Nonexistence of almost Moore digraphs of diameter three*

J. Conde, J. Gimbert

Departament de Matemàtica
Universitat de Lleida
Jaume II 69, 25001 Lleida, Spain
{jconde,joangim}@matematica.udl.cat

J. Gonzàlez

Departament de Matemàtica Aplicada IV
Universitat Politècnica de Catalunya
Víctor Balaguer s/n, 08800 Vilanova i la Geltrú, Spain
josepg@ma4.upc.edu

J.M. Miret, R. Moreno

Departament de Matemàtica
Universitat de Lleida
Jaume II 69, 25001 Lleida, Spain
{miret,ramiro}@matematica.udl.cat

Submitted: Jul 18, 2007; Accepted: Jun 21, 2008; Published: Jun 30, 2008
Mathematics Subject Classification: 05C20, 05C50, 11R18

Abstract

Almost Moore digraphs appear in the context of the *degree/diameter problem* as a class of extremal directed graphs, in the sense that their order is one less than the unattainable *Moore bound* $M(d,k) = 1 + d + \cdots + d^k$, where $d > 1$ and $k > 1$ denote the maximum out-degree and diameter, respectively. So far, the problem of their existence has only been solved when $d = 2, 3$ or $k = 2$. In this paper, we prove that almost Moore digraphs of diameter $k = 3$ do not exist for any degree d.

The enumeration of almost Moore digraphs of degree d and diameter $k = 3$ turns out to be equivalent to the search of binary matrices A fulfilling that $AJ = dJ$ and $I + A + A^2 + A^3 = J + P$, where J denotes the all-one matrix and P is a *permutation matrix*. We use spectral techniques in order to show that such equation has no

*Partially supported by the Ministry of Science and Technology, Spain, under the projects TIC2003-09188, MTM2006-15038-C02-02 and MTM2007-66842-C02-02.

(0, 1)-matrix solutions. More precisely, we obtain the factorization in $\mathbb{Q}[x]$ of the characteristic polynomial of A, in terms of the *cycle structure* of P, we compute the trace of A and we derive a contradiction on some algebraic multiplicities of the eigenvalues of A. In order to get the factorization of $\det(xI - A)$ we determine when the polynomials $F_n(x) = \Phi_n(1 + x + x^2 + x^3)$ are irreducible in $\mathbb{Q}[x]$, where $\Phi_n(x)$ denotes the n-th cyclotomic polynomial, since in such case they become 'big pieces' of $\det(xI - A)$. By using concepts and techniques from algebraic number theory, we prove that $F_n(x)$ is always irreducible in $\mathbb{Q}[x]$, unless $n = 1, 10$. So, by combining tools from matrix and number theory we have been able to solve a problem of graph theory.

Keywords: Almost Moore digraph, characteristic polynomial, cyclotomic polynomial, permutation cycle structure, trace.

1 Introduction

It is well known that interconnection networks can be modeled by graphs whose vertices represent the processing elements and whose edges represent their links. The graphs thus obtained can be undirected or directed depending on whether the communication between nodes is two-way or only one-way. In this context the following problem arises quite naturally:

- *Degree/diameter problem*: given two natural numbers d and k, find the largest possible number of vertices $n(d, k)$ in a [directed] graph with maximum [out-] degree d and diameter k.

In the directed case, it has been proved that

$$n(d, k) < 1 + d + \cdots + d^k = M(d, k),$$

unless $d = 1$ or $k = 1$ (see [15, 4]). Then, the question of finding for which values of $d > 1$ and $k > 1$ we have $n(d, k) = M(d, k) - 1$, where $M(d, k)$ is known as the *Moore bound*, becomes an interesting problem. In this case, any extremal digraph turns out to be d-regular (see [11]). From now on, regular digraphs of degree $d > 1$, diameter $k > 1$ and order $n = d + \cdots + d^k$ will be called *almost Moore* (d, k)*-digraphs* (or (d, k)*-digraphs* for short).

Every (d, k)-digraph G has the property that for each vertex $v \in V(G)$ there exists only one vertex, denoted by $r(v)$ and called the *repeat* of v, such that there are exactly two $v \to r(v)$ walks of length at most k. If $r(v) = v$, which means that v is contained in one k-cycle, v is called a *selfrepeat* of G. The map r, which assigns to each vertex $v \in V(G)$ its repeat $r(v)$, is an automorphism of G (see [1]). Seeing it as a permutation, r has a *cycle structure*, which corresponds to its unique decomposition in disjoint cycles. Such cycles will be called *permutation cycles* of G. The number of permutation cycles of G of each length $i \le n$ will be denoted by m_i and the vector $(m_1, \ldots, m_n)$ will be referred to as the *permutation cycle structure* of G.

Using the basic properties of a (d,k)-digraph G, it can be seen that its adjacency matrix A fulfills that $AJ = dJ$ and

$$I + A + \cdots + A^k = J + P, \tag{1}$$

where J denotes the all-one matrix and $P = (p_{ij})$ is the $(0,1)$-matrix associated with the permutation r of $V(G) = \{1,\ldots,n\}$; that is to say, $p_{ij} = 1$ iff $r(i) = j$.

So far, the problem of the existence of almost Moore (d,k)-digraphs has only been solved when $d = 2, 3$ or $k = 2$. Thus, fixing the degree, Miller and Fris [12] proved that the $(2,k)$-digraphs do not exist for values of $k > 2$ and, subsequently, Baskoro et al. [3] established the nonexistence of $(3,k)$-digraphs unless $k = 2$. On the other hand, Fiol et al. [5] showed that the $(d,2)$-digraphs do exist for any degree. The digraph constructed is the line digraph $L\,K_{d+1}$ of the complete digraph K_{d+1}. Concerning the enumeration of $(d,2)$-digraphs it is known that there are exactly three non isomorphic $(2,2)$-digraphs (see [13]). The classification of $(d,2)$-digraphs was completed in [7] by proving that $L\,K_{d+1}$ is the unique solution, if $d \geq 3$.

