ISTITUTO DI ANALISI DEI SISTEMI ED INFORMATICA
"Antonio Ruberti"
CONSIGLIO NAZIONALE DELLE RICERCHE

S. Nicoloso, U. Pietropaoli

ISOMORPHISM TESTING FOR CIRCULANT GRAPHS

R. 664 Giugno 2007

Sara Nicoloso – IASI - CNR, Viale Manzoni 30, 00185 Roma, Italia.
Email: nicoloso@disp.uniroma2.it.

Ugo Pietropaoli – Università di Roma Tor Vergata, Dipartimento di Ingegneria dell'Impresa, Via del Politecnico 1, 00133 Roma, Italia.
Email: pietropaoli@disp.uniroma2.it.

ISSN: 1128–3378

Collana dei Rapporti dell'Istituto di Analisi dei Sistemi ed Informatica "Antonio Ruberti", CNR

viale Manzoni 30, 00185 ROMA, Italy

tel. ++39-06-77161
fax ++39-06-7716461
email: iasi@iasi.rm.cnr.it
URL: http://www.iasi.rm.cnr.it

Abstract

In this paper we focus on connected directed/undirected circulant graphs $C_n(a, b)$. We investigate some topological characteristics of the graphs, and define a simple combinatorial model for them, which is new for the topic. Building on such a model, we derive a necessary and sufficient condition to test, in $O(\log^2 n)$ time, 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. As a by-product we get an alternative proof of the validity of Ádám's conjecture on all the $C_n(a, b)$'s. In addition, simple methods are proposed for computing the positive integer that, given two isomorphic circulant graphs, "transforms" one of them into the other one, and for generating all the circulant graphs isomorphic to a given one.

Key words: isomorphism, circulant graphs, 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*. 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*. Examples are drawn in Fig. 1. 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.

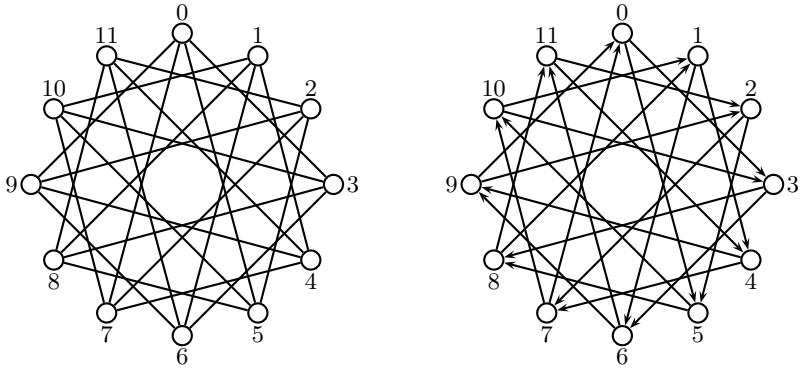

Figure 1: On the left, the undirected circulant graph $C_{12}(3,5)$ (thus also $C_{12}(9,5)$, $C_{12}(3,7)$, $C_{12}(9,7)$, $C_{12}(5,3)$, $C_{12}(5,9)$, $C_{12}(7,3)$, and $C_{12}(7,9)$). On the right, the directed circulant graph $C_{12}(3,5)$ (thus also $C_{12}(5,3)$).

W.l.o.g. we shall always 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, while 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 definition of E shows that $C_n(a,b)$ and $C_n(b,a)$ identify the same graph, both in the directed and in the undirected case; while $C_n(a,b)$, $C_n(-a,b)$, $C_n(a,-b)$, $C_n(-a,-b)$, $C_n(b,a)$, $C_n(b,-a)$, $C_n(-b,a)$, $C_n(-b,-a)$ identify the same graph in the undirected case, only.

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 $k = 2$ (we denote by a, b the two parameters a_1, a_2). 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 [15, 36, 37]. 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 $a_1 = 1$ [24, 35, 39]. Circulant graphs $C_n(1,b)$ are called double loops [21, 28, 30], cyclic graphs [21], or 2-jumps [8].

In this paper we investigate on 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 in $O(\log^2 n)$ time. The method derives from basic topological properties of circulant graphs $C_n(a, b)$'s: the necessary and sufficient condition of 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. It also allows for building the mapping function in linear time. The overall complexity compares favourably with the known results on the $C_n(a_1, a_2, \ldots, a_k)$'s [10, 16, 17, 33, 38] (see Section 1.1). It is worth observing that, as a by-product of Theorem 4.1, one gets an alternative proof, based on elementary concepts, of the validity of *Ádám's conjecture* (stated in Section 1.1 and already proved by [13, 18, 30, 37]), for all directed and undirected connected (3- or 4-regular) $C_n(a, b)$'s.

We also deal with the problem of finding the positive integer μ that "transforms" a given $C_n(a, b)$ into a given isomorphic $C_n(a', b')$ (its existence is implied by Theorem 2.4), stated as follows:

μ-SEARCH

Given	two directed (undirected, resp.) isomorphic connected circulant graphs $C_n(a, b)$ and $C_n(a', b')$
Find	an integer $\mu \in \{1, \ldots, n-1\}$
Such That	$\{a', b'\} \equiv \{\mu a, \mu b\} \pmod n$ ($\{a', b'\} \equiv \{\pm\mu a, \pm\mu b\} \pmod n$, resp.).

The last problem we face was suggested in [35] for the graphs $C_n(1, a_2, \ldots, a_k)$, and is defined as follows:

ALL-ISO

Given	a connected circulant graph $C_n(a, b)$
Find	all the graphs isomorphic to it.

An immediate application of Theorem 2.4 allows for solving this problem. In this paper an alternative algorithm is discussed.

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 the related problems μ-SEARCH and ALL-ISO are solved; Section 6 concludes.

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 [10, 38] for n prime, while, for arbitrary n, it is shown to be polynomial-time solvable in [16, 17] and solved in $O(n^2)$ in [33].

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 [11]. It is also proved to be equivalent to testing for a *colour-preserving isomorphism* on circulant graphs whose arbitrary edge $(v_i, v_{(i+a_t) \bmod n})$ has colour a_t [5].

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 [15] 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 colour-preserving). The conjecture also fails, among the other cases, when n is divisible by 8 or by an odd square [31], 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 [15, 38]; when the adjacency matrix has non-repeated eigenvalues [15]; when $n = pq$, for p and q distinct primes [2, 26]; when n is square-free [31] or twice square-free [32]; when $a_1, a_2, \ldots, a_k$ are all coprime with n [14, 37]. Other cases are reported in [3, 8, 31, 36].

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 [37]; (4-regular) $C_n(1, b)$ with $n = p^c$, where p is a prime number and c is a positive integer [37]; (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) [28]; on all the $C_n(1, b)$'s [21]; and, finally, on all the (4-regular) graphs $C_n(a, b)$'s [18, 30]. The results by [18, 21, 28, 30], however, were already known: see [13] 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, 17, 18, 19, 26, 27, 31, 32, 33, 34, 36], and the study of the eigenvalues [4, 10, 15, 28] and [29, 30, 35].

Many problems other than isomorphism have been studied on circulant graphs. For example, planarity, crossing number, coloring, diameter, decomposition into hamiltonian cycles, connectivity (see, for instance [6, 7, 8, 21, 22, 23, 25]). In [35] the problem of counting the number of graphs isomorphic to $C_n(1, a_2, \ldots, a_k)$ is addressed.

Circulant graphs are of interest as models of communication networks. In particular, isomorphism between circulant graphs arises in the area of distributed computer networks, communication networks, and in VLSI-design. Since the algorithmic performances of a network also depend on its layout [6, 24, 28], and isomorphic graphs may have different layouts (see Fig. 2), it is important to recognize isomorphic graphs (ISOMORPHISM TESTING) and to generate all the graphs isomorphic to a given one (ALL-ISO).

