ELSEVIER

Discrete Mathematics 254 (2002) 309–329

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

On the spectral Ádám property for circulant graphs

Bernard Mans[a,*], Francesco Pappalardi[b], Igor Shparlinski[a]

[a] *Department of Computing, Macquarie University, Sydney, NSW 2109, Australia*

[b] *Dipartimento di Matematica, Terza Università degli Studi, Largo S. L. Murialdo, 1, Roma 00146, Italy*

Received 3 March 1998; received in revised form 21 December 1999; accepted 23 July 2001

Abstract

We investigate a certain condition for isomorphism between circulant graphs (known as the Ádám property) in a stronger form by referring to isospectrality rather than to isomorphism of graphs. We describe a wide class of graphs for which the Ádám conjecture holds. We apply these results to establish an asymptotic formula for the number of non-isomorphic circulant graphs and connected circulant graphs.

Circulant graphs arise in many applications including telecommunication networks, VLSI design and distributed computation and have been extensively studied in the literature. In the important case of double loops (particular circulant graphs of degree 4) we give a complete classification of all possible isospectral graphs.

Our method is based on studying the graph spectra with the aid of some deep results of algebraic number theory.

Keywords: Circulant graphs; Graph isomorphism; Graph spectrum

1. Introduction

In this paper we study the condition for isomorphism between circulant graphs. Such graphs have a vast number of applications to telecommunication networks, VLSI design and distributed computation [4,17,19,20,22] (they are usually used as topologies and

* Corresponding author.

E-mail addresses: bmans@comp.mq.edu.au (B. Mans), pappa@mat.uniroma3.it (F. Pappalardi), igor@comp.mq.edu.au (I. Shparlinski).

PII: S0012-365X(01)00374-0

are called loop networks or chordal rings). The relative independence of link length from delay time opens up the possibility of distinguishing among isomorphic networks on the basis of their algorithmic performance. A network that does provide labelled edges should be able to exploit the same properties as one with different labelling if the underlying graphs are isomorphic.

For general graphs the isomorphism problem is known to be in **NP**, not known to be in **P**, and probably is not **NP**-complete, see the book of Babai [3, Section 6]. It has been conjectured by Ádám [1] that for circulant graphs there is a very simple rule to decide the isomorphism of two graphs. Although this rule is known to be false in general, even for undirected graphs (see [10]), for several special cases it holds (see in particular [23,24], and other references such as [5,19,20,26]).

The *purpose* of this paper is to extend essentially the class of graphs having the Ádám property and having the (even more general) spectral Ádám property. In particular, we settle the aforementioned Ádám conjecture [1] for a wide class of circulant graphs which are not covered by the previously known results. We introduce a new technique based on the combination of the spectral techniques from [8,10,20,25] with some deep results of algebraic number theory on linear equations in roots of unity [6,9,11,21,28–30]. It can be extended to other graph problems such as weighted circulant graphs and general *Cayley* graphs (see [26]). Indeed, at least in the case of Cayley graphs generated by an *Abelian* group, the corresponding eigenvalues are linear combinations of group characters, that is, they are linear combinations of roots of unity (see [3, Section 3.12] or [13, Lemma 9.2]).

We recall that an n-vertex *circulant graph* G is a graph whose adjacency matrix $A=(a_{ij})_{i,j=1}^n$ is a circulant. That is, the ith rows of A is the cyclic shift of the first row by $i-1$,

$$a_{ij}=a_{1,j-i+1},\quad i,j=1,\ldots,n.$$

Hereafter, the subscripts are taken modulo n, that is $a_{i,j}=a_{i+n,j}=a_{i,j+n}$ for all integers i and j (it is more convenient to keep the interval $[1,n]$ as our main working range). We also assume that $a_{ii}=0,\ i=1,\ldots,n$.

Therefore with every circulant graph, one can associate a set $S\subseteq\mathbb{Z}_n$ of the positions of non-zero entries of the first row of the adjacency matrix of the graph. Respectively, we denote by $\langle S\rangle_n$ the corresponding graph.

We also recall that two graphs G_1,G_2 are *isomorphic*, and write $G_1\simeq G_2$, if their adjacency matrices differ by a permutation of their rows and columns.

We say that two sets $S,T\subseteq\mathbb{Z}_n$ are *proportional*, and write $S\sim T$, if for some integer l with $\gcd(l,n)=1$, $S=lT$ where the multiplication is taken over $\mathbb{Z}_n$.

Obviously, $S\sim T$ implies $\langle S\rangle_n\simeq\langle T\rangle_n$. For example, in Fig. 1 ($S=\{\pm 1,\pm 5\}$, $T=\{\pm1,\pm9\}$, and $n=23$), $\langle S\rangle_n\simeq\langle T\rangle_n$ since $S\sim T$ ($l=5$).

Ádám [1] conjectured that the inverse statement is true as well. We say that a set $S\subseteq\mathbb{Z}_n$ has the *Ádám property* if for any other set $T\subseteq\mathbb{Z}_n$ of the same cardinality $\#T=\#S$, the isomorphism $\langle S\rangle_n\simeq\langle T\rangle_n$ implies the proportionality $S\sim T$. Thus, the *Ádám conjecture* is equivalent to the statement that all sets $S\subseteq\mathbb{Z}_n$ have Ádám property.

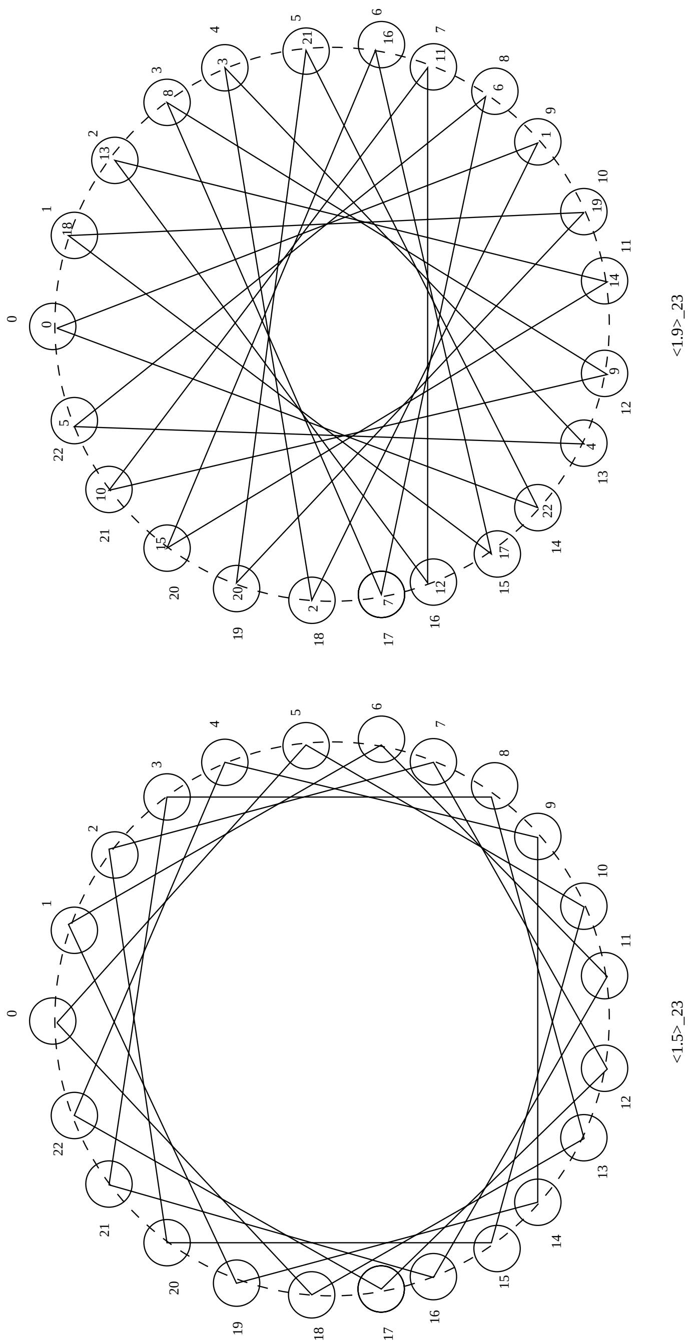

Fig. 1.

