PERIODIC ORBITS ON 2-REGULAR CIRCULANT DIGRAPHS

ISAAC ECHOLS, JON HARRISON, AND TORI HUDGINS

ABSTRACT. Periodic orbits (equivalence classes of closed cycles up to cyclic shifts) play an important role in applications of graph theory. For example, they appear in the definition of the Ihara zeta function and exact trace formulae for the spectra of quantum graphs. Circulant graphs are Cayley graphs of \mathbb{Z}_n . Here we consider directed Cayley graphs with two generators (2-regular Cayley digraphs). We determine the number of primitive periodic orbits of a given length (total number of directed edges) in terms of the number of times edges corresponding to each generator appear in the periodic orbit (the step count). Primitive periodic orbits are those periodic orbits that cannot be written as a repetition of a shorter orbit. We describe the lattice structure of lengths and step counts for which periodic orbits exist and characterize the repetition number of a periodic orbit by its winding number (the sum of the step sequence divided by the number of vertices) and the repetition number of its step sequence. To obtain these results, we also evaluate the number of Lyndon words on an alphabet of two letters with a given length and letter count.

1. Introduction

Periodic orbits play an important role in graph theory, where the Ihara zeta function is defined via an Euler product over primitive backtrack-less tail-less cycles, see e.g. [23, 11, 22]. Graphs are also widely employed in mathematical physics, for example to model nanomaterials, waveguides, photonic crystals and quantum chaos, see e.g. [15, 4, 17]. One advantage of quantum graphs is that they are endowed with an exact trace formula, where a spectral quantity is expressed via a sum over periodic orbits (cycles) on the graph. Such a trace formula was first derived by Roth [21] for the heat kernel and independently by Kottos and Smilansky for the density of states [13, 14], with subsequent extensions [5, 12, 16, 6].

In addition to the exact trace formula, there is an exact expansion of the characteristic polynomial of a graph as a finite sum over pseudo orbits (sets of periodic orbits) on the graph. This was originally described by Kottos and Smilansky [14] and refined with an explicit formulation in terms of irreducible pseudo orbits (pseudo orbits where each bond appears at most once) [2]. Similarly, Akkermans et al. [1] derive the spectral determinant of the graph as a product over periodic orbits. The pseudo orbit expansion can be employed to evaluate the variance of coefficients of the characteristic polynomial [3]. In particular, for a quantum graph with Fast Fourier Transform scattering matrices at the vertices the variance can be evaluated precisely in terms of the sizes of certain sets of pseudo orbits with self-intersections [8, 9]. As a first step to extend such exact combinatorial calculations of spectral statistics, in this article, we construct methods to categorize and count the primitive periodic orbits on 2-regular circulant directed graphs.

Circulant graphs with n vertices are Cayley graphs of the cyclic group \mathbb{Z}_n . The distribution of the diameters of random circulant graphs was investigated by Marklof and Strömbergson [19] and spectral properties of quantum circulant graphs were described in [10].

Date: October 31, 2024.

Here we consider 2-regular directed circulant graphs and count the number of primitive periodic orbits (periodic orbits that are not a repetition of a shorter orbit). On 2-regular circulant graphs the bonds (directed edges) fall into two classes, denoted by a choice of two step sizes 0 < a < b < n. An edge runs from an origin vertex $i \in \mathbb{Z}_n$ to a terminal vertex $j \in \mathbb{Z}_n$ if j = i + a or j = i + b (where addition is modulo n), see figure 1 for examples of directed circulant graphs. The length l of a path on the graph is the number of edges in the path and we use k to denote the number of times the path uses bonds from class b (the b-count). Hence a path is closed if n|(l-k)a+kb. In this case $la+k(b-a)=\omega n$ for an integer ω and we call ω the winding number of the path. We can now state the main results.

Theorem 1. Let $C_n(a,b)$ be a connected 2-regular circulant digraph, and suppose $la + k(b-a) = \omega n$. Let W be the set of prime divisors of $gcd(l,k,\omega)$. The number of primitive periodic orbits of length l with b-count k is,

$$\frac{n}{l} \sum_{m \mid \gcd(l,k,\omega)} \mu(m) \binom{l/m}{k/m} ,$$

where μ is the Möbius function.

Then summing over the allowed b-counts we obtain the total number of primitive periodic orbits of length l, a formula proposed with numerical evidence in [7].

Theorem 2. Let $C_n(a,b)$ be a connected 2-regular circulant digraph, the number of primitive periodic orbits of length l is

$$\frac{n}{l} \sum_{\omega = \lceil la/n \rceil}^{\lfloor lb/n \rfloor} \sum_{m \mid \omega} \mu(m) \binom{l/m}{k_{\omega}/m} ,$$

where $k_{\omega} = (\omega n - la)/(b - a)$, and μ is the Möbius function. We interpret $\binom{x}{y}$ as zero if $x, y \notin \mathbb{N}_0$.

To count primitive periodic orbits we exploit a connection with Lyndon words on an alphabet of two letters. Lyndon words are words that are earlier (in lexicographic order) than all of their rotations. In the process of counting primitive orbits we obtain the following formula for the number of Lyndon words on an alphabet of two letters with a given letter count.

