ELSEVIER
Linear Algebra and its Applications 285 (1998) 123–142
LINEAR ALGEBRA AND ITS APPLICATIONS

Hardness results and spectral techniques for combinatorial problems on circulant graphs

Bruno Codenotti [a,1], Ivan Gerace [a,b,2], Sebastiano Vigna [c,*]

[a] *Istituto di Matematica Computazionale (C.N.R), Via S. Maria 46, 56126 Pisa, Italy*
[b] *Dipartimento di Matematica, Università degli Studi di Milano, Via Saldini 50, 20133 Milano, Italy*
[c] *Dipartimento di Scienze dell'Informazione, Università degli Studi di Milano, Via Comelico 39/41, 20135 Milano, Italy*

Received 28 October 1997; received in revised form 4 June 1998; accepted 12 June 1998

Submitted by R.A. Brualdi

Abstract

We show that computing (and even approximating) MAXIMUM CLIQUE and MINIMUM GRAPH COLORING for circulant graphs is essentially as hard as in the general case. In contrast, we show that, under additional constraints, e.g., prime order and/or sparseness, GRAPH ISOMORPHISM and MINIMUM GRAPH COLORING become easier in the circulant case, and we take advantage of spectral techniques for their efficient computation. © 1998 Elsevier Science Inc. All rights reserved.

AMS classification: 05C15; 05C50; 05C85; 15A18; 68R10

Keywords: Circulant matrices; Circulant graphs; Eigenvalues; Eigenvectors; Chromatic number; Clique; Approximation algorithms

1. Introduction

Circulant matrices have been extensively studied over the years. Both the linear algebra and the combinatorics communities have paid attention to this

* Corresponding author. E-mail: vigna@acm.org
[1] E-mail: codenotti@imc.pi.cnr.it
[2] E-mail: gerace@imc.pi.cnr.it

PII: S0024-3795(98)10126-X

important class of matrices. The algebraic properties of circulant matrices have led to efficient algorithms for several related computations, notably the Winograd Fourier Transform is based on circulants [16], and several preconditioners for solving Toeplitz or other related systems use circulant matrices [7]. Circulants also have several applications in combinatorics and counting [11], e.g., the solution of the well-known *rencontres* and *menage* problems can be obtained as a permanent one of a circulant matrix.

In this paper, we start an investigation on the complexity of the computation of some combinatorial objects on $\{0, 1\}$ circulant matrices, and we show that there seems to be a *complexity gap* depending on certain properties, such as whether or not the matrices have enough ones.

More precisely, we show that MAXIMUM CLIQUE (finding the size of the largest complete subgraph) and MINIMUM GRAPH COLORING (finding the minimum number of colors to be assigned to vertices so that no two adjacent vertices have the same color) are NP-hard, even if restricted to circulant graphs (graphs whose adjacency matrix is circulant). We show that not only is the above true, but also that it is NP-hard even to get good approximations for both problems (in the case of MAXIMUM CLIQUE, this holds also for graphs of prime order).

On the other hand we show that, unlike in the general case, some combinatorial problems become more tractable via linear algebra techniques when the circulant graph is either sparse (in other words, when the adjacency matrix has a few ones on each row) or of prime order.

More precisely, for MINIMUM GRAPH COLORING we find proper colorings using information given by the sign pattern of certain eigenvectors; $\lceil \log k \rceil$ vectors are necessary for correctly coloring a k-chromatic graph, and in the sparse case (i.e., degree less than 5) we can prove a matching upper bound, thus supporting the conjecture that some problems are substantially easier in this case. For MAXIMUM CLIQUE, we present estimates depending on some eigenvalues.

All graphs in this paper are simple and nonempty (i.e., they contain at least one edge). We denote by $\div$ integer division, and by $[n]$ the set $\{0, 1, \ldots, n-1\}$. In our expressions, the modulo operator has lowest priority. Moreover, δ will always denote the exponent of the best approximation bound for MAXIMUM CLIQUE, i.e., MAXIMUM CLIQUE is not approximable within a factor better than n^{δ}, where n is the number of vertices of the graph; note that δ may depend on the separation assumption ($\mathrm{P} \neq \mathrm{NP}$ [2] and $\mathrm{NP} \neq \mathrm{ZPP}$ [9], for instance). We denote with $\omega(G)$ and $\alpha(G)$ the maximum number of vertices of a clique (independent set, respectively) of G. By the notation $s[a, b]$ we mean the interval $[sa, sb]$. Finally, in our $n \times n$ matrices, the row and column indices run from 0 to $n-1$, and their arithmetic will be always modulo n.

The rest of the paper is organized as follows. In Section 2 we prove the NP-hardness and the nonapproximability of MINIMUM GRAPH COLORING and MAXIMUM CLIQUE for circulant graphs. In Section 3 we recall some results from algebraic graph theory. In Section 4 we present the spectral properties of circulant graphs. In Section 5 we give lower bounds for clique and independence sets for circulant graphs. In Section 6 we show how to color a circulant graph using spectral information.

2. Hardness results

This section is devoted to the proof of the fact that MAXIMUM CLIQUE and MINIMUM GRAPH COLORING are difficult both to compute and to approximate on circulant graphs (in the case of MAXIMUM CLIQUE, even if the graph is of prime order). We build sequences of numbers whose sums are distinct, and use them in order to map an instance into a circulant graph. Note that throughout the paper we shall assume that instances of problems restricted to circulant graphs are represented by the first row of a circulant adjacency matrix.

Lemma 1. *For all $n \in \mathbb{N}$, there are nonnegative numbers $a_0, a_1, \dots, a_{n-1}$ distinct modulo $8^{\lceil \log n \rceil} < 8n^3$, such that all sums $a_i + a_j$ are distinct modulo $8^{\lceil \log n \rceil} - 1$ and all sums $a_i + a_j + a_k$ are distinct modulo $8^{\lceil \log n \rceil} - 1$. Moreover, the sequence $a_0, a_1, \dots, a_{n-1}$ is computable in time polynomial in n, and the distinctness claims remain true modulo any integer m satisfying $m > 3 \cdot (8^{\lceil \log n \rceil} - 2)$.*

Proof. We recall that, for every prime number p, positive integer n and $\varepsilon > 0$, one can find an irreducible polynomial of degree n over $\mathbf{F}_p$ using

$$O(n^{3+\varepsilon} p^{1/2+\varepsilon} + n^{4+\varepsilon} \log^2 p)$$

arithmetical operations in $\mathbf{F}_p$ [12]. Moreover, if $\mathbf{F}$ is a field and f and g are two polynomials in $\mathbf{F}[x]$ of degree at most n, then fg [6] and $f \bmod g$ [13] can be computed using $O(n \log n \log \log n)$ arithmetic operations in $\mathbf{F}$. Thus, $\mathbf{F}_{2^k}$ (the Galois field of order 2^k) can be presented as $\mathbf{F}_2[x]/\langle f \rangle$, for some irreducible polynomial f of degree k, and both the representation and the operations of $\mathbf{F}_{2^k}$ can be computed in polynomial time.