In [10], Elspas and Turner give a counterexample of 6-element sets

$$S_1 = \{\pm 1, \pm 2, \pm 7\} \subseteq \mathbb{Z}_{16}, \quad S_2 = \{\pm 1, \pm 6, \pm 7\} \subseteq \mathbb{Z}_{16},$$

that shows that the Ádám conjecture is *false*. It is easy to verify that the isomorphism $\langle S_1 \rangle_{16} \simeq \langle S_2 \rangle_{16}$ is given by the following permutation on $\mathbb{Z}_{16}$:

$$i \mapsto \begin{cases} -5i & \text{if } i \equiv 0 \,(\text{mod}\, 2), \\ -5i-4 & \text{if } i \not\equiv 0 \,(\text{mod}\, 2), \end{cases} \quad i \in \mathbb{Z}_{16},$$

but $S_1 \not\sim S_2$.

In fact, counterexamples exist for any values of n except, maybe, n of the form $n = 2^{\alpha} 3^{\beta} m$, where $\alpha \in \{0,1,2,3\}$, $\beta \in \{0,1,2\}$, $\gcd(m,6) = 1$ and m is squarefree (see [2]).

Nevertheless, there are several very important families of circulant graphs for which the Ádám conjecture holds. In particular, Muzychuk has obtained substantial results by showing that the Ádám conjecture is true for circulant graphs with a squarefree number of vertices [23] and with a twice squarefree number of vertices [24].

The conjecture also holds for 4-element sets S (see [7,12,18]). The corresponding graphs, known as *double loops*, have many applications to computer science.

In fact, it has been discovered in several papers that, under some additional restrictions, the isomorphism property of graphs can be replaced by the property of their isospectrality.

We recall that the spectrum $\operatorname{Spec} G$ of a graph G is the set of eigenvalues with multiplicities of its adjacency matrix. In particular, isomorphic graphs have the same spectra (although the inverse statement is obviously false, see [15]).

Respectively, we say that a set $S \subseteq \mathbb{Z}_n$ has the *spectral Ádám property* if for any other set $T \subseteq \mathbb{Z}_n$ the isospectrality $\operatorname{Spec} S \simeq \operatorname{Spec} T$ implies the proportionality $S \sim T$.

Here we describe a general class of sets having the spectral Ádám property.

For example, it is shown in [20] that any 4-element set $S = \{\pm 1, \pm d\} \subseteq \mathbb{Z}_n$ (an important sub-family of double loop circulant graphs), has the spectral Ádám property, provided that $2 \leqslant d < \min\{n/4, \varphi(n)/2\}$, where $\varphi(n)$ is the Euler function. Here, we settle the question completely and give a complete classification of all possible isospectral graphs.

We also show that for any fixed m the probability that a random m-element set $S \subseteq \mathbb{Z}_n$ does not have the spectral Ádám property, is $O(n^{-1})$.

2. Auxiliary results

Let us define $\zeta = \exp(2\pi\imath/n)$ where $\imath = \sqrt{-1}$.

We consider the equation

$$a_0 + \sum_{j=1}^{k-1} a_j \zeta^{w_j} = 0 \quad (w_1, \ldots, w_{k-1}) \in \mathbb{N}^{k-1}, \tag{1}$$

where $a_0, \ldots, a_{k-1}$ are non-zero integers.

We call a solution $(w_1,\dots,w_{k-1})$ of (1) *irreducible* if

$$\sum_{j\in J} a_j\zeta^{w_j}\neq 0$$

for any *proper* subset $J\subset\{1,\dots,k-1\}$.

Such equations and their various generalizations have been studied in the literature a great deal [6,9,11,21,28–30].

We summarize the results of [6,21] in the following lemma.

Lemma 1. *For any irreducible solution of Eq.* (1) *the ratio*

$$Q=\frac{n}{\gcd(n,w_1,\dots,w_{k-1})}$$

is squarefree and

$$\sum_{p|Q}(p-2)\leqslant k-2,$$

where the sum is taken over all prime divisors of Q.

In particular, one can see that $Q=1$ if all prime divisors of n are greater than k and that $Q\in\{1,2\}$ if n is a power of 2.

Let us denote

$$Q_k=\max\left\{m\mid m\text{ is square free and }\sum_{p|m}(p-2)\leqslant k-2\right\},$$

where both, the product and the sum, are taken over distinct prime numbers. Thus for the quantity Q of Lemma 1 we have $Q\leqslant Q_k$.

From the known results on the distribution of prime numbers one easily derives that

$$Q_k\leqslant\exp((1+\mathrm{o}(1))k^{1/2}\log^{1/2}k),$$

see [6,29,30].

There are also generalizations of Lemma 1 to equations with coefficients from algebraic number fields, see [9,29,30]. We do not present these results in the full generality but just formulate the following statement which we need for the classification double loop graphs and which can easily be derived from [9,29,30].

To prove Lemma 8 we need the following:

Lemma 2. *Suppose that (w_1,w_2,w_3) is an irreducible solution of the equation $a_0+a_1\zeta^{w_1}+a_2\zeta^{w_2}+a_3\zeta^{w_3}=0$, with $a_0,a_1,a_2,a_3\in\mathbb{Q}(\imath\sqrt{3})$. Then*

$$\frac{n}{\gcd(n,w_1,w_2,w_3)}\,\Bigg|\,6.$$

If (w_1, w_2, w_3, w_4) *is an irreducible solution of the equation* $a_0 + a_1\zeta^{w_1} + a_2\zeta^{w_2} + a_3\zeta^{w_3} + a_4\zeta^{w_4} = 0$, *with* $a_0, a_1, a_2, a_3, a_4 \in \mathbb{Q}(\imath\sqrt{3})$. *Then*

$$\left.\frac{n}{\gcd(n, w_1, w_2, w_3, w_4)}\right| 30.$$

This is a particular case of a result due to Zannier [29, Theorem 1], see also [9,30].
It is easy to verify that for $S \subset \mathbb{Z}_n$,

$$\mathrm{Spec}\,\langle S\rangle_n = \left\{ \sum_{s\in S} \zeta^{ls} \mid l = 0, 1, \ldots, n-1 \right\}.$$

The following result is based on the previous representation and provides a connection between circulant graphs and equations roots of unity. It extends the approach of [20] (see the proof of Theorem 2).

Lemma 3. *Let* $S, T \subseteq \mathbb{Z}_n$ *be such that* $\mathrm{Spec}\,\langle S\rangle_n = \mathrm{Spec}\,\langle T\rangle_n$ *but* $S \not\sim T$. *Then there exists* l, $1 \leqslant l \leqslant n-1$, *such that the polynomial*

$$F(X) = \sum_{s\in S} X^s - \sum_{t\in T} X^{lt}$$

is not identical to zero modulo $X^n - 1$ *and* $F(\zeta) = 0$.

We remark that, in other words, the polynomial $F(X)$ does not vanish if one replaces the exponents lt, $t \in T$, by its smallest positive residues modulo n.

3. General estimates

Here we obtain a general condition under which a set $S \subseteq \mathbb{Z}_n$ has the spectral Ádám property.