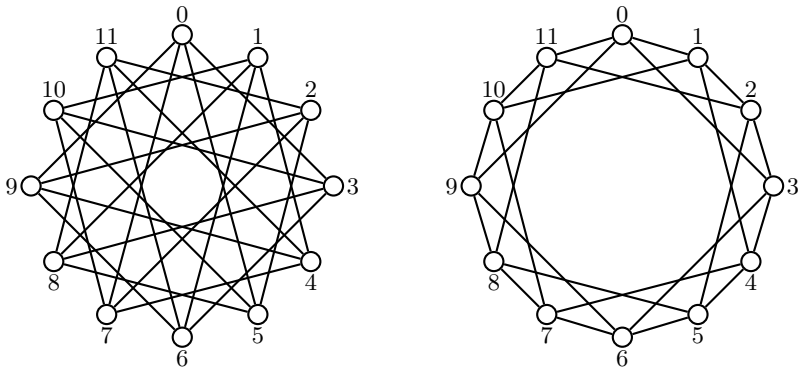

Figure 2: The isomorphic undirected graphs $C_{12}(3, 5)$ and $C_{12}(1, 3)$.

2. Some 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. [8] *The graph $C_n(a,b)$ is connected if and only if* $\gcd(n,a,b)=1$.

Notice that $C_n(a,b)$ has $\gcd(n,a,b)$ connected components. In particular, if $\gcd(n,a,b)>1$ its $\gcd(n,a,b)$ connected components are all isomorphic to $C_{n'}(a',b')$, where $n'=\frac{n}{\gcd(n,a,b)}$, $a'=\frac{a}{\gcd(n,a,b)}$, and $b'=\frac{b}{\gcd(n,a,b)}$ [8]. 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 $|E|=|E'|$).

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.). 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 $\{a',b'\}=\{\pm21,\pm45\}$, namely $C_{175}(21,45)$, $C_{175}(154,45)$, $C_{175}(21,130)$, $C_{175}(154,130)$, $C_{175}(45,21)$, $C_{175}(45,154)$, $C_{175}(130,21)$, $C_{175}(130,154)$. If it is directed, then $\mu=3$ transforms it into the 2 Ádám-isomorphic circulants $C_{175}(21,45)$ and $C_{175}(45,21)$. Observe that two different multipliers, generally speaking, are needed to compute $C_n(a',b')$ from $C_n(a,b)$, or $C_n(a,b)$ from $C_n(a',b')$, and they are the inverse of one another. For example: $C_{175}(21,45)$ is obtained from $C_{175}(7,15)$ for $\mu=3$, while $C_{175}(7,15)$ is obtained from $C_{175}(21,45)$ for $\mu=3^{-1} \bmod 175=117$.

Notice that $C_n(a,b)$ and $C_n\left(\frac{a}{\gcd(a,b)},\frac{b}{\gcd(a,b)}\right)$ are Ádám-isomorphic. In fact, $\gcd(a,b)$ is coprime with n, as $\gcd(n,a,b)=1$, and Ádám's isomorphism can be applied. For example, since $\gcd(42,90)=6$, the graphs $C_{175}(42,90)$ and $C_{175}(7,15)$ are Ádám-isomorphic.

The following two propositions are examples of Ádám-isomorphism. When $\gcd(n,a)=1$, we have:

Proposition 2.2. [22] *Let n,a verify* $\gcd(n,a)=1$*, and let t be an integer such that* $(ta) \bmod n=1$*. 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 $\gcd(n,a)>\gcd(n,b)=1$, swap a and b, and the above proposition applies again. Moreover, 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 $C_n(a,b)$. For example: the above proposition applies twice to $C_{31}(3,2)$, yielding $C_{31}(1,11)$ and $C_{31}(17,1)$.

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 such that* $(ta) \bmod n=\gcd(n,a)$*. 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.

For symmetry reasons, the above proposition can be applied to parameter b, too. For example: consider the graph $C_{175}(42, 90)$; since $\gcd(175, 42) = 7$ and $\gcd(175, 90) = 5$, applying Proposition 2.3 twice, we obtain the graphs $C_{175}(7, 15)$ (for $t = 146$) and $C_{175}(119, 5)$ (for $t = 107$).

Many authors [13, 18, 30, 37] contributed to prove Ádám's conjecture for two circulant graphs $C_n(a, b)$ and $C_n(a', b')$ (see Section 1.1). Thus, the following theorem holds:

Theorem 2.4. [13, 18, 30, 37] *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 $C_n(a, b)$. We traverse an a-cycle in a *positive direction* if we move from vertex v_x to vertex $v_{(x+a) \bmod n}$, and in the *negative direction* if we move from vertex v_x to vertex $v_{(x-a) \bmod n}$ (in the directed case, the positive direction coincides with the direction of the edges). Notice that an arbitrary $C_n(a, b)$ has the same a-cycles as $C_n(-a, b)$, but traversing an a-cycle of either graph corresponds to traversing the same a-cycle of the other one in the opposite direction.

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 are assumed to belong to the same a-cycle 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, $x \equiv y \pmod{\gcd(n, a)}$. ∎

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

By what above, we are allowed to introduce the following

Definition 3.2. *A_t denotes the (unique) a-cycle such that every vertex v_x in it verifies $x \equiv t \pmod{\gcd(n,a)}$, for $t = 0, \ldots, \gcd(n,a)-1$.*

Notice that $v_0 \in A_0$, $v_1 \in A_1$, $\ldots$, $v_{\gcd(n,a)-1} \in A_{\gcd(n,a)-1}$, and that the indices of all the vertices in A_0 are multiples of $\gcd(n,a)$, and viceversa. 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 $M_n^*(a,b)$

Matrix $M_n^*(a,b)$ is a matrix with an infinite number of rows and columns, and can be correctly defined for any connected circulant graph $C_n(a,b)$ (see Fig. 3). Each element corresponds to a vertex of the graph. On the contrary, 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 [7, 9, 20, 39].

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

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

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.

Traversing an arbitrary row (column, resp.) of $M_n^*(a,b)$ from left to right (top to bottom, resp.) corresponds to infinitely cycling over the corresponding a-cycle (b-cycle, resp.) in the positive direction.

If we read the elements of an arbitrary row of $M_n^*(a,b)$ from left to right we actually read the elements of the corresponding row of $M_n^*(-a,b)$ from right to left. In fact, traversing an a-cycle

of an arbitrary $C_n(a,b)$ corresponds to traversing the same a-cycle of $C_n(-a,b)$ in the opposite direction. The same holds w.r.t. b-cycles and columns. That is to say, considering $-a$ or $-b$, i.e., complementing a or b w.r.t. n has the effect of reversing the elements of the infinitely many rows or columns, thus exchanging the positive/negative direction defined on the cycles.

From what above it is clear that a graph $C_n(a,b)$ must be connected in order to fit into $M_n^*(a,b)$, otherwise it is not possible to represent all vertices.

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 $m_{1,1}$ in the upper left corner of $M_n(a,b)$. Thus an arbitrary element $m_{i,j}$ corresponds to vertex v_x where $x = \big((i-1)b+(j-1)a\big) \bmod n$ for $i = 1,\ldots,R$, and $j = 1,\ldots,C$ (see matrix $M_{36}(3,8)$ in Fig. 4). Observe that $M_n(a,b)$ repeats itself periodically in the infinite matrix $M_n^*(a,b)$.

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

Figure 4: Matrix $M_{36}(3,8)$.

