Nonexistence of almost Moore digraphs of diameter four

J. Conde*, J. Gimbert*
Dept. de Matemàtica, Universitat de Lleida
Jaume II, 69, 25001 Lleida, Spain
{jconde, joangim}@matematica.udl.cat

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

J.M. Miret‡, R. Moreno‡
Dept. de Matemàtica, Universitat de Lleida
Jaume II, 69, 25001 Lleida, Spain
{miret, ramiro}@matematica.udl.cat

Submitted: Jul 20, 2013; Accepted: Mar 25, 2013; Published: Mar 31, 2013
Mathematics Subject Classifications: 05C20, 05C50, 11R18

Abstract

Regular digraphs of degree $d > 1$, diameter $k > 1$ and order $N(d,k) = d + \cdots + d^k$ will be called almost Moore $(d,k)$-digraphs. So far, the problem of their existence has only been solved when $d = 2, 3$ or $k = 2, 3$. In this paper we prove that almost Moore digraphs of diameter 4 do not exist for any degree $d$.

Keywords: Almost Moore digraph, characteristic polynomial, cyclotomic polynomial.

1 Introduction

The degree/diameter problem finds, given two natural numbers $d$ and $k$, the largest possible number of vertices in a [directed] graph with maximum [out-]degree $d$ and diameter $k$ (for

*Partially supported by DGI Grant TIN2010-18978
†Partially supported by DGI Grant MTM2009–13060–C02–02
‡Partially supported by DGI Grant MTM2010–21580–C02–01
a survey of it see [12]). In the directed case, W.G. Bridges and S. Toueg in [4] proved that this number of vertices is less than the Moore bound, \( M(d, k) = 1 + d + \cdots + d^k \), unless \( d = 1 \) or \( k = 1 \). Then, the question of finding for which values of \( d > 1 \) and \( k > 1 \) there exist digraphs of order \( N(d, k) = M(d, k) - 1 \)

becomes an interesting problem. In this case, any extremal digraph turns out to be \( d \)-regular (see [10]). From now on, regular digraphs of degree \( d > 1 \), diameter \( k > 1 \) and order \( N(d, k) \) will be called almost Moore \((d,k)\)-digraphs (or \((d,k)\)-digraphs for short).

The problem of the existence of almost Moore \((d,k)\)-digraphs has been solved when \( d = 2, 3 \) or \( k = 2, 3 \). M. Miller and I. Fris [11] proved that the \((2,k)\)-digraphs do not exist for values of \( k > 2 \) and Baskoro et al. [3] established the nonexistence of \((3,k)\)-digraphs unless \( k = 2 \). On the other hand, Fiol et al. [6] showed that the \((d,2)\)-digraphs do exist for any degree. Their classification was completed by J. Gimbert in [8]. Moreover, J. Conde et al. [5] proved the nonexistence of \((d,3)\)-digraphs.

In this paper we prove that almost Moore digraphs of diameter four do not exist for any degree. The paper is organized as follows: Section 2 is devoted to determine the characteristic polynomial of a \((d,4)\)-digraph in terms of the polynomials \( F_{n,4}(x) = \Phi_n(1+x+x^2+x^3+x^4) \), being \( \Phi_n(x) \) the \( n \)th cyclotomic polynomial and \( 2 \leq n \leq N(d,4) \). In Section 3, assuming the cyclotomic conjecture (see [7]) for \( k = 4 \), which says that \( F_{n,4}(x) \) is irreducible unless \( n = 3, 6 \), we prove the nonexistence of \((d,4)\)-digraphs for \( d \geq 2 \). Finally, in Section 4 we show the conjecture for \( k = 4 \).

### 2 On the characteristic polynomial of a \((d,4)\)-digraph

Given a \((d,k)\)-digraph \( G \), its adjacency matrix \( A \) fulfills the equation

\[
I + A + \cdots + A^k = J + P,
\]

where \( J \) denotes the all-one matrix and \( P = (p_{ij}) \) is the \((0,1)\)-matrix associated with a distinguished permutation \( r \) of the set of vertices \( V(G) = \{1, \ldots, N\} \); that is to say, \( p_{ij} = 1 \) iff \( r(i) = j \) (see [1]).

Notice that \( r \) has a cycle structure which corresponds to its unique decomposition in disjoint cycles. The number of permutation cycles of \( G \) of each length \( n \leq N \) will be denoted by \( m_n \) and the vector \((m_1, \ldots, m_N)\) will be referred to as the permutation cycle structure of \( G \).

The factorization of \( \det(xI - (J + P)) \) in \( \mathbb{Q}[x] \) in terms of the cyclotomic polynomials \( \Phi_i(x) \) is given by (see [2, 5])

\[
\det(xI - (J + P)) = (x - (N + 1))(x - 1)^{m(1) - 1} \prod_{n=2}^{N} \Phi_n(x)^{m(n)},
\]

where \( m(n) = \sum_{n|i} m_i \) represents the total number of permutation cycles of order multiple of \( n \).
From Equations (1) and (2), the problem of the factorization in $\mathbb{Q}[x]$ of the characteristic polynomial of $G$, $\phi(G, x) = \det(xI - A)$, was connected by J. Gimbert in [7] with the study of the irreducibility in $\mathbb{Q}[x]$ of the polynomials

$$F_{n,k}(x) = \Phi_n(1 + x + \cdots + x^k).$$

The idea is that, when such polynomials are irreducible, they appear as factors 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 $2 \leq n \leq N$. If $F_{n,k}(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$, then it is a factor of $\phi(G, x)$ and its multiplicity is $m(n)/k$.

This result was proved in [7]. Moreover, it was proved that $F_{2,k}(x) = 2 + x + \cdots + x^k$ is irreducible in $\mathbb{Q}[x]$, for any positive integer $k$. On the other hand, it was shown that for each $n > 2$ there are infinitely many values of $k$ for which $F_{n,k}(x)$ is reducible in $\mathbb{Q}[x]$.