Let the element $\vartheta \in \mathbf{F}_{8^{\lceil \log n \rceil}}$ be a generator of the multiplicative cyclic group $\mathbf{F}^*_{8^{\lceil \log n \rceil}}$ obtained by omitting the zero element (such a generator can be found by exhaustive search). Let $A = \{a_0, a_1, \dots, a_{n-1}\}$ denote the set of integers satisfying $1 \leqslant a_i \leqslant 8^{\lceil \log n \rceil} - 1$ for which $\vartheta^{a_i} = \vartheta + c$, for some $c \in \mathbf{F}_{2^{\lceil \log n \rceil}}$. In Ref. [5] it is shown that all sums of two or three terms of A are distinct modulo $8^{\lceil \log n \rceil} - 1$.

Suppose now that

$$a_{i_1} + a_{i_2} + a_{i_3} \not\equiv a_{j_1} + a_{j_2} + a_{j_3} \pmod{8^{\lceil \log n \rceil} - 1},$$

which a fortiori implies

$$a_{i_1} + a_{i_2} + a_{i_3} \neq a_{j_1} + a_{j_2} + a_{j_3}.$$

Since $m > 3 \cdot (8^{\lceil \log n \rceil} - 2)$, we have that $a_{i_1} + a_{i_2} + a_{i_3}, a_{j_1} + a_{j_2} + a_{j_3} < m$, which implies

$$a_{i_1} + a_{i_2} + a_{i_3} \not\equiv a_{j_1} + a_{j_2} + a_{j_3} \pmod{m}.$$

The case of two summands follows analogously. □

Note that Lemma 1 trivially implies that all differences $a_i - a_j$ are distinct for $i \neq j$, because $a_i - a_j = a_k - a_l$ gives $a_i + a_l = a_k + a_j$, so $i = k$ and $l = j$.

Theorem 1. *MAXIMUM CLIQUE restricted to circulant graphs is NP-hard, and not approximable by a factor better than $\lceil n/8 \rceil^{\delta/3}$, where n is the number of vertices of the graph and δ is the exponent of the best approximation bound for MAXIMUM CLIQUE.*

Proof. Let $G = \langle V, E \rangle$ and k be an instance of MAXIMUM CLIQUE, $|V| = n$ and $|E| = m$. Consider now a circulant graph C with $8^{\lceil \log n \rceil} - 1$ vertices such that the first row of its adjacency matrix [3] has a one in position $a_i - a_j$ whenever $\langle i, j \rangle \in E$ (note that since G is symmetric, this implies that we have a one also in position $a_j - a_i$, so C is symmetric, too). We denote with $f(i, j)$ the difference $a_i - a_j$; thus, $f(i, j)$ is a vertex of C, the mapping $\langle i, j \rangle \mapsto f(i, j)$ is injective by Lemma 1 and $-f(i, j) = f(j, i)$.

If there is a clique of size K in C, then certainly by vertex-transitivity there is a clique of size K in the neighborhood N of vertex 0 (i.e., in the subgraph induced by the vertex labeled by 0 and all vertices adjacent to 0). We now proceed to show that such a clique has the same number of vertices as a clique in G. In order to do so, we analyze the structure of N.

A vertex v of C is a neighbor of 0 iff $v = f(i, j)$ for some $i, j \in V$. Two vertices in v, w in N are thus of the form $f(i, j)$ and $f(k, l)$ (we shall always assume that the arguments of f are distinct). They are adjacent iff there are $s, t \in V$ such that $\langle t, s \rangle \in E$ and

$$a_i - a_j + a_s - a_t = a_k - a_l,$$

which is equivalent to

$$a_i + a_s + a_l = a_j + a_t + a_k.$$

By Lemma 1, we have that $\{i, s, l\} = \{j, t, k\}$; of the six permutations of S_3 we can use in order to solve the set equation, four fix one element and thus are

[3] We assume that all computations on vertices of C are carried out modulo $8^{\lceil \log n \rceil} - 1$.

ruled out by our assumption about the indices. The only remaining possibilities are $i = t$, $s = k$ and $l = j$, or $i = k$, $s = j$ and $l = t$. In both cases, the edges e and e' of G corresponding to v and w have a vertex in common, and the equations $i = t$ and $s = k$ ($s = j$ and $l = t$, respectively) imply that there is a third edge of G closing the triangle defined by e and e'.

Stated otherwise, two vertices of N are adjacent iff the corresponding edges of G are adjacent and part of a clique on three vertices (3-clique).

We now show that for every 3-clique $\{i, j, k\}$ of G, the subgraph $D \subseteq C$ induced by the six vertices of C corresponding to the edges of the clique contains no triangle. Indeed, the edges of D correspond to solutions of the equation

$$\pm(a_i - a_j) \pm (a_j - a_k) = \pm(a_i - a_k),$$

with $i < j < k$, and there are eight possibilities for the choice of the signs. It is immediate to see that except for

$$+(a_i - a_j) + (a_j - a_k) = +(a_i - a_k)$$

and

$$-(a_i - a_j) - (a_j - a_k) = -(a_i - a_k),$$

all choices to against our assumption about the indices. The first equation claims the existence of edges $\{f(i,j), f(i,k)\}$, $\{f(i,j), -f(j,k)\}$ and $\{f(j,k), f(i,k)\}$, while the second one of edges $\{-f(i,j), -f(i,k)\}$, $\{-f(i,j), f(j,k)\}$ and $\{-f(j,k), -f(i,k)\}$. In the end, we get the following list of edges:

$$\begin{aligned}
&\{f(i,j), f(k,j)\}\\
&\{f(k,j), f(k,i)\}\\
&\{f(k,i), f(j,i)\}\\
&\{f(j,i), f(j,k)\}\\
&\{f(j,k), f(i,k)\}\\
&\{f(i,k), f(k,j)\}
\end{aligned}$$

which is a simple 6-cycle; thus, no triangle is present.

Suppose now there is a K-clique in N with vertices $v_1 = 0, v_2, \ldots, v_K$. We are going to show that for all $2 \leqslant p \leqslant K$, the edge e_p of G corresponding to v_p is adjacent to a certain vertex of G independent of p. This implies that G has a K-clique, because for every pair of edges e_p and e_q, the other endpoints are necessarily part of a triangle, in view of the fact that v_p and v_q are adjacent in N.

Indeed, for all $2 \leqslant p, q \leqslant K$, the pair $\{v_p, v_q\}$ corresponds to two edges e_p, e_q of a triangle of G. In particular, $\{v_p, v_q\}$ uniquely identifies a vertex of G, which is the common vertex of e_p and e_q, denoted $e_p \wedge e_q$. Suppose by contradiction that, for some $2 \leqslant p, q, r \leqslant K$, $e_p \wedge e_q \neq e_p \wedge e_r$. Thus we have just two possibilities: either e_p, e_q and e_r from a triangle, which is false because they would not induce a triangle in N, or e_q and e_r have no vertex in common, which is false because they belong to the same triangle (remember that $\{v_p, v_q\}$ is an edge of N).