Theorem 3. Let $\mathbb{L}_2(l,k)$ be the set of Lyndon words of length l on the alphabet $\{a,b\}$ where b appears k times. Then,

(1)
$$|\mathbb{L}_2(l,k)| = \frac{1}{l} \sum_{m | \gcd(l,k)} \mu(m) \binom{l/m}{k/m}.$$

The article is organized as follows. In section 2 we introduce the notation for circulant graphs and periodic orbits. In section 3 we describe the lattice structure of the allowed values of periodic orbit lengths and b-counts corresponding to primitive periodic orbits. In section 4 we obtain theorem 3 for the number of Lyndon words of length l and b-count k. In section 5 we use theorem 3 to prove theorem 1 counting the number of primitive periodic orbits on 2-regular circulant digraphs. Finally, in section 6, we discuss the results and illustrate them with some examples.

2. CIRCULANT GRAPHS

A directed graph (digraph) is a set \mathcal{V} of vertices, together with a set \mathcal{B} of ordered pairs of vertices, called bonds (directed edges). For a bond $e = (v_1, v_2)$, the vertex v_1 is called the origin of e, denoted o(e), and the vertex v_2 is called the terminus of e, denoted t(e). In this paper, we assume graphs are simple, that is, \mathcal{V} is a finite set and \mathcal{B} has no repeated bonds or bonds of the form (v, v) (loops). Note that we do allow pairs of bonds which are the reverse of each other, (v, u) and (u, v).

Given integers $0 < a_1 < a_2 < \cdots < a_m < n$, the directed circulant graph on n vertices with step sizes a_1, \ldots, a_m , denoted $C_n(a_1, \ldots, a_m)$, is the directed graph with vertex set $\mathcal{V} = \mathbb{Z}_n$ and bond set $\mathcal{B} = \{(v, v + a_i) | v \in \mathcal{V}, 1 \leq i \leq m\}$, where addition in \mathbb{Z}_n is modulo n. While undirected circulant graphs require $a_m \leq n/2$ to prevent repeated edges, the results in this paper hold for directed circulant graphs with $a_m < n$. Figure 1 shows the circulant digraphs $C_5(1,4)$, $C_8(1,2,3)$ and $C_{12}(2,4)$. For a bond $e = (v, v + a_i)$ where $0 < a_i < n$, the step size of e, denoted |e|, is the number a_i . Note that $C_n(a_1, \ldots, a_m)$ is m-regular, that is, each vertex has m incoming bonds and m outgoing bonds.

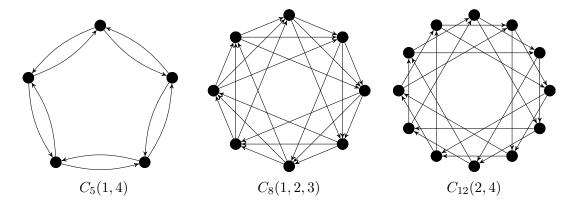


Figure 1. Examples of directed circulant graphs

On a directed graph, a path from a vertex v to a vertex u is a sequence of bonds $c = (e_1, e_2, \ldots, e_l)$ for which $o(e_1) = v$, $t(e_l) = u$, and $t(e_j) = o(e_{j+1})$ for each j. A path is called a circuit if additionally v = u. The number of (possibly repeated) bonds l is called the length of the path. For a circulant graph, the transit distance, denoted $\Delta(c)$, is $|e_1| + \cdots + |e_l|$. Note that $u \equiv v + \Delta(c) \pmod{n}$. As such, c is a circuit if and only if $n|\Delta(c)$, in which case we define the winding number of c to be $\Delta(c)/n$, denoted ω_c , or ω when there is no confusion. The step sequence of a path c is $\operatorname{st}(c) = (|e_1|, \ldots, |e_l|)$.

A directed graph is strongly connected if, for any two vertices v and u, there is a path from v to u. In figure 1, $C_{12}(2,4)$ is disconnected; it has two strongly connected components, namely $\{0, 2, 4, 6, 8, 10\}$ and $\{1, 3, 5, 7, 9, 11\}$. In this paper, we consider circulant graphs that are strongly connected, or equivalently $\gcd(n, a_1, \ldots, a_m) = 1$, see [20].

Given a circuit $c = (b_1, b_2, \ldots, b_l)$, the *periodic orbit* containing c, denoted p = [c], is the equivalence class of c, up to rotation. That is, $p = \{\sigma^x(c) : x = 0, \ldots, l-1\}$, where $\sigma(b_1, b_2, \ldots, b_l) = (b_2, b_3, \ldots, b_l, b_1)$. Note that length, transit distance, and winding number of circuits in p is invariant, so they are well-defined for p. A periodic orbit p is called *primitive* if it is not a repetition of a shorter periodic orbit, that is, if there is no circuit c_0 and c > 1 such that $c = [c_0^r]$. For nonprimitive $c = [c_0^r]$, there is a unique primitive periodic orbit $c = [c_0^r]$.

the root of p, such that $p = q^r$, in which case r is called the repetition number of p. We write $\mathcal{P}_l(G)$ for the set of primitive periodic orbits of length l in a directed graph G.