**Lemma 2.** Let $n > 2$ and $k > 1$ be integers. Then, the following statements hold.

(i) If $n$ is odd and $k \equiv -2 \pmod{2n}$, then $\Phi_{2n}(x)$ divides $F_{n,k}(x)$.

(ii) If $n \equiv 0 \pmod{4}$ and $k \equiv -2 \pmod{n}$, then $\Phi_{n}(x)$ divides $F_{n,k}(x)$.

(iii) If $n \equiv 2 \pmod{4}$ and $k \equiv -2 \pmod{\frac{n}{2}}$, then $\Phi_{\frac{n}{2}}(x)$ divides $F_{n,k}(x)$.

On the other hand, in [7] it was conjectured that $F_{n,k}(x)$ is irreducible in $\mathbb{Q}[x]$ if $n$ and $k$ do no satisfy any of the conditions of Lemma 2.

**Conjecture 3.** Let $n > 2$ and $k > 1$ be integers. One has that

(i) If $k$ is even, then $F_{n,k}(x)$ is reducible in $\mathbb{Q}[x]$ if and only if $n \mid (k + 2)$, in which case $F_{n,k}(x)$ has just two factors.

(ii) If $k$ is odd, then $F_{n,k}(x)$ is reducible in $\mathbb{Q}[x]$ if and only if $n$ is even and $n \mid 2(k + 2)$, in which case $F_{n,k}(x)$ has just two factors.

We will refer to this conjecture as the cyclotomic conjecture. The case $k = 2$ was proved by H.W. Lenstra Jr. and B. Poonen [9] and, recently, the authors proved the case $k = 3$ in [5].

The remainder of this section is devoted to finding the conditions in order to obtain a factorization of the characteristic polynomial of a $(d, 4)$-digraph $G$ in terms of $F_{n,4}(x)$. Thus, let $G$ be a $(d, 4)$-digraph of degree $d > 3$ and let $(m_1, \ldots, m_N)$ be its permutation cycle structure, where $N = d + d^2 + d^3 + d^4$.

We will assume the cyclotomic conjecture is true for $k = 4$, that is $F_{n,4}(x)$ is irreducible in $\mathbb{Q}[x]$ except $n = 3, 6$, which will be proven in the last section. From now on, we will write $F_n(x)$ instead of $F_{n,4}(x)$. 

THE ELECTRONIC JOURNAL OF COMBINATORICS 20(1) (2013), #P75

3
Then, by applying Proposition 1 we have that
\[
\prod_{2 \leq n \leq N \atop n \neq 3, 6} (F_n(x))^{\frac{m(n)}{4}} \text{ is a factor of } \phi(G, x).
\]

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;
- Taking into account that \( x - 1 \) is a factor of \( \det(xI - (J + P)) \) with multiplicity \( m(1) - 1 \) and since
  \[
  F_1(x) = (x + 1)(x^2 + 1)x,
  \]
  we have that \( x + 1, x^2 + 1 \) and \( x \) are factors of \( \phi(G, x) \) with multiplicities \( a_1, a_2 \) and \( a_3 \), respectively, where \( a_1 + 2a_2 + a_3 = m(1) - 1 \);
- Since \( \Phi_3(x) = x^2 + x + 1 \) is a factor of \( \det(xI - (J + P)) \) with multiplicity \( m(3) \) and taking into account the factorization of \( F_3(x) \) in \( \mathbb{Q}[x] \),
  \[
  F_3(x) = (x^2 - x + 1)(x^6 + 3x^5 + 5x^4 + 6x^3 + 7x^2 + 6x + 3),
  \]
  we have that \( \Phi_6(x) = x^2 - x + 1 \) and \( F_3(x)/\Phi_6(x) \) are factors of \( \phi(G, x) \) with multiplicities \( b_1 \) and \( b_2 \), respectively, where \( 2b_1 + 6b_2 = 2m(6) \); that is, \( b_1 = m(3) - 3b_2 \). Analogously, since the factorization of \( F_6(x) \) in \( \mathbb{Q}[x] \) is
  \[
  F_6(x) = (x^2 + x + 1)(x^6 + x^5 + x^4 + 2x^3 + x^2 + 1),
  \]
  we have that \( \Phi_3(x) \) and \( F_6(x)/\Phi_3(x) \) are factors of \( \phi(G, x) \) with multiplicities \( c_1 \) and \( c_2 \), respectively, where \( c_1 = m(6) - 3c_2 \).

As a result, the characteristic polynomial of \( G \) is
\[
\phi(G, x) = (x - d)(x + 1)^{a_1}(x^2 + 1)^{a_2}x^{a_3}\Phi_6(x)^{b_1}(F_3(x)/\Phi_6(x))^{b_2} \times \Phi_3(x)^{c_1}(F_6(x)/\Phi_3(x))^{c_2} \prod_{2 \leq n \leq N \atop n \neq 3, 6} (F_n(x))^{\frac{m(n)}{4}}. \tag{3}
\]

\[
\prod_{2 \leq n \leq N \atop n \neq 3, 6} (F_n(x))^{\frac{m(n)}{4}} \tag{4}
\]

### 3 On the nonexistence of \((d, 4)\)-digraphs

In this section, we will derive the nonexistence of a \((d, 4)\)-digraph from the irreducibility of the polynomials \( F_n(x) \) which appear in the factorization of its characteristic polynomial and from the behaviour of the first three powers of its adjacency matrix.

**Theorem 4.** Assuming that the cyclotomic conjecture is true for \( k = 4 \), there is no almost Moore digraph of diameter four.
Proof. Let $G$ be a $(d, 4)$-digraph with adjacency matrix $A$. We compute the graph spectral invariants $\text{Tr} A^\ell$ ($\ell = 1, 2, 3$) in terms of the sum of the $\ell$th powers of the roots of each factor of $\phi(G, x)$.