Let us denote

$$\rho_m = \min_{2\leqslant k\leqslant m} \max\left\{ \frac{1}{Q_{2k}}, \frac{k-1}{Q_{m+k-\lceil m/k\rceil+1}} \right\}.$$

Obviously $\rho_m \geqslant 1/Q_{2m}$ thus we have the asymptotic inequality

$$\rho_m \geqslant \exp(-(2^{1/2} + \mathrm{o}(1))m^{1/2} \log^{1/2} m),$$

which can be shown to be tight in the sense $\log \rho_m \sim -\log Q_{2m}$, $m \to \infty$. However, for smaller values of m one can obtain numerical estimates which are better than

$\rho_m \geqslant 1/Q_{2m}$. For example:

m	ρ_m	$1/Q_{2m}$	m	ρ_m	$1/Q_{2m}$
2	1/6	1/6	7	2/105	1/210
3	1/15	1/30	8	2/105	1/330
4	1/15	1/42	9	4/231	1/462
5	2/35	1/70	10	3/770	1/2310
6	1/42	1/210			

Theorem 4. *Let $S=\{s_1,\ldots,s_m\}\subseteq\mathbb{Z}_n$ be an m-element set which does not satisfy the spectral Ádám property. Then the bound*

$$\max_{1\leqslant i<j\leqslant m} |\, s_i - s_j \,| \geqslant \rho_m n$$

holds.

Proof. From Lemma 3 we conclude that for some non-empty subsets $U\subseteq S$ and $V\subseteq lT$ with $U\cap V=\emptyset$ we have

$$\sum_{u\in U}\zeta^u - \sum_{v\in V}\zeta^v = 0.$$

We split this equation into the largest possible set of r, $m\geqslant r\geqslant 1$, subequations

$$\sum_{u\in U_\mu}\zeta^u - \sum_{v\in V_\mu}\zeta^v = 0, \quad \mu=1,\ldots,r$$

with a non-empty set U_μ, $1\leqslant\mu\leqslant r$, where

$$U=\bigcup_{\mu=1}^{r} U_\mu, \quad V=\bigcup_{\mu=1}^{r} V_\mu$$

and

$$U_\mu\cap U_v = V_\mu\cap V_v=\emptyset, \quad 1\leqslant\mu<v\leqslant r.$$

Let R be the set of $\mu=1,\ldots,r$ for which $\#U_\mu\geqslant 2$. We put

$$L=\#R, \quad M=\sum_{\mu\in R}\#U_\mu.$$

Because $\#U_\mu=\#V_\mu=1$ is not possible, $\mu=1,\ldots,r$, we see that there are $r-L=m-M$ values of $\mu=1,\ldots,r$ with $\mu\notin R$ and $\#V_\mu\geqslant 2$ for each such μ. Therefore for any $\mu\in R$

$$\#V_\mu \leqslant m-L-2(m-M)+1 = 2M-m-L+1. \tag{2}$$

First of all let us select a pair (U_μ,V_μ), $\mu\in R$, for which the total cardinality $N=\#U_\mu+\#V_\mu$ is minimal.

Denote

$$\Delta = \max_{1 \leqslant i < j \leqslant m} |s_i - s_j|.$$

Select two arbitrary distinct elements $u_1, u_2 \in U_\mu$ with $0 < |u_1 - u_2| \leqslant \Delta$. Dividing out the corresponding equation by ζ^{u_1} we obtain the equation

$$1 + \zeta^{u_2 - u_1} + \sum_{u \in U \setminus \{u_1, u_2\}} \zeta^u - \sum_{v \in V} \zeta^v = 0.$$

Applying Lemma 1 we derive

$$\Delta \geqslant \gcd(|u_1 - u_2|, n) \geqslant \frac{n}{Q_N}. \tag{3}$$

Now we select a pair (U_η, V_η) for which the first set has the largest cardinality

$$K = \#U_\eta \geqslant \#U_\nu, \quad \nu \neq \eta.$$

Then the selected subset $U_\eta \subseteq S$ contains at least one pair $u_1, u_2 \in U_\eta$ with $0 < |u_1 - u_2| \leqslant (\Delta - 1)/(K - 1)$. Dividing out the corresponding equation by ζ^{u_1}, using bound (2) and applying Lemma 1 we obtain that

$$\Delta \geqslant \frac{n(K-1)}{Q_{2M+K-m-L+1}} + 1.$$

We have $K \geqslant M/L$, thus $L \geqslant \lceil M/K \rceil$ and we derive

$$Q_{2M+K-m-L+1} \leqslant Q_{M+K-\lceil M/K \rceil + 1} \leqslant Q_{m+K-\lceil m/K \rceil + 1}$$

hence

$$\Delta \geqslant \frac{n(K-1)}{Q_{m+K-\lceil m/K \rceil + 1}} + 1. \tag{4}$$

Obviously

$$\sum_{\mu \in R} \#V_\mu = m - \sum_{\mu \notin R} \#V_\mu \leqslant m - \sum_{\mu \notin R} 1 = \sum_{\mu \in R} \#U_\mu = M.$$

Since $N \leqslant 2M/L \leqslant 2K$, combining bounds (3) and (4) we derive the desired estimate. □

Similar arguments show that if the smallest prime divisor of n is greater than m then the spectral Ádám property holds for all m-element sets $S = \{s_1, \ldots, s_m\} \subseteq \mathbb{Z}_n$.

It also easy to see that, when n is a power of 2 (a popular application case), the sets $S = \{s_1, \ldots, s_m\} \subseteq \mathbb{Z}_n$, satisfy the Ádám property if

$$\max_{1 \leqslant i < j \leqslant m} |s_i - s_j| < n/2.$$

Denote by $A_m(n)$ the number of m-element sets $S = \{s_1, \ldots, s_m\} \subseteq \mathbb{Z}_n$ which do not satisfy the spectral Ádám property.

Theorem 5. *For any fixed* m, *the bound*

$$A_m(n) = \mathrm{O}(n^{m-1})$$

holds.

Proof. Let $S = \{s_1, \dots, s_m\} \subseteq \mathbb{Z}_n$ be an m-element set which does not satisfy the spectral Ádám property. We use the same notations as in the proof of Theorem 4.

Then for every pair $u_1, u_2 \in U_\mu$ we have $\gcd(|u_1 - u_2|, n) \geqslant n/Q_{2m}$. Therefore if u_1 is fixed then u_2 can take at most $Q_{2m} = \mathrm{O}(1)$ possible values. It is easy to see that there are at most $\mathrm{O}(n^{m-1})$ m-element sets $S \subseteq \mathbb{Z}_n$ satisfying this condition. □

We can easily deduce from Theorem 5 that, for any fixed m, the probability that a random m-element set $S \subseteq \mathbb{Z}_n$ does not have the spectral Ádám property, is $\mathrm{O}(n^{-1})$. In fact, Theorem 5 can be used to obtain an asymptotic formula for the number of non-isomorphic circulant graphs.

For an integer $r \geqslant 1$, $\mu(r)$ denotes the Möbius function. We recall that $\mu(1)=1$, $\mu(r) = 0$ if $r \geqslant 2$ is not square-free and $\mu(r) = (-1)^{\nu(r)}$ otherwise, where $\nu(r)$ denotes the number of prime divisors of r.

We also define

$$\varphi_m(n) = n^m \sum_{d|n} \frac{\mu(d)}{d^m}.$$

In particular, $\varphi_1(n) = \varphi(n)$ is the Euler function of n. It is well known that

$$\varphi(n) \geqslant c \frac{n}{\log(\log n + 2)} \tag{5}$$

for some absolute constant $c > 0$ and, see [27, Theorem 5.1 of Chapter 1]. It is easy to see that the same considerations show that

$$n^m \geqslant \varphi_m(n) \geqslant C n^m, \quad m \geqslant 2$$

for some absolute constant $C > 0$.

Let $I_m(n)$ denote the number of non-isomorphic circulant graphs and let $J_m(n)$ denote the number of non-isomorphic connected circulant graphs.