In this article, we consider 2-regular circulant graphs $C_n(a, b)$. We write $\mathcal{P}_{l,k}(C_n(a, b))$ for the set of primitive periodic orbits of length l for which the number of bonds of step size b is k, we refer to k as the b-count of an orbit or circuit. Note that these sets are disjoint for different values of k, so

(2)
$$|\mathcal{P}_{l}(C_{n}(a,b))| = \sum_{k=0}^{l} |\mathcal{P}_{l,k}(C_{n}(a,b))|.$$

This sum can be simplified by classifying the values of k for which $\mathcal{P}_{l,k}(C_n(a,b)) \neq \emptyset$ which is the goal of the next section.

3. The lattice of periodic orbits

In this section we classify periodic orbits in $C_n(a, b)$ by length l and b-count k, and describe the lattice structure of all corresponding (l, k) in \mathbb{Z}^2 . If $\mathcal{P}_{l,k}(C_n(a, b))$ is nonempty then

(3)
$$\Delta(p) = \omega_p n = (l - k)a + kb = la + kd ,$$

where d = b - a. Let $\bar{S}_n(a, b) = \{(l, k) \in \mathbb{Z}^2 : la + kd = \omega n \text{ for some } \omega \in \mathbb{Z}\}$. This includes negative l and k, so let $S_n(a, b)$ be the subset of $\bar{S}_n(a, b)$ that correspond to actual orbits, i.e., for which $0 \le k \le l$ and l > 0.

Rather than search for orbits directly in terms of length and b-count, it is more efficient to search by the winding number, which is a multiple of $g = \gcd(a, d) = \gcd(a, b)$.

Proposition 1. Let $g = \gcd(a, d)$ and suppose $\gcd(a, d, n) = 1$. Then the equation $la + kd = \omega n$ has an integer solution l, k if and only if $g|\omega$.

Proof. By the Chinese remainder theorem, an integer solution l, k exists if and only if $g|\omega n$. But gcd(g, n) = gcd(a, d, n) = 1. Then $g|\omega n$ if and only if $g|\omega$ as g and ω are coprime. \square

Now that we know the set of possible winding numbers, we will find points in $\bar{S}_n(a,b)$ with a fixed winding number.

Proposition 2. Suppose la + kd = t has an integer solution $l = l_0, k = k_0$. Then $l = l_1, k = k_1$ is another integer solution if and only if there exists $x \in \mathbb{Z}$ such that $l_1 = l_0 + xd'$ and $k_1 = k_0 - xa'$, where a' = a/g, d' = d/g.

Proof. Suppose $l_0a + k_0d = l_1a + k_1d$. Dividing by g, we have $l_0a' + k_0d' = l_1a' + k_1d'$. Then $x = (l_1 - l_0)/d' = (k_0 - k_1)/a'$. To show $x \in \mathbb{Z}$, note that $(l_1 - l_0)a'/d' = k_0 - k_1 \in \mathbb{Z}$. Thus $d'|(l_1 - l_0)a'$. Since $\gcd(a', d') = 1$, we have $d'|(l_1 - l_0)$.

Conversely, suppose $l_1 = l_0 + xd'$, and $k_1 = k_0 - xa'$, with $x \in \mathbb{Z}$. Then $l_1, k_1 \in \mathbb{Z}$. Note that d'a = a'd. Thus $l_1a + k_1d = l_0a + x(d'a - a'd) + k_0d = t$.

Combining the two previous results we see the set of solutions of $la + kd = \omega n$ form a lattice. Figure 2 shows the lattice $\bar{S}_7(1,3)$.

Corollary 1. The set $\bar{S}_n(a,b)$ is a lattice in \mathbb{Z}^2 containing (0,0). In particular, there are integers l_0, k_0 such that $l_0a + k_0d = gn$, and $\bar{S}_n(a,b) = \{x(d',-a') + y(l_0,k_0) : x,y \in \mathbb{Z}\}$. The matrix

$$(4) M = \begin{bmatrix} d' & l_0 \\ -a' & k_0 \end{bmatrix}^{-1} = \frac{1}{n} \begin{bmatrix} k_0 & -l_0 \\ a' & d' \end{bmatrix}$$

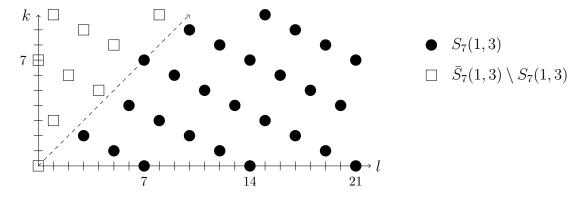


FIGURE 2. The lattice $S_7(1,3)$.

is a bijection from $\bar{S}_n(a,b)$ to \mathbb{Z}^2 .

Note that the choice of l_0, k_0 is not unique, in fact it need not satisfy the constraints for actual orbits. Applying M to $(l, k) \in \bar{S}_n(a, b)$, the y-coordinate represents an increment in the winding number. Precisely, $y = (la' + kd')/n = \omega/g$, is the number of repetitions of a step sequence of length l_0 with b-count k_0 (followed by possible rearrangement), while the x-coordinate, $x = (lk_0 - l_0k)/n$, represents how many times the length and b-count have been shifted away from yl_0 and yk_0 respectively, while preserving the winding number.

While a periodic orbit corresponds to one point (l, k), there are $\binom{l}{k}$ orderings of the corresponding step sequence and the majority of these orderings correspond to distinct primitive periodic orbits with respect to a given starting vertex. To take this into account when counting periodic orbits we will employ a connection to Lyndon words.

