Some properties of unitary Cayley graphs

Walter Klotz and Torsten Sander
Institut für Mathematik
Technische Universität Clausthal, Germany
klotz@math.tu-clausthal.de
torsten.sander@math.tu-clausthal.de

Submitted: Feb 21, 2007; Accepted: May 25, 2007; Published: Jun 21, 2007
Mathematics Subject Classification: 05C25, 05C50

Abstract

The unitary Cayley graph X_n has vertex set $Z_n = \{0, 1, \ldots, n-1\}$. Vertices a, b are adjacent, if $\gcd(a-b, n) = 1$. For X_n the chromatic number, the clique number, the independence number, the diameter and the vertex connectivity are determined. We decide on the perfectness of X_n and show that all nonzero eigenvalues of X_n are integers dividing the value $\varphi(n)$ of the Euler function.

1 Introduction

Let Γ be a multiplicative group with identity 1. For $S \subseteq \Gamma$, $1 \notin S$ and $S^{-1} = \{s^{-1} : s \in S\} = S$ the *Cayley Graph* $X = \mathrm{Cay}(\Gamma, S)$ is the undirected graph having vertex set $V(X) = \Gamma$ and edge set $E(X) = \{\{a, b\} : ab^{-1} \in S\}$. By right multiplication Γ may be considered as a group of automorphisms of X acting transitively on $V(X)$. The Cayley graph X is regular of degree $|S|$. Its connected components are the right cosets of the subgroup generated by S. So X is connected, if S generates Γ. More information about Cayley graphs can be found in the books on algebraic graph theory by Biggs [3] and by Godsil and Royle [10].

For a positive integer $n > 1$ the *unitary Cayley graph* $X_n = \mathrm{Cay}(Z_n, U_n)$ is defined by the additive group of the ring Z_n of integers modulo n and the multiplicative group U_n of its units. If we represent the elements of Z_n by the integers $0, 1, \ldots, n-1$, then it is well known [13] that

$$U_n = \{a \in Z_n : \gcd(a, n) = 1\}.$$

So X_n has vertex set $V(X_n) = Z_n = \{0, 1, \ldots, n-1\}$ and edge set

$$E(X_n) = \{\{a, b\} : a, b \in Z_n, \gcd(a-b, n) = 1\}.$$

The graph X_n is regular of degree $|U_n| = \varphi(n)$, where $\varphi(n)$ denotes the Euler function. If $n = p$ is a prime number, then $X_n = K_p$ is the complete graph on p vertices. If $n = p^\alpha$ is a prime power then X_n is a complete p-partite graph which has the residue classes modulo p in Z_n as maximal sets of independent (pairwise nonadjacent) vertices. Unitary Cayley graphs are highly symmetric. They have some remarkable properties connecting graph theory and number theory.

In some recent papers induced cycles in X_n were investigated. Berrizbeitia and Giudici [2] studied the number $p_k(n)$ of induced k-cycles in X_n. Fuchs and Sinz [8, 9] showed that the maximal length of an induced cycle in X_n is 2^r+2, where r is the number of different prime divisors of n.

In Section 2 we deal with some basic invariants of X_n. We show that the chromatic number $\chi(X_n)$ and the clique number $\omega(X_n)$ equal the smallest prime divisor p of n. For the complementary graph $\bar{X}_n$ of X_n we have $\chi(\bar{X}_n) = \omega(\bar{X}_n) = n/p$. Unitary Cayley graphs represent very *reliable networks*, which means that the vertex connectivity $\kappa(X_n)$ equals the degree of regularity of X_n, $\kappa(X_n) = \varphi(n)$. We show that the diameter of X_n is at most 3.

A graph G is *perfect*, if for every induced subgraph $G' \subseteq G$ chromatic number and clique number coincide, $\chi(G') = \omega(G')$. In Section 3 we prove that X_n is perfect, if and only if n is even or if n is odd and has at most two different prime divisors.

The eigenvalues of a graph G are the eigenvalues of an arbitrary adjacency matrix of G. In Section 4 we show that all nonzero eigenvalues of X_n are divisors of $\varphi(n)$. The definition of X_n is extended to *gcd-graphs* $X_n(D)$, where vertices a, b are adjacent, if $\gcd(a-b,n) \in D$, D a given set of divisors of n. All eigenvalues of $X_n(D)$ also turn out to be integral.

2 Basic invariants

First we determine the chromatic number and the clique number of X_n and of the complementary graph $\bar{X}_n$. We remark that $\omega(\bar{X}_n)$ and $\chi(\bar{X}_n)$ are also called the *independence number* and the *clique covering number* of X_n. From now on we always assume that n is an integer, $n \geq 2$.