Theorem 6. *For any fixed* $m \geqslant 2$ *and sufficiently large* n *the asymptotic formulas*

$$I_m(n) = \frac{n^m}{\varphi(n)} + \mathrm{O}(n^{m-1}) \quad \textit{and} \quad J_m(n) = \frac{\varphi_m(n)}{\varphi(n)} + \mathrm{O}(n^{m-1})$$

hold.

Proof. First of all, we remark that for any fixed l such that $\gcd(l, n) = 1$ and $l \neq 1$ there are at most $\mathrm{O}(n^{m/2})$ sets $S = \{s_1, \dots, s_m\} \subseteq \mathbb{Z}_n$ with $S = lS$. Indeed, if l if or multiplicative order t modulo n then any such set S consists of conjunction or subsets of the form $\{s, sl, \dots, sl^{t-1}\} \in \mathbb{Z}_n$. Thus at each such set S has no more than $m/t \leqslant m/2$ "free" elements.

Therefore, there are at most $O(n^{m/2}\varphi(n))$ sets $S \subseteq \mathbb{Z}_n$ for which $S = lS$ with some $l \in \mathbb{Z}_n$ such that $\gcd(l, n) = 1$ and $l \neq 1$.

From all other sets we select the collection $S_1, \dots, S_A \subseteq \mathbb{Z}_n$ of pairwise nonproportional sets which do not satisfy the spectral Ádám property and a collection $S_1, \dots, S_B \subseteq \mathbb{Z}_n$ of pairwise nonproportional sets which satisfy the spectral Ádám property.

It is clear that

$$(A + B)\varphi(n) = \binom{n}{m} + O(n^{m/2}\varphi(n))$$

and that $A\varphi(n) \leqslant A_m(n)$. Therefore,

$$I_m(n) = B + O(A) = \frac{1}{\varphi(n)}\left(\binom{n}{m} + O(n^{m/2} + A_m(n))\right).$$

Applying Theorem 5 we obtain the desired asymptotic formula for $I_m(n)$.

To obtain an asymptotic formula for $J_m(n)$ we estimate the number $N_m(n)$ of sets $S = \{s_1, \dots, s_m\} \subseteq \mathbb{Z}_n$ with $\gcd(s_1, \dots, s_m, n) = 1$. Indeed, using the same considerations as above, we obtain

$$J_m(n) = \frac{1}{\varphi(n)} N_m(n) + O(n^{m-1}).$$

Let $M_m(d, n)$ be the number of sets $S = \{s_1, \dots, s_m\} \subseteq \mathbb{Z}_n$ with

$$\gcd(s_1, \dots, s_m, n) \equiv 0 \pmod{d}.$$

Obviously,

$$M_m(d, n) = \binom{n/d}{m} = \left(\frac{n}{d}\right)^m + O\left(\left(\frac{n}{d}\right)^{m-1}\right).$$

From the inclusion–exclusion principle we see

$$N_m(n) = \sum_{d|n} \mu(d) M_m(d, n) = \varphi_m(n) + O\left(n^{m-1} \sum_{d|n} d^{-m+1}\right).$$

Using that the bound

$$\sum_{d|n} d^{-m+1} \leqslant \sum_{d|n} d^{-1} = \frac{1}{n} \sum_{d|n} d = O(\log\log n)$$

see [16, Theorem 323] and bound (5), we obtain the desired result. □

4. Double loops

In this section we concentrate on double-loop circulant graphs. They are generated by sets $S=\{\pm a, \pm b\} \in \mathbb{Z}_n$ with the condition that $1 \leqslant a < b < n/2$.

Assuming that the graphs are connected is equivalent to the solvability of the congruence $ax + by \equiv 1 \pmod n$, thus to the condition $\gcd(a, b, n) = 1$.

Lemma 7. *Any set* $S=\{\pm a, \pm b\} \subseteq \mathbb{Z}_n$ *with* $\gcd(a, b, n) = 1$ *which is not of the form*

$$W_e = \{\pm e, \pm(n/2 - e)\}, \quad X_h = \{\pm h, \pm n/4\}, \tag{6}$$

$$Y_f = \{\pm f, \pm(n/3 - f)\}, \quad Z_g = \{\pm g, \pm(n/6 - g)\} \tag{7}$$

satisfies the spectral Ádám property. Furthermore, the only graphs that have to be considered, among the four special cases, are those for which the involved fractions are integers.

Proof. Without loss of generality, we assume that

$$0 < a, b < n/2. \tag{8}$$

We start by noticing that the eigenvalues of $\langle\{\pm a, \pm b\}\rangle$ are

$$\lambda_k = \zeta^{ka} + \zeta^{-ka} + \zeta^{kb} + \zeta^{-kb} = 4\cos\left(\frac{\pi k}{n}(a+b)\right)\cos\left(\frac{\pi k}{n}(a-b)\right)$$

where $k = 1, \ldots, n$.

We can assume that $\lambda_1 \neq 0$ since if $\lambda_1 = 0$ then we would have that $2 \mid n$ and either $a - b = n/2$ which is impossible by (8) or $a + b = n/2$ which implies (again by (8)) that $\{\pm a, \pm b\} = W_a$.

We can also assume that $\zeta^b + \zeta^{-b} \neq 0$ and since if $\zeta^b + \zeta^{-b} = 2\cos(2\pi b/n) = 0$ then we would have $b = n/4$. This implies that $\{\pm a, \pm b\} = X_a$. For the same reason we can assume that $\zeta^a + \zeta^{-a} \neq 0$.

Let us now suppose that $\mathrm{Spec}\langle S\rangle_n = \mathrm{Spec}\langle T\rangle_n$, where $T = \{\pm c, \pm d\} \subseteq \mathbb{Z}_n$.

We know that there exists k, $1 \leqslant k \leqslant n$, such that

$$\zeta^a + \zeta^{-a} + \zeta^b + \zeta^{-b} - \zeta^{kc} - \zeta^{-kc} - \zeta^{kd} - \zeta^{-kd} = 0. \tag{9}$$

We claim that either n is a divisor of 420 (and for these values Lemma 7 can be verified via extensive calculations) or the sum in (9) must have a subsum of length 2 that vanishes.

So assume that (9) does not have any subsum of length two that vanishes, then there are 3 possibilities:

(1) *The sum in* (9) *does not have any proper subsum that vanishes*. In this case Lemma 1 implies that $n/\gcd(n, 2a, b-a, b+a)$ has to be a factor of 210 and by an

easy argument we have that $\gcd(n, 2a, b-a, b+a)$ divides 2, since $\gcd(n, a, b) = 1$. Therefore n is a divisor of 420.

(2) *The sum in* (9) *splits as the sum of two terms of length four each vanishing and no other subsum vanishing*. Here we have to distinguish between two subcases according to where ζ^a, ζ^{-a}, ζ^b and ζ^{-b} lie relatively to these two terms (note that they cannot all lie in one sum otherwise we would have $\lambda_1 = 0$):

(a) If one of the two terms contains at the same time ζ^a and ζ^{-a} and the other term contains at the same time ζ^b and ζ^{-b}, then by Lemma 1 we would conclude that $n/\gcd(n, 2a)$ divides 6 and also $n/\gcd(n, 2b)$ divides 6 and this implies that $n \mid 12$. Indeed, if

$$\frac{n}{\gcd(n, 2a)} \Bigg| \, 6$$

then $a = cn/12$ for some $1 \leqslant c \leqslant 12$. Similarly $b = dn/12$ for some $1 \leqslant d \leqslant 12$. Since $\gcd(a, b, n) = 1$, for some $l_1, l_2, l_3 \in \mathbb{Z}$ we have the identity $1 = l_1 a + l_2 b + l_3 n$ from which we get $12 = (l_1 c + l_2 d + 12 l_3)n$, thus, $n \mid 12$.

