S. Vigna. Hardness results and spectral techniques for combinatorial problems on circulant graphs. *Linear Algebra and its Applications*, 285:123–142, 1998.

[8] D. Coppersmith, N. Howgrave-Graham, P.Q. Nguyên, and I. Shparlinski. Testing set proportionality and the Ádám isomorphism of circulant graphs. *J. of Discrete Algorithms*, 4:324–335, 2006.

[9] T.H. Cormen, C.E. Leiserson, R.L. Rivest, and C. Stein. *Introduction to Algorithms, Second Edition.* McGraw Hill, 2001.

[10] C. Delorme, O. Favaron, and M. Maheo. Isomorphisms of Cayley multigraphs of degree 4 on finite abelian groups. *European J. of Combinatorics*, 13:59–61, 1992.

[11] E. Dobson and J. Morris. Toida's conjecture is true. *Electronic J. Combinatorics*, 9(#R35), 2002.

[12] B. Elspas and J. Turner. Graphs with circulant adjacency matrices. *J. Combinatorial Theory*, 9:297–307, 1970.

[13] S. Evdokimov and I. Ponomarenko. Circulant graphs: Efficient recognizing and isomorphism testing. In *Proceedings of the 7th International Colloquium on Graph Theory, ICGT '05,* Giens, France, September 12-16, 2005, volume 22 of *Electronic Notes in Discrete Mathematics*, pages 7–12. Elsevier, 2005.

[14] S.A. Evdokimov and I.N. Ponomarenko. Circulant graphs: Recognizing and isomorphism testing in polynomial time. *St. Petersburg Math. J.*, 15:813–835, 2004.

[15] X. Fang and M. Xu. On isomorphisms of Cayley graphs of small valency. *Algebra Colloq.*, 1(1):67–76, 1994.

[16] M.A. Fiol, L.A. Yebra, I. Alegre, and M. Valero. A discrete optimization problem in local networks and data alignment. *IEEE Transactions on Computers*, C-36:702–713, 1987.

[17] F. Göbel and N.A. Neutel. Cyclic graphs. *Discrete Applied Mathematics*, 99:3–12, 2000.

[18] C. Heuberger. On planarity and colorability of circulant graphs. *Discrete Mathematics*, 26:153–169, 2003.

[19] F.K. Hwang. A survey on multi-loop networks. *Theoretical Computer Science*, 299:107–121, 2003.

[20] M.H. Klin and R. Pöschel. "The König Problem, the isomorphism problem for cyclic graphs and the method of Schur Rings", volume 25 of *Colloq. Math. Soc. J. Bolyai*, chapter in *Algebraic Methods in Graph Theory*, pages 405–434. North-Holland, Amsterdam, 1981.

[21] B. Litow and B. Mans. A note on the Ádám conjecture for double loops. *Information Processing Letters*, 66:149–153, 1998.

[22] B. Mans, F. Pappalardi, and I. Shparlinski. On the spectral Ádám property for circulant graphs. *Discrete Mathematics*, 254:309–329, 2002.

[23] M. Muzychuk. Ádám conjecture is true in the square-free case. *J. Combinatorial Theory A*, 72:118–134, 1995.

[24] M. Muzychuk. On Ádám's conjecture for circulant graphs. *Discrete Mathematics*, 176:285–298, 1997.

[25] M. Muzychuk. A solution of the isomorphism problem for circulant graphs. *Proc. London Math. Soc.*, 3(88):1–41, 2004.

[26] A. Nayak, V. Acciaro, and P. Gissi. A note on isomorphic chordal rings. *Information Processing Letters*, 55:339–341, 1995.

[27] P.P. Pálfy. Isomorphism problem for relational structures with a cyclic automorphism. *Europ. J. Combinatorics*, 8:35–43, 1987.

[28] S. Toida. A note on Ádám's conjecture. *J. Combinatorial Theory B*, 23:239–246, 1977.

[29] J. Turner. Point-symmetric graphs with a prime number of points. *J. Combinatorial Theory*, 3:136–145, 1967.

[30] J. Zerovnik and T. Pisanski. Computing the diameter in multiple-loop networks. *J. Algorithms*, 14:226–243, 1993.