Theorem 1. *If p is the smallest prime divisor of n, then we have*

$$\chi(X_n) = \omega(X_n) = p, \quad \chi(\bar{X}_n) = \omega(\bar{X}_n) = \frac{n}{p} \ .$$

Proof. As the vertices 0,1,..., p-1 induce a clique in X_n, we have

$$\chi(X_n) \geq \omega(X_n) \geq p. \tag{1}$$

On the other hand the residue classes modulo p in $Z_n = \{0, 1, \ldots, n-1\}$ constitute p sets of independent vertices of X_n. These sets can be taken as color classes to show $\chi(X_n) \leq p$, which proves equality in (1). In $\bar{X}_n$ the residue classes induce cliques showing

$$\chi(\bar{X}_n) \geq \omega(\bar{X}_n) \geq \frac{n}{p} \ . \tag{2}$$

Now the integer intervals

$$\{kp,\ kp+1, \ldots,\ (k+1)p-1\}, \quad 0 \le k \le \frac{n}{p} - 1,$$

consist of indpendent vertices of $\bar{X}_n$. These sets can be taken as color classes for $\bar{X}_n$ to establish $\chi(\bar{X}_n) \le n/p$, which proves equality in (2). □

Corollary 2. *[7] The unitary Cayley graph $X_n,\ n \ge 2$, is bipartite if and only if n is even.*

Corollary 3. *There is no selfcomplementary unitary Caley graph X_n for $n \ge 2$.*

Proof. Suppose X_n is selfcomplementary. Then X_n and $\bar{X}_n$ must have the same chromatic number, which by Theorem 1 implies $n = p^2,\ p$ a prime. As $X_n \cup \bar{X}_n = K_n$ is the complete graph on n vertices and as X_n and $\bar{X}_n$ must have the same degree of regularity, we conclude

$$\varphi(n) \ = \ \frac{n-1}{2}. \tag{3}$$

Inserting $n = p^2$ we get $2\varphi(p^2) = 2p(p-1) = p^2 - 1$, which is impossible. □

We remark that Corollary 3 supports a still open conjecture of Lehmer [12], which states that equation (3) is unsolvable.

Let $a \in U_n$, i.e. $1 \le a \le n-1,\ \gcd(a,n) = 1$. If $n \ge 3$, then the sequence

$$(x_k),\ x_k \equiv ka \bmod n,\ 0 \le k \le n-1,$$

defines a hamiltonian cycle C_a of X_n. We notice that a and $n-a$ define the same hamiltonian cycle. There are $\varphi(n)/2$ edge disjoint hamiltonian cycles $C_a,\ a \in U_n$, which completely partition the edge set $E(X_n)$. This implies that X_n has edge connectivity $\varphi(n)$. We show that this is also the value of the vertex connectivity of X_n.

Theorem 4. *The unitary Cayley graph X_n has vertex connectivity $\kappa(n) = \varphi(n)$.*

Proof. For $a \in Z_n$ and $b \in Z_n$ we define the affine transformation

$$\psi_{a,b} :\ Z_n \longrightarrow Z_n \ \text{ by } \ \psi_{a,b}(x) \equiv ax + b \bmod n \ \text{ for } \ x \in Z_n\ .$$

We check that $\psi_{a,b}$ is an automorphism of X_n, if and only if $a \in U_n$. Moreover, $A(X_n) = \{\psi_{a,b} :\ a \in U_n,\ b \in Z_n\}$ is a subgroup of the automorphism group $\mathrm{Aut}(X_n)$. We call $A(X_n)$ the group of affine automorphisms of X_n.

According to Biggs [3] a graph G is called *symmetric*, if for all vertices $x,\ y,\ u,\ v$ of G such that x is adjacent to y and u is adjacent to v, there is an automorphism σ of G for which $\sigma(x) = u$ and $\sigma(y) = v$. If $G = X_n$, then we find exactly one automorphism $\sigma \in A(X_n)$ satisfying these conditions. So X_n is symmetric.

It has been shown by Watkins [15], see also [4], that the vertex connectivity $\kappa(G)$ of a connected graph G, which is regular and edge transitive, equals its degree of regularity. This result especially applies to connected, symmetric graphs, because symmetry includes regularity and edge transitivity [3]. Therefore, we conclude $\kappa(X_n) = \varphi(n)$. □

The following lemma will be used to determine the number of common neighbors of a pair of vertices in X_n.