In this paper, we prove that almost Moore digraphs of diameter $k = 3$ do not exist for any degree d. We use the simplest spectral invariant, the trace of a matrix, in order to show that the equation $I + A + A^2 + A^3 = J + P$ has no $(0,1)$-matrix solutions such that $AJ = dJ$. More precisely, we derive a contradiction on some algebraic multiplicities of the eigenvalues of A (see Section 3). We remark that instead of working with the eigenvalues of A, as it is usually done in spectral graph theory, we collect them into irreducible factors of the characteristic polynomial of A (see Section 2). Such a polynomial approach has also been used in the literature (see, for instance, [8, 9]). In our case, we have been able to get the factorization of $\det(xI - A)$ in $\mathbb{Q}[x]$ by using two fundamental facts:

- The known relations between the spectrum of A and the cycle structure of P (see [6]);
- The irreducibility in $\mathbb{Q}[x]$ of the polynomials $F_n(x) = \Phi_n(1+x+x^2+x^3)$, if $n \neq 1, 10$, where $\Phi_n(x)$ denotes the n-th cyclotomic polynomial (see Section 2).

In order to determine the irreducibility of the polynomials $F_n(x)$ in $\mathbb{Q}[x]$ we use concepts and techniques from algebraic number theory. So, by combining tools from matrix and number theory we have been able to solve a problem of graph theory. Remarkably, the notion of trace, used in different contexts, has become crucial.

2 Characteristic polynomial of an almost Moore digraph of diameter three

Let G be a (d,k)-digraph with permutation cycle structure $(m_1,\ldots,m_n)$ and let A be its adjacency matrix. From Equation (1), the spectrum of A and $J + P$ are closely related. It is known that the characteristic polynomial of $J + P$ is

$$\det(xI - (J+P)) = (x - (n+1))(x-1)^{m_1-1}\prod_{i=2}^{n}(x^i - 1)^{m_i}$$

(see [2]). Since $x^l - 1 = \prod_{i|l} \Phi_i(x)$, where $\Phi_i(x)$ denotes the i-th cyclotomic polynomial, the factorization of $\det(xI - (J+P))$ in $\mathbb{Q}[x]$ is

$$\det(xI - (J+P)) = (x-(n+1))(x-1)^{m(1)-1} \prod_{i=2}^{n} \Phi_i(x)^{m(i)},$$

where $m(i) = \sum_{i|l} m_l$ represents the total number of permutation cycles of order multiple of i. In [6], the problem of the factorization in $\mathbb{Q}[x]$ of the characteristic polynomial of G, $\phi(G,x) = \det(xI - A)$, was connected with the study of the irreducibility in $\mathbb{Q}[x]$ of the polynomials $\Phi_i(1+x+\cdots+x^k)$. The idea is that, when such polynomials are irreducible, then they become 'big pieces' of the characteristic polynomial of G.

Proposition 1. *Let $(m_1,\ldots,m_n)$ be the permutation cycle structure of a (d,k)-digraph G and $2 \le i \le n$. If $\Phi_i(1+x+\cdots+x^k)$ is an irreducible polynomial in $\mathbb{Q}[x]$, then it is a factor of $\phi(G,x)$ and its multiplicity is $m(i)/k$.*

Moreover, a conjecture about the irreducibilitity of $F_{n,k}(x) = \Phi_n(1+x+\cdots+x^k)$ in $\mathbb{Q}[x]$ was formulated in [6]. For k even and $n > 2$, it states that $F_{n,k}(x)$ is irreducible unless $n \mid (k+2)$. The case $k=2$ was proved by H.W. Lenstra Jr. and B. Poonen [10, 6]. For k odd and $n > 2$, it states that $F_{n,k}(x)$ is irreducible unless n is even and $\frac{n}{2} \mid (k+2)$. Besides, the irreducibility of $F_{2,k}(x)$, for any k, was proved in [6].

The rest of this section is devoted to prove the previous conjecture in the case $k=3$; that is, we show that the polynomial $F_{n,3}(x)$ is irreducible in $\mathbb{Q}[x]$, when $n > 1$ and $n \neq 10$. From now on, we write $F_n(x)$ instead of $F_{n,3}(x)$.

As a first step, we show that the condition of being $F_n(x)$ reducible in $\mathbb{Q}[x]$ implies a divisibility relation by a cyclotomic polynomial.

Lemma 1. *Let $n > 2$ be an integer and $F_n(x) = \Phi_n(1+x+x^2+x^3)$.*

(i) In the case n even, if $F_n(x)$ is reducible in $\mathbb{Q}[x]$ then there exists a polynomial

$$p_\ell(x) = (x^2-1)^3(x^{4\ell+2}+1)^4 - x^{3\ell+2}(x^{\ell-2}+1)(x^{3\ell+4}-1)^3,$$

$1 \le \ell < 2n$, such that $\Phi_{2n}(x)$ divides $p_\ell(x)$.

(ii) In the case n odd, if $F_n(x)$ is reducible in $\mathbb{Q}[x]$ then there exist two polynomials

$$q_\ell(x) = (x-1)^3(x^{4\ell+1}+1)^4 - x^{3\ell+1}(x^{\ell-1}+1)(x^{3\ell+2}-1)^3,$$

$$r_\ell(x) = (x-1)^3(x^{4\ell+1}+1)^4 + x^{3\ell+1}(x^{\ell-1}-1)(x^{3\ell+2}+1)^3,$$

$1 \le \ell < n$, such that $\Phi_n(x)$ divides either $q_\ell(x)$ or $r_\ell(x)$.

Proof. Let us suppose that $F_n(x)$ is reducible in $\mathbb{Q}[x]$ and let us consider a root ε of $F_n(x)$. Then

$$1+\varepsilon+\varepsilon^2+\varepsilon^3 = \zeta_n, \tag{2}$$

where ζ_n is a primitive n-th root of unity. Using properties about the degrees of the algebraic extensions $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\varepsilon)$, we derive that $F_n(x)$ has an irreducible factor in $\mathbb{Q}[x]$ of degree $\varphi(n)$, where $\varphi(n)$ stands for Euler's function.