4. Lyndon words of fixed letter count

We can view the step sequences of circuits on $C_n(a, b)$ as words on the alphabet $A = \{a, b\}$, with lexicographic order $a \prec b$. In this section we evaluate the number of Lyndon words with a fixed b-count, which will be applied in the formula for $|\mathcal{P}_{l,k}(C_n(a, b))|$ in the next section.

As with cycles, for a word $w = w_1 w_2 \dots w_n$ we use [w] for the equivalence class of w under rotation, that is, $[w] = \{\sigma^s(w) : s = 0, \dots, l-1\}$, where l is the length of w and $\sigma(w_1 w_2 \dots w_l) = w_2 w_3 \dots w_l w_1$. Note that w is primitive if and only if |[w]| = l. A word w is a $Lyndon\ word$ if it precedes all of its rotations in lexicographic order, i.e., $w \prec \sigma^s(w)$ for $s = 1, \dots, l-1$ [18]. Note that all Lyndon words are primitive. Given a word w, if [w] contains a Lyndon word, we call that word the $Lyndon\ rotation$ of w, denoted Lyn(w).

We will write $\mathbb{W}_2(l, k)$ for the set of words on $\{a, b\}$ of length l with b-count k, and write $\mathbb{P}_2(l, k)$ and $\mathbb{P}_2^c(l, k)$, and $\mathbb{L}_2(l, k)$ for the subsets of primitive, nonprimitive, and Lyndon words, contained in $\mathbb{W}_2(l, k)$ respectively.

Lemma 1. The order of the set of Lyndon words with fixed b-count is,

(5)
$$|\mathbb{L}_2(l,k)| = \frac{1}{l} \left[\binom{l}{k} - |\mathbb{P}_2^c(l,k)| \right].$$

Proof. There is a natural bijection between $\mathbb{L}_2(l,k)$ and the set of equivalence classes [w] contained in $\mathbb{P}_2(l,k)$, namely $w \mapsto [w]$ with inverse $[x] \mapsto \text{Lyn}(x)$. Since w is primitive note

|[w]| = l, and since $|\mathbb{W}_2(l,k)| = {l \choose k}$, we have

(6)
$$|\mathbb{L}_2(l,k)| = \frac{1}{l} |\mathbb{P}_2(l,k)| = \frac{1}{l} \left[\binom{l}{k} - |\mathbb{P}_2^c(l,k)| \right] .$$

We can count nonprimitive words by breaking $\mathbb{P}_2^c(l,k)$ into subsets depending on the repetition number. Denote $\mathbb{P}_2^c(l,k,p) = \{w \in \mathbb{P}_2^c(l,k) : w = x^p\}$. Note that x need not be primitive, i.e., p need not be the repetition number of w. For p > 1, we have $\mathbb{P}_2^c(l,k,p) = \{x^p : x \in \mathbb{W}_2(l/p,k/p)\}$ and thus,

(7)
$$|\mathbb{P}_2^c(l,k,p)| = \binom{l/p}{k/p} .$$

Clearly $\mathbb{P}_2^c(l, k, p)$ is the empty set unless l and k are divisible by p, which implies,

(8)
$$\mathbb{P}_2^c(l,k) = \mathbb{P}_2^c(l,k,1) = \bigcup_{p>1, \, p|\gcd(l,k)} \mathbb{P}_2^c(l,k,p) .$$

Notice that this union is not disjoint. For example, $(abb)^{10} \in \mathbb{P}_2^c(30, 20, 10)$, which can also be written as $(abbabb)^5 \in \mathbb{P}_2^c(30, 20, 5)$ or $(abbabbabbabbabbabbabb)^2 \in \mathbb{P}_2^c(30, 20, 2)$.

Proposition 3. Suppose p_1 and p_2 are distinct divisors of l and k greater than 1. Then $p_2|p_1$ if and only if $\mathbb{P}_2^c(l,k,p_1) \subseteq \mathbb{P}_2^c(l,k,p_2)$.

Proof. First, we assume 0 < k < l, as k = 0 or k = l correspond to the trivial cases $\mathbb{W}_2(l,k) = \{a^l\}$ or $\{b^l\}$. We will denote $l_1 = l/p_1$ and similarly $l_2 = l/p_2$, with $k_1 = k/p_1$, and $k_2 = k/p_2$. The conditions $p_2|p_1$, $l_1|l_2$, and $k_1|k_2$ are all equivalent. Now suppose $p_2|p_1$, so $p_1 = zp_2$ for some $z \in \mathbb{Z}$. For all $w \in \mathbb{P}_2^c(l,k,p_1)$, there exists a word x such that $w = x^{p_1} = (x^z)^{p_2} \in \mathbb{P}_2^c(l,k,p_2)$.