Lemma 5. *For integers $n,\ s,\ n \geq 2$, denote by $F_n(s)$ the number of solutions of the congruence*

$$x + y \ \equiv \ s \ mod\, n,\ x \in U_n,\ y \in U_n. \tag{4}$$

Then we have

$$F_n(s) \ = \ n \prod_{p|n,\ p\ prime} (1 - \frac{\varepsilon(p)}{p}),\ where\ \varepsilon(p) = \begin{cases} 1, & if\ p \mid s \\ 2, & if\ p \not| \ s \end{cases} .$$

Proof. Let $p_1, p_2, \ldots, p_r$ be the different prime divisors of n,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ \cdots \ p_r^{\alpha_r},\ m = p_1 p_2 \ \cdots \ p_r \ .$$

If x and y satisfy (4), then y is uniquely determined modulo n by x. So we have to find out the number of possible entries for x. We partition the interval of integers $[0, n-1] = \{0, 1, \ldots, n-1\}$ into the disjoint intervals $I_k = [(k-1)m, km-1],\ k = 1, \ldots, n/m$. By the Chinese Remainder Theorem [13] every integer $x \in I_k$ is uniquely determined by its values x_i modulo p_i, $1 \leq i \leq r$, i.e. by the congruences

$$x \equiv x_i \bmod p_i,\ 0 \leq x_i \leq p_i - 1,\ 1 \leq i \leq r.$$

To guarantee $x \in I_k \cap U_n$ all x_i must be nonzero. There remain $p_i - 1$ possible choices for x_i. An additional value for x_i has to be ruled out, if $s \equiv s' \bmod p_i,\ 0 < s' < p_i$. In this case $x_i = s'$ would have the consequence $y \equiv 0 \bmod p_i$ implying $y \notin U_n$. So the number of possible choices for $x \in I_k \cap U_n$ to satisfy (4) is $(p_1 - \varepsilon(p_1)) \ \cdots \ (p_r - \varepsilon(p_r))$. Multiplying this number by the number n/m of intervals I_k proves Lemma 5. $\square$

Theorem 6. *In the notation of Lemma 5 the number of common neighbors of distinct vertices $a,\ b$ in the unitary Cayley graph X_n is given by $F_n(a-b)$.*

Proof. Let $a,\ b,\ z$ be elements of $V(X_n) = Z_n = \{0, 1, \ldots, n-1\}$. Vertex z is a common neighbor of a and b, if and only if $\gcd(a-z, n) = \gcd(z-b, n) = 1$. There exist unique $x, y \in Z_n$ such that

$$a - z \ \equiv \ x \ \bmod n, \quad z - b \ \equiv \ y \bmod n.$$

Now $z \equiv a - x \equiv b + y$ becomes a common neighbor of a and b, if and only if

$$x + y \ \equiv \ a - b \bmod n,\ x \in U_n,\ y \in U_n.$$

By Lemma 5 this means that the number of common neighbors of a and b is $F_n(a-b)$. $\square$

Corollary 7. *Every pair of adjacent vertices of X_n has the same number $\lambda(n)$ of common neighbors,*

$$\lambda(n) \ = \ n \prod_{p|n,\ p\ prime} (1 - \frac{2}{p}) \ .$$

Corollary 8. *[7] The number $T(n)$ of triangles in X_n is*

$$T(n) \;=\; \frac{n^3}{6} \prod_{p|n,\ p\ prime} (1-\frac{1}{p})(1-\frac{2}{p})\ .$$

Proof. By Corollary 7 every edge of X_n is contained in $\lambda(n)$ triangles. If we multiply $\lambda(n)$ by the number $n\varphi(n)/2$ of edges in X_n, then every triangle is counted three times. So we have $T(n) = n\varphi(n)\lambda(n)/6$. The result follows, if we insert $\lambda(n)$ from Corollary 7 and the analogous product expansion for $\varphi(n)$ [13]. $\square$

The *distance* $\mathrm{d}(x, y)$ of vertices x and y of a graph G is the length (number of edges) of a shortest x, y-path. The *diameter* $\mathrm{diam}(G)$ is the maximal distance any two vertices of G may have.

Theorem 9. *For $n \geq 2$ we have*

$$diam(X_n) \;=\; \begin{cases} 1, & \text{if } n \text{ is a prime number,} \\ 2, & \text{if } n = 2^\alpha,\ \alpha > 1, \\ 2, & \text{if } n \text{ is odd, but not a prime number,} \\ 3, & \text{if } n \text{ is even and has an odd prime divisor .} \end{cases}$$

Proof. If n is a prime number, then $X_n = K_n$ is the complete graph, which has diameter 1. In the other cases X_n is not complete, $\mathrm{diam}(X_n) \geq 2$. If $n = 2^\alpha,\ \alpha > 1$, then X_n is the complete bipartite graph with vertex partition $V(X_n) = \{0, 2, \ldots, n-2\} \cup \{1, 3, \ldots, n-1\}$, which has diameter 2.