Note that by keeping a (polynomial size) table of the differences $a_i - a_j$, we can easily build the clique of G corresponding to a clique of N (i.e., to a clique of C). A generic clique $v_1, v_2, \ldots, v_K$ of C can be easily transformed into the clique $0, v_2 - v_1, \ldots, v_K - v_1$ of N.

Conversely, suppose there is a K-clique in G with vertices $i_1, i_2, \ldots, i_K$. Fix a vertex j from the list, and consider the set of $K - 1$ edges of the clique which are adjacent to j. We claim that the subgraph formed by vertex 0 and by the $2(K - 1)$ vertices corresponding to those edges contains a K-clique. Indeed, the equation

$$a_{i_p} - a_j + a_{i_q} - a_{i_p} = a_{i_q} - a_j$$

shows that all vertices of the form $f(i_p, j)$ are connected, and form a clique with 0 (the same holds for the vertices of the form $f(j, i_p)$).

Thus, we have proved that for every K-clique in G we can build (in polynomial time) a K-clique in C, and vice versa. This implies that MAXIMUM CLIQUE restricted to circulant graphs is NP-complete.

Suppose now by contradiction that there is a polynomial time algorithm approximating MAXIMUM CLIQUE on circulant graphs by a factor better than $\lceil n/8 \rceil^{\delta/3}$. Then we could take an instance of MAXIMUM CLIQUE with n vertices and map it to a circulant graph on $8^{\lceil \log n \rceil} - 1$ vertices, thus approximating MAXIMUM CLIQUE by a factor

$$\lceil (8^{\lceil \log n \rceil} - 1)/8 \rceil^{\delta/s} \leqslant \lceil 2^{3\lceil \log n \rceil - 3} \rceil^{\delta/3} \leqslant (2^{3 \log n})^{\delta/3} = n^{\delta}. \quad \square$$

Note that the previous proof can be easily modified in order to obtain the following.

Theorem 2. *MAXIMUM CLIQUE restricted to circulant graphs of prime order is NP-hard, and not approximable by a factor better than* $\lceil n/48 \rceil^{\delta/3}$.

Indeed, we can find in polynomial time a prime number P satisfying $3 \cdot (8^{\lceil \log n \rceil} - 2) < P < 6 \cdot (8^{\lceil \log n \rceil} - 2)$. Notice that the size of P is logarithmic in n (since P is cubic in n). The bound then follows noting that $P/48 < (8^{\lceil \log n \rceil} - 2)/8$. The reader should also contrast the previous result with the following.

Theorem 3. *GRAPH ISOMORPHISM for circulant graphs of prime order is decidable in polynomial time.*

The proof uses the fact that circulant graphs with a prime number of vertices are isomorphic iff they have the same eigenvalues [14], and that two graphs have the same eigenvalues iff they have the same characteristic polynomial, which can be computed and compared in polynomial time (adjacency matrices contain only zeros and ones).

In order to prove the hardness of MINIMUM GRAPH COLORING, we use a variation of the classical technique used in Ref. [10]. First of all, we prove the existence of certain (circulant) graphs, derived from our instance, whose stability index and chromatic number are tightly connected.

Lemma 2. *Let $G = \langle V, E\rangle$ be a circulant graph and r coprime with $n = |V|$. There exists a (polynomially computable from G) circulant graph G_r of order nr such that $\alpha(G_r) = \min\{r, \alpha(G)\}$. Moreover, if $r = \alpha(G)$ then $\chi(G_r) = n$.*

Proof. We describe a graph G_r having the stated properties, and prove it isomorphic to a circulant graph C_r.

We recall from Ref. [10] that the graph G_r has vertex set $[r] \times V$. Two vertices of G_r are connected if their first coordinate is the same; the vertices $\langle i, v\rangle$ and $\langle j, w\rangle$ are connected if $v = w$ or $\langle v, w\rangle \in E$. The graph C_r has also vertex set $[r] \times V$; for all $\langle v, w\rangle \in E$, and $v = w$ vertices $\langle i, rv \bmod n\rangle$ and $\langle j, rw \bmod n\rangle$ are connected, and for all $k \in \mathbb{Z} \setminus \{0\}$ vertex $\langle i, v\rangle$ is connected to vertex $\langle i + (v + rk) \div n \bmod r, v + rk \bmod n\rangle$.

Since r is coprime with n, we define a map $\beta(x) = (x/r \bmod n)$, and functions $\varphi : G_r \to C_r, \psi : C_r \to G_r$

$$\langle i, v\rangle \overset{\varphi}{\mapsto} \langle i + rv \div n \bmod r, rv \bmod n\rangle$$

$$\langle i, v\rangle \overset{\psi}{\mapsto} \langle i - r\beta(v) \div n \bmod r, \beta(v)\rangle.$$

Note that

$$r\beta(x) \equiv \beta(rx) \equiv x \pmod n,$$

and that φ and ψ and inverse bijections:

$$\begin{aligned}
\psi(\varphi(i, v)) &= \psi(i + rv \div n \bmod r, rv \bmod n) \\
&= \langle i + rv \div n - r\beta(rv \bmod n) \div n \bmod r, \beta(rv \bmod n)\rangle = \langle i, v\rangle, \\
\varphi(\psi(i, v)) &= \varphi(i - r\beta(v) \div n \bmod r, \beta(v)) \\
&= \langle i - r\beta(v) \div n + r\beta(v) \div n \bmod r, r\beta(v) \bmod n\rangle = \langle i, v\rangle.
\end{aligned}$$

We now show that φ and ψ are in fact inverse isomorphisms. Let $\langle i, v\rangle$ and $\langle i, w\rangle$ be adjacent vertices of G_r; they are mapped by φ to the vertices

$\langle i + rv \div n \bmod r, rv \bmod n\rangle$ and $\langle i + rw \div n \bmod r, rw \bmod n\rangle$ of C_r. By taking $k = w - v$ (see the definition of adjacency in C_r) we have

$$\begin{aligned}
&i + rv \div n + [(rv \bmod n) + r(w-v)] \div n \\
&\quad \equiv i + rv \div n + [rv \bmod n + n(rw \div n) + (rw \bmod n) - n(rv \div n) \\
&\qquad - (rv \bmod n)] \div n \\
&\quad \equiv i + rv \div n + [n(rw \div n) + (rw \bmod n) - n(rv \div n)] \div n \\
&\quad \equiv i + rv \div n + rw \div n - rv \div n \\
&\quad \equiv i + rw \div n \pmod r,
\end{aligned}$$

and, of course, $rw = rv + r(w - v)$, so $\varphi(i, v)$ and $\varphi(j, w)$ are adjacent. If we consider instead adjacent vertices $\langle i, v\rangle$ and $\langle j, w\rangle$ with $i \neq j$ and v equal or adjacent to w in G, we just notice that vertices whose second coordinates are $rv \bmod n$ and $rw \bmod n$ are always adjacent in C_r. Thus, φ is a graph morphism.