Given a monic polynomial of degree $n \geq 1$, $a(x) = x^n + \sum_{i=1}^{n} a_{n-i}x^{n-i}$, and given an integer $\ell \geq 1$, we define $S_\ell(a(x))$ to be the sum of the $\ell$th powers of all the roots of $a(x)$. Using Newton’s formulas [14], which express $\sum_{i=1}^{n} a_{n-i}x^{n-i}$, we have

$$S_1(a(x)) = -a_{n-1},$$

$$S_2(a(x)) = a_{n-1}^2 - 2a_{n-2},$$

$$S_3(a(x)) = -a_{n-1}^3 + 3a_{n-1}a_{n-2} - 3a_{n-3}.$$ 

Since $S_\ell(a(x)b(x)) = S_\ell(a(x))S_\ell(b(x))$, for all pairs of polynomials, and taking into account that

$$F_n(x) = \Phi_n(1 + x + x^2 + x^3 + x^4) = (1 + x + x^2 + x^3 + x^4)^{\varphi(n)} + O(x^{4\varphi(n)-4}),$$

where $\varphi(n)$ stands for Euler’s function, we obtain

$$S_\ell(F_n(x)) = \varphi(n)S_\ell(x^4 + x^3 + x^2 + x + 1) = -\varphi(n), \quad \ell = 1, 2, 3.$$

Besides, it can be easily checked that

<table>
<thead>
<tr>
<th></th>
<th>$S_1$</th>
<th>$S_2$</th>
<th>$S_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x+1$</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>$x^2+1$</td>
<td>0</td>
<td>-2</td>
<td>0</td>
</tr>
<tr>
<td>$\Phi_6(x)$</td>
<td>1</td>
<td>-1</td>
<td>-2</td>
</tr>
<tr>
<td>$\Phi_3(x)$</td>
<td>-1</td>
<td>-1</td>
<td>2</td>
</tr>
</tbody>
</table>

Now, for each $\ell = 1, 2, 3$ we can express the trace of the $\ell$th power of the adjacency matrix $A$ of $G$ in terms of the sums $S_\ell$ of all factors of $\phi(G, x)$. Thus,

$$\text{Tr} A = d - a_1 + b_1 - 3b_2 - c_1 - c_2 - \frac{1}{4}T,$$

$$\text{Tr} A^2 = d^2 + a_1 - 2a_2 - b_1 - b_2 - c_1 - c_2 - \frac{1}{4}T,$$

$$\text{Tr} A^3 = d^3 - a_1 - 2b_1 + 2c_1 - 4c_2 - \frac{1}{4}T,$$

where $T = \sum_{2 \leq n \leq N \atop n \neq 3, 6} m(n)\varphi(n)$. From the identity $\sum_{n=1}^{N} m(n)\varphi(n) = N$ (see [7]),

$$T = N - m(1) - 2m(3) - 2m(6).$$

So, taking into account that $b_1 = m(3) - 3b_2$ and $c_1 = m(6) - 3c_2$,

$$\text{Tr} A = d - \frac{1}{4}N + \frac{3}{4}m(1) + \frac{3}{2}m(3) - \frac{1}{2}m(6) - a_1 - 6b_2 + 2c_2,$$

$$\text{Tr} A^2 = d^2 - \frac{1}{4}N + \frac{1}{4}m(1) - \frac{1}{2}m(3) - \frac{1}{2}m(6) + a_1 - 2a_2 + 2b_2 + 2c_2,$$

$$\text{Tr} A^3 = d^3 - \frac{1}{4}N + \frac{1}{4}m(1) - \frac{3}{2}m(3) + \frac{5}{2}m(6) - a_1 + 6b_2 - 10c_2.$$
Since $G$ has no cycles of length $\leq 3$, we know that $\text{Tr} A^\ell = 0$ ($\ell = 1, 2, 3$). As a consequence,

$$
4a_1 + 24b_2 - 8c_2 = 4d - N + m(1) + 6m(3) - 2m(6),
-4a_1 + 8b_2 - 8c_2 = 4d^2 - N + m(1) - 2m(3) - 2m(6),
4a_1 - 24b_2 + 40c_2 = 4d^3 - N + m(1) - 6m(3) + 10m(6).
$$

Applying Gauss reduction method to the previous linear system, it follows that

$$
8a_2 + 16b_2 - 16c_2 = 4d^2 + 4d - 2N + 2m(1) + 4m(3) - 4m(6),
-48b_2 + 48c_2 = 4d^3 - 4d - 12m(3) + 12m(6).
$$

Taking into account that $N = d^4 + d^3 + d^2 + d$, from (5) and (6) we derive that

$$
24a_2 = 4d^3 + 12d^2 + 8d + 6m(1) - 6N.
$$

Notice that $m(1) = \sum_{n=1}^N m_n$ 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 $k \geq 3$ (see [1]). So, $m(1) \leq 4 + \frac{N-4}{2}$ and, consequently,

$$
24a_2 \leq 4d^3 + 12d^2 + 8d + 12 - 3N = -3d^4 + d^3 + 9d^2 + 5d + 12.
$$

Hence, if $d > 3$ then $a_2 < 0$, which is impossible since $a_2$ is a nonnegative integer. \qed

## 4 The cyclotomic conjecture for $k = 4$

This section is devoted to proving the cyclotomic conjecture in the case $k = 4$, that is, we show that the polynomial $F_n(x) = \Phi_n(1 + x + x^2 + x^3 + x^4)$ is irreducible in $\mathbb{Q}[x]$, when $n > 1$ and $n \neq 3, 6$.