Suppose n is odd, but not a prime number. By Theorem 6 the number of common neighbors of vertices $a \neq b$ is $F_n(a-b)$. According to Lemma 5 all factors in the expansion of $F_n(a-b)$ are positive, if n has only odd prime divisors. In this case there is a common neighbor to every pair of distinct vertices, which implies $\mathrm{diam}(X_n) = 2$.

Finally, we consider the case where n is even and has an odd prime divisor p. The vertices 0 and p of X_n are not adjacent and by Theorem 6 they have no common neighbor. Therefore, we have $\mathrm{diam}(X_n) \geq \mathrm{d}(0, p) \geq 3$. Suppose now that a and b, $a \neq b$, are arbitrary nonadjacent vertices of X_n, which have no common neighbor. Any two vertices x and y, $x \neq y$, of X_n, which are both even or both odd have a common neighbor by Theorem 6. So we may assume that a is even and b is odd. All $\varphi(n)$ neighbors of a are odd. Let c be one of them. Now c and b are both odd and therefore have a common neighbor d. Passing along $a,\ c,\ d,\ b$ shows $\mathrm{d}(a, b) \leq 3$, $\mathrm{diam}(X_n) = 3$. $\square$

3 Perfectness

A graph G is *perfect* [1], if for every induced subgraph $G' \subseteq G$ the clique number and the chromatic number coincide, $\omega(G') = \chi(G')$. Clearly, induced cycles of odd length at least 5, popularly called *odd holes*, prevent a graph from being perfect. Chudnovsky, Robertson, Seymour, and Thomas [5] in 2002 turned the corresponding famous conjecture of Berge into the following theorem, the Strong Perfect Graph Theorem (SPGT).

SPGT. *A graph G is perfect if and only if G and its complement $\bar{G}$ have no odd holes.*

If n is even or a power of a prime p, then X_n is bipartite or completely p-partite. As these graphs are perfect, we may assume that n is odd and has at least two different prime divisors.

Lemma 10. *If n is odd and has at least three different prime divisors, then X_n contains an induced cycle C_5 of length 5.*

Proof. Let $p_1, \ldots, p_r$ (in ascending order) be the prime divisors of the odd integer n, $r \geq 3$, $m = p_1 p_2 \cdots p_r$. As the cycle C_5 is selfcomplementary, it suffices to show that there is an induced C_5 in the complement $\bar{X}_n$. We define the vertices x_0, x_1, x_2, x_3 by

$$x_0 = 0,\ x_1 = p_r,\ x_2 = p_r + p_1 \cdots p_{r-1},\ x_3 = 2p_r + p_1 \cdots p_{r-1}. \tag{5}$$

According to the Chinese Remainder Theorem we can define $x_4 \in Z_m$ uniquely by the following congruences.

$$\begin{aligned} &x_4 \equiv 0 \bmod p_1,\ x_4 \equiv 2p_r \bmod p_2,\ x_4 \equiv 2p_1 \cdots p_{r-1} \bmod p_r\ , \\ &x_4 \equiv 0 \bmod p_j \text{ for } j = 3, \ldots, r-1 \end{aligned} \tag{6}$$

One checks that the vertices $x_0, \ldots, x_4$ are distinct. They define a cycle C_5 of $\bar{X}_n$, because

$$\begin{aligned} &x_1 - x_0 \equiv x_3 - x_2 \equiv 0 \bmod p_r, \\ &x_2 - x_1 \equiv x_4 - x_0 \equiv 0 \bmod p_1,\ x_4 - x_3 \equiv 0 \bmod p_2 \end{aligned}$$

imply that the edges $\{x_0, x_1\}, \ldots, \{x_4, x_0\}$ belong to $\bar{X}_n$. It remains to show that this C_5 has no chords in $\bar{X}_n$.