Let now v and w be equal or adjacent vertices of G. Then, the adjacent vertices $\langle i, rv \bmod n\rangle$ and $\langle j, rw \bmod n\rangle$ of C_r are mapped by ψ to vertices of G_r whose second coordinate is v and w, which are adjacent. On the other hand, for every vertex $\langle i, v\rangle$ and every $k \in \mathbb{Z} \setminus \{0\}$ we have

$$\begin{aligned}
&\psi(i + (v + rk) \div n \bmod r, v + rk \bmod n) \\
&\quad = \langle i + (v + rk) \div n - r\beta(v + rk \bmod n) \div n \bmod r, \beta(v + rk \bmod n)\rangle.
\end{aligned}$$

We now show that the first coordinate of $\psi(i, v)$ and $\psi(i + (v + rk) \div n \bmod r, v + rk \bmod n)$ are always the same. In fact, letting $h, h' \in \mathbb{Z}$ be such that $r\beta(v) = v + hn$ and $\beta(v + rk \bmod n) = \beta(v) + k + h'n$, we have

$$\begin{aligned}
&i + (v + rk) \div n - r\beta(v + rk \bmod n) \div n \\
&\quad \equiv i + (v + rk) \div n - r(\beta(v) + k - h'n) \div n \\
&\quad \equiv i + (v + rk) \div n - (hn + v + rk - rh'n) \div n \\
&\quad \equiv i + (v + rk) \div n - h - (v + rk) \div n - rh' \\
&\quad \equiv i - h \equiv i - r\beta(v) \div n \pmod r.
\end{aligned}$$

This shows that ψ is a graph morphism, and concludes the proof that φ and ψ are inverse isomorphisms. In order to prove that C_r is circulant, consider adjacent vertices $\langle i, rv \bmod n\rangle$ and $\langle j, rw \bmod n\rangle$, where v and w are either equal or adjacent in G. Then, their distance (in the lexicographic ordering) is $d = (j - i)n + (rw \bmod n) - (rv \bmod n) \bmod rn$. Let now $\langle k, u\rangle = \langle k, r\beta(u) \bmod n\rangle$ be an arbitrary vertex of C_r; the vertex at distance d has second coordinate equal to $r\beta(u) + rw - rv \bmod n$, but $\beta(u)$ and $\beta(u) + w - v \bmod n$ are equal or adjacent in G (their distance is equal to the distance between v and w).

Finally, we notice that

$$\begin{aligned}&[i + (v + rk) \div n - i]n + (v + rk \bmod n) - v \\ &\equiv [(v + rk) \div n]n + (v + rk \bmod n) - v \equiv v + rk - v \equiv rk \pmod{nr}\end{aligned}$$

holds independently of the values of i and v; thus all vertices at distance $rk \bmod nr$, for all $k \in \mathbb{Z}$, are connected by the second condition on C_r. This shows that C_r is the union of two partial graphs which are circulant, and is thus circulant.

We are just left with the issue of proving the claimed properties of G_r. The first statement is proved in Ref. [10]. The second part follows by noting that if $\alpha(G) = r$, then $\alpha(G_r) = r$; moreover, given a maximal independent set $v_1, v_2, \ldots, v_r$ of G, it is immediate that $\langle 0, v_1\rangle, \langle 1, v_2\rangle, \ldots, \langle r-1, v_r\rangle$ is an independent set of G_r, and that

$$\langle 0, v_1 + k \bmod n\rangle, \langle 1, v_2 + k \bmod n\rangle, \ldots, \langle r-1, v_r + k \bmod n\rangle$$

remains an independent set of every $k \in \mathbb{N}$. This gives a correct n-coloring of G_r (a correct coloring with less than n colors would yield by pigeonholing the existence of an independent set with more than r elements). □

Theorem 4. *MINIMUM GRAPH COLORING restricted to circulant graphs is NP-hard and not approximable by a factor better than* $[n/25]^{\delta/4}$.

Proof. Let $G = \langle V, E\rangle$ be an instance of MAXIMUM CLIQUE, and $|V| = n$. For each $3 \leqslant r \leqslant n$, by a trivial modification of the proof of Theorem 1 we build a circulant graph $C(r)$ such that the number of vertices n_r of $C(r)$ is coprime with r and $\alpha(C(r)) = \alpha(\overline{G}) = \omega(G)$; it is easy to check that we have the upper bound $n_r \leqslant 3 \cdot (8^{\lceil \log n\rceil} - 2) + r$.

Using the same notation of Lemma 2, by elementary graph theory we have

$$\chi(C(r)_r) \geqslant \frac{n_r r}{\alpha(C(r)_r)} \geqslant \frac{n_r r}{\alpha(C(r))} = \frac{n_r r}{\omega(G)}.$$

This implies that by computing $\chi(C(r)_r)$ for all r and minimizing the ratio $n_r r/\chi(C(r)_r)$ we could compute $\omega(G)$, which is NP-hard.

Analogously, if by contradiction we could compute $\chi(C(r)_r)$ within an approximation factor of $[n_r r/25]^{\delta/4}$, we could compute the ratios $n_r r/\chi(C(r)_r)$ within the same approximation factor; this implies that we could approximate $\omega(G)$ within

$$\lceil [3 \cdot (8^{\lceil \log n\rceil} - 2) + r]r/25\rceil^{\delta/4} \leqslant \lceil (24n^4 + n^2)/25\rceil^{\delta/4} \leqslant \lceil n^4\rceil^{\delta/4} \leqslant n^\delta. \quad \square$$

3. The spectrum of a graph

The spectrum of a graph is the spectrum of its adjacency matrix. The spectrum is related to the properties of the graph, and since it is invariant by symmetric permutations of the matrix, isomorphic graphs have the same spectrum. Some important spectral properties of adjacency matrices are summarized in the following theorem [8].

Theorem 5. *Let G be a connected (undirected) graph with $n > 1$ vertices and A its adjacency matrix. Then*

1. *the eigenvalues $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ of A are real (labeled with $\lambda_0 > \lambda_1 \geqslant \cdots \geqslant \lambda_{n-1}$);*
2. *the corresponding eigenvectors $\boldsymbol{u}_0, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_{n-1}$ can be chosen to be orthonormal;*
3. $\sum_{i=0}^{n-1} \lambda_i = 0$;
4. *the maximum eigenvalue λ_0 is the spectral radius of A and is simple;*
5. *$\boldsymbol{u}_0$ can be chosen to have positive components.*

There are moreover several relations between the chromatic number and eigenvalues of a graph, the most significant being [4,8]

$$\chi(G) \leqslant 1 + \lambda_0.$$

Assuming that the eigenvalues have been labelled so that $\lambda_0 \geqslant \lambda_1 \geqslant \cdots \geqslant \lambda_{n-1}$, we also have

$$\chi(G) \geqslant 1 + \min\left\{ k \,\middle|\, \lambda_0 + \sum_{i=1}^{k} \lambda_{n-i} \leqslant 0 \right\},$$

from which one easily derives

$$\chi(G) \geqslant 1 + \frac{\lambda_0}{-\lambda_{n-1}},$$

as $\sum_{i=1}^{k} \lambda_{n-i} \geqslant k\lambda_{n-1}$. Finally, 2-colorable (bipartite) graphs are characterized by having a spectrum symmetric with respect to zero [8].

