On the Ádám Conjecture on Circulant Graphs

Bernard Mans[1], Francesco Pappalardi[2] and Igor Shparlinski[1]

[1] Dept of Computing, MPCE, Macquarie University, Sydney, NSW 2109, Australia.
{bmans,igor}@mpce.mq.edu.au
[2] Departimento di Matematica, Terza Università delgi Studi, Roma, 00146, Italy.
pappa@mat.uniroma3.it

1 Introduction

In this paper we study isomorphism between circulant graphs. Such graphs have a vast number of applications to telecommunication network, VLSI design and distributed computation [4, 13, 15, 17]. By suitably choosing the length of the chord between two nodes of the network, one can achieve the appropriate property: e.g., low diameter, high connectivity, or implicit routing. 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 graph the problem is known to be in **NP**, not known to be in **P**, and probably is not **NP**-complete, see Section 6 of [3]. 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 know to be false in general, even for undirected graphs [9], for several special cases it holds [5, 15, 18, 19, 20].

The *purpose* of this paper is to extend essentially the class of graphs having the Ádám property and even more general spectral Ádám property as well as to introduce a new technique, which is based on some number theoretic results about equations in roots of unity, which we believe can be applied to several other questions of graph theory. In particular, we believe that our method can be applied to study general *Cayley* graphs, see [20]. 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 Section 3.12 of [3] or Lemma 9.2 of [12].

The new approach, which we propose here, is based on the combination of the spectral technique from [8, 9, 15] with some deep results of algebraic number theory on linear equations in roots of unity [6, 10, 16, 21, 22, 23]. In fact it can be extended to weighted circulant graphs as well. 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 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 $a_{ij} = a_{1,j-i+1}$, $i, j = 1, \ldots, n$. Hereafter, subscripts are taken modulo n. We 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 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 $\gcd(l, n) = 1$, such that $S = lT$ 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 ($S = \{1, 5\}$, $T = \{1, 9\}$, 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 $T \subseteq \mathbb{Z}_n$ 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.

The discovered in [9] counterexample of 6-element sets $S_1 = \{\pm 1, \pm 2, \pm 7\} \subseteq \mathbb{Z}_{16}$, $S_2 = \{\pm 1, \pm 6, \pm 7\} \subseteq \mathbb{Z}_{16}$ 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 furnished by the permutation on $\mathbb{Z}_{16}$ given by

$$i \to \begin{cases} -5i, & \text{if } i \equiv 0 \pmod 2; \\ -5i - 4, & \text{if } i \not\equiv 0 \pmod 2; \end{cases} \qquad i \in \mathbb{Z}_{16},$$

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 [2].

Nevertheless, there are several very important families of circulant graphs for which the Ádám conjecture holds. For example, Muzychuk has shown that the Ádám conjecture is true for circulant graphs with a squarefree number of vertices [18] and with a twice squarefree number of vertices [19]. It also holds for 4-element sets S [7, 11], see also [14]. The corresponding graphs are known as *double loops* are have many applications to computer science. In fact it has been discovered in several paper 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 the eigenvalues of its adjacency matrix. In particular, isomorphic graphs have the same spectra (although the inverse statement is obviously false). 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 [15] 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 $2 \le d < \min\{n/4, \varphi(n)/2\}$, where $\varphi(n)$ is the Euler function. Here we settle the question almost completely, with only 5 possible exceptions, for this type of graphs; for all of them $d \ge n/6$. For more general sets of the form $S = \{\pm a, \pm b\}$ there are at most 12 possible exceptions. Moreover, if $\gcd(n, 12) < 3$ then there is no exceptions at all. 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 $O(n^{-m/4})$.

2 Auxiliary Results

Let us consider the equation

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

where $\zeta = \exp(2\pi i/n)$ and $a_0, \ldots, a_{k-1}$ are nonzero integers.

We call a solution $(w_1, \ldots, w_{k-1})$ of (1) *irreducible* if $\sum_{j \in J} a_j \zeta^{w_j} \neq 0$ for any *proper* subset $J \subset \{1, \ldots, k-1\}$.