We can assume that ε is a root of such a factor. Since $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\zeta_n)$, from Equation (2) it follows that ε belongs to the ring of algebraic integers of $\mathbb{Q}(\zeta_n)$, which is $\mathbb{Z}[\zeta_n]$ (see [16, Theorem 2.6]). Taking into account that $\varepsilon(1+\varepsilon+\varepsilon^2) = \zeta_n - 1$ and since $\zeta_n - 1$ is either a prime element or a unit of $\mathbb{Z}[\zeta_n]$, when $n > 1$ (see [16, Lemma 1.4 and Proposition 2.8]), at least one of the two elements in $\{\varepsilon, 1+\varepsilon+\varepsilon^2\}$ is a unit of $\mathbb{Z}[\zeta_n]$. If ε is a unity then its conjugate can be expressed as $\overline{\varepsilon} = \alpha \cdot \varepsilon$, where α is a root of unity (see [16, Lemma 1.6]). Furthermore, since the only roots of unity in $\mathbb{Q}(\zeta_n)$ are of the form $\pm\zeta_n^\ell$, it follows that α is a $2n$-th root of unity. If $1+\varepsilon+\varepsilon^2$ is a unity then $\varepsilon = \beta(\zeta_n - 1)$, where $\beta = 1/(1+\varepsilon+\varepsilon^2)$ is a unity. Since $\overline{\beta} = \beta a$, where $a^{2n} = 1$, we obtain that

$$\overline{\varepsilon} = \overline{\beta}(\overline{\zeta_n} - 1) = \frac{a\beta(1-\zeta_n)}{\zeta_n} = -\frac{a}{\zeta_n}\varepsilon.$$

So, in any case, $\overline{\varepsilon} = \alpha\varepsilon$, where $\alpha^{2n} = 1$.

In order to find a polynomial relation between α and ζ_n, we use the following identities:

$$1+\varepsilon+\varepsilon^2+\varepsilon^3 = \frac{\varepsilon^4 - 1}{\varepsilon - 1} = \zeta_n, \tag{3}$$

$$\overline{\varepsilon} = \alpha\varepsilon. \tag{4}$$

From them, and taking into account that $\overline{\zeta_n} = 1/\zeta_n$, it can be seen that

$$\zeta_n = \frac{\alpha\varepsilon - 1}{\alpha^4\varepsilon^4 - 1}. \tag{5}$$

By using (3) and (5), we have

$$\alpha^4\varepsilon^3(1+\varepsilon+\varepsilon^2+\varepsilon^3) - \alpha - (1+\varepsilon+\varepsilon^2) = \varepsilon^3(\alpha^4\zeta_n + 1) - (\alpha + \zeta_n) = 0.$$

Notice that if $\alpha^4\zeta_n + 1 = 0$ then $\alpha = -\zeta_n$, which implies that $\zeta_n^5 = -1$ and, consequently, $n = 10$. So, apart from this particular case, we can write

$$\varepsilon^3 = \frac{\zeta_n + \alpha}{\alpha^4\zeta_n + 1}. \tag{6}$$

Then, since $\varepsilon^3 + \frac{\varepsilon^3 - 1}{\varepsilon - 1} = \zeta_n$, we obtain

$$\varepsilon = \frac{1-\zeta_n}{\varepsilon^3 - \zeta_n} = \frac{1-\zeta_n}{\frac{\zeta_n + \alpha}{\alpha^4\zeta_n + 1} - \zeta_n} = \frac{(\zeta_n - 1)(\alpha^4\zeta_n + 1)}{\alpha(\alpha^3\zeta_n^2 - 1)}. \tag{7}$$

Therefore, from (6) and (7), we get

$$(\zeta_n - 1)^3(\alpha^4\zeta_n + 1)^4 - \alpha^3(\zeta_n + \alpha)(\alpha^3\zeta_n^2 - 1)^3 = 0, \tag{8}$$

which also holds for $n = 10$.

We recall that $\alpha^{2n} = 1$. Besides $\alpha \neq \pm 1$ since otherwise $\varepsilon \in \mathbb{R}$, which contradicts the fact that Equation (2) has no real solutions. Therefore we can take, in expression (8), $\alpha = \zeta_{2n}^{\ell}$ ($1 \leq \ell < 2n$ and $\ell \neq n$) and $\zeta_n = \zeta_{2n}^2$. So, in the case n even, replacing ζ_{2n} by x in (8) we obtain the polynomial equation $p_\ell(x) = 0$, which has a zero in $x = \zeta_{2n}$. Consequently, $\Phi_{2n}(x)$ must divide $p_\ell(x)$. In the case n odd, the degree of $p_\ell(x)$ can be reduced. Indeed, $\alpha^{2n} = 1$ implies that either $\alpha = \zeta_n^{\ell}$ or $\alpha = -\zeta_n^{\ell}$, where $1 \leq \ell < n$. Replacing now ζ_n by x in (8) we get two polynomial equations $q_\ell(x) = 0$ and $r_\ell(x) = 0$, according to α or $-\alpha$ is a n-th root of unity. Then it follows that ζ_n is either a root of $q_\ell(x)$ or $r_\ell(x)$. Hence $\Phi_n(x)$ divides either $q_\ell(x)$ or $r_\ell(x)$. $\square$

Next, we show that the divisibility conditions, given in Proposition 1, can be simplified taking into account that the polynomials $p_\ell(x)$, $q_\ell(x)$ and $r_\ell(x)$ factorize in $\mathbb{Q}[x]$ as follows,

$$p_\ell(x) = (x^\ell - 1)\, p_{\ell,1}(x)\, p_{\ell,2}(x)\, a_\ell(x) \tag{9}$$

$$q_\ell(x) = (x^\ell - 1)\, q_{\ell,1}(x)\, q_{\ell,2}(x)\, b_\ell(x) \tag{10}$$

$$r_\ell(x) = (x^\ell + 1)\, r_{\ell,1}(x)\, r_{\ell,2}(x)\, c_\ell(x) \tag{11}$$