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 $i = 1,\ldots,R$, corresponds to a-cycle A_{ρ_i} with $\rho_i = \big((i-1)b\big) \bmod R$. Notice that $\rho_1, \rho_2, \ldots, \rho_R$ represent a "regular" permutation of $\{0,1,\ldots,R-1\}$, in the sense that $\rho_i - \rho_{i-1} \equiv b \pmod R$ for $i = 2,\ldots,R$, and $\rho_1 - \rho_R \equiv b \pmod R$ (consider $C_{30}(5,3)$: the first row of $M_{30}(5,3)$ corresponds to A_0, the second row corresponds to A_3, the third to A_1, the fourth to A_4, and the fifth to A_2, resulting in $\rho_1, \rho_2, \ldots, \rho_5 = 0,3,1,4,2$). This property also shows that the a-cycles $A_0, A_1, \ldots, A_{R-1}$ are "regularly" assigned to the rows of $M_n(a,b)$, that is, "equally spaced" modulo R (two rows separate any A_{i+1} from A_i in the last example).

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 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 $j = 1,\ldots,C$, corresponds to b-cycle $B_{((j-1)a) \bmod C}$, and that the b-cycles $B_0, B_1, \ldots, B_{C-1}$ are "regularly" assigned to the columns of $M_n(a,b)$. 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 3.3. *Consider an arbitrary element $m_{R,h}$ in the last row of $M_n(a,b)$. Then, there exists a unique element $m_{1,k}$ in the first row of $M_n(a,b)$ which is b-adjacent to it.*

Proof. Let v_x be the vertex corresponding to $m_{R,h}$. 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 $x \equiv (R-1)b \pmod R$. Actually, 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 $m_{R-1,h}$, by definition. We claim that the other one corresponds to $m_{1,k}$. Since the vertices corresponding to the elements in the first row 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. ∎

The above lemma 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. 5).

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

Figure 5: Matrix $M_{36}(3,8)$; highlighted the elements $m_{R,k} = m_{3,1}$ and $m_{1,h} = m_{1,9}$, showing that $\lambda_{36}(3,8) = 8$.

Consider an element $m_{R,h}$ in the last row of $M_n(a,b)$, and its b-adjacent element $m_{1,k}$ in the first row of $M_n(a,b)$. Then, for any $t \in \mathbb{Z}^+$, $m_{R,(h+t) \bmod C}$ and $m_{R,(k+t) \bmod C}$ are b-adjacent too (in fact they are both a-adjacent in the positive direction to the considered element). This shows that the quantity $(k-h) \bmod C$ is a constant.

Definition 3.4. *The* column-jump *of $M_n(a,b)$ is $\lambda_n(a,b) = (k-h) \bmod C$, where k and h are such that $m_{R,h}$ and $m_{1,k}$ are b-adjacent.*

Example: $\lambda_{36}(3,8) = 8$, and in fact b-cycle B_0 goes from column 1 to column $1 + \lambda_{36}(3,8) = 9$, then to column $(9+\lambda_{36}(3,8)) \bmod C = 5$ as $C = 12$, and back to column $(5+\lambda_{36}(3,8)) \bmod C = 1$ (see Fig. 5).

Notice that $\lambda_n(a,b) \in \{0, \ldots, C-1\}$, by definition, and 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 $H = 1$).

Generally speaking, $\lambda_n(a,b) \neq \lambda_n(b,a)$: for example $4 = \lambda_{36}(33,8) \neq \lambda_{36}(8,33) = 3$. 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. Example: $\lambda_{36}(33,8) = C - \lambda_{36}(3,8) = 4$, as $C = 12$ and $\lambda_{36}(3,8) = 8$, and $\lambda_{36}(33,28) = \lambda_{36}(3,8)$.

By definition of column-jump, $m_{R,1}$ is b-adjacent to $m_{1,(\lambda+1) \bmod C}$ (λ stands for $\lambda_n(a,b)$), that is, vertex $v_{((R-1)b) \bmod n}$ is b-adjacent to vertex $v_{(\lambda a) \bmod n}$. That is to say, $\big((R-1)b + b\big) \equiv \lambda a \pmod n$. Recalling that $R = \gcd(n,a)$, we set the following relation (also defined in [7, 9, 20, 39]):

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

This equivalence can be interpreted on the graph as follows. Consider an arbitrary vertex v_i and traverse $\lambda_n(a,b)$ a-edges in the positive direction reaching vertex v_j with $j = (i + \lambda_n(a,b)a) \bmod n$. Then, there also exists a b-path from v_i to v_j made of $\gcd(n,a)$ b-edges, taken in the positive direction. Thus, the equivalence above describes the way a-cycles and b-cycles are "linked", in a topological sense (see Fig. 6, where $v_i = v_0$).

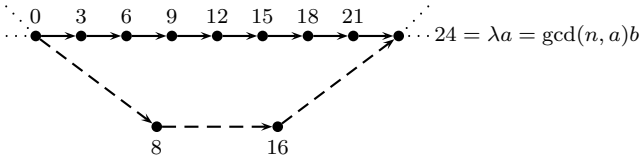

Figure 6: The parameter λ: a measure of the way a- and b-cycles are linked in $C_{36}(3,8)$. Solid lines represent a-edges, while dashed lines represent b-edges.

It is interesting to study how $\lambda_n(a,b)$ reflects onto the structure of $M_n(a,b)$ (here too λ denotes $\lambda_n(a,b)$). We claim that $M_n(a,b)$ 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 $\big(j+(H-1)\lambda+\lambda\big) \bmod C = (j + H\lambda) \bmod C = j$. As a consequence, $(H\lambda) \bmod C = 0$. 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 3.5. *The* block-jump *of* $M_n(a,b)$ *is* $\Lambda_n(a,b) = \frac{k-h}{\gcd(n,b)} \bmod H = \frac{\lambda_n(a,b)}{\gcd(n,b)}$, *where* k *and* h *are such that* $m_{R,h}$ *and* $m_{1,k}$ *are* b*-adjacent.*

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

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

Notice that $\Lambda_n(a,b) \neq \Lambda_n(b,a)$, generally speaking: for example $2 = \Lambda_{108}(33,16) \neq \Lambda_{108}(16,33) = 5$. In addition, $\Lambda_n(-a,b) = H - \Lambda_n(a,b)$, since $\frac{C}{\gcd(n,b)} = H$; the same holds if we consider $-b$, that is, if we complement b w.r.t. n; on the contrary, $\Lambda_n(-a,-b) = \Lambda_n(a,b)$. In this context, complementing either one among a and b w.r.t. n corresponds to complementing the block-jump w.r.t. H. Example: $\Lambda_{36}(3,8) = 2$ and $\Lambda_{36}(33,8) = H - \Lambda_{36}(3,8) = 1$, as $H = 3$ (see Fig. 7).

The re-construction process of an arbitrary b-cycle gives a peculiar (and "regular") permutation of the blocks (λ, Λ will denote $\lambda_n(a,b)$, $\Lambda_n(a,b)$, resp.). In fact, b-cycle B_{γ_j} visits column j,

12.

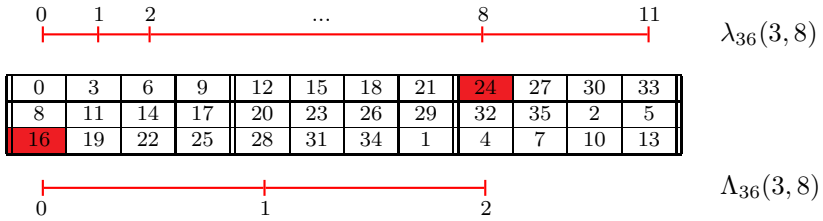

Figure 7: Partition into blocks (separated by double lines) of $M_{36}(3,8)$, resulting in $\Lambda_{36}(3,8) = \frac{\lambda_{36}(3,8)}{\gcd(n,b)} = \frac{8}{4} = 2$.

which is the j-th column of block β_0, then it visits column $(j+\lambda) \bmod C$, which is the j-th column of block β_Λ , then it visits column $(j+2\lambda) \bmod C$, which is the j-th column of block $\beta_{(2\Lambda) \bmod C}$, and so on.