Such equations and their various generalizations have been studied in the literature a great deal [6, 10, 16, 21, 22, 23]. We summarize the results of [6, 16] in the following lemma.

Lemma 1. *For any irreducible solution of the equation (1), the fraction*

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

is squarefree and

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

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 $Q \leq 2$ if n is a power of 2. Let us denote

$$Q_k = \max \left\{ \prod_p p \mid \sum_p (p-2) \leq k-2 \right\}$$

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

From the known results on the distribution of prime numbers (see [6, 22, 23]) one easily derives that $Q_k \leq \exp\left((1 + o(1))\, k^{1/2} \log^{1/2} k\right)$.

It is easy to verify that for $S \subset \mathbb{Z}_n$, $\operatorname{Spec} \langle S \rangle_n = \left\{ \sum_{s \in S} \zeta^{ls} \mid l = 0, 1, \ldots, n-1 \right\}$.

The following result is based on the previous representation and provides a connection between circulant graphs and equations roots of unity. It lies in the background of the approach of [15] (see the proof of Theorem 4 from [15]).

Lemma 2. *Let* $S, T \subseteq \mathbb{Z}_n$ *be such that* $\operatorname{Spec}\langle S\rangle_n = \operatorname{Spec}\langle T\rangle_n$ *but* $S \not\sim T$. *Then there exists* l, $1 \le l \le n-1$, *such that the polynomials*

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

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

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

3 General Estimates

Let us denote

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

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

$$\rho_m \ge \exp\left(-\left(2^{1/2} + o(1)\right) m^{1/2}\log^{1/2} m\right),$$

which apparently 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 better than $\rho_m \ge 1/Q_{2m}$ numerical estimates. For example:

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

Theorem 3. *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*

$$\max_{1\le i<j\le m} |s_i - s_j| \ge \rho_m n.$$

Proof. From Lemma 2 we conclude that for some subsets $U \subseteq S$ and $V \subseteq T$ 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 maximal possible set of r, $m \ge r \ge 1$, subequations

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

where $U = \bigcup_{\mu=1}^r U_\mu$, $V = \bigcup_{\mu=1}^r V_\mu$ and $U_\mu \bigcap U_\nu = V_\mu \bigcap V_\nu = \emptyset$, $1 \le \mu < \nu \le r$.

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

$$L = \#R \qquad \text{and} \qquad M = \sum_{\mu \in R} \#U_\mu .$$

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 $\#V_\mu \geq 2$ for each of such μ. Therefore for any $\mu \in R$

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

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

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. Select two arbitrary distinct elements $u_1, u_2 \in U_\mu$ with $0 < |u_1 - u_2| \leq \Delta$. Dividing out the corresponding equation by u_1 and applying Lemma 1 we obtain $\Delta \geq n/Q_N$.

Now we select select a pair (U_μ, V_μ) for which the total cardinality $K = \#U_\mu$ is maximal. Then the selected subset $U_\mu \subseteq S$ contains at least one pair $u_1, u_2 \in U_\mu$ with $0 < |u_1 - u_2| \leq (\Delta - 1)/(K - 1)$. Dividing out the corresponding equation by u_1 and applying Lemma 1 we obtain that

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

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

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

We also remark that $N \leq 2M/L \leq 2K$. Combining the above inequalities we obtain the desired estimate. $\square$

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 in the most interesting for applications case when n is a power of 2 sets $S = \{s_1, \ldots, s_m\} \subseteq \mathbb{Z}_n$, satisfy the Ádám property if

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

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 4. *For any fixed m, the bound $A_m(n) = O(n^{3m/4})$ holds.*

Proof. Let $S = \{s_1, \ldots, s_m\} \subseteq \mathbb{Z}_n$ be an m-element set which does not satisfy the spectral Ádám property. We use the the same notations as in the proof of Theorem 3. Then for every pair $u_1, u_2 \in U_\mu$ we have $\gcd(|u_1 - u_2|, n) \geq n/Q_{2m}$. Therefore there are at least

$$\sum_{\mu=1}^{r} \frac{\#V_\mu(\#V_\mu - 1)}{2} \geq \sum_{\mu=1}^{r} \frac{\#V_\mu}{2} = M/2 \geq m/4$$

pairs $u_1, u_2 \in S$, $u_1 \neq u_2$, with $\gcd(|u_1 - u_2|, n) \geq n/Q_{2m}$. It is easy to see that there are at most $O(n^{3m/4})$ m-element sets $S \subseteq \mathbb{Z}_n$ satisfying this condition. $\square$

Obviously, this bound can be slightly improved as $A_m(n) = O\left(n^{m - \lceil m/4 \rceil}\right)$.