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. In order to prove this, let us suppose that $F_n(x)$ is reducible in $\mathbb{Q}[x]$ and let us consider a root $\varepsilon$ of $F_n(x)$. Denoting

$$
p_1(x, z) = 1 - z + x + x^2 + x^3 + x^4,
$$

and taking a suitable primitive $n$th root of unity $\zeta_n$, we get

$$
p_1(\varepsilon, \zeta_n) = 0.
$$

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 $\varphi(n)$ or $2\varphi(n)$. We can assume that $\varepsilon$ is a root of such a factor. In particular, $\varepsilon$ is an algebraic integer and $[\mathbb{Q}(\varepsilon) : \mathbb{Q}(\zeta_n)]$ is either 1 or 2.
If \([\mathbb{Q}(\varepsilon) : \mathbb{Q}(\zeta_n)] = 1\), we consider the element \(\overline{\varepsilon}/\varepsilon \in \mathbb{Q}(\varepsilon, \overline{\varepsilon})\), where \(\overline{\varepsilon}\) denotes the complex conjugation. By using arguments given in [5] we obtain that \(\overline{\varepsilon}/\varepsilon\) is a root of unity and hence the same procedure given for diameter 3 to state the irreducibility of \(F_3(x)\) follows.

Now, assume that \([\mathbb{Q}(\varepsilon) : \mathbb{Q}(\zeta_n)] = 2\) for all \(\varepsilon\) such that \(p_1(\varepsilon, \zeta_n) = 0\). We denote by \(\varepsilon'\) the conjugate root of \(\varepsilon\) over \(\mathbb{Q}(\zeta_n)\), that is to say, the polynomial \(p_1(x, \zeta_n)/(x - \varepsilon)(x - \varepsilon')\) is irreducible in \(\mathbb{Q}(\zeta_n)[x]\). Changing the root of \(p_1(x, \zeta_n)\) if necessary, we can assume that \(\varepsilon\varepsilon'\) is not real. Since \(\varepsilon\) is an algebraic integer and \(1 - \zeta_n\) is a unity or a prime element of \(\mathbb{Z}[\zeta_n]\), \(\varepsilon\varepsilon'\) is also a unity or a prime element of \(\mathbb{Z}[\zeta_n]\). Therefore,

\[
\alpha = \frac{\varepsilon\varepsilon'}{\overline{\varepsilon}\varepsilon'} \in \mathbb{Z}[\zeta_n]
\]

is a unity of \(\mathbb{Z}[\zeta_n]\) whose conjugates have absolute value 1. Hence, \(\alpha \neq 1\) is a root of unity of order \(2n\) [15, Lemma 1.6]. Notice that if \(n\) is even, \(\alpha\) is a root of unity of order \(n\).

Now, we search for a polynomial relation between \(\zeta_n\) and \(\alpha = \beta\beta'\), where \(\beta = \overline{\varepsilon}/\varepsilon\) and \(\beta' = \overline{\varepsilon'}/\varepsilon'\). In order to find such an expression we give first a relation between \(\zeta_n\) and \(\beta\). We use the following identities:

\[
1 + \varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 = \zeta_n, \quad \overline{\varepsilon} = \beta \varepsilon.
\]

From them, and taking into account that \(\overline{\zeta_n} = 1/\zeta_n\), it can be seen that \(p_2(\varepsilon, \beta, \zeta_n) = 0\) where

\[
p_2(x, y, z) = 1 - z - xyz - x^2y^2z - x^3y^3z - x^4y^4z.
\]

Similarly, \(p_2(\varepsilon', \beta', \zeta_n) = 0\). Notice as well that \(p_3(\alpha, \beta, \beta') = 0\) where

\[
p_3(y, y', w) = w - yy'.
\]

Therefore, the relation between \(\zeta_n\) and \(\alpha\) we are looking for is \(R(\zeta_n, \alpha) = 0\), where

\[
R_1(y, z) = \text{Res}(p_1(x, z), p_2(x, y, z), x), \quad R_2(y', z, w) = \text{Res}(R_1(y, z), p_3(y, y', w), y),
\]

\[
R(z, w) = \text{Res}(R_1(y', z), R_2(y', z, w), y').
\]

This polynomial factorizes as follows

\[
R(z, w) = (z - 1)^{20} q_1(z, w) q_2^2(z, w) q_3^2(z, w) q_4^4(z, w),
\]

where \(q_1(z, w)\) has degree 14 in \(z\) and 16 in \(w\), \(q_2(z, w)\) and \(q_3(z, w)\) have degree 21 in \(z\) and 24 in \(w\), and \(q_4(z, w)\) has degree 27 in \(z\) and 36 in \(w\).

**Proposition 5.** Let \(n > 2\) be an integer and \(F_n(x) = \Phi_n(1 + x + x^2 + x^3 + x^4)\). If \(F_n(x)\) is reducible in \(\mathbb{Q}[x]\) then:
If \( n \) is even, then there exists an integer \( k, 1 \leq k < n \), such that \( \Phi_n(x) \) divides one of the polynomials \( q_i(x, x^k), i \in \{1, 2, 3, 4\} \), given in (12).

If \( n \) is odd, then there exists an integer \( k, 1 \leq k < n \), such that \( \Phi_n(x) \) divides one of the polynomials \( q_i(x, x^k) \) or \( q_i(x, -x^k), i \in \{1, 2, 3, 4\} \), given in (12).

**Proof.** Since the cyclotomic polynomial \( \Phi_n(x) \) is irreducible in \( \mathbb{Q}[x] \) and it does not divide \( x - 1 \), then when \( n \) is even it must divide at least one of the polynomials \( q_i(x, x^k), i \in \{1, 2, 3, 4\} \), \( 1 \leq k < n \). When \( n \) is odd, \( \alpha \) or \( -\alpha \) is a root of unity of order \( n \). Hence, \( \Phi_n(x) \) must divide \( q_i(x, x^k) \) or \( q_i(x, -x^k), i \in \{1, 2, 3, 4\} \). \( \square \)

Our main goal is to show that \( F_n(x) \) is irreducible in \( \mathbb{Q}[x] \), for \( n > 1 \) and \( n \neq 3, 6 \). It is enough to prove that \( \Phi_n(x) \) does not divide, for \( i \in \{1, 2, 3, 4\} \), any of the polynomials \( q_i(x, x^k), 1 \leq k < n \), when \( n \) is even and it does not divide any of the polynomials \( q_i(x, x^k) \) or \( q_i(x, -x^k), 1 \leq k < n \), when \( n \) is odd. This is equivalent to proving that \( \Phi_{2n}(x) \) does not divide any of the polynomials \( q_i(x^2, x^\ell), 1 \leq \ell < 2n \).