Conversely, suppose that $p_2 \nmid p_1$. Let $x = a^{l_1 - k_1}b^{k_1}$ and $w = x^{p_1}$. Suppose that $w \in \mathbb{P}^c_2(l,k,p_2)$. Then $w = x^{p_1} = y^{p_2}$, where the length and b-count of y are l_2 and k_2 , respectively. If $l_2 > l_1$, then y begins with x^z for some $z \geq 1$. Since $l_1 \nmid l_2$, the word y terminates partway through a repetition of x. Since the last letter of w is b, the last letter of y must also be b, that is, $y = x^z a^{l_1 - k_1} b^s$ where $0 < s < k_1$. Since the first letter of x (and thus of y) is a, we know $w = y^{p_2}$ contains the string $ab^s a$, which is a contradiction since w is a repetition of $a^{l_1 - k_1} b^{k_1}$. If $l_2 < l_1$, then y is a substring of x. Since y must contain a b, we have $y = a^{l_1 - k_1} b^s$ for $0 < s < k_1$, which again implies the contradiction that w contains the string $ab^s a$. \square

Corollary 2. Let p_1, \ldots, p_d be the prime divisors of gcd(l, k). Then

(9)
$$\mathbb{P}_{2}^{c}(l,k) = \bigcup_{j=1}^{d} \mathbb{P}_{2}^{c}(l,k,p_{j}) .$$

To count $\mathbb{P}_2^c(l,k)$ it remains to quantify the intersection of $\mathbb{P}_2^c(l,k,p)$ for p a prime divisor of $\gcd(l,k)$. In the previous example $(abb)^{10} \in \mathbb{P}_2^c(30,20,5) \cap \mathbb{P}_2^c(30,20,2)$ which we will see is precisely $\mathbb{P}_2^c(30,20,10)$.

Proposition 4. Suppose p_1 and p_2 are coprime and divisors of l and k. Then

(10)
$$\mathbb{P}_2^c(l, k, p_1) \cap \mathbb{P}_2^c(l, k, p_2) = \mathbb{P}_2^c(l, k, p_1 p_2) .$$

Proof. By proposition 3 we have $\mathbb{P}_2^c(l, k, p_1 p_2) \subseteq \mathbb{P}_2^c(l, k, p_1) \cap \mathbb{P}_2^c(l, k, p_2)$. Suppose $w = w_1 \dots w_l \in \mathbb{P}_2^c(l, k, p_1) \cap \mathbb{P}_2^c(l, k, p_2)$. Let $l_1 = l/p_1$, with $l_2 = l/p_2$, and $l_3 = l/(p_1 p_2)$. Note that $w = \sigma^{l_1}(w) = \sigma^{l_2}(w)$, that is, for each $j \in \{1, \dots, l\}$ and each $z \in \mathbb{Z}$, $w_j = w_{j+zl_1} = w_{j+zl_2}$. Since $\gcd(p_1, p_2) = 1$, there exist $u, v \in \mathbb{Z}$ such that $up_1 + vp_2 = 1$. Multiplying by l_3 on both sides, $l_3 = ul_2 + vl_1$. Thus, for each j, we have $w_{j+l_3} = w_{j+ul_2+vl_1} = w_j$. In other words, $w = \sigma^{l_3}(w)$, so $w \in \mathbb{P}_2^c(l, k, p_1 p_2)$.

Using the previous results,

(11)
$$|\mathbb{P}_2^c(l,k)| = \left| \bigcup_{j=1}^d \mathbb{P}_2^c(l,k,p_j) \right|$$

(12)
$$= \sum_{m | \gcd(l,k), m > 1} -\mu(m) | \mathbb{P}_2^c(l,k,m) |$$

(13)
$$= \sum_{m \mid \gcd(l,k), m > 1} -\mu(m) \binom{l/m}{k/m} ,$$

where μ is the Möbius function,

(14)
$$\mu(m) = \begin{cases} 1 & \text{if } m = 1\\ (-1)^h & \text{if } m \text{ is the product of } h \text{ distinct primes } .\\ 0 & \text{if } m \text{ is divisible by a square } > 1 \end{cases}$$

Theorem 3 follows immediately.

To illustrate this result, consider l = 9 and k = 3, with $|\mathbb{W}_2(9,3)| = 84$. In this case m = 1, 3 and $\mathbb{P}_2^c(9,3,3) = \{(113)^3, (131)^3, (311)^3\}$. The other 81 words are primitive, and up to rotation there are 9 distinct groups of 9 words, with one word in each group being Lyndon. In particular,

(15)
$$|\mathbb{L}_2(9,3)| = \frac{1}{9} \left[\binom{9}{3} - \binom{3}{1} \right] = 9.$$

Figure 4 shows the primitive periodic orbits corresponding on $C_9(1,4)$ corresponding to these 9 words. In the next section we define a natural bijection between $\mathbb{L}_2(l,k)$ and the set of primitive periodic orbits on $C_n(a,b)$ starting at a given vertex.

5. Counting Periodic orbits

Let v be a vertex in $C_n(a,b)$. For $w \in \mathbb{W}_2(l,k)$, let $\psi(w,v)$ denote the unique path c starting at v such that $\operatorname{st}(c) = w$. Note that $\psi(w,v)$ is a circuit if and only if $(l,k) \in S_n(a,b)$, in which case we denote $\varphi(w,v) = [\psi(w,v)]$, see figure 4. Clearly φ is a surjective function, from $\mathbb{W}_2(l,k) \times \mathbb{Z}_n$ to the set of all periodic orbits of length l and b-count k, as each periodic orbit contains a circuit with some initial vertex and step sequence. If $c = \psi(w,v)$ is nonprimitive, then the step sequence w is also nonprimitive. The converse, however, is not true, since there are n distinct bonds corresponding to each step size. For example, in $C_9(1,4)$, the step sequence $w = (114)^3$ is primitive, but $\psi(w,v)$ is a nonprimitive circuit for any v (see figure 3). Moreover, $\varphi : \mathbb{P}_2(l,k) \times \mathbb{Z}_n \to \mathcal{P}_{l,k}(C_n(a,b))$ is not injective, since for any orbit p = [c], we also have $p = \varphi(\sigma^j(\operatorname{st}(c)), v_j)$ where v_j is the jth vertex in c. Replacing primitive words with Lyndon words corrects this by keeping only one rotation of a primitive step sequence.