It is worth noticing that the matrix which results by putting block β_0 on top of β_Λ on top of $\beta_{(2\Lambda) \bmod C}$ on top of ... on top of $\beta_{((H-2)\Lambda) \bmod C}$ on top of $\beta_{((H-1)\Lambda) \bmod C}$ is another rectangular submatrix of $M_n^*(a,b)$ defined on $\frac{n}{\gcd(n,b)}$ consecutive rows and $\gcd(n,b)$ columns (here too, without loss of generality, vertex v_0 matches to the element in the upper left corner). By doing so, each b-cycle corresponds to one column of the matrix, while each a-cycle is (regularly) split onto the H blocks.

4. Isomorphism testing

This section is devoted to describe an easy-to-evaluate necessary and sufficient condition (Theorem 4.1) 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. As a by-product of this result, we give an alternative proof of Theorem 2.4.

Recalling that $\Lambda_n(a,b), \Lambda_n(a',b') \in \{0,\ldots,H-1\}$, by definition, 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. $\gcd(n,a) \le \gcd(n,b)$ and $\gcd(n,a') \le \gcd(n,b')$. 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 $\Lambda_n(a,b) = \Lambda_n(a',b')$ ($\Lambda_n(a,b) \equiv \pm\Lambda_n(a',b') \pmod H$, resp.)*

2. *$\gcd(n,a) = \gcd(n,a') = \gcd(n,b) = \gcd(n,b')$ and either $\Lambda_n(a,b) = \Lambda_n(a',b')$ or $\Lambda_n(a,b) = \Lambda_n(b',a')$ (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.).*

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 $v(m_{i,j}) = v_{((i-1)b+(j-1)a) \bmod n}$ onto the homologous $v(m'_{i,j}) = v_{((i-1)b'+(j-1)a') \bmod n}$. 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 $i = 1, \ldots, R$ and for all $j = 1, \ldots, C$. 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 $\big(v(m_{R,j}), v(m_{1,(j+\Lambda_n(a,b) \gcd(n,b)) \bmod C})\big)$, is mapped onto the homologous b'-edge $\big(v(m'_{R,j}), v(m'_{1,(j+\Lambda_n(a',b') \gcd(n,b')) \bmod C})\big)$, for $j = 1, \ldots, C$, 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 $i = 1, \ldots, R-1$ and $j = 1, \ldots, C$.

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 3.5. 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. 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 $\Lambda_n(a',b') a' \gcd(n,b') \equiv b' \gcd(n,a')$ $\equiv b' \gcd(n,a)$ $\equiv \pm f(b \gcd(n,a))$ $\equiv \pm f(\Lambda_n(a,b) a \gcd(n,b))$ $\equiv \pm\Lambda_n(a,b) a' \gcd(n,b) \equiv$ $\equiv \pm\Lambda_n(a,b) a' \gcd(n,b')$, 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, only.

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 $\gcd(n,a) \le \gcd(n,b)$ and $\gcd(n,a') \le \gcd(n,b')$ 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 $O(\log^2 n)$ time, by Euclid's algorithm [12].

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 $v(m_{i,j}) = v_{((j-1)b+(i-1)a) \bmod n}$, associated to element $m_{i,j}$ of $M_n(a,b)$, is mapped onto the homologous vertex $v(m'_{i,j}) = v_{((j-1)b'+(i-1)a') \bmod n}$, 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. 8. The mapping function, for example, maps vertex $v(m_{3,2}) = 19$ of $M_{36}(3,8)$ onto vertex $v(m'_{3,2}) = 23$ 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 $v(\overline{m}_{i,j}) = v_{((j-1)b'-(i-1)a') \bmod n}$, 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 $v(m_{1,j})$ of $M_n(a,b)$ is mapped onto the homologous vertex $v(m'_{1,j})$ of $M_n(a',b')$, while if $\Lambda_n(a,b) = \Lambda_n(b',a')$, vertex $v(m_{1,j})$ of $M_n(a,b)$ is mapped onto the vertex associated to the (homologous) element in the j-th column 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 latter 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 8: The representative matrices of the two isomorphic graphs $C_{36}(3, 8)$ and $C_{36}(15, 4)$.

The above theorem suggests an alternative proof of the *only if part* of Theorem 2.4, which we here illustrate (the *if part* is immediate).

We have to prove that if two (directed or undirected, 3- or 4-regular) circulant graphs $C_n(a, b)$ and $C_n(a', b')$ are isomorphic, then they are Ádám-isomorphic. Throughout this paragraph, the "minus", when present, applies to the undirected case, only. Since the given graphs are isomorphic, we can apply Theorem 4.1. Thus either $\gcd(n, a) = \gcd(n, a') < \gcd(n, b) = \gcd(n, b')$ or $\gcd(n, a) = \gcd(n, a') = \gcd(n, b) = \gcd(n, b')$.

Let $\gcd(n, a) = \gcd(n, a') < \gcd(n, b) = \gcd(n, b')$ (otherwise swap a' and b'), and consider $\mu_a, \mu_b \in \{1, \ldots, n-1\}$ such that $\mu_a a \equiv \pm a' \pmod n$ and $\mu_b b \equiv \pm b' \pmod n$. Since $\gcd(n, x \bmod n) = \gcd(n, x)$ for any integer x, $\gcd(n, a) = \gcd(n, a')$ implies that $\gcd(\mu_a, n) = 1$ and $\gcd(n, b) = \gcd(n, b')$ implies that $\gcd(\mu_b, n) = 1$. By definition of Λ', and recalling that $\mu_a a \equiv \pm a' \pmod n$ and $\mu_b b \equiv \pm b' \pmod n$, we can write $\gcd(n, a)\mu_b b \equiv \pm\Lambda' \gcd(n, b)\mu_a a \pmod n$, that is to say $\mu_b \frac{b}{\gcd(n,b)} \equiv \pm\Lambda' \mu_a \frac{a}{\gcd(n,a)} \pmod H$. Since the two graphs are isomorphic, by Theorem 4.1, $\Lambda \equiv \pm\Lambda' \pmod H$. By definition of Λ, it follows that $\mu_a = \mu_b$.

Let, now, $\gcd(n, a) = \gcd(n, a') = \gcd(n, b) = \gcd(n, b')$. Since the gcd's are all equal, we do not know whether a corresponds to a' or to b' (thus b to b' or to a', resp.). That is to say, it may happen that the role of a' and b' has to be exchanged. Having in mind this fact, we can basically apply the proof above. For this reason, consider $\mu_a, \mu_b, \bar{\mu}_a, \bar{\mu}_b \in \{1, \ldots, n-1\}$ such that $\mu_a a \equiv \pm a' \pmod n$, $\mu_b b \equiv \pm b' \pmod n$, $\bar{\mu}_a a \equiv \pm b' \pmod n$, and $\bar{\mu}_b b \equiv \pm a' \pmod n$. We finally get that either one equality among $\mu_a = \mu_b$ and $\bar{\mu}_a = \bar{\mu}_b$ holds, and the proof is complete.

5. Other results

This section is devoted to study the two problems μ-SEARCH and ALL-ISO stated in the Introduction. In particular, in Subsection 5.1 an algorithm to solve μ-SEARCH is proposed, while in Subsection 5.2 an exact procedure to solve ALL-ISO is discussed, and its complexity is compared to a direct application of Ádám's isomorphism.