4 Double Loops

In this section we concentrate on double loop circulant graphs. That is consider circulant graphs generated by sets $S = \{\pm a, \pm b\} \in \mathbb{Z}_n$ with the condition that $1 \leq a < b < n/2$. We restrict ourselves with connected graphs which is equivalent to the solvability of the congruence $ax + by \equiv 1 \pmod{n}$, thus to the condition $\gcd(a, b, n) = 1$. We define the following 4 special families of graphs

$$\begin{aligned} W_e &= \{\pm e, \pm(n/2 - e)\}, & X_e &= \{\pm e, \pm n/4\}, \\ Y_e &= \{\pm e, \pm(n/3 - e)\}, & Z_e &= \{\pm e, \pm(n/6 - e)\}. \end{aligned}$$

First of all we need the following two simple lemmas which are based on elementary number theory

Lemma 5. *Let integers $1 \leq a < b < n/2$ be such that $\gcd(n, a, b) = 1$. If either $n/\gcd(n, a+b)$ or $n/\gcd(n, b-a)$ divides 6, then the set $\{\pm a, \pm b\}$ is proportional to one of the following 12 sets*

$$W_1; \qquad Y_e,\ e = \pm 1, 3; \qquad Z_e,\ e = \pm 1, \pm 2, \pm 3, \pm 6. \tag{3}$$

Lemma 6. *Let integers $1 \leq a < b < n/2$ be such that $\gcd(n, a, b) = 1$. If both $n/\gcd(n, 2a)$ and $n/\gcd(n, 2b)$ divides 6, then $n|12$.*

Theorem 7. *Any set $S = \{\pm a, \pm b\} \subseteq \mathbb{Z}_n$ with $\gcd(a, b, n) = 1$ except possibly one of the following 12 exceptional sets*

$$X_1; \qquad Y_e,\ e = \pm 1, 3; \qquad Z_e,\ e = \pm 1, \pm 2, \pm 3, \pm 6;$$

satisfies the spectral Ádám property.

Proof. First of all we prove the theorem assuming that S is neither one of the sets (3) nor one of the sets X_e, $e = 1, 2, 4$. Then we will rule out some of the remaining possibilities. The eigenvalues of $\langle\{\pm a, \pm b\}\rangle_n$ are

$$\begin{aligned}\lambda_k &= \zeta^{ka} + \zeta^{-ka} + \zeta^{kb} + \zeta^{-kb} \\ &= 2\left(\cos\left(\frac{2\pi ka}{n}\right) + \cos\left(\frac{2\pi kb}{n}\right)\right) = 4\cos\left(\frac{\pi k}{n}(a+b)\right)\cos\left(\frac{\pi k}{n}(a-b)\right),\end{aligned}$$

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

Assume that $\langle\{\pm a, \pm b\}\rangle_n$ has the eigenvalue $\lambda_1 = 0$. This happens only when n is even and since $0 < b - a < n/2$ we must have $a + b = n/2$. By Lemma 5, $\{\pm a, \pm b\} \sim W_1$. From now on we suppose that $\zeta^a + \zeta^{-a} + \zeta^b + \zeta^{-b} \neq 0$. Note that if it happens that $\zeta^b + \zeta^{-b} = 0$ (respectively $\zeta^a + \zeta^{-a} = 0$) this forces $b = n/4$ (respectively $a = n/4$) and since $\gcd(a, n/4) = 1$, we see that $\{\pm a, \pm b\} \sim X_e$, with some $e = 1, 2, 4$.