**Theorem 6.** The polynomial \( F_n(x) \) is irreducible in \( \mathbb{Q}[x] \) for \( n > 1 \), unless \( n = 3, 6 \).

**Proof.** If \( F_n(x) \) is reducible, then taking into account Proposition 5 there exist polynomials \( q_i(x^2, x^\ell), i \in \{1, 2, 3, 4\} \), given by (12) such that the cyclotomic polynomial \( \Phi_{2n}(x) \) divides one of them. Now, we show that \( \Phi_{2n}(x) \) does not divide \( q_1(x^2, x^\ell) \). To see this, from part (i) of Lemma 3 in [5] (see also [13]), we know that
\[
\Phi_{2n}(x) \equiv \Phi_r(x)^{\varphi(p^r)} \pmod{p \mathbb{Z}[x]},
\]
where \( p \) is a prime number dividing \( 2n \) with \( 2n = p^r \ell \) and \( (p, \ell) = 1 \). Consequently
\[
\Phi_r(x)^{\varphi(p^r)-1} | \gcd(q_1(x^2, x^\ell), xq'_1(x^2, x^\ell)) \pmod{p \mathbb{Z}[x]).
\]
Now, we consider the polynomial
\[
A_1(z, w) = 2z \frac{\partial}{\partial z} q_1(z, w) + \ell w \frac{\partial}{\partial w} q_1(z, w) \in \mathbb{Z}[z, w],
\]
that is \( A_1(x^2, x^\ell) = xq'_1(x^2, x^\ell) \). Therefore
\[
\Phi_r(x)^{\varphi(p^r)-1} \mid P_1(x) \pmod{p \mathbb{Z}[x]), \tag{13}
\]
where \( P_1(x) \) is the following resultant
\[
P_1(x) = \text{Res} \left( q_1(x^2, w), A_1(x^2, w), w \right).
\]
It can be checked that
\[
P_1(x) = 5^1 x^{264} \Phi_1^S(x) \Phi_2^S(x) \Phi_4^S(x) \Phi_3^S(x) \Phi_6^S(x) \Phi_6^S(x) P_{1,0}^2(x) P_{1,\ell}(x), \tag{14}
\]
with \( P_{1,0}(x) \) a polynomial of degree 36 and \( P_{1,\ell}(x) \) a polynomial of degree at most 60.
Notice that for those integers $n$ which have a prime factor $p$ such that $P_1(x) \neq 0 (\text{mod } p\mathbb{Z}[x])$ for all $\ell (\text{mod } p)$, the degree of $P_1(x)$ (mod $p\mathbb{Z}[x]$) provides us an upper bound $K$ for $\varphi(n)$. Hence, for those values of $n$ such that $\varphi(n) > K$, $F_n(x)$ is irreducible in $\mathbb{Q}[x]$, and for those $n$ with $\varphi(n) \leq K$, we can computationally check the irreducibility of $F_n(x)$ unless $n = 3, 6$.

The coefficients of $P_{1,0}(x)$ do not depend on $\ell$ and its gcd is one. Hence, this polynomial does not vanish for any prime $p$. The polynomial $P_{1,\ell}(x)$ is given by

$$P_{1,\ell}(x) = \sum_{i=0}^{30} a_i(\ell)x^{2i},$$

where the coefficients $a_i(\ell)$ are polynomials on $\mathbb{Q}[\ell]$ of degree 16 given by the expressions

$$a_0(\ell) = 2^{32}5^{12}(\ell + 1)^{16},$$

$$a_1(\ell) = -2^{26}5^{11}(\ell + 1)^{12}(9353\ell^4 + 37412\ell^3 + 57248\ell^2 + 39552\ell + 10368),$$

$$a_2(\ell) = 2^{17}5^{10}(\ell + 1)^8(338813683\ell^8 + 2710509464\ell^7 + 9562778864\ell^6$$

$$+ 19424004680\ell^5 + 24833262080\ell^4 + 20453500928\ell^3 + 10593286144\ell^2$$

$$+ 3152707584\ell + 412581888),$$

$$\vdots$$

$$a_{29}(\ell) = -2^{26}5^{11}(\ell + 1)^{12}(9353\ell^4 + 37412\ell^3 + 57248\ell^2 + 39552\ell + 10368),$$

$$a_{30}(\ell) = 2^{32}5^{12}(\ell + 1)^{16}.$$

From the first coefficient it turns out that the factors which can vanish $P_{1,\ell}(x)$ are 2, 5 and those that divide $\ell + 1$. The polynomials $a_j(\ell), \ j = 4, \ldots, 26$, are not divisible by $\ell + 1$. The greatest common divisor of the remaining divisions of these polynomials by $\ell + 1$ in $\mathbb{Z}[x]$ is 1. Thus, there are no primes dividing $\ell + 1$ that vanish $P_{1,\ell}(x)$. For the prime $p = 2$, the polynomial $P_{1,\ell}(x)$ only vanishes when $\ell$ is even. Concerning the prime $p = 5$, the polynomial $P_{1,\ell}(x)$ only vanishes when $\ell \equiv 4 \pmod{5}$.

Now, if the factorization of $n$ has a prime factor $p$ different from 2 and 5, by using (13) and taking into account the factorization of $P_1(x)$ (mod $p\mathbb{Z}[x]$) given in (14), the degree of the maximum power $\Phi_r(x)$ that could divide $P_1(x)$ (mod $p\mathbb{Z}[x]$) is bounded by $\deg P_1(x) - \deg x^{264} = 368$. This is a bound for $(\varphi(p^e) - 1)\varphi(r)$. Hence,

$$\varphi(n) \leq \varphi(2n) = \varphi(p^e)\varphi(r) \leq 368 + \varphi(r) \leq 736.$$

For these integers $n$ which have a prime factor different from 2 and 5 and such that $\varphi(n) > 736$, $F_n(x)$ is irreducible in $\mathbb{Q}[x]$. For those integers $n$ such that $\varphi(n) \leq 736$, it has been computationally checked that $F_n(x)$ is reducible in $\mathbb{Q}[x]$ only when $n = 3$ and $n = 6$. Therefore, the remaining cases to consider are $n = 2^e5^d$, with $e \geq 1$ or $d \geq 1$.