(b) If one of the two terms contains at the same time three elements out of ζ^a, ζ^{-a}, ζ^b, ζ^{-b} (say the first three), then by Lemma 1, $n/\gcd(n, 2a, b-a)$ divides 6 and this again implies that $n \mid 12$.

(c) If one of the two terms contains a and b or a and $-b$ then by Lemma 1 we see that $n/\gcd(n, a \pm b)$ divides 6. Therefore $b = cn/6 \pm a$ and therefore $\{\pm a, \pm b\} = Y_{\pm a}$ or $\{\pm a, \pm b\} = Z_{\pm a}$.

(3) *The sum in* (9) *splits as the sum of two terms*, *one of length 5 and one of length 3*, *each one vanishing and no other subsum vanishes*. If the sum of length 5 contains at least three elements of $\{\pm a, \pm b\}$ then we immediately deduce that $n \mid 60$ and we have already ruled out these possibilities. If the sum of length 3 contains three elements of $\{\pm a, \pm b\}$, then we come to the same conclusion. Therefore, we assume that both the sums of length 3 and the one of length 5 contains two elements of $\{\pm a, \pm b\}$. Note that the two elements in the term of length three have to be ζ^a and ζ^{-a} or ζ^b and ζ^{-b} since if it is not the case, by conjugating this term, we obtain a subsum of the term of length 5 that vanishes. Finally by Lemma 1 applied to the sum of length 3 we obtain

$$\frac{n}{\gcd(n, 2a)} \Bigg| \, 6$$

and by Lemma 1 applied to the sum of length 5, we obtain

$$\frac{n}{\gcd(n, 2b)} \Bigg| \, 30.$$

These two conditions imply (by the same argument as in (2)(a) above, since $\gcd(n, a, b) = 1$) that $n \mid 60$.

This proves the claim that there is a subsum of (9) of length two that vanishes.

Now, we affirm that the condition $\lambda_1 \neq 0$ implies that if the sum in (9) contains a subsum of length 2 that vanishes of the form

$$\zeta^t + \zeta^s = 0.$$

Then we must have $s = -t$ and therefore $t = n/4$ or $3n/4$.

Indeed, if $\zeta^t + \zeta^s = 0$ for some $t \neq -s$, then either $t, s \in \{\pm a, \pm b\}$ or $t, s \in \{\pm kc, \pm kd\}$. In both case, by taking the conjugates, we deduce that $\zeta^{-t} + \zeta^{-s} = 0$. This implies that $\lambda_1 = 0$ which contradicts our assumption.

So, if $t = \pm n/4 \in \{\pm a, \pm b\}$, then we are left with $S = X_s$ which we had excluded. If $t = \pm n/4 \in \{\pm kc, \pm kd\}$, then the sum in (9) splits as a sum of length two that vanishes plus a sum of length 6 that vanishes. Three cases may occur for the latter sum:

(1) *It does not have any subsum that vanishes.* In this case

$$\left.\frac{n}{\gcd(n, 2a, b-a, b+a)}\right| 30$$

and so $n \mid 60$ (as before, we remark that $\gcd(n, 2a, b-a, b+a)$ divides 2).

(2) *It splits as the sum of two subsums of length three that vanish.* In this case we proceed as above and conclude that S is be one of the exceptional sets Y_f or Z_g.

(3) *It contains a subsum of length two that vanishes.* This subsum cannot be again of the form $\zeta^s + \zeta^t$ since this implies that $\lambda_1 = 0$.

Finally, the only subsums that can possibly vanish are of the form $\zeta^t - \zeta^s$ for some t, s. Then $\{\pm a, \pm b\}$ and $\{\pm ck, \pm kd\}$ have at least two elements in common. It is now easy to deduce that the two sets have to coincide and that $(k, n) = 1$. Therefore $S = kT$. $\square$

The next step consists in classification of the special graphs. Note that we only need to show that: if any two graphs of the special cases have the same spectra then they are obtained with proportional sets.

The graphs X_h will be considered separately. We first prove the following.

Lemma 8. *If S and T are two sets among W_e, Y_f and Z_g with $e, f, g \in \mathbb{Z}_n$, with $\mathrm{Spec}\langle S\rangle_n = \mathrm{Spec}\langle T\rangle_n$, then $S \sim T$.*

Proof. We can write the eigenvalues of the special graphs in Lemma 8 as

$$\mathrm{Spec}\langle W_e\rangle = \{(1 + (-1)^k)(\zeta^{ke} + \zeta^{-ke}) \mid k = 1, \ldots, n\},$$

$$\mathrm{Spec}\langle Y_f\rangle = \{(1 + \omega^k)\zeta^{kf} + (1 + \omega^{-k})\zeta^{-kf} \mid k = 1, \ldots, n\},$$

$$\mathrm{Spec}\langle Z_g\rangle = \{(1 + \vartheta^k)\zeta^{kg} + (1 + \vartheta^{-k})\zeta^{-kg} \mid k = 1, \ldots, n\},$$

where

$$\omega = \zeta^{-n/3} = \exp(-2\pi\imath/3) = -(1 + \imath\sqrt{3})/2,$$

$$\vartheta = \zeta^{-n/6} = \exp(-\pi\imath/3) = (1 - \imath\sqrt{3})/2.$$

Note that

$$|1+\omega^k| = \begin{cases} 2 & \text{if } k \equiv 0 \pmod 3, \\ 1 & \text{if } k \equiv \pm 1 \pmod 3 \end{cases} \tag{10}$$

and

$$|1+\vartheta^k| = \begin{cases} 2 & \text{if } k \equiv 0 \pmod 6, \\ 0 & \text{if } k \equiv 3 \pmod 6, \\ \sqrt{3} & \text{if } k \equiv \pm 1 \pmod 6, \\ 1 & \text{if } k \equiv \pm 2 \pmod 6. \end{cases} \tag{11}$$

Suppose that S and T are sets in the families of statement of Lemma 8 with Spec $\langle S\rangle_n =$ Spec $\langle T\rangle_n$. Then we have the equation

$$\alpha\zeta^x + \bar{\alpha}\zeta^{-x} - \beta\zeta^{ky} - \bar{\beta}\zeta^{-ky} = 0, \tag{12}$$

where we take $x=f$ (respectively $x=g$) if $S=Y_f$ (respectively $S=Z_g$) and $x=2e$ if $S=W_e$. Note that $\alpha,\beta\in\mathbb{Q}(\imath\sqrt{3})$, $\alpha\neq 0$ and so $\beta\neq 0$, $y\in T$ and $1\leqslant k\leqslant n$.

There are two possibilities.

(1) *The sum in* (12) *does not have any proper subsum that vanishes.* In this case we immediately deduce from Lemma 2 that

$$\left.\frac{n}{\gcd(n,4x)}\right| 6.$$

Since the condition that $\langle S\rangle_n$ is connected implies that $\gcd(n,4x)$ divides 24, we deduce that n divides $6\times 24 = 144$. For these values of n the claimed result has been verified numerically.

(2) *The sum in* (12) *has two subsums of length two that vanish.* We remark that one of the subsums of length two that vanish has to be of the form

$$\alpha\zeta^x = \beta\zeta^{ky} \quad \text{or} \quad \alpha\zeta^x = \bar{\beta}\zeta^{-ky}.$$

Let us assume, without loss of generality, that the first one holds. Taking absolute values, we obtain

$$|\alpha| = |\beta|.$$

Now, using (10) and (11), we obtain:

(a) if $S=Y_f$ (for some f) then $\alpha=(1-\imath\sqrt{3})/2=\zeta^{-n/6}$, $|\alpha|=1$. Since T cannot be W_e because $(1+(\pm 1)^k)\in\{0,2\}$, only the following two cases are possible.