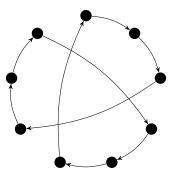


FIGURE 3. The periodic orbit $\varphi(114114114,0)$ on $C_9(1,4)$, which is a primitive periodic orbit with a nonprimitive step-sequence.

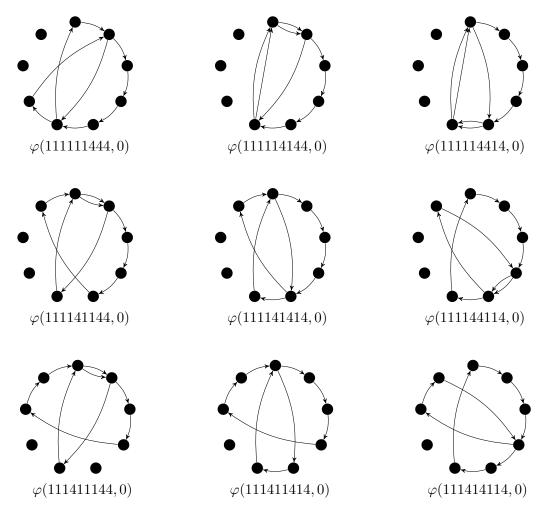


FIGURE 4. The periodic orbits $\varphi(w,0)$ for each $w \in \mathbb{L}_2(9,3)$, where $G = C_9(1,4)$. Repeated bonds are shown twice. The bonds are the same in $\varphi(1111111444,0)$ and $\varphi(111141414,8)$, but these orbits are distinct due to the orders of step sequences.

Lemma 2. The map $\varphi : \mathbb{L}_2(l,k) \times \mathbb{Z}_n \to \mathcal{P}_{l,k}(C_n(a,b))$ is injective.

Proof. Let $w, y \in \mathbb{L}_2(l, k)$ and $v, u \in \mathbb{Z}_n$. Write $c = \psi(w, v)$ and $d = \psi(y, u)$, so $[c] = \varphi(w, v)$, and $[d] = \varphi(y, u)$. If [c] = [d], there exists $s \in \{0, \ldots, l-1\}$ such that $c = \sigma^s(d)$. Then $y = \sigma^s(w)$, and as y and w are Lyndon words, y = w, consequently s = 0, and u = v. \square

Since $\varphi : \mathbb{L}_2(l,k) \times \mathbb{Z}_n \to \mathcal{P}_{l,k}(C_n(a,b))$ is not surjective, we add back nonprimitive words which map to primitive circuits. For example, each orbit in figure 4 has 9 distinct rotations, one for each starting vertex, while the orbit in figure 3 only has 3 distinct rotations, since 3 is the repetition number of its step sequence. We classify nonprimitive words by their primitive roots, with a condition on the winding number which identifies those words which map to nonprimitive orbits.

Proposition 5. Suppose $(l, k) \in S_n(a, b)$, that is, $la + kd = \omega n$ for some ω , and $w = x^r \in W_2(l, k)$ where r is the repetition number of w. Then, for a given vertex v, the periodic orbit $p = \varphi(w, x)$ is primitive if and only if $gcd(r, \omega) = 1$. In general, if $p = q^t$ for some periodic orbit q, then q is primitive if and only if $t = gcd(r, \omega)$.

Proof. Suppose $\gcd(r,\omega) = h > 1$. Let s = r/h, and $c = \psi(x^s,v)$. Note that c is a path of length l/h and b-count k/h, so the transit distance $\Delta(c) = \Delta(p)/h = \omega n/h$. Since $h|\omega$, the path c is a circuit. Then $p = [c^h]$ is not primitive.

Conversely, suppose p is not primitive. Then there is a primitive circuit c such that $p = [c^s]$ and s > 1. In particular, $(l/s, k/s) \in S_n(a, b)$ with winding number ω/s , so $s|\omega$. Now it suffices to show s|r. Write $y = \operatorname{st}(c)$ and l_x, l_y for the length of x and y, respectively. Since $l = l_y s = l_x r$, it suffices to show that $l_x|l_y$. As x is the root of w, so we have $l_x \leq l_y$. For the sake of contradiction, suppose $l_x \nmid l_y$. Then $l_y = \mu l_x + \rho$ for some $\mu > 0$, $0 < \rho < l_x$. As in the proof of proposition 3, y is a repetition of x followed by a truncation of x, so $y = x^{\mu}x_1 \dots x_{\rho}$. Thus, as $y^s = x^r$, we have,

(16)
$$x^{\mu}x_{1} \dots x_{\rho}x_{1}x_{2}x_{3} \dots = x^{\mu}x_{1} \dots x_{\rho}x_{\rho+1}x_{\rho+2}x_{\rho+3} \dots$$

Hence, $x = \sigma^{\rho}(x)$ for $0 < \rho < l_x$, which is a contradiction since x is primitive.