where $p_{\ell,i}(x)$, $q_{\ell,i}(x)$, $r_{\ell,i}(x)$ are given by

	$i=1$	$i=2$
$p_{\ell,i}(x)$	$-1 - x^\ell - x^{2\ell} - x^{3\ell} + x^{2+3\ell}$	$-1 + x^2 + x^{2+\ell} + x^{2+2\ell} + x^{2+3\ell}$
$q_{\ell,i}(x)$	$-1 - x^\ell - x^{2\ell} - x^{3\ell} + x^{1+3\ell}$	$-1 + x + x^{1+\ell} + x^{1+2\ell} + x^{1+3\ell}$
$r_{\ell,i}(x)$	$1 - x^\ell + x^{2\ell} - x^{3\ell} + x^{1+3\ell}$	$1 - x + x^{1+\ell} - x^{1+2\ell} + x^{1+3\ell}$

and

$$\begin{aligned}
a_\ell(x) = \;& 1 - 2x^2 + x^4 + x^{2+\ell} - x^{4+\ell} + x^{2+2\ell} + x^{2+3\ell} - 2x^{4+3\ell} + x^{6+3\ell} \\
& -3x^{4+4\ell} + 2x^{6+4\ell} + 2x^{4+5\ell} - 3x^{6+5\ell} + x^{4+6\ell} - 2x^{6+6\ell} + x^{8+6\ell} \\
& +x^{8+7\ell} - x^{6+8\ell} + x^{8+8\ell} + x^{6+9\ell} - 2x^{8+9\ell} + x^{10+9\ell}. \\
b_\ell(x) = \;& 1 - 2x + x^2 + x^{1+\ell} - x^{2+\ell} + x^{1+2\ell} + x^{1+3\ell} - 2x^{2+3\ell} + x^{3+3\ell} \\
& -3x^{2+4\ell} + 2x^{3+4\ell} + 2x^{2+5\ell} - 3x^{3+5\ell} + x^{2+6\ell} - 2x^{3+6\ell} + x^{4+6\ell} \\
& +x^{4+7\ell} - x^{3+8\ell} + x^{4+8\ell} + x^{3+9\ell} - 2x^{4+9\ell} + x^{5+9\ell}. \\
c_\ell(x) = \;& -1 + 2x - x^2 + x^{1+\ell} - x^{2+\ell} - x^{1+2\ell} + x^{1+3\ell} - 2x^{2+3\ell} + x^{3+3\ell} \\
& +3x^{2+4\ell} - 2x^{3+4\ell} + 2x^{2+5\ell} - 3x^{3+5\ell} - x^{2+6\ell} + 2x^{3+6\ell} - x^{4+6\ell} \\
& +x^{4+7\ell} + x^{3+8\ell} - x^{4+8\ell} + x^{3+9\ell} - 2x^{4+9\ell} + x^{5+9\ell}.
\end{aligned}$$

In the proof of the following lemma, as well as in the main result of this section, we will use the notion of the trace of an element in a finite extension and some of its properties. We recall that given two fields E and F such that E is a finite extension of F, the trace of $\alpha \in E$, $\mathrm{Tr}_{E/F}(\alpha)$, is defined as the trace of the F–linear map $f_\alpha : E \longrightarrow E$ given by $f_\alpha(x) = \alpha x$. The following properties are well-known:

P1. The map $\mathrm{Tr}_{E/F}\colon E \to F$ is F-linear.

P2. $\mathrm{Tr}_{E/F}(1) = [E:F]$, where $[E:F]$ is the degree extension.

P3. If $F \subseteq L \subseteq E$ are finite extensions then $\mathrm{Tr}_{E/F} = \mathrm{Tr}_{L/F} \circ \mathrm{Tr}_{E/L}$.

Lemma 2. *Let $n > 2$ be an integer and $F_n(x) = \Phi_n(1+x+x^2+x^3)$. Assume that $F_n(x)$ is reducible in $\mathbb{Q}[x]$.*

(i) If n is even, then there exists a positive integer ℓ, $1 \leq \ell < 2n$, such that $a_\ell(x)$ is divisible by $\Phi_{2n}(x)$.

(ii) If n is odd, then there exists a positive integer ℓ, $1 \leq \ell < n$, such that either $b_\ell(x)$ or $c_\ell(x)$ is divisible by $\Phi_n(x)$.

Proof. Since the cyclotomic polynomials are irreducible in $\mathbb{Q}[x]$, the result follows from Proposition 1 by taking into account expressions (9)—(11) and by proving that

- $\Phi_{2n}(x)$ does not divide $x^\ell - 1$ nor $p_{\ell,i}(x)$, $i = 1,2$, if $1 \leq \ell < 2n$ and n is even;
- $\Phi_n(x)$ does not divide $(x^\ell - 1)(x^\ell + 1)$ nor $q_{\ell,i}$ nor $r_{\ell,i}$, $i = 1,2$, if $1 \leq \ell < n$ and n is odd.

It is clear that, in the case n even, $\Phi_{2n}(x)$ does not divide $x^\ell - 1$ and, in the case n odd, $\Phi_n(x)$ does not divide $(x^{2\ell} - 1)$, since otherwise $2n|\ell$ and $n|\ell$, respectively.

Now, we will show that, for n even and $n \neq 10$, $\Phi_{2n}(x)$ does not divide $p_{\ell,1}(x)$, $1 \leq \ell < 2n$. Suppose that $\Phi_{2n}(x)$ divides $p_{\ell,1}(x)$; that is, $p_{\ell,1}(\zeta_{2n}) = 0$. Then,

$$1 = -\zeta_{2n}^{-3\ell} - \zeta_{2n}^{-2\ell} - \zeta_{2n}^{-\ell} + \zeta_{2n}^{2}. \tag{12}$$

Taking traces in (12), and using properties (P1) and (P2), we get

$$\varphi(2n) = [\mathbb{Q}(\zeta_{2n}) : \mathbb{Q}] = \mathrm{Tr}_{\mathbb{Q}(\zeta_{2n})/\mathbb{Q}}(1) \leq \sum_{i=1}^{3} \mid \mathrm{Tr}_{\mathbb{Q}(\zeta_{2n})/\mathbb{Q}}(\zeta_{2n}^{-i\ell}) \mid + \mid \mathrm{Tr}_{\mathbb{Q}(\zeta_{2n})/\mathbb{Q}}(\zeta_{2n}^{2}) \mid . \tag{13}$$