(i) $T=Y_{f'}$ (for some f'), $k\equiv \pm 1 \pmod 3$ and we lead to the identities:

$$\zeta^{f-n/6} = \begin{cases} \zeta^{kf'-n/6} & \text{if } k\equiv 1 \pmod 3, \\ \zeta^{kf'+n/6} & \text{if } k \equiv -1 \pmod 3. \end{cases}$$

In the first case we deduce that $f=kf'$ and since $k\equiv 1 \pmod 3$, $n/6-f=k(n/6-f')$. In the second case we deduce that $f=kf'+$

$n/3 = k(f - n/3)$ (since $k \equiv -1 \pmod 3$) and $n/3 - f = -kf'$. In both cases $S = kT$.

(ii) $T = Z_g$ (for some g), $k \equiv \pm 2 \pmod 6$, we are lead to the identities

$$\zeta^{f-n/6} = \begin{cases} \zeta^{kg-n/6} & \text{if } k \equiv 2 \pmod 6, \\ \zeta^{kg+n/6} & \text{if } k \equiv -2 \pmod 6. \end{cases}$$

In the first case we deduce that $f = kg$ and since $k \equiv 2 \bmod 6)$, $n/3 - f = k(n/6 - g)$. In the second case we deduce that $f = kg + n/3 = k(g - n/6)$ (since $k \equiv -2 \pmod 6$) and $n/3 - f = -kg$. In both cases $S = kT$.

(b) if $S = Z_g$, then $|\alpha| = \sqrt{3}$ and therefore we can exclude $T = Y_f$ or $T = W_e$. The only condition to check is that if $\mathrm{Spec}\langle Z_g\rangle_n = \mathrm{Spec}\langle Z_{g'}\rangle_n$, then $Z_g \sim Z_{g'}$. Indeed $\alpha = \imath\sqrt{3}\omega$. So, either we have

$$\imath\sqrt{3}\zeta^{g-n/3} = \imath\sqrt{3}\zeta^{kg'-n/3}$$

(with $k \equiv 1 \pmod 6$) or we have

$$\imath\sqrt{3}\zeta^{g-n/3} = \imath\sqrt{3}\zeta^{kg'-n/6}$$

(with $k \equiv -1 \pmod 6$). In the first case $g = kg'$ and $n/6 - g = n/6 - kg' = k(n/6 - g')$ so $S = kT$, in the second case $g = kg' + n/6 = -k(n/6 - g')$ and $n/6 - g = -kg'$ so $S = -kT$.

(c) if $S = W_e$ then, since $\alpha = 2$ and since we have already excluded the possibility that $T = Y_f$ and $T = Z_g$, let us assume $T = W_{e'}$ (for some e'). Note that since the graphs are connected, we have $(n/2, e) = 1 = (n/2, e')$. Therefore, up to proportional sets, we can assume that $e = 1$ and $e' = 2$. Furthermore $e' = 2$ is only possible when $4 \nmid n$. This implies that $(n/2 + 2)W_1 = W_2$.

This completes the proof of Lemma 8. □

We are now prepared to prove the following:

Theorem 9. *Any set $S = \{\pm a, \pm b\} \subseteq \mathbb{Z}_n$ with $\gcd(a, b, n) = 1$ satisfies the spectral Ádám property.*

Proof. It follows from Lemmas 7 and 8 that it is enough to show that X_h in never isospectral to any of Y_f, $X_{h'}$, W_e, Z_g unless X_h is proportional to one of them.

Note that, by simple trigonometric properties, we have that, if $\mu_0(S)$ is the multiplicity of the eigenvalue 0 in $\mathrm{Spec}\langle S\rangle_n$, then $\mu_0(W_e) \geqslant n/2$, $\mu_0(Z_g) \geqslant n/6$ and $\mu_0(Y_f) \equiv 0 \pmod 2$ while

$$\mu_0(X_h) = \begin{cases} 2 & \text{if } n \equiv 4 \pmod 8 \text{ and } 2 \nmid h, \\ 1 & \text{otherwise.} \end{cases}$$

So the only possibility for $\langle X_h\rangle_n$ to be isospectral to one of the others is either $n < 6$ or $n \equiv 4 \pmod 8$, $2 \nmid h$, and the possible exception is $\langle Y_f\rangle_n$. The case $\langle X_h\rangle_n$ isospectral to $\langle X_{h'}\rangle_n$ needs also to be considered separately.

Note that

$$\operatorname{Spec}\langle X_h\rangle_n=\{\imath^l+\imath^{-l}+\zeta^{lh}+\zeta^{-lh}\mid l=1,\ldots,n\}.$$

Take $l=4$ and consider the eigenvalue

$$2+\zeta^{4h}+\zeta^{-4h}=2+2\cos(8\pi h/n)$$

We can assume that $2+\zeta^{4h}+\zeta^{-4h}\neq 0$ and that $\zeta^{4h}+\zeta^{-4h}\neq 0$ since if is not the case, then h is a multiple of $n/16$, which in virtue of the fact that $(h,n/4)=1$, implies $n=16$ that we have already excluded.

If $\langle X_h\rangle_n$ and $\langle Y_f\rangle_n$ are isospectral, we obtain the equation

$$2+\zeta^{4h}+\zeta^{-4h}=(1+\omega^k)\zeta^{kf}+(1+\omega^{-k})\zeta^{-kf}.$$

It cannot happen that a term of the left-hand side equals one on the right-hand side. If for example $\zeta^{4h}=(1+\omega^k)\zeta^{kf}$ then $2+\zeta^{-4h}=(1+\omega^{-k})\zeta^{-kf}$ and taking the conjugates of this last identity we would obtain $\zeta^{4h}=(1+\omega^k)\zeta^{kf}=2+\zeta^{4h}$ that is a contradiction.

Therefore, the above is an irreducible sum of roots of unity and by Lemma 2 we conclude that

$$\left.\frac{n}{\gcd(n,4h)}\right|30$$

and since $\gcd(n,4h)\mid 4$ we obtain $n\mid 120$.

The last case when $\langle X_h\rangle_n$ and $\langle X_{h'}\rangle_n$ are isospectral can be dealt in a similar way. Consider the eigenvalue $\zeta^h+\zeta^{-h}=2\cos(2\pi h/n)$ of $\langle X_h\rangle_n$ which again can be assumed to be not zero. If $\langle X_h\rangle_n$ and $\langle X_{h'}\rangle_n$ are isospectral, we obtain the equation

$$\zeta^h+\zeta^{-h}=\imath^l+\imath^{-l}+\zeta^{lh'}+\zeta^{-lh'}.$$

If $2\mid l$ then we would again obtain an irreducible sum of roots of unity and by Lemma 1 we conclude that

$$\left.\frac{n}{\gcd(n,h)}\right|30$$

and thus $n\mid 120$. If $2\nmid l$, then $\imath^l+\imath^{-l}=0$ and therefore $h\equiv\pm\, lh' \bmod n$ and X_h and $X_{h'}$ would be proportional. $\square$

5. Triple loops

The example of a triple loop given at the beginning of this paper (to disprove the Ádám conjecture) can be generalized to the following. Suppose that $8\mid n$ and

$$S_1(n)=\{\pm 1,\pm 2,\pm(n/2-1)\}$$

and

$$S_2(n)=\{\pm 1,\pm(n/2-2),\pm(n/2-1)\}.$$

Then is easy to verify that the map

$$i \mapsto \begin{cases} -5i & \text{if } i \equiv 0 \,(\mathrm{mod}\, 2), \\ -5i - n/2 & \text{if } i \not\equiv 0 \,(\mathrm{mod}\, 2), \end{cases} \quad i \in \mathbb{Z}_n$$

provides an isomorphism of $\langle S_1(n)\rangle_n$ onto $\langle S_2(n)\rangle_n$. On the other hand, if $S_1(n) \sim S_2(n)$ with $S_1(n) = kS_2(n)$ then necessarily $k = \pm(n/2 - 1)$ and immediately one verifies that this leads to a contradiction. The authors wonder whether these are the only possible exceptions to the Ádám property.