Now suppose $p = q^t$ where q is a periodic orbit. Since x is primitive, we have $q = \varphi(x^{r/t}, v)$ where r/t is the repetition number of $\operatorname{st}(q)$. Note that ω/t is the winding number of q, so $(l/t)a + (k/t)d = (\omega/t)n$. In particular, t is a common divisor of r and l. By the first part of the proposition, q is primitive if and only if $\gcd(r/t, \omega/t) = 1$, or equivalently, $\gcd(r, \omega) = t$.

To generate orbits that do not correspond with Lyndon words, we can use the nonprimitive words $w = x^r$ where x is a Lyndon word and r is coprime with ω . Denote by $\mathbb{L}_2^q(l,k)$ the set $\{x^q : x \in \mathbb{L}_2(l/q,k/q)\}$. Note that the notation is intentionally different to $\mathbb{P}_2^c(l,k,p)$, since q, unlike p, must be the repetition number. In particular, note that $\mathbb{L}_2^{q_1}(l,k)$ and $\mathbb{L}_2^{q_2}(l,k)$ are disjoint if $q_1 \neq q_2$.

Now we show that it is sufficient to count over all common divisors of l and k coprime with ω .

Lemma 3. Suppose $la+kd=\omega n$ for some $\omega\in\mathbb{Z}^+$. For each $p\in\mathcal{P}_{l,k}(C_n(a,b))$, $p=\varphi(w,v)$ for some $w\in\mathbb{L}_2^q(l,k)$ where $q|\gcd(l,k)$ and $\gcd(q,\omega)=1$.

Proof. Let $p = [c] \in \mathcal{P}_{l,k}(C_n(a,b))$. Write $\operatorname{st}(c) = w_0 = x_0^q$ where x_0 is primitive. Then $q | \operatorname{gcd}(l,k)$. Since p is primitive, $\operatorname{gcd}(q,\omega) = 1$ by proposition 5. Then for $w = \operatorname{Lyn}(x_0)^q \in \mathbb{L}_2^q(l,k)$, we have $p = \varphi(w,v)$ for some vertex v in c.

Corollary 3. Suppose $la+kd=\omega n$. Let Q be the set of divisors of gcd(l,k) that are coprime with ω . Then

(17)
$$\varphi: \bigcup_{q \in Q} \mathbb{L}_2^q(l,k) \times \mathbb{Z}_n \to \mathcal{P}_{l,k}(C_n(a,b))$$

is surjective.

Conversely, each word in $\mathbb{L}^q(l,k)$ maps to n/q distinct orbits, so restricting the starting vertices can make φ injective.

Proposition 6. Suppose $la + kd = \omega n$. Let Q be the set of divisors of gcd(l, k) that are coprime with ω . Then

(18)
$$\varphi: \bigcup_{q \in Q} \mathbb{L}_2^q(l,k) \times \mathbb{Z}_{n/q} \to \mathcal{P}_{l,k}(C_n(a,b))$$

is bijective.

Proof. Let $w \in \mathbb{L}_2^q(l,k)$ where $q \in Q$. It suffices to show that $\varphi(w,0) = \varphi(w,v)$ if and only if $v \equiv jn/q \pmod{n}$ for some $j = 0, \ldots, q-1$, as then for every orbit p with step sequence w, there is a unique vertex $u \in \mathbb{Z}_{n/q}$ such that $p = \varphi(w,u)$.

Suppose $v \equiv jn/q \pmod{n}$ for some j = 0, ..., q - 1. Since $gcd(\omega, q) = 1$, there exist integers m, z such that $zq - m\omega = j$. Note that the step sequence is a repetition $w = x^q$ where $\Delta(x) = \omega n/q$, so we have $v + m\Delta x = zn$ and $\varphi(w, v) = \varphi(w, v + m\Delta(x)) = \varphi(w, 0)$.

Conversely, suppose $\varphi(w,0) = \varphi(w,v)$. Then $\psi(w,0) = \sigma^s(\psi(w,v))$ for some $s=0,\ldots,l-1$, that is, the *p*-th vertex of $\sigma^s(\psi(w,v))$ is the (s+p)-th vertex of $\psi(w,0)$. Since $w=x^q$ where x is Lyndon, we know that s=ml/q for some $m\in\{0,\ldots,q-1\}$. Thus,

(19)
$$w_1 + w_2 + \dots + w_{m(l/q)+p} = v + w_1 + w_2 + \dots + w_p$$

(20)
$$m(x_1 + \dots + x_{l/q}) + w_1 + w_2 + \dots + w_p = v + w_1 + w_2 + \dots + w_p$$

$$(21) m\Delta(x) = v$$

$$m\frac{\omega n}{q} = v ,$$

and since $gcd(\omega, q) = 1$, we have $v \equiv jn/q \pmod{n}$ for some $j = 0, \dots, q - 1$.

Theorem 4. Let $C_n(a,b)$ be a connected 2-regular circulant digraph and suppose $la + k(b-a) = \omega n$. Let Q be the set of divisors of gcd(l,k) that are coprime with ω . Then,

(23)
$$|\mathcal{P}_{l,k}(C_n(a,b))| = \frac{n}{l} \sum_{q \in Q} \sum_{m | \gcd(l,k)/q} \mu(m) \binom{l/(qm)}{k/(qm)} ,$$

where μ is the Möbius function.