The previous method works as well taking $p = 2$ in (13) when $\ell$ is odd. On the other hand, if $5 \mid n$ and $p = 5$, then $P_1(x) = 0$ (mod $p\mathbb{Z}[x]$) but the following relation holds

$$\Phi_r(x)^e(p^e - 2) \mid Q_1(x) \pmod{p\mathbb{Z}[x]}, \quad (15)$$
where \( Q_1(x) \) is the resultant

\[
Q_1(x) = \text{Res}\left( q_1(x^2, w), B_1(x^2, w), w \right),
\]

being

\[
B_1(z, w) = 2z \frac{\partial}{\partial z} A_1(z, w) + kw \frac{\partial}{\partial w} A_1(z, w).
\]

Since we must consider the cases \( n = 2^e 5^d \), we can apply (15) with \( p = 5 \) and we proceed in the same way as in (13). Nevertheless, the polynomial \( Q_1(x) \) (mod \( 5 \mathbb{Z}[x] \)) is identically zero only for \( \ell \equiv 4 \pmod{5} \). Thus, taking into account these remarks, the cases we must study have been reduced to the following:

1. \( n = 2^e 5^d \), with \( e \geq 0, d > 0, \ell \text{ even and } \ell \equiv 4 \pmod{5} \),
2. \( n = 2^e \), with \( e \geq 1 \), and \( \ell \text{ even} \).

1. We shall prove that \( \Phi_{2n}(x) \) (mod \( 5 \mathbb{Z}[x] \)) does not divide \( q_1(x^2, x^\ell) \) (mod \( 5 \mathbb{Z}[x] \)), for \( \ell \text{ even and } \ell \equiv 4 \pmod{5} \). It is known that \( \Phi_{2n}(x) = \Phi_{2e+1}(x)^{4(5^{d-1})} \) (mod \( 5 \mathbb{Z}[x] \)), where

\[
\Phi_{2n}(x) \pmod{5 \mathbb{Z}[x]} = \begin{cases} 
  x + 4 & \text{if } m = 0, \\
  x + 1 & \text{if } m = 1, \\
  (x^{2m-2} + 2)(x^{2m-2} + 3) & \text{if } m \geq 2.
\end{cases}
\]

We have that

\[
q_1(z, w) = q_{1,1}(z, w)^2 q_{1,2}(z, w) q_{1,3}(z, w) q_{1,4}(z, w) \pmod{5 \mathbb{Z}[z, w]},
\]

where

\[
q_{1,1}(z, w) = w^2 z - 1, \\
q_{1,2}(z, w) = w^4 z^4 - 2w^4 z^3 + w^4 z^2 + w^3 z^2 - 2w^2 z^3 + w^2 z^2 - 2w^2 z + wz^2 + z^2 - 2z + 1, \\
q_{1,3}(z, w) = w^4 z^4 - 2w^4 z^3 + w^4 z^2 - 2w^3 z^3 - 2w^3 z^2 - 2w^2 z^3 + 2w^2 z^2 - w^2 z - wz^2 - 2w z + z^2 - 2z + 1, \\
q_{1,4}(z, w) = w^4 z^4 - 2w^4 z^3 + w^4 z^2 - w^3 z^3 - 2w^2 z^3 + w^2 z^2 - 2w^2 z - wz + z^2 - 2z + 1.
\]

So, we will prove that \( \Phi_{2e+15d}(x) \) (mod \( 5 \mathbb{Z}[x] \)) does not divide \( q_{1,i}(x^2, x^\ell) \) (mod \( 5 \mathbb{Z}[x] \)), for any \( i \in \{1, 2, 3, 4\} \), when \( e > 0 \) and \( e = 0 \).

**Case** \( e > 0 \). First, we claim that

\[
\gcd\left( \Phi_{2e+1}(x) \pmod{5 \mathbb{Z}[x]}, q_{1,1}(x^2, x^\ell) \pmod{5 \mathbb{Z}[x]} \right) = 1.
\]

Indeed, let \( \gamma \) be a root of \( \Phi_{2e+1}(x) \) (mod \( 5 \mathbb{Z}[x] \)), that is \( \gamma^{2e-1} \) is equal to 2 or 3. Then, \( \gamma^{2e+1} \) is the smallest power of \( \gamma \) equal to 1. Therefore, if \( \gamma \) is a root of \( q_{1,1}(x^2, x^\ell) = x^{2(\ell+1)} - 1 \) then \( 2^{e+1} \mid 2(\ell + 1) \), which contradicts that \( \ell \) is even.

Assume \( \Phi_{2e+1}(x) \) (mod \( 5 \mathbb{Z}[x] \)) divides \( q_{1,2}(x^2, x^\ell) q_{1,3}(x^2, x^\ell) q_{1,4}(x^2, x^\ell) \). Then each irreducible divisor of \( \Phi_{2e+1}(x) \) (mod \( 5 \mathbb{Z}[x] \)) is a divisor of some of the polynomials \( q_{1,i}(x^2, x^\ell) \).
(mod 5\mathbb{Z}[x]), i \in \{2, 3, 4\}, with multiplicity greater than 1. Then, for i \in \{2, 3, 4\} we consider the resultant

\[ T_{1,i}(x) = \text{Res}(q_{1,i}(x^2, w), S_{1,i}(x^2, w), w), \]

where

\[ S_{1,i}(z, w) = 2z \frac{\partial}{\partial z} q_{1,i}(z, w) + \ell w \frac{\partial}{\partial w} q_{1,i}(z, w). \]