Open Question 10. *Is it true that the Ádám property holds for all triple loops in* $\mathbb{Z}_n$ *if and only if* $n \not\equiv 0 \,(\mathrm{mod}\, 8)$?

Note that the methods of the previous sections, if applied to triple loops, imply that the n is coprime to 210 then the Ádám property holds (with at most a finite number of exceptions that can be verified by extensive computations). The authors might consider this problem in a future paper.

It is very important to notice that the spectral Ádám property is *weaker* than the Ádám property in the sense that there are isospectral circulant graphs which are not isomorphic. Such graphs (isospectral but not isomorphic) are called *cospectral* and have been studied extensively for other particular cases (for example, see [15,14]).

To show this we assume that 12 divides n and define the sets

$$S^-(n) = \{\pm 1, \pm(n/6 - 1), \pm(n/3 + 1)\},$$
$$S^+(n) = \{\pm 1, \pm(n/6 + 1), \pm(n/3 - 1)\}.$$

Then one can easily show that

$$\mathrm{Spec}\langle S^-(n)\rangle_n = \mathrm{Spec}\langle S^+(n)\rangle_n.$$

Indeed, let

$$\lambda_m^\pm = 2\left(\cos\left(\frac{2\pi m}{n}\right) + \cos\left(\frac{2\pi m}{n}(n/6 \mp 1)\right) + \cos\left(\frac{2\pi m}{n}(n/3 \pm 1)\right)\right).$$

Then $\mathrm{Spec}\langle S^\pm(n)\rangle = \{\lambda_m^\pm \mid m = 1,\ldots,n\}$ and we can write

$$\lambda_m^\pm = 2\left(\cos\frac{2\pi m}{n}\left(1 + \cos\frac{\pi m}{3} + \cos\frac{2\pi m}{3}\right)\right.$$
$$\left.\pm \sin\frac{2\pi m}{n}\left(\sin\frac{\pi m}{3} - \sin\frac{2\pi m}{3}\right)\right).$$

Now note that $1 + \cos \pi m/3 + \cos 2\pi m/3 = 0$ for $m \equiv \pm 2 \,(\mathrm{mod}\, 6)$ while $\sin \pi m/3 - \sin 2\pi m/3 = 0$ for $m \equiv 0, \pm 1, 3 \,(\mathrm{mod}\, 6)$. We deduce that for $m \equiv 0, \pm 1, 3 \,(\mathrm{mod}\, 6)$, $\lambda_m^+ = \lambda_m^-$. while for $m \equiv \pm 2 \,(\mathrm{mod}\, 6)$,

$$\lambda_m^+ = -\lambda_m^- \quad \text{and} \quad \lambda_m^+ = \begin{cases} 2\sqrt{3}\sin(2\pi m/n) & \text{if } m \equiv 2 \,(\mathrm{mod}\, 6), \\ -2\sqrt{3}\sin(2\pi m/n) & \text{if } m \equiv -2 \,(\mathrm{mod}\, 6) \end{cases}$$

and since 4 divides n, $\lambda^{\pm}_{m+n/2} = -\lambda^{\pm}_{m}$ so that $\lambda^{+}_{m} = \lambda^{-}_{m+n/2}$ for these values of m. This proves the claim.

On the other hand, numerical computation for $n \equiv 0 \pmod{12}$ $(n \leqslant 180)$ shows that these graphs are not isomorphic.

Moreover, for $n = 24$ and 36 it is easy to provide simple combinatorial proofs of this statement which do not refer to extensive numerical computation.

First of all we show that, for $\mathbb{Z}_{24}$, with $S^{-}(24) = \{\pm 1, \pm 3, \pm 9\}$ and $S^{+}(24) = \{\pm 1, \pm 5, \pm 7\}$,

$$\langle S^{-}(24) \rangle_{24} \not\simeq \langle S^{+}(24) \rangle_{24}.$$

To prove this, we build the *surroundings* $T^{-}_{24}(0)$ and $T^{+}_{24}(0)$ for each graph, respectively, and show that they are not isomorphic. We recall that the *surrounding* $T_n(u)$ of a node u of a given graph G of order n is a rooted graph isomorphic to G such that an appropriate isomorphism maps the children of the node u to the children of the root, and recursively the children of a node to the, not yet reached, neighbors of that node (until all nodes have been mapped). Since these graphs are bipartite, we can define $A_u(v)$ ($D_u(v)$) as the set of ancestors (respectively, the set of descendants) of the node v in the surrounding $T_n(u)$. By definition, $A_u(u) = \emptyset$ and $D_u(u)$ is the set of all neighbors of u.

In our cases, since the graphs are vertex transitive, without loss of generality, it is sufficient to compare $T_n(0)^{-}$ and $T^{+}_{n}(0)$.

For T^{-}_{24}, we have $D^{-}_{0}(0) = \{1, 3, 9, 15, 21, 23\}$, and hence

$$\begin{array}{lccccccccccccc}
D^{-}_{0}(1) = & \{ & 2, & 4, & & & 10, & & & 16, & & & 22 & \}, \\
D^{-}_{0}(3) = & \{ & 2, & 4, & 6, & & & 12, & & & 18, & & & \}, \\
D^{-}_{0}(9) = & \{ & & & 6, & 8, & 10, & 12, & & & 18, & & & \}, \\
D^{-}_{0}(15) = & \{ & & & 6, & & & 12, & 14, & 16, & 18, & & & \}, \\
D^{-}_{0}(21) = & \{ & & & 6, & & & 12, & & & 18, & 20, & 22 & \}, \\
D^{-}_{0}(23) = & \{ & 2, & & & 8, & & & 14, & & & 20, & 22 & \}.
\end{array}$$

Similarly, for T^{+}_{24}, we have $D^{+}_{0}(0) = \{1, 5, 7, 17, 19, 23\}$, and hence

$$\begin{array}{lccccccccccccc}
D^{+}_{0}(1) = & \{ & 2, & & 6, & 8, & & & & & 18, & 20, & & \}, \\
D^{+}_{0}(5) = & \{ & & 4, & 6, & & 10, & 12, & & & & & 22 & \}, \\
D^{+}_{0}(7) = & \{ & 2, & & 6, & 8, & & 12, & 14, & & & & & \}, \\
D^{+}_{0}(17) = & \{ & & & & & 10, & 12, & & 16, & 18, & & 22 & \}, \\
D^{+}_{0}(19) = & \{ & 2, & & & & & 12, & 14, & & 18, & 20, & & \}, \\
D^{+}_{0}(23) = & \{ & & 4, & 6, & & & & & 16, & 18, & & 22 & \}.
\end{array}$$

In both surroundings, at distance 2 from node 0, only node 2 and node 22 have 3 ancestors. To prove that these two graphs are not isomorphic, it is sufficient to prove that a mapping between the two surroundings sets for nodes 2 and 22 cannot exist.

For the surrounding T^{-}_{24} we have $A^{-}_{0}(2) = \{1, 3, 23\}$ and $A^{-}_{0}(22) = \{1, 21, 23\}$, hence $A^{-}_{0}(2) \cap A^{-}_{0}(22) = \{1, 23\}$, that is, nodes 2 and 22 have two common ancestors.

Whereas, for $T{+}_{24}$ we have $A^{+}_{0}(2) = \{1, 7, 19\}$ and $A^{+}_{0}(22) = \{5, 17, 23\}$, hence $A^{+}_{0}(2) \cap A^{+}_{0}(22) = \emptyset$, that is, nodes 2 and 22 have no common ancestors.