From now on we suppose that $\operatorname{Spec}\langle S\rangle_n = \operatorname{Spec}\langle T\rangle_n$, where $T = \{\pm c, \pm d\} \subseteq \mathbb{Z}_n$, that $S \not\sim T$ and that neither S nor T is of the sets X_e, with some $e = 1, 2, 4$.

We conclude that there exists k, $1 \leq k \leq n$, such that

$$\zeta^a + \zeta^{-a} + \zeta^b + \zeta^{-b} - \zeta^{kc} - \zeta^{-kc} - \zeta^{kd} - \zeta^{-kd} = 0. \tag{4}$$

First of all we show that is the sum in (4) contains a subsum of length 2 that vanished that this is of the form $\zeta^t + \zeta^{-t} = 0$ with $t = n/4$ or $t = 3n/4$. Indeed, $\zeta^t + \zeta^s = 0$ is possible for $s = -t = n/2 \pm n/4$ only. If $\zeta^t - \zeta^s = 0$ for some t, s then $\{\pm a, \pm b\}$ and $\{\pm kc, \pm kd\}$ have at least two elements in common. It is now easy to deduce that if this is the case, then the two sets have to coincide and $(k, n) = 1$ in this case. Given the previous argument we have the following 5 possibilities:

i. The sum in (4) does not have any proper subsum that vanishes. Lemma 1 implies that $n/\gcd(n, 2a, b-a, b+a)$ has to be a factor of 210. An easy argument shows that $\gcd(n, 2a, b-a, b+a) = \gcd(n, 2a, 2b)$ which can be 1 or 2 since $\gcd(n, a, b) = 1$. Therefore n is a divisor of 420. It is proven in [18, 19] that for values of n that are squarefree or twice a squarefree number the spectral Ádám property holds.

ii. The sum in (4) splits as a vanishing sum with 6 terms plus a sum with 2 terms and no other subsums vanish. Because sets X_e, $e = 1, 2, 4$, are excluded we may assume that none of a and b equals $n/4$. Then the sum of length 6 contains $\zeta^b + \zeta^{-b} + \zeta^a + \zeta^{-a}$ as a subsum and we can proceed and in the case **i**, concluding that $n|60$. For these values of n the statement of the theorem can be verified by the exhaustive search.

iii. The sum in (4) splits as the sum of three terms each vanishing, one of length 2, and two of length 3. Once again we may assume that none of a and b equals $n/4$. By a similar argument as above and applying Lemma 6, we can assume that one of the two sums of length three is of the form $\zeta^a + \zeta^b - \zeta^r$

or $\zeta^a + \zeta^{-b} - \zeta^r$ with $r \in \{\pm kc, \pm kd\}$. By Lemma 1, we see that $n/\gcd(n, a \pm b)$ divides 6 and by Lemma 5 we have that $\{\pm a, \pm b\}$ is proportional to one of the exceptional sets (3).

vi. The sum in (4) splits as the sum of two terms of length four each vanishing and no other subsum vanishing. We can exclude all the sums that contain at the same time either ζ^a and ζ^{-a} or ζ^b and ζ^{-b} since in this case we would deduce that n divides 240. However if a and b or a and $-b$ belongs to the same sum of length 4 then in a similar way by Lemma 1 we see that $n/\gcd(n, a \pm b)$ divides 6 and by Lemma 5 we have that $\{\pm a, \pm b\}$ is proportional to one of the exceptional sets (3).

v. The sum in (4) splits as the sum of two terms, one of length 5 and one of length 3, each one vanishing. If the sum of length 5 contains at least three elements of $\{\pm a, \pm b\}$ then we immediately deduce that $n|60$ 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 $\{\pm a, \pm b\}$. By a similar analysis as has been made in the case **iii**, we have that either $n/\gcd(n, a + b)$ or $n/\gcd(n, b - a)$ divide 6 or both $n/\gcd(n, 2a)$ and $n/\gcd(n, 2b)$ divide 6. By Lemma 5 and Lemma 6, we can conclude that $\{\pm a, \pm b\}$ is proportional to one of the exceptional sets (3).