We have $x_2 - x_0 = p_r + p_1 \cdots p_{r-1}$, which implies $\gcd(x_2 - x_0, m) = 1$ and $\{x_0, x_2\} \notin E(\bar{X}_n)$. A similar argument applies to the edges $\{x_0, x_3\}$ and $\{x_1, x_3\}$. Consider now the edge $\{x_1, x_4\}$. By (5) and (6) we conclude that

$$\begin{aligned} &x_4 - x_1 \equiv -p_r \bmod p_1,\ \text{which implies } p_1 \not| \,(x_4 - x_1), \\ &x_4 - x_1 \equiv \ \ p_r \bmod p_2,\ \text{which implies } p_2 \not| \,(x_4 - x_1), \\ &x_4 - x_1 \equiv -p_r \bmod p_j,\ j = 3, \ldots, r-1,\ \text{which implies } p_j \not| \,(x_4 - x_1), \\ &x_4 - x_1 \equiv \ 2p_1 \cdots p_{r-1} \bmod p_r,\ \text{which implies } p_r \not| \,(x_4 - x_1). \end{aligned}$$

Now $\gcd(x_4 - x_1, m) = 1$ implies that the edge $\{x_1, x_4\}$ does not belong to $\bar{X}_n$. Similarly, we confirm $\{x_2, x_4\} \notin E(\bar{X}_n)$. □

It has been shown by Fuchs and Sinz [8, 9] that the length of a longest induced cycle in X_n is $2^r + 2$, if $r \geq 2$ is the number of distinct prime divisors of n. We remark that their arguments can also be used to show that the length of a longest induced path in X_n is 2^r.

To complete our decision concerning the perfectness of X_n, it remains to investigate the case where n has exactly two different odd prime divisors. By the just mentioned result we know that a longest induced cycle in X_n has length 6. So the only possible odd hole X_n may have is C_5. But this is excluded by the next lemma.

Lemma 11. *If n is odd and has exactly two different prime divisors, then $\bar{X}_n$ has no odd hole $C_{2k+1},\ k \geq 2$.*

Proof. Assume that $\bar{X}_n$ contains the induced cycle $C_{2k+1},\ k \geq 2$, which runs through the vertices $x_0,\ x_1, \ldots, x_{2k}$ in this order. If $p_1,\ p_2$ are the two odd prime divisors of n, then for every edge $\{x_j, x_{j+1}\}$ (indices modulo $2k+1$) we must have $p_1 \mid (x_{j+1} - x_j)$ or $p_2 \mid (x_{j+1} - x_j)$. For every pair of consecutive edges $\{x_j, x_{j+1}\},\ \{x_{j+1}, x_{j+2}\}$ of C_{2k+1} the prime divisors $p_1,\ p_2$ must alternate. Otherwise we would have e.g. $x_j - x_{j+1} = sp_1,\ x_{j+2} - x_{j+1} = tp_1$, which would imply $x_{j+2} - x_j = (t-s)p_1$. But this would mean that $\{x_j, x_{j+2}\} \in E(\bar{X}_n)$ is a chord of C_{2k+1} contradicting our asumption. On the other hand the alternation of prime divisors along the edges of C_{2k+1} forces the cycle to have even length, which again is a contradiction. $\square$

With the help of SPGT, Lemma 10 and Lemma 11 we have established the following theorem.

Theorem 12. *The unitary Cayley graph $X_n,\ n \geq 2$, is perfect if and only if n is even or if n is odd and has at most two different prime divisors.*

4 Eigenvalues

The eigenvalues of a graph G are the eigenvalues of an arbitrary adjacency matrix of G. We establish the adjacency matrix A_n of X_n with respect to the natural order of the vertices $0, 1, \ldots, n-1$. The entries $a_0, a_1, \ldots, a_{n-1}$ of the first row of A_n generate the entries of the other rows by a cyclic shift.

$$A_n = \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & \ldots & a_{n-2} \\ . & . & \ldots & . \\ . & . & \ldots & . \\ a_1 & a_2 & \ldots & a_0 \end{pmatrix}$$

Matrices of this kind are called *circulant matrices.* A *circulant graph* is a graph, which has a circulant adjacency matrix. Circulant graphs with n vertices are exactly the graphs isomorphic to a Cayley graph with respect to the additive group Z_n of integers modulo n. Unitary Cayley graphs are circulant graphs.