It can be easily proved that $\mathrm{Tr}_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(\zeta_k) = \mu(k)$, where ζ_k is a primitive k-th root of unity and $\mu(k)$ denotes Möbius's function. In particular, we have that

$$\mid \mathrm{Tr}_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(\zeta_k) \mid \leq 1 .$$

Now, combining this fact with the properties (P1), (P2) and the transitivity of the trace (P3) with respect to the algebraic extensions $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_k^r) \subseteq \mathbb{Q}(\zeta_k)$, we obtain

$$\mid \mathrm{Tr}_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(\zeta_k^r) \mid = \mid \mathrm{Tr}_{\mathbb{Q}(\zeta_k^r)/\mathbb{Q}}(\zeta_k^r) \mid [\mathbb{Q}(\zeta_k) : \mathbb{Q}(\zeta_k^r)] \leq [\mathbb{Q}(\zeta_k) : \mathbb{Q}(\zeta_k^r)] .$$

So, from (13), we derive that

$$\varphi(2n) \leq \sum_{i=1}^{3} [\mathbb{Q}(\zeta_{2n}) : \mathbb{Q}(\zeta_{2n}^{i\ell})] + [\mathbb{Q}(\zeta_{2n}) : \mathbb{Q}(\zeta_{2n}^{2})].$$

Besides, taking into account that $\zeta_{2n}^2 = 1 + \sum_{i=1}^{3} (\zeta_{2n}^{-\ell})^i$ belongs to $\mathbb{Q}(\zeta_{2n}^{\ell})$ and since

$$\mathbb{Q}(\zeta_{2n}^2) \subseteq \mathbb{Q}(\zeta_{2n}^{\ell}) \subseteq \mathbb{Q}(\zeta_{2n}) \quad \text{and} \quad \mathbb{Q}(\zeta_{2n}^{i\ell}) \subseteq \mathbb{Q}(\zeta_{2n}^{\ell}) \subseteq \mathbb{Q}(\zeta_{2n}),$$

we have that

$$[\mathbb{Q}(\zeta_{2n}) : \mathbb{Q}(\zeta_{2n}^{\ell})] \leq 2 \quad \text{and} \quad [\mathbb{Q}(\zeta_{2n}) : \mathbb{Q}(\zeta_{2n}^{i\ell})] \leq 2i, \quad 1 \leq i \leq 3.$$

Consequently,

$$\varphi(2n) \leq 2 + \sum_{i=1}^{3} 2i = 14; \text{ that is } \varphi(n) \leq 6.$$

It can be checked that for all n even such that $\varphi(n) \leq 6$, the polynomial $F_n(x)$ is irreducible in $\mathbb{Q}[x]$ except for $n = 10$. Hence, $\Phi_{2n}(x) \nmid p_{\ell,1}(x)$ when n is even and $n \neq 10$. In the particular case $n = 10$, $\Phi_{20}(x)$ divides $p_{\ell,1}$ and $a_\ell(x)$ for $\ell = 12$ (so the result also holds for $n = 10$).

The remaining cases $\Phi_{2n}(x) \nmid p_{\ell,2}(x)$, for n even and $n \neq 10$, $\Phi_n(x) \nmid q_{\ell,i}(x)$ and $\Phi_n(x) \nmid r_{\ell,i}(x)$, for n odd, can be proved in a similar way (the corresponding divisibility condition also implies that $\varphi(n) \leq 6$). $\square$

Our main goal is to show that $F_n(x)$ is irreducible in $\mathbb{Q}[x]$, for $n > 1$ and $n \neq 10$. Taking into account previous results, it is enough to see that $\Phi_{2n}(x) \nmid a_\ell(x)$, for n even and $n \neq 10$, and $\Phi_n(x) \nmid b_\ell(x)$ and $\Phi_n(x) \nmid c_\ell(x)$, for $n > 1$ odd.

From now on, we use the following notation. Let p be a rational prime and $a(x), b(x) \in \mathbb{Z}[x]$. We denote by $a(x) \pmod p$ the polynomial obtained from $a(x)$ by reducing its coefficients modulo p; that is, $a(x) \pmod p \in \mathbb{F}_p[x]$, where $\mathbb{F}_p$ is the finite field of p elements. The notation $a(x) \equiv b(x) \pmod p$ means that $a(x) \pmod p = b(x) \pmod p$.

Next, we present several properties on cyclotomic polynomials modulo p, which will be used through this section.

Lemma 3. *Let p be a rational prime.*

(i) If $n = m\,p^e$, where m is an integer coprime to p, then

$$\Phi_n(x) \equiv \Phi_m(x)^{\varphi(p^e)} \pmod p\,.$$

(ii) For a pair of integers n and n' coprime to p, the condition

$$\gcd\left(\Phi_n(x) \pmod p\,,\ \Phi_{n'}(x) \pmod p\right) \neq 1$$

implies that $n = n'$.

Proof. It is well known (cf. [14, p. 160]) that

$$\Phi_{m\,p^e}(x) = \frac{\Phi_m(x^{p^e})}{\Phi_m(x^{p^{e-1}})}\,.$$

Now, part (i) follows from $\Phi_m(x^{p^i}) \equiv \Phi_m(x)^{p^i} \pmod{p}$.

Let us prove (ii). Set $a(x) = \gcd(\Phi_n(x) \pmod{p}, \Phi_{n'}(x) \pmod{p})$ and assume that $\deg a(x) \geq 1$. Let $d > 0$ be the minimum integer such that $a(x) \mid x^d - 1 \pmod{p}$. Notice that d is the least common multiple of the orders of all roots of $a(x) \pmod{p}$. Since such orders divide n and n', then $d \mid \gcd(n, n')$. Taking into account that

$$x^n - 1 = \prod_{k|n} \Phi_k(x) = (x^d - 1) \prod_{\substack{k|n \\ k\nmid d}} \Phi_k(x),$$

if $n > d$ then $a(x)^2 \mid x^n - 1 \pmod{p}$ and, in particular, $x^n - 1 \pmod{p}$ has multiple roots, which is not possible since n and p are coprime. Hence, $n = d$. The statement is obtained by applying the same argument to n'. □

Theorem 1. *Let $n > 1$ be an integer. Then, $F_n(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if $n \neq 10$.*

Proof. We assume that $F_n(x)$ is reducible in $\mathbb{Q}[x]$. According to Lemma 2, such condition implies a divisibility relation involving a cyclotomic polynomial, Φ_{2n}, if n is even, and $\Phi_n(x)$, if n is odd. In both situations, we will derive that n is less than a certain bound, which will be deduced from a bound of $\varphi(n)$.