The signs of the eigenvectors associated with negative eigenvalues also give useful information on correct colorings of the graph. Indeed, intuitively, we know that the value of the ith entry of the eigenvector multiplied by some negative value (the eigenvalue) must be equal to the sum of the entries of the eigenvector corresponding to vertices adjacent to the vertex i. So if the magnitude of the eigenvalue is big enough, it is likely that such entries will have a different sign than the ith entry. This means that by choosing a subset of eigenvectors and assigning a color to vertex i depending on the list of signs of the ith entries of the selected eigenvectors, we can expect an approximation of a coloring. For instance, in Ref. [3] it is shown that the signs of all eigenvectors color the graph assigning a different color to each vertex, while Ref. [1] refines algorithmically the eigenvector information so as to obtain a correct minimum coloring with high probability.

4. Spectral properties of circulant graphs

A circulant graph is a graph with circulant adjacency matrix (or, equivalently, the Cayley graph of a finite cyclic group). Consider a generic circulant adjacency matrix, and suppose that the nonzero elements in the first half of the first row are in positions $p_1 < p_2 < \cdots < p_s \leqslant n/2$, where n is the size of the matrix. Due to the symmetry of the adjacency matrix, the elements in the first row positions $-p_1 > -p_2 > \cdots > -p_s$ are also nonzero (recall that indices are computed modulo n).

Let G be a circulant graph of degree d with n vertices and adjacency matrix A. Note that if G is not connected, it breaks into isomorphic circulant components. Let also $\boldsymbol{a} = [a_0\ a_1 \ldots a_{n-1}]^{\mathrm{T}}$ be the first row of A. If n is odd, we have that the eigenvalues of G, not necessarily ordered, are as follows.

$$\lambda_0 = \sum_{k=1}^{(n-1)/2} 2a_k, \qquad \lambda_j = \lambda_{n-j} = \sum_{k=1}^{(n-1)/2} 2a_k \cos\left(\frac{2jk\pi}{n}\right), \quad 1 \leqslant j \leqslant (n-1)/2.$$

If n is even, we have

$$\lambda_0 = a_{n/2} + \sum_{k=1}^{n/2-1} 2a_k,$$

$$\lambda_j = \lambda_{n-j} = a_{n/2}\cos(j\pi) + \sum_{k=1}^{n/2-1} 2a_k \cos\left(\frac{2jk\pi}{n}\right), \quad 1 \leqslant j \leqslant n/2.$$

Note that while we do not assume that the eigenvalues are ordered, λ_0 is always the largest eigenvalue, and thus the spectral radius.

For the rest of the paper we fix a choice of eigenvectors. The eigenvector related to $\lambda_0 = d$ will be $\boldsymbol{u}_0 = [1\,1 \ldots 1]^{\mathrm{T}}$, and the eigenvectors related to λ_j and λ_{n-j} will be given by

$$\boldsymbol{u}_j = \left[1 \quad \cos\left(j\frac{2\pi}{n}\right) \quad \cos\left(2j\frac{2\pi}{n}\right) \quad \cos\left(3j\frac{2\pi}{n}\right) \quad \ldots \quad \cos\left((n-1)j\frac{2\pi}{n}\right)\right]^{\mathrm{T}}$$

$$\boldsymbol{v}_j = \left[0 \quad \sin\left(j\frac{2\pi}{n}\right) \quad \sin\left(2j\frac{2\pi}{n}\right) \quad \sin\left(3j\frac{2\pi}{n}\right) \quad \ldots \quad \sin\left((n-1)j\frac{2\pi}{n}\right)\right]^{\mathrm{T}},$$

while if n is even, the eigenvector of $\lambda_{n/2}$ will be $\boldsymbol{u}_{n/2} = [1\ -1\ 1\ -1\ \ldots\ -1]^{\mathrm{T}}$ (and $\boldsymbol{v}_{n/2} = \boldsymbol{0}$). Said otherwise, if ω is a primitive nth root of unity then

$\boldsymbol{u}_j(k) = \frac{1}{2}(\omega^{jk} + \omega^{-jk})$, while $\boldsymbol{v}_j(k) = (1/2\mathrm{i})(\omega^{jk} - \omega^{-jk})$. Note that our choice gives an *orthogonal* eigenvector basis, but in the following we will be sometimes interested in an *orthonormal* basis. We just remark that

$$\|\boldsymbol{u}_j\|^2 = \sum_{k=0}^{n-1}\left[\frac{1}{2}\left(\omega^{jk} + \omega^{-jk}\right)\right]^2 = \sum_{k=0}^{n-1}\omega^{2jk} + \sum_{k=0}^{n-1}\omega^{-2jk} + \frac{n}{2} = \frac{n}{2},$$

because every nontrivial nth root of unity ξ satisfies $\sum_{k=0}^{n-1}\xi^k = 0$. Analogous considerations can be made about the v_j's. However, notice that $\|\boldsymbol{u}_0\|^2 = n$ and that $\|\boldsymbol{u}_{n/2}\|^2 = n$ if n is even.

5. Lower bounds

In this section we sharpen the bounds on $\omega(G)$ and $\alpha(G)$ given in Ref. [15] using the exact knowledge of the eigenvalues and eigenvectors of G.

Theorem 6. *Let G be a circulant graph, and $\bar{\lambda} \leqslant \lambda_0 = d$ its second largest eigenvalue. Then*

$$\omega(G) \geqslant \frac{n}{n - d - \bar{\lambda}/2}.$$

Proof. We can assume that G be connected, for otherwise $\bar{\lambda} = d$ and Wilf's bound for regular graphs $\omega(G) \geqslant n/(n-d)$ gives $\omega(G) \geqslant (n/h)/(n/h - d) = n/(n - hd) \geqslant n/(n - d - d/2)$, where $h > 1$ is the number of connected components. Since G is regular we have [15]

$$\omega(G) \geqslant \frac{n}{n - \lambda_0 - nM}, \tag{1}$$

where M is the maximum of $\bar{\lambda}(\vartheta_1^2 + \vartheta_2^2)$ subject the linear constraints

$$\vartheta_1\sqrt{\frac{2}{n}}\boldsymbol{u}_j(k) + \vartheta_2\sqrt{\frac{2}{n}}\boldsymbol{v}_j(k) \geqslant -\frac{1}{n}, \quad k = 1, 2, \ldots, n,$$

and $\boldsymbol{u}_j$, $\boldsymbol{v}_j$ belong to the eigenspace of $\bar{\lambda}$, which can be assumed at least of multiplicity two and positive (for otherwise the bound trivializes – cf. [15], Theorem 3). Thus, we have to maximize $\vartheta_1^2 + \vartheta_2^2$ subject to the constraints

$$\vartheta_1\sqrt{\frac{2}{n}}\cos\left(kj\frac{2\pi}{n}\right) + \vartheta_2\sqrt{\frac{2}{n}}\sin\left(kj\frac{2\pi}{n}\right) \geqslant -\frac{1}{n}, \quad k = 1, 2, \ldots, n. \tag{2}$$

In order to do so, we study the inequality

$$\vartheta\,\cos(x) + t\vartheta\,\sin(x) \geqslant -\frac{1}{\sqrt{2n}},$$

where we set $\vartheta_1 = \vartheta$ and $\vartheta_2 = t\vartheta$; moreover, ϑ and t can be chosen to be positive without loss of generality (just exchange x with $-x$ or $\pi - x$).