So we have proved the statement of the theorem for all sets S except possible the sets (3) and X_e, $e = 1, 2, 4$. To reduce the number of exceptions let us define $\mu_\alpha(S)$ as the multiplicity of α as an eigenvalue of $\langle S \rangle_n$. So $\mu_\alpha(S) = 0$ if α is not an eigenvalue of $\langle S \rangle_n$.

It is also easy to see that $n/6 \le \mu_0(Z_e) \le n/6 + 6$, for $e = \pm1, \pm2, \pm3, \pm6$.

In the following table we present $\mu_\alpha(S)$ of other potentially exceptional graphs (together with the condition on n for which these graphs exist and are connected):

$\langle S \rangle_n$	Conditions on n	$\mu_0(\langle S \rangle_n)$
$\langle W_1 \rangle_n$	$2 \mid n$	$\begin{cases} n/2 + 2, \text{ if } n \equiv 0 \pmod 8; \\ n/2, \quad \text{ if } n \not\equiv 0 \pmod 8. \end{cases}$
$\langle X_1 \rangle_n$	$n \equiv 0 \pmod 4$	$\begin{cases} 1, \text{ if } n \equiv 0 \pmod 8; \\ 2, \text{ if } n \not\equiv 0 \pmod 8. \end{cases}$
$\langle X_2 \rangle_n$	$n \equiv 4 \pmod 8$	1
$\langle X_4 \rangle_n$	$n \equiv 4 \pmod 8$	1
$\langle Y_1 \rangle_n$	$n \equiv 0 \pmod 3$	$\begin{cases} 6, \text{ if } n \equiv 24 \pmod{36}; \\ 2, \text{ if } n \equiv 0, 12 \pmod{36}; \\ 0, \text{ if } n \not\equiv 0 \pmod{12}. \end{cases}$
$\langle Y_{-1} \rangle_n$	$n \equiv 0 \pmod 3$	$\begin{cases} 6, \text{ if } n \equiv 12 \pmod{36}; \\ 2, \text{ if } n \equiv 0, 24 \pmod{36}; \\ 0, \text{ if } n \not\equiv 0 \pmod{12}. \end{cases}$
$\langle Y_3 \rangle_n$	$n \equiv 3 \pmod 9$	$\begin{cases} 2, \text{ if } n \equiv 0 \pmod{12}; \\ 0, \text{ if } n \not\equiv 0 \pmod{12}. \end{cases}$

For $n \leq 18$ the theorem can be proved by the exhaustive search. For $n > 18$ we see that the spectrum of $\langle W_1 \rangle_n$ is unique, so it cannot be an exceptional set. The sets X_2 and X_4 when $n \equiv 4 \pmod 8$ have both $\mu_0(X_2) = \mu_0(X_4) = 1$ (but not in the case when $\mu_0(X_1) = 1$). However $\mu_2(X_2) = 0$ while $\mu_2(X_4) = 2$. So the two graphs cannot be isomorphic and their spectra are distinct from spectra of all other possible exceptions. So X_2 and X_4 can be eliminated from the list of exceptions as well. $\square$

So we have 12 sets of the form $\{\pm a, \pm b\}$ with $\gcd(a, b, n) = 1$ which do not satisfy the spectral Ádám property, and only 5 of them are of the form $\{\pm 1, \pm d\}$, the case of main interest.

5 Remarks

Naively speaking one can expect $12 \times 11/2 = 66$ 'suspicious' pairs $\operatorname{Spec} \langle S \rangle_n = \operatorname{Spec} \langle T \rangle_n$ for which $S \not\sim T$. However, by comparing the multiplicities of zero eigenvalues we see that sets Z_e, $e = \pm 1, \pm 2, \pm 3, \pm 6$, cannot form a suspicious pair with sets X_1, Y_e, $e = \pm 1, 3$. Hence there are only $4 \times 3/2 + 8 \times 7/2 = 34$ suspicious pairs. Similarly, we have only $3 \times 2/2 + 2 \times 1/2 = 4$ suspicious pairs of sets of the form $\{\pm 1, \pm d\}$. In fact, the number of suspicious pairs can be essentially reduced if one computes $\mu_0(Z_e)$ precisely for each $e = \pm 1, \pm 2, \pm 3, \pm 6$. Other eigenvalues may help as well. It is also easy to see that if $\gcd(n, 12) < 3$ then there is no exceptions at all.