• *Case n odd*: Let $n = m\,p^e$, where $p > 2$ is a rational prime, $e \geq 1$ and m is an odd integer coprime to p. First, we assume that $\Phi_n(x) \mid b_\ell(x)$ for some $1 \leq \ell < n$.

Let $A(x, y) \in \mathbb{Z}[x, y]$ be the polynomial such that $A(x, x^\ell) = b_\ell(x)$ and let

$$A_1(x, y) = \frac{\partial A}{\partial x}(x, y) + \ell \frac{\partial A}{\partial y}(x, y) \frac{y}{x} \in \mathbb{Z}[x, y].$$

Obviously, $A_1(x, x^\ell) = b'_\ell(x)$, where $b'_\ell(x)$ denotes the derivate of $b_\ell(x)$. From part (i) of Lemma 3, it follows that

$$\Phi_m(x)^{\varphi(p^e)-1} \mid \gcd(b_\ell(x),\, b'_\ell(x)) \pmod{p}$$

and, therefore,

$$\Phi_m(x)^{\varphi(p^e)-1} \mid P(x) \pmod{p},$$

where $P(x)$ is the following resultant

$$P(x) = \mathrm{Res}\left(A(x, y), A_1(x, y), y\right). \tag{14}$$

It can be checked that

$$P(x) = -x^{18}\Phi_1(x)^6\Phi_2(x)^6\Phi_{10}(x)^2 Q_\ell(x), \tag{15}$$

where $Q_\ell(x)$ is a polynomial of degree 16, unless $3\ell \equiv -1 \pmod{p}$ and $p > 3$, in which case its degree is 13. So, $P(x) \not\equiv 0 \pmod{p}$.

From (15) and Lemma 3, the maximum power of $\Phi_m(x)$ that could divide $P(x)$ (mod p) is 22, if $m=1$, and 16, otherwise. These are bounds for the exponent $\varphi(p^e)-1$ of $\Phi_m(x)$. As a result, in any case,

$$\varphi(n)=\varphi(m)\varphi(p^e)\leq 32.$$

The same bound is derived when we assume that $\Phi_n(x)\mid c_\ell(x)$, since the corresponding resultant is $-P(x)$.

• *Case n even*: Let $n=m\,2^e$, being $e\geq 1$ and m an odd integer. Let us suppose that there exists an integer ℓ, $1\leq\ell<2n$, such that $\Phi_{2n}(x)\mid a_\ell(x)$. We will distinguish two cases according to ℓ is odd or even.

⋆ *Subcase ℓ odd:* From Lemma 3, since $e+1\geq 2$, we have that

$$\Phi_m(x)^{2^e}\mid a_\ell(x) \pmod 2 \quad\text{and}\quad \Phi_m(x)^{2^e}\mid a'_\ell(x) \pmod 2.$$

We take $A(x,y)\in\mathbb{Z}[x,y]$ such that $A(x,x^\ell)=a_\ell(x)$. This polynomial satisfies

$$\frac{\partial A(x,y)}{\partial x}+\frac{\partial A(x,y)}{\partial y}\frac{y}{x}\equiv x\,yA_1(x,y)^2 \pmod 2\,,$$

with

$$A_1(x,y)=1+x+y+x^2\,y+x^2\,y^2+x^3\,y^3+x^2\,y^4+x^4\,y^4\,.$$

Then $\Phi_m(x)^{2^e}$ divides $x^{1+\ell}A_1(x,x^\ell)^2 \pmod 2$ and, therefore, $\Phi_m(x)^{2^{e-1}}$ divides $A_1(x,x^\ell)$ (mod 2). Due to the fact that

$$\operatorname{Res}\left(A(x,y),A_1(x,y),y\right)\equiv x^{24}\Phi_1(x)^{14}\Phi_5(x)^2 \pmod 2\,,$$

it follows that either $m=5$ and $\varphi(2^e)\leq 2$ or $m=1$ and $\varphi(2^e)\leq 14$. In any case,

$$\varphi(n)=\varphi(m)\varphi(2^e)\leq 14.$$

⋆ *Subcase ℓ even:* Since $\Phi_{2n}(x)=\Phi_n(x^2)$ and $a_\ell(x)=b_{\ell/2}(x^2)$, the relation $\Phi_{2n}(x)\mid a_\ell(x)$, for some ℓ even and $1\leq\ell<2n$, can be reformulated as $\Phi_n(x)\mid b_k(x)$, where $1\leq k<n$. Notice that we have come across the same divisibility condition as in the case n odd, which allow us to reason on the resultant $P(x)$ defined in (14).

- If $n=m2^e$, with $m>1$, we can consider an odd prime $p|n$ and take $P(x)$ modulo p. Then, analogously to the case n is odd, we derive that $\varphi(n)\leq 32$.
- If $n=2^e$ $(m=1)$, with $e\geq 2$, then

$$P(x)\equiv(1+k)^3x^{24}\Phi_1(x)^{12}\Phi_{10}(x)^2\left(1+k^6+k^2\,x^2+(1+k^6)x^4\right) \pmod 2\,.$$

  - If k is even, $P(x)\equiv x^{24}\Phi_1(x)^{16}\Phi_{10}(x)^2 \pmod 2$ and, consequently, the maximum power of $\Phi_1(x)$ that divides $P(x) \pmod 2$ is 16. So, $\varphi(n)\leq 16$.

– If k is odd then $P(x) \equiv 0 \pmod 2$. Since we cannot use the same arguments than in the other cases, we will take traces on the equation $b_k(\zeta_n) = 0$, where ζ_n is a primitive root of unity of order $n = 2^e > 2$.