Calculus shows that at its minima the function $\cos(x) + t\sin(x)$ takes the value $-\sqrt{1+t^2}$. Thus, (Eq.2) is certainly satisfied when $\vartheta \leqslant (2n(t^2+1))^{-1/2}$. But this means that, by choosing equality, we have

$$\max_{\vartheta_1,\vartheta_2} \vartheta_1^2 + \vartheta_2^2 \geqslant \max_t \frac{1}{2n(t^2+1)} + t^2\frac{1}{2n(t^2+1)} = \frac{1}{2n},$$

which is independent of t. Substituting in (Eq.1) yields immediately the thesis. □

Note that it is possible to prove that the choice of $\boldsymbol{u}_j$ and $\boldsymbol{v}_j$ as eigenvectors is in fact made without loss of generality, i.e., using an arbitrary basis does not lead to better bounds. Moreover, the bound can be easily transformed into a bound for the stability index.

Corollary 1. *Let G be a circulant graph and $\tilde{\lambda}$ be its smallest eigenvalue. Then*

$$\alpha(G) \geqslant \frac{n}{1 + d + (1+\tilde{\lambda})/2}.$$

Proof. Let A be the adjacency matrix of G, and assume that G is connected. Since G is regular, the all-ones matrix J is in the algebra generated by A [4], and the eigenvalues of $\overline{G}$ can be obtained as $p(\lambda_i) - \lambda_i - 1$, where λ_i is an eigenvalue of G and $p(x) \in \mathbb{C}[x]$ is a polynomial satisfying $p(A) = J$. The matrix J has a unique nonzero eigenvalue n, which is associated with the eigenspace generated by the all-ones eigenvector. Thus, all the other eigenvalues of $\overline{G}$ are of the form $-\lambda_i - 1, i > 0$, and the two largest eigenvalues are $n - d - 1$ (by regularity) and $-\tilde{\lambda} - 1$. If G is not connected, the lower bound is true for every component C of G; since independent sets from different components can be combined into a new independent set, and all components have, up to multiplicity, the same spectrum as G, we have

$$\alpha(G) \geqslant h\alpha(C) \geqslant h\frac{n/h}{1 + d + (1+\tilde{\lambda})/2} = \frac{n}{1 + d + (1+\tilde{\lambda})/2},$$

where h is the number of components of G. □

In order to see that Theorem 6 gives in fact sharper estimates than the general bound $\omega(G) \geqslant n/(n-d)$, one can consider, for instance, circulant graphs whose first row contains in its first half just a small number k of consecutive ones starting at position 1. In this case, $\tilde{\lambda} \geqslant 2[\cos(2\pi/n) + \cos(4\pi/n) + \cdots + \cos(2k\pi/n)]$, so

$$\frac{n}{n-d} < \frac{n}{n-d-[\cos(2\pi/n)+\cos(4\pi/n)+\cdots+\cos(2k\pi/n)]} \leqslant \frac{n}{n-d-\overline{\lambda}/2}.$$

As an example, for $n = 10$ and $k = 2$ we have $\omega = 3, n/(n-d) \approx 1.67$ but $n/(n-d-\overline{\lambda}/2) \approx 2.05$, while for $k = 3$ we have $\omega = 4$, $n/(n-d) \approx 2.5$ but $n/(n-d-\overline{\lambda}/2) \approx 3.13$.

6. Coloring circulant graphs

In this section we give results about correct colorings derived from information contained in the signs of certain eigenvectors. As we suggested in Section 3, given a choice of indices $J \subseteq \{1,\ldots,\lfloor n/2 \rfloor\}$, the color of a vertex t will be given by the $2|J|$-dimensional vector $[\mathrm{sgn}(\boldsymbol{u}_j(t)), \mathrm{sgn}\ (\boldsymbol{v}_j(t))]_{j\in J}$.

Theorem 7. *Let G be a circulant graph of order n whose adjacency matrix A has nonzero elements of index* $p_1 < p_2 < \cdots < p_s \leqslant n/2$ *in the first half of the first row.* Let $\boldsymbol{u}_j$ and $\boldsymbol{v}_j$ *denote the choice of eigenvectors defined in Section* 4. *Let* $J \subseteq \{1,\ldots,\lfloor n/2 \rfloor\}$ *be a subset of indices such that, for all* $1 \leqslant h \leqslant s$, *there exists* $j \in J$ *for which* $\boldsymbol{u}_j(p_h) < 0$. *Then the signs of* $\{\boldsymbol{u}_j, \boldsymbol{v}_j | j \in J\}$ *correctly color the graph.*

Proof. It is sufficient to show that given a vertex t, the vertex $t + p_h$ has a different sign pattern in $\{\boldsymbol{u}_j, \boldsymbol{v}_j | j \in J\}$. Since $\boldsymbol{u}_j(p_h) < 0$ for some j, we have

$$\frac{\pi}{2} + 2k\pi < \frac{2p_h j\pi}{n} < \frac{3}{2}\pi + 2k\pi,$$

where k is an integer. Consider the vector

$$[\boldsymbol{u}_j(t), \boldsymbol{v}_j(t)] = \left[\cos\left(\frac{2tj\pi}{n}\right), \sin\left(\frac{2tj\pi}{n}\right)\right]$$

defined by the angle $2tj\pi/n$. The signs of $\boldsymbol{u}_j$ and $\boldsymbol{v}_j$ in position $t + p_h$ are determined by the angle $2(t+p_h)j\pi/n$, which satisfies

$$\frac{2tj\pi}{n} + \frac{\pi}{2} + 2k\pi < \frac{2(t+p_h)j\pi}{n} < \frac{2tj\pi}{n} + \frac{3}{2}\pi + 2k\pi.$$

It is easy to see that the vector $[\boldsymbol{u}_j(t+p_h), \boldsymbol{v}_j(t+p_h)]$ is not in the same quadrant as the first one, and thus at least one sign changes (no matter whether 0 is considered positive or negative). $\square$

As a consequence, we obtain the following.

Corollary 2. *The pairs of eigenvectors associated with negative eigenvalues correctly color a circulant graph of degree* 2.