Clearly, since $|A_0^-(2) \cap A_0^-(22)| \neq |A_0^+(2) \cap A_0^+(22)|$, the surroundings cannot map which proves that $\langle S^-(24)\rangle_{24} \not\simeq \langle S^+(24)\rangle_{24}$.

A similar study can be done for $\mathbb{Z}_{36}$, with $S^-(36) = \{\pm 1, \pm 5, \pm 13\}$ and $S^+(36) = \{\pm 1, \pm 7, \pm 11\}$. To prove that

$$\langle S^-(36)\rangle_{36} \not\simeq \langle S^+(36)\rangle_{36}$$

we proceed as before, building surroundings T_{36}^- and T_{36}^+.

In both surroundings, at distance 3 from node 0, only two nodes have 4 ancestors (nodes 15 and 21 for T_{36}^-, and nodes 9 and 27 for T_{36}^+).

For T_{36}^-, $A_0^-(15) = \{2, 10, 14, 28\}$ and $A_0^-(21) = \{8, 22, 26, 34\}$, hence nodes 15 and 21 have no common ancestors.

Whereas, for T_{36}^+, $A_0^+(9) = \{2, 8, 10, 34\}$ and $A_0^+(27) = \{2, 10, 26, 28\}$, hence $A_0^+(9) \cap A_0^+(27) = \{2, 10\}$, that is, two common ancestors. Clearly, this proves that the surroundings cannot map, and thus, that the two graphs are not isomorphic.

As the computational results, and the simple combinatorial arguments for cases $n = 24$ and 36, suggest, the authors believe that, in fact, these graphs are never isomorphic.

Open Question 11. *Prove that* $S^-(n) \not\simeq S^+(n)$ *for all* $n \equiv 0 \pmod{12}$.

One can also construct similar examples of cospectral triple loops on n vertices with $n \equiv 6 \pmod{12}$.

6. Remarks

Here instead of using the isomorphism property of graphs our method is based on a weaker property of their spectral identity. Thus, our results are more general than the original Ádám conjecture. On the other hand, this is an obvious weakness of our approach which does not use all the available information.

One can probably extend our results to the case of weighted circulant graphs. Indeed, in this case, the question can be reduced to the equation of the form (1) where instead of ± 1-coefficients it has coefficient depending on the weights. For integer weights one can use Lemma 1 and obtain essentially the same results. For graphs with algebraic weights one can use more general results of [9,29,30]. This case can also be considered without introducing any new ideas.

For equations with roots of unity with complex coefficients very general and strong results applicable to equations with arbitrary complex coefficients are available [11,28], however, it is still not quite clear how to extract analogies of Theorems 4, 5 and 9.

One more possible generalization we can be approached by our method is studying circulant graphs for which spectra have large intersection. It seems that for any $\varepsilon > 0$ one can obtain some non-trivial conclusions about sets $S, T \subseteq \mathbb{Z}_n$ such that the spectra of $\langle S\rangle_n$ and $\langle T\rangle_n$ have at least n^ε common elements, that is

$$\# \operatorname{Spec}\langle S\rangle_n \cap \operatorname{Spec}\langle T\rangle_n \geqslant n^\varepsilon.$$

Finally we remark, that we hope that our approach will be useful for some other types of graphs, including Cayley graphs.

Acknowledgements

We would like to thank Cai Heng Li for his comments on our original paper and for pointing out the reference to [12].

References

[1] A. Ádám, Research problem 2–10, J. Combin. Theory 3 (1967) 393.
[2] B. Alspach, T. Parsons, Isomorphism of circulant graphs and digraphs, Discrete Math. 25 (1979) 97–108.
[3] L. Babai, Automorphism groups, isomorphism, reconstruction, Handbook of Combinatorics, Elsevier, Amsterdam, 1995, pp. 1749–1783.
[4] J.-C. Bermond, F. Comellas, D.F. Hsu, Distributed loop computer networks: a survey, J. Parallel Distributed Comput. 24 (1995) 2–10.
[5] F. Boesch, R. Tindell, Circulants and their connectivities, J. Graph Theory 8 (1984) 487–499.
[6] J.H. Conway, A.J. Jones, Trigonometric diophantine equations (On vanishing sums of roots of unity), Acta Arith. 30 (1976) 171–182.
[7] C. Delorme, O. Favaron, M. Maheo, Isomorphisms of Cayley multigraphs of degree 4 on finite abelian groups, European J. Combin. 13 (1992) 59–61.
[8] N. Deo, M. Krishnamoorthy, Toeplitz networks and their properties, IEEE Trans. Circuits Systems 3 (1989) 1089–1092.
[9] R. Dvornicich, U. Zannier, On sums of roots of unity, Monatsh. Math. 129 (2000) 97–108.
[10] B. Elspas, J. Turner, Graphs with circulant adjacency matrices, J. Combin. Theory 9 (1970) 229–240.
[11] J.-H. Evertse, H.P. Schlickewei, The absolute subspace theorem and linear equations with unknowns from a multiplicative group, Number Theory in Progress, Vol. 1, de Gruyter, Berlin, 1999, pp. 121–142.
[12] X.G. Fang, M.Y. Xu, On isomorphisms of Cayley graphs of small valency, Algebra Coll. 1 (1994) 67–76.
[13] C. Godsil, Algebraic Combinatorics, Chapman & Hall, NY, 1993.
[14] C. Godsil, B. McKay, Constructing cospectral graphs, Aequationes Math. 25 (1982) 257–268.
[15] F. Harary, C. King, A. Mowshowitz, R.C. Read, Cospectral graphs and digraphs, Bull. London Math. Soc. 3 (1971) 321–328.
[16] G.H. Hardy, E.M. Wright, An Introduction to the Number Theory, Oxford University Press, Oxford, 1993.
[17] F.T. Leighton, Introduction to Parallel Algorithms and Architectures: Arrays, Trees, Hypercubes, M. Kaufmann, Los Altos, CA, 1992.
[18] C.H. Li, The cyclic groups with the m-DCI property, European J. Combin. 18 (1997) 655–665.
[19] B. Litow, B. Mans, On isomorphic chordal rings, Proceedings of the Seventh Australasian Workshop on Combinatorial Algorithms (AWOCA'96), University of Sydney, BDCS-TR-508, 1996, pp. 108–111.
[20] B. Litow, B. Mans, A note on the Ádám conjecture for double loops, Inform. Process. Lett. 66(3) (1998) 149–153.
[21] H.B. Mann, On linear relations between roots of unity, Mathematika 12 (1965) 171–182.
[22] B. Mans, Optimal distributed algorithms in unlabeled tori and chordal rings, J. Parallel Distributed Comput. 46(1) (1997) 80–90.
[23] M. Muzychuk, Ádám's conjecture is true in the square free case, J. Combin. Theory Ser. A 72 (1995) 118–134.
[24] M. Muzychuk, On Ádám's conjecture for circulant graphs, Discrete Math. 167/168 (1997) 497–510 (Erratum: ibid. 176 (1997) 285–298).

[25] A. Nayak, V. Acciaro, P. Gissi, A note on isomorphic chordal rings, Inform. Process. Lett. 55 (1995) 339–341 (Erratum: ibid. 57 (1996) 115).
[26] P.P. Pálfy, Isomorphism problem for relational structures with a cyclic automorphism, European J. Combin. 8 (1987) 35–43.
[27] K. Prachar, Primzahlverteilung, Springer, Berlin, 1957.
[28] H.P. Schlickewei, Equations in roots of unity, Acta Arith. 76 (1996) 171–182.
[29] U. Zannier, On the linear independence of roots of unity, Acta Arith. 50 (1989) 171–182.
[30] U. Zannier, Vanishing sums of roots of unity, Rend. Sem. Mat. Univ. Politec. Torino 53 (1995) 487–495.