Let $K = \mathbb{Q}(\zeta_n)$, with $n = 2^e > 2$. Since ζ_n^h is a primitive root of unity of order $n/\gcd(h,n)$, it can be seen that

$$\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_n^h) = \begin{cases} \varphi(n) & \text{if } \gcd(h,n) = n, \\ -\varphi(n) & \text{if } \gcd(h,n) = n/2, \\ 0 & \text{if } \gcd(h,n) < n/2. \end{cases}$$

Notice that $\zeta_n^h \in \mathbb{Q}$ if and only if $\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_n^h) \neq 0$. Since many terms of $b_k(\zeta_n)$ are of the form ζ_n^h, with $\gcd(h,n) \leq 4$, in order to vanish their corresponding traces we will assume that $n/2 > 4$.

So, from $\mathrm{Tr}_{K/\mathbb{Q}}(b_k(\zeta_n)) = 0$, we get

$$\begin{aligned} -\varphi(n) &= 2\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_n^{1+k}) + 2\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_n^{1+3k}) \\ &\quad -3\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_n^{3+5k}) + \mathrm{Tr}_{K/\mathbb{Q}}(\zeta_n^{2+6k}) + \mathrm{Tr}_{K/\mathbb{Q}}(\zeta_n^{5+9k})\,. \end{aligned}$$

In the case $k \equiv -1 \pmod 4$, we have that

$$-\varphi(n) = 2\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_n^{1+k}) + \mathrm{Tr}_{K/\mathbb{Q}}(\zeta_n^{5+9k})\,.$$

If $\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_n^{1+k}) \neq 0$ then $\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_n^{5+9k}) \neq 0$ and, consequently, we have $\zeta_n^4 = (\zeta_n^{1+k})^9/\zeta_n^{5+9k} \in \mathbb{Q}$, which is impossible since $n > 8$. Therefore, $\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_n^{1+k}) = 0$ and $\zeta_n^{5+9k} = -1$. As a consequence, ζ_n is a root of the polynomial

$$m(x) = \left(b_k(x) - 1 - x^{5+9k}\right)/x.$$

Taking traces we obtain

$$-2\varphi(n) = 2\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_n^{1+5k}) + \mathrm{Tr}_{K/\mathbb{Q}}(\zeta_n^{3+7k})\,.$$

Then $\zeta_n^{1+5k} \in \mathbb{Q}$ and $\zeta_n^{16} = (\zeta_n^{5+9k})^5/(\zeta_n^{1+5k})^9 \in \mathbb{Q}$, which implies $\varphi(n) \leq 16$.

In the case $k \equiv 1 \pmod 4$, using similar techniques, we derive that $\varphi(n) \leq 8$.

As a result, we have seen that if $F_n(x)$ is reducible in $\mathbb{Q}[x]$ then $\varphi(n) \leq 32$; that is, $n \leq 90$. For these particular values, it has been computationally checked that $F_n(x)$ is reducible in $\mathbb{Q}[x]$ only when $n = 1, 10$.

□

3 Nonexistence of almost Moore digraphs of diameter three

As we have already mentioned, the irreducibility of the polynomials $F_n(x)$ ($n \neq 1, 10$) plays a key role in the factorization of the characteristic polynomial of a $(d,3)$-digraph G.

Their corresponding multiplicities depend on the permutation cycle structure of G and they are uniquely determined, apart from the two cases where $F_n(x)$ is reducible. Then, by computing the simplest spectral invariant of G, as it is the trace of its adjacency matrix A, we are able to conclude that some of the unkown multiplicities must be negative, which provides us a proof of the nonexistence of G.

Theorem 2. *There is no almost Moore digraph of diameter three.*

Proof. Let G be a $(d,3)$-digraph and let $(m_1,\ldots,m_n)$ be its permutation cycle structure, where $n = d + d^2 + d^3$.

First, we obtain the factorization of the characteristic polynomial $\phi(G,x)$ of G. Since for any integer $n > 1$ and $n \neq 10$ the polynomial $F_n(x) = \Phi_n(1+x+x^2+x^3)$ is irreducible in $\mathbb{Q}[x]$ (see Theorem 1), applying Proposition 1 we have that

$$\prod_{\substack{2\leq i\leq n\\ i\neq 10}} (F_i(x))^{\frac{m(i)}{3}} \quad \text{is a factor of } \phi(G,x).$$

The remaining factors of $\phi(G,x)$ are derived as follows:

- Since G is d-regular and strongly connected, $\phi(G,x)$ has the linear factor $x-d$ with multiplicity 1, which is associated with the factor $x-(n+1)$ of $\det(xI-(J+P))$;
- Taking into account that $x-1$ is a factor of $\det(xI-(J+P))$ with multiplicity $m(1)-1$ and since $F_1(x) = (x^2+x+1)x$, we have that x^2+x+1 and x are factors of $\phi(G,x)$ with multiplicities a_1 and a_2, respectively, such that $2a_1 + a_2 = m(1) - 1$;
- Since $\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$ is a factor of $\det(xI-(J+P))$ with multiplicity $m(10)$ and taking into account the factorization of $F_{10}(x) = \Phi_{10}(1+x+x^2+x^3)$ in $\mathbb{Q}[x]$,

  $$F_{10}(x) = (x^4+x^3+x^2+x+1)(x^8+3x^7+6x^6+9x^5+9x^4+7x^3+4x^2+x+1),$$

  we have that $\Phi_5(x) = x^4+x^3+x^2+x+1$ and $F_{10}(x)/\Phi_5(x)$ are factors of $\phi(G,x)$ with multiplicities b_1 and b_2, respectively, such that $4b_1 + 8b_2 = 4m(10)$; that is, $b_1 + 2b_2 = m(10)$.