Here instead of using the isomorphism property of graphs our approach is based on a weaker property of their spectral identity. Thus our results are more general than the original Ádám conjecture.

One can probably extend our results to the case of weighted circulant graphs. Indeed, in the case the question can be reduced to the equation of the form (1) as well however, instead of ± 1-coefficients it will have 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 [22, 23]. This case can also be considered with attracting 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 [10, 21], however it is still now quite clear how to extract analogies of Theorems 3, 4 and 7.

One more possible generalization we can be tackled 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 $\# \operatorname{Spec} \langle S \rangle_n \bigcap \operatorname{Spec} \langle T \rangle_n \geq n^\varepsilon$.

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

References

1. A. Ádám, 'Research problem 2-10', *J. Combinatorial Theory*, **3** (1967), 393.
2. B. Alspach and 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, 1749–1783.
4. J.-C. Bermond, F. Comellas and D. F. Hsu, 'Distributed loop computer networks: A survey', *Journal of Parallel and Distributed Computing*, **24** (1995), 2–10.
5. F. Boesch and R. Tindell, 'Circulants and their connectivities', *J. of Graph Theory*, **8** (1984), 487–499.
6. J. H. Conway and A. J. Jones, 'Trigonometric diophantine equations (On vanishing sums of roots of unity)', *Acta Arithm.*, **30** (1976), 171–182.
7. C. Delorme, O. Favaron and M. Maheo, 'Isomorphisms of Cayley multigraphs of degree 4 on finite abelian groups', *European J. of Comb.*, **13** (1992), 59–61.
8. N. Deo and M. Krishnamoorthy, 'Toeplitz networks and their properties', *IEEE Trans. on Circuits and Sys.*, **36** (1989), 1089–1092.
9. B. Elspas and J. Turner, 'Graphs with circulant adjacency matrices', *J. Comb. Theory*, **9** (1970), 229–240.
10. J.-H. Evertse and H. P. Schlickewei, 'The absolute subspace theorem and linear equations with unknowns from a multiplicative group', *Preprint*, 1997, 1–22.
11. X. G. Fang and M. Y. Xu, ' On isomorphisms of Cayley graphs of small valency', *Algebra Colloquium*, **1** (1994), 67–76.
12. C. Godsil, *Algebraic Combinatorics*, Chapman and Hall, NY, 1993.
13. F. T. Leighton, *Introduction to parallel algorithms and architectures: Arrays, trees, hypercubes*, M. Kaufmann, 1992.
14. C.H. Li, 'The cyclic groups with the m-DCI property', *European J. of Comb.*, **18** (1997), 655-665.
15. B. Litow and B. Mans, 'A note on the Ádám conjecture for double loops', *Inf. Proc. Lett.*, (to appear).
16. H. B. Mann, 'On linear relations between roots of unity', *Mathematika*, **12** (1965), 171–182.
17. B. Mans, 'Optimal Distributed algorithms in unlabeled tori and chordal rings', *Journal on Parallel and Distributed Computing*, **46(1)** (1997), 80-90.
18. M. Muzychuk, 'Ádám's conjecture is true in the square free case', *J. of Combinatorial Theory, Series A*, **72** (1995), 118–134.
19. M. Muzychuk, 'On Ádám's conjecture for circulant graphs', *Discrete Math.*, **167/168** (1997), 497–510.
20. P. P. Pálfy, 'Isomorphism problem for relational structures with a cyclic automorphism', *Europ. J. Combin.*, **8** (1987), 35–43.
21. H.P. Schlickewei, 'Equations in roots of unity', *Acta Arithm.*, **76** (1996), 171–182.
22. U. Zannier, 'On the linear independence of roots of unity', *Acta Arithm.*, **50** (1989), 171–182.
23. U. Zannier, 'Vanishing sums of roots of unity', *Rend. Sem. Mat. Univ. Politec. Torino*, **53** (1995), 487–495.

This article was processed using the LaTeX macro package with LLNCS style