Proof. A circulant graph of degree 2 has only one nonzero position $p_1 \leqslant n/2$ in the first half of the first row (of course, by symmetry also $-p_1$ is nonzero). Moreover in the odd case we have

$$0 > \lambda_j = 2 \cos\left(p_1 j \frac{2\pi}{n}\right) = 2\boldsymbol{u}_j(p_1),$$

and the thesis follows from Theorem 7. In the even case, if $p_1 \neq n/2$ the result can be obtained analogously, since $a_{n/2} = 0$. Otherwise, G is just a disjoint union of copies of K_2, and the thesis follows trivially. □

Example 1. Let us consider a circulant graph with $n = 18$ vertices whose circulant adjacency matrix is defined by the following first row:

$$[0\,0\,1\,1\,1\,0\,0\,0\,1\,1\,1\,0\,0\,0\,1\,1\,1\,0].$$

Then, the sign patterns of $\boldsymbol{u}_3$ and $\boldsymbol{v}_3$ are

$$[+\;+\;-\;-\;-\;+\;+\;+\;-\;-\;-\;+\;+\;+\;-\;-\;-\;+],$$

and

$$[+\;+\;+\;+\;-\;-\;+\;+\;+\;+\;-\;-\;+\;+\;+\;+\;-\;-],$$

respectively, By Theorem 7, we have that $\{\boldsymbol{u}_3, \boldsymbol{v}_3\}$ correctly colors the graph. Letting $R = (+,+), Y = (+,-), B = (-,+)$ and $G = (-,-)$ we obtain the coloring

$$[R\,R\,B\,B\,G\,Y\,R\,R\,B\,B\,G\,Y\,R\,R\,B\,B\,G\,Y]$$

which is indeed correct.

It is interesting to note that in the case of bipartite circulant graphs there is always a specific single vector which can be used to color the graph. In fact, the choice of the vector characterizes bipartiteness, under a connectedness hypothesis.

Lemma 3. *A connected circulant graph with n vertices of degree d is bipartite iff n is even and* $\lambda_{n/2} = -d$.

Proof. A circulant graph with an odd number of vertices certainly contains an odd cycle, and thus cannot be bipartite. Moreover, in a bipartite graph the spectrum is symmetric w.r.t. zero, and in a circulant graph of even order all eigenvalues except for λ_0 and $\lambda_{n/2}$ have even multiplicity, so $\lambda_{n/2} = -\lambda_0 = -d$.

On the other hand, a connected graph in which $-\lambda_0$ is an eigenvalue does not contain odd cycles [8], and it is thus bipartite. □

Lemma 4. *A connected circulant graph with n vertices is bipartite iff n is even and the vector $\boldsymbol{u}_{n/2}$ correctly colors the graph.*

Proof. By the previous lemma we know that a connected circulant graph is bipartite if and only if n is even and $\lambda_{n/2} = -d$, but a simple calculation shows that this happens iff the vector $\boldsymbol{u}_{n/2} = [1\ -1\ 1\ -1 \ldots 1\ -1]$ correctly colors the graph. □

We note that, as it is easy to check, the left-to-right implications of the two previous lemmas are true independently of the connectedness hypothesis; thus, we have the following.

Theorem 8. *A circulant bipartite graph is correctly colored by $\boldsymbol{u}_{n/2}$.*

We now proceed towards the main result of this section, which provides estimates of colorability by means of eigenvector signs when $d = 3, 4$.

Lemma 5. A circulant graph of degree 4 contains a clique of order 5 if and only if $n/p_1 = 5$ and $p_2 = 2p_1$.

Proof. First we note that the only circulant graphs of degree 4 that can contain a clique of order 5 are disjoint unions of cliques of order 5. Moreover, since all edges incident to a fixed vertex must belong to the same clique, each clique contains 5 edges of offset p_1 and 5 edges of offset p_2. Thus,

$$5p_i \equiv 0 \pmod{n}$$

for $i = 1, 2$, i.e., $5p_i = n$ or $5p_i = 2n$ (recall that $p_i \leqslant n/2$), and the condition $p_1 < p_2$ implies $5p_1 = n$ and $5p_2 = 2n$. □

Lemma 6. *A circulant graph of degree* 3 *or* 4 *is colorable by vectors $\boldsymbol{u}_i$ and $\boldsymbol{v}_i$ for some i iff there exists an integer j such that*

$$j \in \frac{n}{p_1}\left[\frac{1}{4} + k_1, \frac{3}{4} + k_1\right] \cap \frac{n}{p_2}\left[\frac{1}{4} + k_2, \frac{3}{4} + k_2\right] \tag{3}$$

for some integers k_1 and k_2.

Proof. Since $d = 3$ or 4, $s = 2$. By Theorem 7 there exists an $0 < i \leqslant n/2$ such that $\boldsymbol{u}_i$ and $\boldsymbol{v}_i$ color the graph iff there are $k_1, k_2 \in \mathbb{Z}$ such that

$$\frac{\pi}{2} + 2k_j\pi \leqslant \frac{2\pi p_j i}{n} \leqslant \frac{3\pi}{2} + 2k_j\pi, \tag{4}$$

for $j = 1, 2$. Since $\cos(x) = \cos(2\pi - x)$, we can relax our assumptions and just require $0 \leqslant i < n$. We can remove all assumptions by noting that if an arbitrary integer satisfies Eq. (4), its remainder modulo n will satisfy Eq. (4), too. The proof is completed by a trivial computation. □

Before proving the main theorem of this section, we notice that all intervals of the form

$$\frac{n}{p}\left[\frac{1}{4} + k, \frac{3}{4} + k\right]$$

contain an integer if $p < n/2$, because the length of such intervals is greater than 1. Moreover, all intervals of the form

$$\left(\frac{n}{p}\right)\left[\frac{3}{8}, \frac{3}{4}\right]$$

contain an integer because either $n/p \leqslant 8/3$, in which case they contain 1 since $n/p \geqslant 2$, or else $n/p > 8/3$, in which case they have length greater than 1.

Theorem 9. *Given a circulant graph of degree* 3 *or* 4, *there exists an integer* $0 < i \leqslant n/2$ *such that* $\boldsymbol{u}_i$ and $\boldsymbol{v}_i$ *correctly color the graph, unless the graph contains a clique of order* 5.

Proof. Let $p_2/p_1 = b/a$, where $(a, b) = 1$. We start by establishing when

$$\frac{n}{p_1}\left[\frac{1}{4} + k_1, \frac{3}{4} + k_1\right] \supseteq \frac{n}{p_2}\left[\frac{1}{4} + k_2, \frac{3}{4} + k_2\right],$$

for some $k_1, k_2 \in \mathbb{Z}$, since in this case the theorem is obviously true. A simple computation shows that this happens when

$$\frac{b}{a}k_1 + \frac{1}{4}\left(\frac{b}{a} - 1\right) \leqslant k_2 \leqslant \frac{b}{a}k_1 + \frac{3}{4}\left(\frac{b}{a} - 1\right) \tag{5}$$

for some $k_1, k_2 \in \mathbb{Z}$. Consider now the line

$$k_2 = \frac{b}{a}k_1 + \frac{1}{2}\left(\frac{b}{a} - 1\right),$$

which lies in the middle of the stripe defined by Eq. (5), as a line on the torus obtained as the quotient of the plane under the action of $\mathbb{Z} \times \mathbb{Z}$. This line intersects the segment S defined by $k_1 = 0$, $k_2 \in [0, 1]$ in the points of ordinate