5.1. Solving μ-SEARCH

Let two isomorphic graphs $C_n(a, b)$ and $C_n(a', b')$ be given. The present subsection is devoted to determine the value of the Ádám's multiplier μ coprime with n such that $\{a', b'\} = \{\mu a, \mu b\} \pmod n$ in the directed case, and $\{a', b'\} = \{\pm\mu a, \pm\mu b\} \pmod n$ in the undirected case. Observe

that the multiplier μ allows for computing $C_n(a', b')$ from $C_n(a, b)$, while a different multiplier is needed to compute $C_n(a, b)$ from $C_n(a', b')$.

We distinguish two cases: either $\gcd(n, a) = \gcd(n, a') < \gcd(n, b) = \gcd(n, b')$ (possibly swapping a' and b'), or $\gcd(n, a) = \gcd(n, a') = \gcd(n, b) = \gcd(n, b')$ (and all equal to 1).

Consider the case $\gcd(n, a) = \gcd(n, a') < \gcd(n, b) = \gcd(n, b')$, first, and let p be the smallest positive integer satisfying $pa \equiv a' \pmod{n}$. Consider the quantity $p + iH \gcd(n, b)$ for an arbitrary integer i. Recalling that $n = H \gcd(n, a) \gcd(n, b)$, it is easy to see that $(p + iH \gcd(n, b))a \equiv a' \pmod{n}$. That is to say, a' is obtained if and only if a is multiplied by $p + iH \gcd(n, b)$ for some i. Since i can be restricted, w.l.o.g., between 0 and $\gcd(n, a) - 1$, it is convenient to define the set P of the multipliers which transform a into a':

$$P = \{p + iH \gcd(n, b), \text{ for } i = 0, \ldots, \gcd(n, a) - 1\}.$$

It must be the case that the searched multiplier μ belongs to P, thus verifies $\mu \equiv p \pmod{H}$.

Now consider b': we distinguish the directed case from the undirected one.

In the directed case, the searched μ must verify $\mu b \equiv b' \pmod{n}$. Let q be the smallest positive integer such that $qb \equiv b' \pmod{n}$. Reasoning as above, only multipliers of the form $q + jH \gcd(n, a)$, with j arbitrary integer, transform b into b'.

In the undirected case, the searched μ must verify $\pm\mu b \equiv b' \pmod{n}$, that is to say, either $\mu b \equiv b' \pmod{n}$ or $\mu b \equiv n - b' \pmod{n}$ (in a few lines we shall be able to decide). Let q', q'' be the smallest positive integers such that $q'b \equiv b' \pmod{n}$ and $q''b \equiv n - b' \pmod{n}$. Reasoning as above, only multipliers of the form $q' + jH \gcd(n, a)$, with j arbitrary integer, transform b into b', and only multipliers of the form $q'' + jH \gcd(n, a)$, with j arbitrary integer, transform b into $n - b'$. Set $q = q'$ if $q' \equiv p \pmod{H}$ and $q = q''$ if $q'' \equiv p \pmod{H}$.

In both the directed and undirected case, define

$$Q = \{q + jH \gcd(n, a), \text{ for } j = 0, \ldots, \gcd(n, b) - 1\}.$$

It must be the case that the multiplier μ, we are looking for, belongs to Q, and satisfies $\mu \equiv q \equiv p \pmod{H}$ (in fact, the choice of q in the undirected case was made in order to satisfy the last equation).

Thus, $\mu \in P \cap Q$, and there exist integers $i \in \{0, \ldots, \gcd(n, a) - 1\}$ and $j \in \{0, \ldots, \gcd(n, b) - 1\}$ such that

$$p + iH \gcd(n, b) = q + jH \gcd(n, a)$$

which gives

$$j = \frac{p - q + iH \gcd(n, b)}{H \gcd(n, a)}.$$

Such a j exists, as we are given two isomorphic graphs. In order j to be integer we can limit ourselves to find the only value $\bar{i} \in \{0, \ldots, \gcd(n, a) - 1\}$ which verifies

$$\left(\frac{p - q}{H} + \bar{i} \gcd(n, b)\right) \equiv 0 \pmod{\gcd)(n, a}$$

(by the expressions of p and q it follows immediately that their difference is multiple of H). Thus,

$$\mu = p + \bar{i} H \gcd(n, b).$$

In a similar way we could have computed $\mu = q + \bar{j}H \gcd(n,a)$, where $\bar{j} \in \{0, \ldots, \gcd(n,b)-1\}$ is the only value which verifies $\left(\frac{q-p}{H} + \bar{j}\gcd(n,a)\right) \equiv 0 \pmod{\gcd}(n,b)$.

Notice that the searched value of μ can also be determined by directly computing the intersection $P \cap Q$, which is sometimes convenient, recalling that $|P| = \gcd(n,a)$ and $|Q| = \gcd(n,b)$. In particular, when $|P| = \gcd(n,a) = 1$ then $\mu = p$ (or, clearly, when $|Q| = \gcd(n,b) = 1$ then $\mu = q$). In addition, if it is the case that $p = q$, the searched μ is $\mu = q = p$, thus the computation of the largest among P and Q, and all what follows, can be avoided.

To illustrate the described method, consider the undirected isomorphic graphs $C_n(a,b) = C_{36}(3,8)$ and $C_n(a',b') = C_{36}(21,8)$, where $\gcd(n,a) = \gcd(n,a') = 3$, $\gcd(n,b) = \gcd(n,b') = 4$, and $H = 3$. We get $p = 7$, $q' = 1$, and $q'' = 8$, thus $q = q' = 1$, as $q' \equiv p \pmod{H}$. The $\bar{i} \in \{0,1,2\}$ we have to find, must verify $(\frac{7-1}{3} + 4 \cdot \bar{i}) \equiv 0 \pmod 3$, resulting in $\bar{i} = 1$, and we finally get $\mu = 7 + 1 \cdot 3 \cdot 4 = 19$. We could also determine the μ by computing $P \cap Q$, instead. As $P = \{7, 19, 31\}$ and $Q = \{1, 10, 19, 28\}$, we get $\mu = 19$, as well.

Now consider the case $\gcd(n,a) = \gcd(n,a') = \gcd(n,b) = \gcd(n,b')$. Since the gcd's are all equal, we do not know whether a transforms into a' or into b' (thus b into b' or into a', resp.), but the method is basically the same described above. Consider a', and let p, $\bar{p}$ be the smallest positive integers satisfying $pa \equiv a' \pmod n$ and $\bar{p}a \equiv b' \pmod n$, respectively. Now consider b', and let q', q'', $\bar{q}'$ $\bar{q}''$ (q'' and $\bar{q}''$ for the undirected case, only), be the smallest positive integers satisfying $q'b \equiv b' \pmod n$, $q''b \equiv n - b' \pmod n$, $\bar{q}'b \equiv a' \pmod n$ and $\bar{q}''b \equiv n - a' \pmod n$. Since the given graphs are isomorphic, either one equality holds among the following four: $p = q'$, $p = q''$, $\bar{p} = \bar{q}'$, and $\bar{p} = \bar{q}''$. The value of μ corresponds to the value of the valid equality.

To illustrate this case, consider the undirected isomorphic graphs $C_n(a,b) = C_{18}(1,11)$ and $C_n(a',b') = C_{18}(7,17)$, where $\gcd(n,a) = \gcd(n,a') = \gcd(n,b) = \gcd(n,b') = 1$. We get $p = 7$, $\bar{p} = 17$, $q' = 13$, $\bar{q}' = 17$, $q'' = 5$, and $\bar{q}'' = 11$. Thus $\mu = \bar{p} = \bar{q}' = 17$.