A detailed exposition of circulant matrices is given by Davis [6]. There is an explicit formula for the eigenvalues $\lambda_r,\ 0 \leq r \leq n-1$, of a circulant matrix such as A_n. Define the polynomial $p_n(z)$ by the entries of the first row of A_n and let w denote a complex primitive n-th root of unity.

$$p_n(z) = \sum_{j=0}^{n-1} a_j z^j \ , \quad w = \exp(\frac{2\pi i}{n})$$

The eigenvalues of A_n are given by (cf. Theorem 3.2.2 [6])

$$\lambda_r \;=\; p_n(w^r),\; 0 \le r \le n-1 \;. \tag{7}$$

Here every eigenvalue of A_n is listed according to its multiplicity. The definition of A_n as a special adjacency matrix of X_n implies

$$a_j \;=\; \begin{cases} 1, & \text{if } \gcd(j,n) = 1 \\ 0, & \text{if } \gcd(j,n) > 1. \end{cases}$$

Therefore, equation (7) leads to

$$\lambda_r \;=\; \sum_{\substack{1\le j<n \\ \gcd(j,n)=1}} w^{rj} \;=\; c(r,n)\;,\; 0 \le r \le n-1\;. \tag{8}$$

The arithmetic function $c(r,n)$ is a *Ramanujan sum*, for which some results are available [14]. For integers $r,\ n,\ n > 0$, Ramanujan sums have only integral values. So all eigenvalues of unitary Cayley graphs are integers. More information can be drawn from the following formula (cf. Corollary 2.4 of [14]).

$$\lambda_r \;=\; c(r,n) \;=\; \mu(t_r)\frac{\varphi(n)}{\varphi(t_r)},\ \text{where } t_r = \frac{n}{\gcd(r,n)},\ 0 \le r \le n-1. \tag{9}$$

Here μ denotes the Möbius function.

Theorem 13. *For $n \ge 2$, the following statements hold.*

1. *Every nonzero eigenvalue of X_n is a divisor of $\varphi(n)$.*
2. *Let m be the maximal squarefree divisor of n. Then*

$$\lambda_{min} \;=\; \mu(m)\frac{\varphi(n)}{\varphi(m)} \tag{10}$$

is a nonzero eigenvalue of X_n of minimal absolute value and multiplicity $\varphi(m)$. Every eigenvalue of X_n is a multiple of λ_{min}. If n is odd, then λ_{min} is the only nonzero eigenvalue of X_n with minimal absolute value. If n is even, then $-\lambda_{min}$ is also an eigenvalue of X_n with multiplicity $\varphi(m)$.

Proof. 1. By the multiplicative properties of the Euler function $\varphi(t)$ divides $\varphi(n)$, if t is a divisor of n [13]. Therefore, (9) implies that the nonzero eigenvalues of X_n are divisors of $\varphi(n)$.

2. For $\lambda_r \ne 0$ we must have $\mu(t_r) \ne 0$, which is equivalent to t_r being a divisor of m. Now by (9) the absolute value of $\lambda_r \ne 0$ is minimal if and only if $\varphi(t_r) = \varphi(m)$. This equation always has the trivial solution $t_r = m$, which implies

$$\lambda_r = \lambda_{min} = \mu(m)\frac{\varphi(n)}{\varphi(m)}.$$

For $0 \le r \le n-1$ we have the equivalences

$$\lambda_r = \lambda_{min} \Longleftrightarrow t_r = \frac{n}{\gcd(r,n)} = m \Longleftrightarrow \gcd(r,n) = \frac{n}{m}$$

$$\Longleftrightarrow r \in Q := \{x\frac{n}{m} : \ 0 \le x < m, \ \gcd(x,m) = 1\}.$$

So λ_{min} has multiplicity $|Q| = \varphi(m)$.

If λ_r is an arbitrary nonzero eigenvalue of X_n, then t_r is a divisor of m and so $\varphi(t_r)$ divides $\varphi(m)$, say $\varphi(m) = k\varphi(t_r)$ with a positive integer k. Now λ_r becomes a multiple of λ_{min} by (9) and (10),

$$\lambda_r = \mu(t_r)\frac{\varphi(n)}{\varphi(t_r)} = k\mu(t_r)\frac{\varphi(n)}{\varphi(m)} = \pm k\lambda_{min}.$$

If n is odd and t_r divides m, then $\varphi(t_r) = \varphi(m)$ has only the trivial solution $t_r = m$ and λ_{min} is the only eigenvalue with minimal absolute value. But if n is even, we have $\varphi(m) = \varphi(m/2)$ and we get another solution for $t_r = m/2$,

$$\lambda'_{min} = \mu(\frac{m}{2})\frac{\varphi(n)}{\varphi(\frac{m}{2})} = -\mu(m)\frac{\varphi(n)}{\varphi(m)} = -\lambda_{min}.$$

As above we deduce the multiplicity $\varphi(m/2) = \varphi(m)$ for the eigenvalue λ'_{min}. □

Remember that X_n is bipartite for even n. The appearence of λ_{min} and $-\lambda_{min}$ in this case reflects the well known fact [3] that the nonzero eigenvalues of bipartite graphs occur in pairs $(\lambda, -\lambda)$ with the same multiplicity. We further mention that for the connected graph X_n the degree of regularity, i.e. $\varphi(n)$, is a simple eigenvalue of maximal absolute value.