When \( \ell = 4 \pmod{5} \), the polynomials \( T_{1,i}(x) \pmod{5\mathbb{Z}[x]} \) are as follows:

\[
T_{1,2}(x) = x^{20}(1 + x)^6(2 + x)^2(3 + x)^2(4 + x)^6(1 + x + x^2)^2(1 + 4x + x^2)^2,
\]

\[
T_{1,3}(x) = x^{20}(1 + x)^4(4 + x)^4(4 + 2x + x^2)^4(4 + 3x + x^2)^4,
\]

\[
T_{1,4}(x) = x^{20}(1 + x)^6(2 + x)^2(3 + x)^2(4 + x)^6(1 + x + x^2)^2(1 + 4x + x^2)^2.
\]

Therefore, \( e \) must be 1 and \( \Phi_4(x)^7 \pmod{5\mathbb{Z}[x]} \) is the greatest power of \( \Phi_4(x) \pmod{5\mathbb{Z}[x]} \) which could divide \( q_{1,2}(x^2, x^\ell)q_{1,3}(x^2, x^\ell)q_{1,4}(x^2, x^\ell) \). Since

\[ \Phi_{2e+15d}(x) = \Phi_{2e+1}(x)^{4\cdot 5^{d-1}} \pmod{5\mathbb{Z}[x]}, \]

for \( d > 1 \) the polynomial \( \Phi_{2e+15d}(x) \pmod{5\mathbb{Z}[x]} \) does not divide \( q_1(x^2, x^\ell) \pmod{5\mathbb{Z}[x]} \). For \( n = 2 \cdot 5 \) we can check that \( F_n(x) \) is irreducible in \( \mathbb{Q}[x] \).

• Case \( e = 0 \). In this case \( \Phi_{2,5d}(x) = (x + 1)^{4\cdot 5^{d-1}} \pmod{5\mathbb{Z}[x]} \). Set \( \ell + 1 = 5^k m \) with \( m \) odd and \( \text{gcd}(5, m) = 1 \). Since \( \ell + 1 = 0 \pmod{5} \) and \( \ell + 1 \leq 2 \cdot 5^d \), it is clear that \( 1 \leq k \leq d \). The polynomial \( (x + 1)^{2 \cdot 5^k} \) is the greatest power of \( x + 1 \) which divides \( q_{1,1}(x^2, x^\ell)^2 = (x^{2(\ell+1)} - 1)^2 = (x^m - 1)^{2 \cdot 5^k} \pmod{5\mathbb{Z}[x]} \). From the following equalities

\[ \text{Res}(q_{1,1}(x^2, w), q_{1,i}(x^2, w), w) = 4x^{10}(x + 1)^2(4 + x)^2, \quad 2 \leq i \leq 4, \]

we get that \( (x + 1)^{2 \cdot 5^k + 6} \) is the greatest power of \( x + 1 \) dividing \( q_1(x^2, x^\ell) \). Hence, \( 4 \cdot 5^{d-1} \leq 2 \cdot 5^k + 6 \) and, thus, \( k = d \). So, \( \ell + 1 \) must be either \( 5^d \) or \( 2 \cdot 5^d \). Since \( \ell \) is even, \( \ell = 5^d - 1 \). Therefore, only for this value of \( \ell \) the polynomial \( \Phi_{2,5d}(x) \) can divide \( q_1(x^2, x^\ell) \). Nevertheless, since the roots of \( \Phi_{2,5d}(x) \) satisfy that \( x^{5d} = -1 \), the polynomial \( \Phi_{2,5d}(x) \) should divide

\[ q_1(x^2, -1/x) = 25(-1 + x)^4(1 + x)^6(1 - x + x^2), \]

which leads to a contradiction.

ii) In this case \( n = 2^e \), with \( e \geq 1 \) and \( \ell = 2k \). We shall prove that \( \Phi_{2^e}(x) \pmod{5\mathbb{Z}[x]} \) does not divide \( q_1(x, x^k) \pmod{5\mathbb{Z}[x]} \). With the same arguments used in the above case, we obtain that

\[ \text{gcd}(\Phi_{2^e}(x) \pmod{5\mathbb{Z}[x]}, q_{1,1}(x, x^k) \pmod{5\mathbb{Z}[x]}) = 1. \]
Let $\gamma \in \mathbb{F}_{5^{2e-2}}$ such that $\Phi_{2e}(\gamma) = 0$, where $\mathbb{F}_{5^{2e-2}}$ is the finite field with $5^{e-2}$ elements. Since $\Phi_{2e}(x) = (x^{2e-2} + 2)(x^{2e-2} + 3)$ is the decomposition in irreducible factors in $\mathbb{F}_5$, we know that $\mathbb{F}_{5^{2e-2}} = \mathbb{F}_5(\gamma)$ and $\gamma^{2e-2} = a$, where $a$ is either 2 or 3. Moreover,

$$
\text{Tr}(\gamma^m) = \begin{cases} 
\varphi(2e)/2 & \text{if } \gcd(m, 2e) = 2e, \\
-\varphi(2e)/2 & \text{if } \gcd(m, 2e) = 2e-1, \\
\pm a\varphi(2e)/2 & \text{if } \gcd(m, 2e) = 2e-2, \\
0 & \text{otherwise},
\end{cases}
$$

where $\text{Tr}$ denotes the trace $\text{Tr}_{\mathbb{F}_{5^{2e-2}}/\mathbb{F}_5}$ and the sign of $a$ depends on the class $m\over 2e-2$ (mod 4).

We can assume that $e > 5$ and, thus, when $\gcd(m, 2e) \mid 8$ we have $\text{Tr}(\gamma^m) = 0$. If

$$
q_{1,4}(\gamma, \gamma^\ell) = 1 + \sum_{i>0} a_i \gamma^i = 0,
$$

taking traces we obtain $\text{Tr}(1) = \varphi(2e)/2 = 0$ (mod 5) which is impossible.