5.2. Solving ALL-ISO

This subsection is devoted to describe how to generate all the graphs isomorphic to a given $C_n(a,b)$.

The first possibility is to compute $a' = (\mu a) \bmod n$ and $b' = (\mu b) \bmod n$ for all $\mu = 1, \ldots, n$ coprime with n. According to Theorem 2.4, the graphs $C_n(a',b')$ generated this way and their equivalent notations are all and only the graphs isomorphic to $C_n(a,b)$.

Another possibility is to find all the pairs a', b' such that $\gcd(n,a') = \gcd(n,a)$, $\gcd(n,b') = \gcd(n,b)$, and $\gcd(n,a)b' \equiv \Lambda_n(a,b)\gcd(n,b)a' \pmod n$. According to Theorem 4.1, the graphs $C_n(a',b')$ generated this way and their equivalent notations are all and only the graphs isomorphic to $C_n(a,b)$.

An alternative way is based on the following result. Given a $C_n(a,b)$, define $\mathcal{A}^c = \{\bar{a} = (\bar{\gamma}a) \bmod n : \gcd(n,\bar{a}) = \gcd(n,a)$, with $\bar{\gamma} = 1, \ldots, n-1$ such that $\bar{\gamma} \bmod H = c\}$, where suitable values for c are in $\{0, \ldots, H-1\}$. $\mathcal{A}^c$ can also be written as

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

Let also

$$\begin{aligned}N(\tilde{a}) = \{&\bar{b} = (\bar{\gamma}b) \bmod n : \gcd(n,\bar{b}) = \gcd(n,b),\\ &(\bar{\gamma}a) \bmod n = \tilde{a}, \text{ for } \bar{\gamma} = 1, \ldots, n-1\}.\end{aligned}$$

Note that, by definition, any graph $C_n(\tilde{a}, \tilde{b})$ with $\tilde{a} \in \mathcal{A}^c$, for some c, and $\tilde{b} \in N(\tilde{a})$, is isomorphic to $C_n(a, b)$.

Lemma 5.1. *Consider a connected circulant graph $C_n(a, b)$. Let $a', a'' \in \mathcal{A}^c$, for some $c \in \{0, \ldots, H-1\}$. Then $N(a') = N(a'')$.*

Proof. Let $\gamma', \gamma'' \in \{1, \ldots, H \gcd(n, b)\}$ be coprime with n and such that $(\gamma' a) \bmod n = a'$ and $(\gamma'' a) \bmod n = a''$.
Since $(\bar{\gamma} a) \bmod n = a'$ if and only if $\bar{\gamma} = \gamma' + k' H \gcd(n, b)$ for $k' = 0, \ldots, \gcd(n, a) - 1$, and $(\bar{\bar{\gamma}} a) \bmod n = a''$ if and only if $\bar{\bar{\gamma}} = \gamma'' + k'' H \gcd(n, b)$ for $k'' = 0, \ldots, \gcd(n, a) - 1$, alternative ways to express $N(a'), N(a'')$ are the following: $N(a') = \big\{\bar{b} = \big((\gamma' + k' H \gcd(n, b))b\big) \bmod n$, for $k' = 0, \ldots, \gcd(n, a) - 1$ and $\gcd(n, \bar{b}) = \gcd(n, b)\big\}$ and $N(a'') = \big\{\bar{\bar{b}} = \big((\gamma'' + k'' H \gcd(n, b))b\big) \bmod n$, for $k'' = 0, \ldots, \gcd(n, a) - 1$ and $\gcd(n, \bar{\bar{b}}) = \gcd(n, b)\big\}$.
Without loss of generality, let $\gamma' \leq \gamma''$ (otherwise swap a' and a''). Then, we can write $\gamma'' = \gamma' + fH$ for a constant $f \in \{0, \ldots, \gcd(n, b) - 1\}$, as $\gamma' \bmod H = \gamma'' \bmod H = c$. Thus, $N(a'') = \big\{\bar{\bar{b}} = \big(\gamma' b + fHb + k'' H \gcd(n, b) b\big) \bmod n$, for $k'' = 0' \ldots, \gcd(n, a) - 1$ and $\gcd(n, \bar{\bar{b}}) = \gcd(n, b)\big\}$.
In order to prove that $N(a') = N(a'')$, it suffices to prove that there exists a suitable $k' \in \{0, \ldots, \gcd(n, a) - 1\}$, say $\bar{k}$, such that $\gamma' b + \bar{k} H \gcd(n, b) b \equiv \gamma' b + fHb \pmod{n}$. Recalling that $n = H \gcd(n, a) \gcd(n, b)$ and that $\frac{b}{\gcd(n,b)}$ is coprime with $\gcd(n, a)$, the last equivalence can be simplified into the following $\bar{k} \gcd(n, b) \equiv f \pmod{\gcd(n, a)}$. Such a $\bar{k}$ always exists, as $\gcd(n, a)$ and $\gcd(n, b)$ are coprime, and the proof is complete. ∎
A similar result holds w.r.t. b, where $\mathcal{B}^c = \big\{\bar{b} = (\bar{\gamma} b) \bmod n : \gcd(n, \bar{b}) = \gcd(n, b)$, with $\bar{\gamma} = c + k'' H$ for $k'' = 0, \ldots, \gcd(n, a) - 1\big\}$, and $N(\tilde{b})$ is suitably derived from $N(\tilde{a})$.

From the definitions of $\mathcal{A}^c$ and $\mathcal{B}^c$ it follows that: *i)* $\mathcal{A}^0$, $\mathcal{B}^0$ are non-empty if and only if $H = 1$; *ii)* $\mathcal{A}^c = \mathcal{B}^c = \emptyset$ for all c such that $\gcd(c, H) > 1$; *iii)* $a' \in \mathcal{A}^c$ if and only if $-a' \in \mathcal{A}^{H-c}$, as well as $b' \in \mathcal{B}^c$ if and only if $-b' \in \mathcal{B}^{H-c}$.

Thus, for some integer $c \in \{0, \ldots, H-1\}$ we have that: $\mathcal{A}^c = \emptyset$ implies $\mathcal{A}^{H-c} = \emptyset$, as well as $\mathcal{B}^c = \emptyset$ implies $\mathcal{B}^{H-c} = \emptyset$; and $(a', b') \in \mathcal{A}^c \times \mathcal{B}^c$ implies $(-a', b') \in \mathcal{A}^{H-c} \times \mathcal{B}^c$, $(a', -b') \in \mathcal{A}^c \times \mathcal{B}^{H-c}$, and $(-a', -b') \in \mathcal{A}^{H-c} \times \mathcal{B}^{H-c}$.
In the directed case, define

$$\mathcal{K} = \big\{C_n(a', b'), C_n(b', a'), \text{ for all } (a', b') \in \bigcup_{c=0}^{H-1} \mathcal{A}^c \times \mathcal{B}^c\big\}.$$

As for the undirected case, define

$$\begin{aligned}
\mathcal{K} &= \big\{C_n(a', b'), C_n(a', -b'), C_n(-a', b'), C_n(b', a'), C_n(-b', a'), C_n(b', -a'), \\
&\quad \text{for all } (a', b') \in \bigcup_{c=0}^{H-1} \mathcal{A}^c \times \mathcal{B}^c\big\} = \\
&= \Big\{C_n(a', b'), C_n(b', a') \\
&\quad \text{for all } (a', b') \in \Big(\big(\bigcup_{c=0}^{H-1} \mathcal{A}^c \times \mathcal{B}^c\big) \cup \big(\bigcup_{c=0}^{H-1} \mathcal{A}^c \times \mathcal{B}^{H-c}\big)\Big)\Big\}
\end{aligned}$$

where the last equality holds thanks to what observed above. The following theorem can be proved:

Theorem 5.2. *Consider a connected circulant graph $C_n(a,b)$, then $C_n(a',b')$ is isomorphic to $C_n(a,b)$ if and only if $C_n(a',b') \in \mathcal{K}$.*

Proof. The only if part immediately follows from the definition of $\mathcal{A}^c$ and $\mathcal{B}^c$. As for the if part, let $(a',b') \in \mathcal{A}^c \times \mathcal{B}^c$ for some integer $c \in \{0,\dots,H-1\}$. Lemma 5.1 states that the set $N(\tilde{a})$ is the same for every element $\tilde{a}$ of $\mathcal{A}^c$, for $c \in \{0,\dots,H-1\}$. Thus, it is convenient to call it $N(\mathcal{A}^c)$, and define it as $\big\{\bar{b} = (\bar{\gamma}b) \bmod n : \gcd(n,\bar{b}) = \gcd(n,b)$ and $(\bar{\gamma}a) \bmod n \in \mathcal{A}^c$, for $\bar{\gamma} = 1,\dots,n-1\big\}$, with $c = 0,\dots,H-1$. Hence, any pair $(\tilde{a},\tilde{b}) \in \mathcal{A}^c \times N(\mathcal{A}^c)$, for $c = 0,\dots,H-1$, gives rise to a graph $C_n(\tilde{a},\tilde{b})$ isomorphic to $C_n(a,b)$. In order to prove the theorem, we have to show that $N(\mathcal{A}^c) = \mathcal{B}^c$. The proof consists in showing that $\bar{b} \in \mathcal{B}^c$ if and only if $\bar{b} \in N(\mathcal{A}^c)$. The if part is immediate, if one recalls that $\bar{\gamma} \bmod H = c$ if $(\bar{\gamma}a) \bmod n \in \mathcal{A}^c$. As for the viceversa, let $\bar{b} = (\bar{\gamma}b) \bmod n$. We have to prove that $\bar{b} \in N(\mathcal{A}^c)$ if $\bar{b} \in \mathcal{B}^c$, that is to say, $(\bar{\gamma}a) \bmod n \in \mathcal{A}^c$, that is, $\bar{\gamma} \bmod H = c$ and $\gcd(n,(\bar{\gamma}a) \bmod n) = \gcd(n,a)$. The former of these two conditions follows from the definition of $\mathcal{B}^c$. As for the latter, we first note that writing $\gcd(n,(\bar{\gamma}a) \bmod n)$ is equivalent to writing $\gcd(n,\bar{\gamma}a)$. Thus, the condition $\gcd(n,(\bar{\gamma}a) \bmod n) = \gcd(n,a)$ becomes $\gcd\left(H\gcd(n,b), \bar{\gamma}\frac{a}{\gcd(n,a)}\right) = 1$. This is true because of the following two facts: *i)* $\gcd(n,(\bar{\gamma}b) \bmod n) = \gcd(n,b)$ implies $\bar{\gamma}$ coprime with n, hence with $H\gcd(n,b)$; *ii)* by definition, $\frac{a}{\gcd(n,a)}$ is coprime with n, hence with $H\gcd(n,b)$, and the proof is complete. ∎

As far as the computational complexity of a direct implementation of the method is concerned, we focus on the number of times a greatest common divisor is computed. We first observe that the construction of $\mathcal{A}^c$ and $\mathcal{B}^c$ requires the computation of $\gcd(n,b)+\gcd(n,a)$ greatest common divisors. In particular, when $H = 1$, we need $\gcd(n,a) + \gcd(n,b)$ greatest common divisor operations to construct $\bigcup_{c=0}^{H-1} \mathcal{A}^c \times \mathcal{B}^c = \mathcal{A}^0 \times \mathcal{B}^0$. When $H > 1$, we need $(H-1)\big(\gcd(n,a) + \gcd(n,b)\big)$ greatest common divisor operations to construct $\bigcup_{c=0}^{H-1} \mathcal{A}^c \times \mathcal{B}^c = \bigcup_{c=1}^{H-1} \mathcal{A}^c \times \mathcal{B}^c$. These quantities have to be compared with $n-1$, which is the number of times a greatest common divisor is computed by Ádám's method (in fact, all $\mu \in \{1,\dots,n-1\}$ are considered, and for each of them $\gcd(\mu,n)$ is evaluated). Recalling that $n = H\gcd(n,a)\gcd(n,b)$, our method is always more efficient than a direct implementation of Ádám's method when $\min\{\gcd(n,a),\gcd(n,b)\} \geq 2$, and also when $\{\gcd(n,a),\gcd(n,b)\} = \{1,x\}$, $x \geq 2$, for $2 \leq H < x-1$.

Actually, the number of gcd's computed by our method can be improved, under certain conditions. Recall that $\mathcal{A}^c$ and $\mathcal{B}^c$ are empty for all c such that $\gcd(c,H) > 1$. Thus, if we check $\gcd(c,H) > 1$ (one more gcd operation for each c), we avoid the computation of $\mathcal{A}^c$ and $\mathcal{B}^c$ (possibly saving on the computation of $\gcd(n,a) + \gcd(n,b)$ greatest common divisors). By doing so for all $c \in \{0,\dots,H-1\}$, on one hand we increase by H the number of computed gcd's, on the other hand we reduce this number by $\gcd(n,a)+\gcd(n,b)$ whenever $\gcd(c,H) > 1$ is satisfied. The last condition is satisfied at least $\frac{H}{f}$ times, where $f \neq 1$ is the smallest factor of H. Thus, the number of gcd's needed to compute $\bigcup_{c=0}^{H-1} \mathcal{A}^c \times \mathcal{B}^c$ amounts to $H + H\big(\gcd(n,a)+\gcd(n,b)\big) - \frac{H}{f}\big(\gcd(n,a)+\gcd(n,b)\big)$, which is definitely better than the previous method when $f < \gcd(n,a)+\gcd(n,b)$. In addition, we can further reduce the total number of gcd's recalling that $\mathcal{A}^0 = \mathcal{B}^0 = \emptyset$ for $H > 1$, and that $a' \in \mathcal{A}^c$ if and only if $-a' \in \mathcal{A}^{H-c}$. Thus, we can limit ourselves to determine $\mathcal{A}^c$ only for the values of $c \leq \left\lceil \frac{H-1}{2} \right\rceil$ such that $\gcd(c,H) > 1$, and then derive $\mathcal{A}^{H-c}$ as $\{-a' : a' \in \mathcal{A}^c\}$. The same can be applied to the sets $\mathcal{B}^c$.