$$\frac{1}{2}\left(\frac{b}{a} - 1\right) + t\frac{b}{a} \quad (\text{mod } \mathbb{Z}),$$

for $t \in \mathbb{Z}$, i.e., in exactly a uniformly spaced points on S. Thus, the origin cannot be farther than $1/2a$ from one of these points; moreover, the stripe is vertically large $\frac{1}{2}\left(\frac{b}{a}-1\right)$. This implies that when

$$\frac{1}{4}\left(\frac{b}{a}-1\right) \geqslant \frac{1}{2a} \quad \Longleftrightarrow \quad b-a \geqslant 2$$

the stripe (5) contains certainly a point of integer coordinates. If $b = a+1$ and $a \geqslant 2$ we have that $p_2/p_1 = b/a = (a+1)/a \leqslant 3/2$, but then

$$\frac{n}{p_1}\left[\frac{1}{4},\frac{3}{4}\right] \supseteq \frac{n}{p_2}\left[\frac{3}{8},\frac{3}{4}\right] \subseteq \frac{n}{p_1}\left[\frac{1}{4},\frac{3}{4}\right],$$

and the second interval certainly contains an integer. We are left with the case $p_2 = 2p_1$.

Let $c/d = n/p_1$, with $(c,d)=1$. We will show that unless $c/d = 5$, the interval

$$I_k = \frac{c}{d}\left[\frac{1}{4}+k,\frac{3}{4}+k\right] \cap \frac{c}{2d}\left[\frac{1}{4}+2k,\frac{3}{4}+2k\right] = \frac{c}{d}\left[\frac{1}{4}+k,\frac{3}{8}+k\right]$$

contains an integer for some value of k. In order to do so, we consider the middle point of I_k, i.e., $(c/d)\left(\frac{5}{16}+k\right)$. Noting that the length of I_k is $c/8d$, the same techniques used in the first part of the proof shows that when

$$\frac{c}{16d} \geqslant \frac{1}{2d} \quad \Longleftrightarrow \quad c \geqslant 8,$$

for some k the interval I_k will contain an integer. Since $2p_1 = p_2 \leqslant n/2$, we have $c/d \geqslant 4$, so we are left with the cases $d=1$ and $c = 4,5,6,7$. But elementary computations show that $1 \in 4\left[\frac{1}{4},\frac{3}{8}\right]$ and $2 \in 6\left[\frac{1}{4},\frac{3}{8}\right], 7\left[\frac{1}{4},\frac{3}{8}\right]$. In the remaining case, the graph is just a disjoint union of 5-cliques by Lemma 5. □

Since (as it is easy to check) $\boldsymbol{u}_1, \boldsymbol{v}_1$ and $\boldsymbol{u}_2$ always correctly color a graph made of 5-cliques, the previous theorem, together with Theorem 8 and Corollary 2, settles the problem of finding the minimum number of eigenvectors that correctly color a circulant graph in the case of low degree.

Theorem 10. *Let G be a k-chromatic circulant graph of degree less than* 5. *Then* $\lceil \log k \rceil$ *eigenvectors of G are necessary and sufficient to color G.*

The general case is open, but we have the following upper bound for the special case in which all entries in the first half of the first row are ones starting from p_1.

Theorem 11. *Let G be a circulant graph whose adjacency matrix A satisfies*

$$p_{j+1} = p_1 + j \quad 0 \leqslant j \leqslant \frac{n}{2} - p_1.$$

Then, $n/2p_1$ *vectors correctly color G.*

Proof. Note that $u_i(j) \leqslant 0$ iff $n/4i \leqslant j \leqslant 3n/4i \leqslant n/2i$. Since for $1 \leqslant i \leqslant n/4p_1$ we have $p_1 \leqslant j \leqslant n/2$, Theorem 9 shows that the corresponding vectors $\boldsymbol{u}_i$ and $\boldsymbol{v}_i$ correctly color the graph. □

7. Conclusions

This paper has provided a first look at using spectral techniques in the analysis of combinatorial problems on sparse circulant graphs. The main remaining open questions concern the possibility of getting optimal colorings for sparse circulant graphs via eigenvector information.

Acknowledgements

We thank Davide Ferrario for the useful topological insights that led to a great simplification of the proof of Theorem 9. We also thank the anonymous refree for his/her comments, which greatly helped to improve the exposition.

References

[1] N. Alon, N. Kahale, A spectral technique for coloring random 3-colorable graphs, in: Proceedings of The 26th Annual Symposium on the Theory of Computing, New York, ACM Press, New York, May 1994, pp. 346–355.

[2] S. Arora, C. Lund, R. Motwani, M. Sudan, M. Szegedy, Proof verification and hardness of approximation problems, in: Proc. The 33rd IEEE Symposium on the Foundations of Computer Science, IEEE Computer Society, 1992, pp. 14–23.

[3] B. Aspvall, J.R. Gilbert, Graph coloring using eigenvalue decomposition, SIAM J. Algebraic Discrete Methods 5 (4) (1984) 526–538.

[4] N.L. Biggs, Algebraic Graph Theory, Cambridge Univ. Press, Cambridge, 1974.

[5] R.C. Bose, S.D. Chowla, Theorems in additive theory of numbers, Comment. Math. Helv. 37 (1962–1963) 141–147.

[6] D.G. Cantor, E. Kaltofen, On fast multiplication of polynomials over arbitrary algebras, Acta Inform. 28 (7) (1991) 693–701.

[7] T.F. Chan, An optimal circulant preconditioner for Toeplitz systems, SIAM J. Sci. Statist. Comput. 9 (1988) 766–771.

[8] D.M. Cvetković, M. Doob, H. Sachs, Spectra of Graphs, Academic Press, New York, 1978.

[9] J. Håstad, Clique is hard to approximate within $n^{1-\varepsilon}$, in: Proceedings of The 37th IEEE Symposium on the Foundations of Computer Science, IEEE Computer Society, 1996, pp. 627–636.

[10] C. Lund, M. Yannakakis, On the hardness of approximating minimization problems, J. ACM 41 (5) (1991) 960–981.

[11] H. Minc, Permanental compounds and permanents of (0,1) circulants, Linear Algebra Appl. 86 (1987) 11–46.

[12] V. Shoup, New algorithms for finding irriducible polynomials over finite fields, Math. Comp. 54 (189) (1990) 435–447.
[13] I.E. Shparlinski, Computational and Algorithmic Problems in Finite Fields, Kluwer Academic Publishers, Dordrecht, 1992.
[14] J. Turner, Point-symmetric graphs with prime number of points, J. Combin. Theory 3 (1967) 136–145.
[15] H.S. Wilf, Spectral bounds for the clique and independence numbers of graphs, J. Combin. Theory Ser. B 40 (1986) 113–117.
[16] S. Winograd, On computing the discrete Fourier transform, Math. Comp. 32 (1978) 175–199.