If $q_{1,2}(\gamma, \gamma^\ell) = 0$, taking traces we obtain

$$
\text{Tr}(1) + \text{Tr}(\gamma^{2+\ell}) + \text{Tr}(\gamma^{2+3\ell}) = 0 \quad (\text{mod } 5). 
$$

(17)

Notice that $\text{Tr}(\gamma^{2+\ell})\text{Tr}(\gamma^{2+3\ell}) = 0$ (mod 5). From (17), we get that either $\gcd(2e, 2+\ell) = 2e-1$ or $\gcd(2e, 2+3\ell) = 2e-1$. In the first case, $2+\ell = 2e-1$ and $2e-\ell = -1$. In the second case, $2+3\ell = 2e-1$ and $2e+\ell = -1$. Since $\Phi_1(x)$ is the unique cyclotomic polynomial dividing

$$
\text{Res}(q_1(x, w), x^2w + 1, w) \cdot \text{Res}(q_1(x, w), x^2w^3 + 1, w),
$$

it follows that $q_{1,2}(\gamma, \gamma^\ell) \neq 0$.

If $q_{1,3}(\gamma, \gamma^\ell) = 0$, taking traces we obtain

$$
\text{Tr}(1) - 2\text{Tr}(\gamma^{2+\ell}) - 2\text{Tr}(\gamma^{2+3\ell}) = 0 \quad (\text{mod } 5). 
$$

(18)

As above $\text{Tr}(\gamma^{2+\ell})\text{Tr}(\gamma^{2+3\ell}) = 0$ (mod 5). Since $\text{Tr}(\gamma^{2+4\ell}) = \text{Tr}(1)/2$ (mod 5), $h \in \{1, 2\}$, is not possible, neither is the equality (18).

Consequently, $\Phi_n(x)$ does not divide $q_{1,i}(x, x^\ell)$ (mod $5\mathbb{Z}[x]$, $i \in \{1, 2, 3, 4\}$, and thus $\Phi_n(x)$ does not divide $q_1(x, x^\ell)$ (mod $5\mathbb{Z}[x]$).

The non divisibility with respect to the other factors $q_i(x^2, x^\ell)$, $i \in \{2, 3, 4\}$, can be proved in a similar way. Indeed, for $2 \leq i \leq 4$, let $P_i(x)$ be the polynomials in $\mathbb{Z}[x]$ obtained as in (14) but from the polynomial $q_i(z, w)$ instead of $q_i(z, w)$. Let us consider

$$
U_i(x) = \text{Res} \left( q_i(x, w), x \frac{\partial}{\partial x} q_i(x, w) + kw \frac{\partial}{\partial w} q_i(x, w), w \right).
$$

Concerning $q_2(x^2, x^\ell)$ and $q_3(x^2, x^\ell)$, the polynomials $P_i(x)$ are non identically zero modulo $p\mathbb{Z}[x]$, except for $p = 2$ with $\ell$ even. Therefore, if $n$ has a factor $p \neq 2$, using
that $\ell$ is never a multiple of $\Phi$ unless $\ell \equiv 4 \pmod{5}$.

Regarding $q_4(x^2, x^\ell)$, the polynomial $P_4(x)$ is non identically zero modulo $p\mathbb{Z}[x]$, except for $p = 2$ and $\ell$ even or $p = 5$. Moreover, $U_4(x) \not\equiv 0 \pmod{2\mathbb{Z}[x]}$. So, we have to consider the case $n = 5^d$, $d \geq 1$. In such a case, we can derive that the corresponding polynomial $Q_4(x)$ obtained as in (16) from $q_4(z, w)$ is not identically zero (mod $5\mathbb{Z}[x]$), unless $\ell \equiv 4 \pmod{5}$. On the other hand, we have that

$$q_4(z, w) = \prod_{i=1}^{10} q_{4,i}(z, w) \pmod{5\mathbb{Z}[z, w]},$$

where

$q_{4,1}(z, w) = w^2z - 1$,
$q_{4,2}(z, w) = (w^2z + 1)^2$,
$q_{4,3}(z, w) = w^2z^2 - w^2z - wz - z + 1$,
$q_{4,4}(z, w) = w^4z^3 - w^4z^2 + w^3z^2 + 2w^2z^2 + 2w^2z - 2wz + z - 1$,
$q_{4,5}(z, w) = w^4z^3 - w^4z^2 + 2w^3z^2 + 2w^2z^2 + 2w^2z - wz + z - 1$,
$q_{4,6}(z, w) = w^4z^3 - w^4z^2 - w^3z^2 + 2w^2z^2 - 2w^2z + wz + z - 1$,
$q_{4,7}(z, w) = w^4z^3 - w^4z^2 + w^3z^2 + 2w^2z^2 - 2w^2z - wz + z - 1$,
$q_{4,8}(z, w) = w^4z^3 - w^4z^2 + w^3z^2 - 2w^2z^2 - 2w^2z - 2wz + z - 1$,
$q_{4,9}(z, w) = w^4z^3 - w^4z^2 + 2w^3z^2 - 2w^2z^2 - 2w^2z - wz + z - 1$,
$q_{4,10}(z, w) = w^4z^4 - 2w^4z^3 + w^4z^2 + w^3z^2 - w^3z^2 + 2w^2z^3 + 2w^2z - wz^2 + wz + z^2 - 2z + 1$.

Now, by using a similar argument as the one given for $q_4(z, w)$ and $n = 5^d$ we obtain that $\ell + 1 = 5^d$, which leads us to a contradiction, since the polynomial

$$q_4(x^2, -1/x) = 5(-1 + x)^5x^2(1 + x)^5(9 + 46x^2 + 9x^4)$$

is never a multiple of $\Phi_{5^d}(x)$.

As we have shown in Theorem 6 the cyclotomic conjecture for $k = 4$, we can apply Theorem 4 to prove the nonexistence of almost Moore digraph of diameter $k = 4$.

References