Corollary 14. *There is an eigenvalue ± 1 of X_n, if and only if n is squarefree. If n is squarefree, then X_n has the eigenvalue $\mu(n)$ with multiplicity $\varphi(n)$. The unitary Cayley graph X_n has both eigenvalues ± 1 with multiplicity $\varphi(n)$, if and only if n is squarefree and even.*

Theorem 15. *Let m be the maximal squarefree divisor of n and let M be the set of positive divisors of m. Then the following statements for the unitary Cayley graph X_n, $n \ge 2$, hold.*

1. *Repeating every term of the sequence*

$$S \ = \ \left(\mu(t)\frac{\varphi(n)}{\varphi(t)}\right)_{t \in M}$$

$\varphi(t)-$times results in a sequence $\tilde{S}$ of length m which consists of all nonzero eigenvalues of X_n such that the number of appearences of an eigenvalue is its multiplicity.

2. The multiplicity of zero as an eigenvalue of X_n is $n-m$.

3. If $\alpha(\lambda)$ is the multiplicity of the eigenvalue λ of X_n, then $\lambda\alpha(\lambda)$ is a multiple of $\varphi(n)$.

Proof. 1. The number of terms in the resulting sequence $\tilde{S}$ is

$$\sum_{t\in M}\varphi(t) \;=\; \sum_{t|m}\varphi(t) \;=\; m.$$

The last equation exhibits the well known summatory function of the Euler function [13].

Equation (9) describes the sequence (λ_r), $0\le r\le n-1$, of all eigenvalues of X_n, in which each eigenvalue is listed according to its multiplicity. As $\mu(t_r)=0$ for $t_r\notin M$, we get the subsequence $\tilde{T}$ of nonzero eigenvalues for $0\le r\le n-1$, $t_r\in M$.

$$\tilde{T} \;=\; \left(\mu(t_r)\frac{\varphi(n)}{\varphi(t_r)}\right)_{0\le r\le n-1,\ t_r\in M}, \quad t_r=\frac{n}{\gcd(r,n)}$$

Let t be an arbitrary element of M. For $0\le r\le n-1$, i.e. $r\in Z_n$, we have $t_r=t$, if and only if $\gcd(r,n)=n/t$. Elementary number theory shows

$$Q_t \;:=\; \{r\in Z_n:\ \gcd(r,n)=\frac{n}{t}\} \;=\; \{x\frac{n}{t}:\ x\in Z_t,\ \gcd(x,t)=1\},$$

which implies that Q_t has $\varphi(t)$ elements. Therefore, the sequence $\tilde{T}$ consists of all terms

$$\mu(t)\frac{\varphi(n)}{\varphi(t)}, \quad t\in M,$$

where each of these terms appears $\varphi(t)$-times. If we take every term only once, then we arrive at the sequence S and see that $\tilde{S}$ and $\tilde{T}$ coincide apart possibly from the order of their elements.

2. By (1.) the length of the sequence $\tilde{S}$ equals the number of nonzero eigenvalues, each of them counted according to its multiplicity. As $\tilde{S}$ has length m, the eigenvalue zero has multiplicity $n-m$.

3. The statement is trivially true for $\lambda=0$. Let λ be a nonzero eigenvalue of X_n. Then there is an integer $t\in M$ such that $\lambda=\mu(t)\varphi(n)/\varphi(t)$. By (1.) λ has at least multiplicity $\varphi(t)$, more precisely

$$\alpha(\lambda) \;=\; k_t\varphi(t), \quad k_t \;=\; |\{\tau\in M:\ \mu(\tau)=\mu(t),\ \varphi(\tau)=\varphi(t)\}|.$$

Now we deduce

$$\lambda\alpha(\lambda) \;=\; \mu(t)\frac{\varphi(n)}{\varphi(t)}\,k_t\varphi(t) \;=\; \mu(t)k_t\varphi(n).$$

□

We extend the class of unitary Cayley graphs. Let D be a set of positive, proper divisors of the integer $n > 1$. Define the *gcd-graph* $X_n(D)$ to have vertex set $Z_n = \{0, 1, \ldots, n-1\}$ and edge set

$$E(X_n(D)) \;=\; \{\{a,b\}: \; a,b \in Z_n, \; \gcd(a-b,n) \in D\}.$$

If $D = \{d_1, \ldots, d_k\}$, then we also write $X_n(D) = X_n(d_1, \ldots, d_k)$, especially $X_n(1) = X_n$.