As a result,

$$\phi(G,x) = (x-d)(x^2+x+1)^{a_1} x^{a_2} \Phi_5(x)^{b_1} (F_{10}(x)/\Phi_5(x))^{b_2} \prod_{\substack{2\leq i\leq n\\ i\neq 10}} (F_i(x))^{\frac{m(i)}{3}}. \qquad (16)$$

Now, we express the trace of the adjacency matrix A of G in terms of the traces of the factors of $\phi(G,x)$. We recall that if $a(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a (monic) polynomial of degree $n \geq 1$, its trace $\operatorname{Tr} a(x)$ is defined as the sum of all its roots; that is,

$\mathrm{Tr}\, a(x) = -a_{n-1}$. Obviously, $\mathrm{Tr}\, a(x)b(x) = \mathrm{Tr}\, a(x) + \mathrm{Tr}\, b(x)$ for all pairs of polynomials. In particular,

$$\mathrm{Tr}\, F_i(x) = \mathrm{Tr}\, \left((x^3+x^2+x+1)^{\varphi(i)} + \cdots\right) = \varphi(i)\, \mathrm{Tr}\,(x^3+x^2+x+1) = -\varphi(i)\,.$$

Thus,

$$\mathrm{Tr}\, A = \mathrm{Tr}\, \phi(G,x) = d - a_1 - b_1 - 3b_2 - \frac{1}{3}\sum_{\substack{2\le i\le n\\ i\ne 10}} m(i)\varphi(i).$$

Then, taking into account the identity $\sum_{i=1}^{n} m(i)\varphi(i) = n$,

$$\sum_{i=1}^{n} m(i)\varphi(i) = \sum_{i=1}^{n}\sum_{i|l} m_l\varphi(i) = \sum_{l=1}^{n} m_l \sum_{i|l}\varphi(i) = \sum_{l=1}^{n} m_l l,$$

it follows that

$$\mathrm{Tr}\, A = d - a_1 - b_1 - 3b_2 - \frac{1}{3}(n - m(1) - 4m(10)).$$

Since $b_1 + 2b_2 = m(10)$, we have

$$\mathrm{Tr}\, A = d - a_1 - b_2 - \frac{1}{3}(n - m(1) - m(10)).$$

Therefore, the condition $\mathrm{Tr}\, A = 0$ (G has no loops) implies that

$$a_1 + b_2 = d - \frac{1}{3}n + \frac{1}{3}(m(1) + m(10)). \tag{17}$$

Notice that $m(1) + m(10) = \sum_{10\nmid i} m_i + 2\sum_{10|i} m_i$ takes its maximum value when all permutation cycles are short as possible. Moreover, the number of selfrepeats m_1 of a (d,k)-digraph is either 0 or k, if $k \ge 3$ (see [1]). So, $m(1) + m(10) \le 3 + \frac{n-3}{2}$ and, consequently,

$$a_1 + b_2 \le d - \frac{1}{6}(n-3) = -\frac{1}{6}(d^3 + d^2 - 5d - 3),$$

since $n = d + d^2 + d^3$.

Hence, if $d > 2$ then $a_1 + b_2 < 0$, which is impossible since a_1 and b_2 are nonnegative integers.

In the case $d = 2$ we have $a_1 = b_2 = 0$, which implies that $m(1) + m(10) = n - 3d$. We will see that there is no permutation cycle structure satisfying such a condition. Thus, since $m(i) = \sum_{i|l} m_l$ must be a multiple of 3, if $i \ne 1, 10$, and since $m_1 = 0, 3$, it follows that

$$m_i \equiv 0 \pmod 3, \text{for each } i \ne 2, 5, 10, \text{ and } m_2 + m_{10} \equiv m_5 + m_{10} \equiv 0 \pmod 3.$$

Therefore,

$$m(1) + m(10) \equiv m_2 + m_5 + 2m_{10} \equiv 0 \pmod 3,$$

which contradicts that $m(1) + m(10) = 8$. □

References

[1] E.T. Baskoro, M. Miller and J. Plesník, On the structure of digraphs with order close to the Moore bound, *Graphs Combin.* **14** (1998) 109–119.

[2] E.T. Baskoro, M. Miller, J. Plesník and Š. Znám, Regular digraphs of diameter 2 and maximum order, *Australas. J. Combin.* **9** (1994) 291-306.

[3] E.T. Baskoro, M. Miller, J. Širáň and M. Sutton, Complete characterisation of almost Moore digraphs of degree three, *J. Graph Theory* **48** 2 (2005) 112–126.

[4] W.G. Bridges and S. Toueg, On the impossibility of directed Moore graphs, *J. Combin. Theory B* **29** (1980) 339–341.

[5] M.A. Fiol, I. Alegre and J.L.A. Yebra, Line digraphs iterations and the (d, k) problem for directed graphs, in: *Proc. 10th Int. Symp. Comput. Arch.* (Stockholm, 1983) 174–177.

[6] J. Gimbert, On the existence of (d, k)-digraphs, *Discrete Math.* **197–198** 1–3 (1999) 375–391.

[7] J. Gimbert, Enumeration of almost Moore digraphs of diameter two, *Discrete Math.* **231** (2001) 177–190.

[8] A.J. Hoffman and R.R. Singleton, On Moore graphs with diameter 2 and 3, *IBM Res. Develop.* **4** (1960) 497–504.

[9] P. Kovács, The non-existence of certain regular graphs of girth 5, *J. Combin. Theory Ser. B* **30** (1981) 282–284.

[10] H.W. Lenstra Jr. and B. Poonen, *Personal communication.*

[11] M. Miller, J. Gimbert, J. Širáň and Slamin, Almost Moore digraphs are diregular, *Discrete Math.* **218** (2000) 265–270.

[12] M. Miller and I. Fris, Maximum order digraphs for diameter 2 or degree 2, *Pullman Volume of Graphs and Matrices, Lecture Notes in Pure and Applied Mathematics* **139** (1992) 269–278.

[13] M. Miller and I. Fris, Minimum diameter of diregular digraphs of degree 2, *Comput. J.* **31** (1988) 71–75.

[14] T. Nagell, *Introduction to Number Theory* (John Wiley & Sons Inc., 1951).

[15] J. Plesník and Š. Znám, Strongly geodetic directed graphs, *Acta F. R. N. Univ. Comen.-Mathematica* **XXIX** (1974) 29–34.

[16] L.C. Washington, *Introduction to Cyclotomic Fields* (Springer, 1997).