The method is illustrated by the following example. Consider $C_{60}(3,5)$, where $\gcd(n,a) = 3$, $\gcd(n,b) = 5$, $H = 4$. Since $f = 2 < 3+5$, the most convenient implementation is the second one. Thus, $\mathcal{A}^0 = \mathcal{B}^0 = \emptyset$, as $H > 1$; then we compute $\gcd(c,H)$ for $c = 1$ and $c = \left\lceil \frac{H-1}{2} \right\rceil = 2$

(totally, 2 gcd's), resulting in $\mathcal{A}^1$, $\mathcal{B}^1$ non-empty, as $\gcd(1,H)=1$; and $\mathcal{A}^2=\mathcal{B}^2=\emptyset$, as $\gcd(2,H)>1$; finally we derive derive $\mathcal{A}^3$ from $\mathcal{A}^1$, as well as $\mathcal{B}^3$ from $\mathcal{B}^1$. Recalling that $\mathcal{A}^1=\{\bar{a}=(\bar{\gamma}3) \bmod 60 : \gcd(60,\bar{a})=3$, with $\bar{\gamma}=1+4k'$ for $k'=0,\ldots,4\}$, we get $\mathcal{A}^1=\{3,27,39,51\}$ (computing 5 gcd's). Then we derive $\mathcal{A}^3=\{9,21,33,57\}$ from $\mathcal{A}^1$ complementing each element w.r.t. n. Recalling that $\mathcal{B}^1=\{\bar{b}=(\bar{\gamma}5) \bmod 60 : \gcd(60,\bar{b})=\gcd(60,5)$, with $\bar{\gamma}=1+4k''$ for $k''=0,1,2\}$ we get $\mathcal{B}^1=\{5,25\}$ (computing 3 gcd's), and then derive $\mathcal{B}^3=\{35,55\}$ from $\mathcal{B}^1$ complementing each element w.r.t. n. Thus, $\bigcup_{c=0}^{H-1}\mathcal{A}^c\times\mathcal{B}^c=\{(3,5),\ (27,5),\ (39,5),\ (51,5),\ (3,25),\ (27,25),\ (39,25),\ (51,25),\ (9,35),\ (9,55),\ (21,35),\ (21,55),\ (33,35),\ (33,55),\ (57,35),\ (57,55)\}$. In order to obtain this result we have computed $2+5+3=10$ gcd's while a direct implementation of Ádám's method would have computed $n-1=59$ gcd's.

Assume that the given $C_{60}(3,5)$ is undirected, first, and consider an arbitrary pair in $\bigcup_{c=0}^{H-1}\mathcal{A}^c\times\mathcal{B}^c$, say $(27,5)$. Complementing none or one of the two parameters, and/or swapping them, we get the following graphs: $C_{60}(27,5)$, $C_{60}(27,55)$, $C_{60}(33,5)$, $C_{60}(5,27)$, $C_{60}(55,27)$, $C_{60}(5,33)$. Doing the same for all the other pairs, we obtain the set of all the (undirected) graphs isomorphic to the given $C_{60}(3,5)$, namely $\mathcal{K}=\{C_{60}(3,5),\ C_{60}(3,25),\ C_{60}(3,35),\ C_{60}(3,55),\ C_{60}(5,3),\ C_{60}(5,9),\ C_{60}(5,21),\ C_{60}(5,33),\ C_{60}(5,39),\ C_{60}(5,51),\ C_{60}(5,57),\ C_{60}(9,5),\ C_{60}(9,25),\ C_{60}(9,35),\ C_{60}(9,55),\ C_{60}(21,5),\ C_{60}(21,25),\ C_{60}(21,35),\ C_{60}(21,55),\ C_{60}(25,3),\ C_{60}(25,9),\ C_{60}(25,21),\ C_{60}(25,33),\ C_{60}(25,39),\ C_{60}(25,51),\ C_{60}(25,57),\ C_{60}(27,5),\ C_{60}(27,25),\ C_{60}(27,35),\ C_{60}(27,55),\ C_{60}(33,5),\ C_{60}(33,25),\ C_{60}(33,35),\ C_{60}(33,55),\ C_{60}(35,3),\ C_{60}(35,9),\ C_{60}(35,21),\ C_{60}(35,33),\ C_{60}(35,39),\ C_{60}(35,51),\ C_{60}(35,57),\ C_{60}(39,5),\ C_{60}(39,25),\ C_{60}(39,35),\ C_{60}(39,55),\ C_{60}(51,5),\ C_{60}(51,25),\ C_{60}(51,35),\ C_{60}(51,55),\ C_{60}(55,3),\ C_{60}(55,9),\ C_{60}(55,21),\ C_{60}(55,33),\ C_{60}(55,39),\ C_{60}(55,51),\ C_{60}(55,57),\ C_{60}(57,5),\ C_{60}(57,25),\ C_{60}(57,35),\ C_{60}(57,55)\}$.

Now assume that the given $C_{60}(3,5)$ is directed, and consider an arbitrary pair in $\bigcup_{c=0}^{H-1}\mathcal{A}^c\times\mathcal{B}^c$, say $(27,5)$, which gives rise to the graphs $C_{60}(27,5)$, $C_{60}(5,27)$. Doing the same for all the other pairs, we obtain the (not listed) set of all the directed graphs isomorphic to the given $C_{60}(3,5)$.

6. Conclusions

In this paper we deal with the isomorphism of circulant graphs $C_n(a,b)$. In particular, we study the topological structure of these graphs, and we give a necessary and sufficient condition for two (directed/undirected) connected $C_n(a,b)$ to be isomorphic. One of the contributions of the paper is that the approach is purely combinatorial and new for the isomorphism problem, which has been mainly addressed by means of algebraic-combinatorial theory, group theory, and the theory of the eigenvalues. As a by-product of this approach, we get an alternative proof of Ádám's conjecture on arbitrary $C_n(a,b)$'s, which is based on elementary concepts.

We show that the topological structure of the studied graphs is very strong, being the union of two families of disjoint cycles (the a-cycles and the b-cycles) suitably linked to one another. The way cycles are linked is described by means of an easily computed integer. By means of these concepts we state the isomorphism condition (Theorem 4.1): two (directed/undirected) circulant graphs are isomorphic if and only if they have the same number of a-cycles and b-cycles, and these cycles are linked "in the same way". This condition is very easy to evaluate, and takes $O(\log^2 n)$ time. It also allows for immediately reading the isomorphism mapping function.

We also solve the problem of finding the Ádám's multiplier among two given isomorphic circulant graphs. In addition we propose a method for generating all the circulant graphs isomorphic

to a given one. This method is different from a direct application of Ádám's isomorphism, in that it does not evaluate all the multipliers from 1 to $n-1$, and in its computational complexity.

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, suitably generalizing Theorem 4.1.

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. Babai. Isomorphism problem for a class of point-symmetric structures. *Acta Math. Acad. Sci. Hungar.*, 29:329–336, 1977.

[4] L. Babai. Spectra of Cayley graph. *J. Combinatorial Theory B*, 27:180–189, 1979.

[5] 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.

[6] J.C. Bermond, F. Comellas, and D.F. Hsu. Distributed loop computer networks: a survey. *J. Parallel and Distributed computing*, 24:2–10, 1995.

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

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

[9] 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.

[10] 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.

[11] 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.

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

[13] 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.

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

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

[16] 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.

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

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

[19] J.G. Fernandes and R.E. Giudici. Isomorphism between Cayley (di)graphs. *Discrete Mathematics*, 305:361–364, 2005.

[20] 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.

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

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

[23] P.T. Ho. The crossing number of $C(3k+1;\{1,k\})$. *Discrete Mathematics*, 307:2771–2774, 2007.

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

[25] F.K. Hwang and Y.H. Xu. Double loop networks with minimum delay. *Discrete Mathematics*, 66:109–118, 1987.

[26] 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.

[27] C.H. Li. On isomorphisms of finite Cayley graphs - a survey. *Discrete Mathematics*, 256:301–334, 2002.

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

[29] B. Mans, F. Pappalardi, and I. Shparlinski. On the Ádám conjecture on circulant graphs. In W.L. Hsu and M.Y. Kao, editors, *Proceedings of the 4th Annual International Conference on Computing and Combinatorics, COCOON '98,* Taipei, Taiwan, R.o.C., August 12-14, 1998, volume 1449 of *Lecture Notes in Computer Science*, pages 251–260. Springer, 1998.

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

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

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

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

[34] M. Muzychuk and R. Pöschel. Isomorphism criteria for circulant graphs. Technical Report MATH-AL-9-1999, Technische Universität Dresden, 1999.

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

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

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

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

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