Theorem 16. *All eigenvalues of gcd-graphs are integers.*

Proof. As $X_n(D)$ is a circulant graph, its eigenvalues are determined by (7),

$$\lambda_r \;=\; \sum_{j=0}^{n-1} a_j w^{rj}, \quad 0 \le r \le n-1, \text{ where}$$

$$a_j \;=\; \begin{cases} 1, & \text{if } \gcd(j,n) \in D \\ 0, & \text{if } \gcd(j,n) \notin D. \end{cases} \quad , \quad w \;=\; \exp(\frac{2\pi i}{n}).$$

Inserting a_j yields

$$\lambda_r \;= \sum_{d \in D} \sum_{\substack{1 \le j < n \\ \gcd(j,n)=d}} w^{rj} \;, \quad 0 \le r \le n-1.$$

Observing

$$\{j : \; 1 \le j < n, \; \gcd(j,n) = d\} = \{td : \; 1 \le t < n/d, \; \gcd(t, n/d) = 1\}$$

leads to

$$\lambda_r \;= \sum_{d \in D} \sum_{\substack{1 \le t < n/d \\ \gcd(t,n/d)=1}} w^{rtd} \;=\; \sum_{d \in D} \sum_{\substack{1 \le t < n/d \\ \gcd(t,n/d)=1}} \exp(\frac{2\pi i}{n/d}\, rt) \;,$$

$$\lambda_r \;=\; \sum_{d \in D} c(r, n/d) \;, \; 0 \le r \le n-1.$$

Similar to (8) we get a representation of the eigenvalues by Ramanujan sums. As these sums are integer valued, we conclude that all eigenvalues of gcd-graphs are integers. $\square$

5 Problems and remarks

1. Investigate the automorphism group $\mathrm{Aut}(X_n)$. For $n > 6$ it seems to be considerably larger than the group $A(X_n)$ of affine automorphisms.
2. Which circulant graphs have only integer eigenvalues? For general considerations about graphs with integral spectra see [11].
3. Investigate the gcd-graphs defined in Section 4. The graph $X_n(d_1, \ldots, d_k)$ is connected, if and only if $\gcd(d_1, \ldots, d_k) = 1$. Examples suggest that chromatic number and clique number of $X_n(D)$ are always divisors of n.

Acknowledgement. We would like to thank our colleague J. W. Sander for some support in number theory.

References

[1] Alfonsin, J. L. R., and Reed, B. A. *Perfect Graphs.* John Wiley & Sons, New York-Chichester-Brisbane, 2001.

[2] Berrizbeitia, P., and Giudici, R. E. On cycles in the sequence of unitary Cayley graphs. *Discrete Math. 282*, 1-3 (2004), 239–243.

[3] Biggs, N. *Algebraic graph theory. Second Edition.* Cambridge Mathematical Library. Cambridge University Press, 1993.

[4] Boesch, F., and Tindell, R. Circulants and their connectivities. *J. Graph Theory 8* (1984), 487–499.

[5] Chudnovsky, Robertson, Seymour, Thomas. The strong perfect graph theorem. *Annals of Math. 164*, (2002), 51–229.

[6] Davis, P. J. *Circulant matrices.* A Wiley-Interscience Publication, Pure and Applied Mathematics. John Wiley & Sons, New York-Chichester-Brisbane, 1979.

[7] Dejter, I. J., and Giudici, R. E. On unitary Cayley graphs. *J. Combin. Math. Combin. Comput. 18* (1995), 121–124.

[8] Fuchs E. D. Longest induced cycles in circulant graphs. *The Electronic J. Comb. 12* (2005), 1–12.

[9] Fuchs E. D., Sinz J. Longest induced cycles in Cayley graphs. *eprint arXiv:math/0410308* (2004), 1–16.

[10] Godsil, C., and Royle, G. *Algebraic graph theory.* Graduate Texts in Mathematics. Vol 207. Springer, 2001.

[11] Harary, F., and Schwenk, A. J. Which graphs have integral spectra? *Lecture Notes in Mathematics 406*, Springer Verlag (1974), 45–50.

[12] Lehmer D. H. On Euler's totient function. *Bull. Amer. Math. Soc. 38* (1932), 745-751.

[13] Rose H. E. *A course in number theory.* Oxford Science Publications. Oxford University Press, 1994.

[14] McCarthy, P. J. *Introduction to arithmetical functions.* Universitext. Springer-Verlag, New York, 1986.

[15] Watkins, M. E. Connectivity of transitive graphs. *J. Comb. Theory 8* (1970), 23–29.