Proof. Note that the union in proposition 6 is disjoint. Thus

$$(24) |\mathcal{P}_{l,k}(C_n(a,b))| = \sum_{q \in Q} |\mathbb{Z}_{n/q}| \cdot |\mathbb{L}_2^q(l,k)|$$

$$= \sum_{q \in Q} \frac{n}{q} \left| \mathbb{L}_2 \left(\frac{l}{q}, \frac{k}{q} \right) \right|$$

(26)
$$= n \sum_{q \in Q} \frac{1}{q} \left(\frac{1}{l/q} \sum_{m | \gcd(l,k)/q} \mu(m) \binom{l/(qm)}{k/(qm)} \right) .$$

Theorem 5. Let $\gamma, \omega \in \mathbb{N}$ and Q be the set of divisors of γ that are coprime with ω , and P_q the set of prime divisors of γ/q . For W the set of prime divisors of ω and γ , and any function $f: \mathbb{N} \to \mathbb{R}$,

(27)
$$\sum_{q \in Q} \sum_{S \subseteq P_q} (-1)^{|S|} f(q\Pi_S) = \sum_{R \subseteq W} (-1)^{|R|} f(\Pi_R) ,$$

where Π_X dentotes the product of elements in X. Equivalenty,

(28)
$$\sum_{q \in Q} \sum_{s|\gamma/q} \mu(s) f(qs) = \sum_{m|\gcd(\gamma,\omega)} \mu(m) f(m) .$$

Proof. Suppose $x = q\Pi_S$ for some $q \in Q$ and $S \subseteq P_q$. Let y be the greatest divisor of x that is coprime with ω . Denote by F_j the set of prime divisors of j, and write $F_z = F_x \setminus F_y$. Note that common divisors of ω and x are square-free, so F_z is precisely the set of divisors of x and x. Now, if $x = q'\Pi_{S'}$ for some $y' \in Q$ and $y' \subseteq P_{q'}$, then y' has no common divisors with $x \in Q$ so $x \in Q$. Since $x \in Q$ contains only prime divisors of $x \in Q$ for some $x \in Q$ and $x \in Q$ for some $x \in Q$ and $x \in Q$ for some $x \in Q$ and $x \in Q$ for some $x \in Q$ and $x \in Q$ for some $x \in Q$ for $x \in Q$ for some $x \in Q$ for some $x \in Q$ for some $x \in Q$ for $x \in Q$ for some $x \in Q$ for some $x \in Q$ for $x \in Q$ for $x \in Q$ for some $x \in Q$ for $x \in Q$ for x

Conversely, suppose $T' \subseteq F_y$ and $S' = F_z \cup T'$. Letting $q' = x/\Pi_{S'}$, we have $q' \in Q$, since $x|\gamma$ and S' contains all prime divisors of x and ω . Since $\Pi_{S'} = x/q'$, S' is the set of prime divisors of x/q', which is a subset of the prime divisors of γ/q' , which is $P_{q'}$.

We have shown that for any x,

(29)
$$\{(q,S): q \in Q, S \subseteq P_q, x = q\Pi_S\} = \{(q,S): S = F_z \cup T', T' \subset F_y, q = x/\Pi_S\}$$
.

Since q is determined by x and S on the right-hand side of equation (29), the contribution of each term where $q\Pi_S = x$ in the left-hand side of (27) can be written as,

(30)
$$\sum_{T' \subseteq F_y} (-1)^{|F_z| + |T'|} f(x) = (-1)^{|F_z|} f(x) \sum_{T' \subseteq F_y} (-1)^{|T'|}$$

(31)
$$= (-1)^{|F_z|} f(x) \sum_{j=0}^{|F_y|} (-1)^j \binom{|F_y|}{j}$$

$$= (-1)^{|F_z|} f(x) \delta_{|F_u|,0} ,$$

where δ is the Kronecker delta. Note that $F_x = F_z$ if and only if x is a square-free divisor of ω , that is, $x = \Pi_{F_z}$ where $F_z \subseteq W$.

Combining theorems 4 and 5, with $\gamma = \gcd(l, k)$ and $f(x) = \binom{l/x}{k/x}$ we obtain theorem 1. A periodic orbit p of length l and winding number ω has b-count $k_{\omega} = (\omega n - la)/(b-a) \leq l$, see equation (3). In particular, such an orbit exists if and only if k_{ω} is an integer and

 $la/n \le \omega \le lb/n$. Using theorem 1 and summing over the allowed values of the b-count we have,

(33)
$$|\mathcal{P}_l(C_n(a,b))| = \frac{n}{l} \sum_{\omega = \lceil la/n \rceil}^{\lfloor lb/n \rfloor} \left(\sum_{m \mid \gcd(l,k_\omega,\omega)} \mu(m) \binom{l/m}{k_\omega/m} \right) .$$

Finally, note that the divisors d of ω for which $\binom{l/d}{k_{\omega}/d} \neq 0$ are precisely the divisors of $\gcd(l, k_{\omega}, \omega)$ which proves theorem 2.

6. Conclusions

To summarize, for 2-regular directed circulant graphs of arbitrary order and step sizes, we have evaluated the number of primitive periodic orbits of a given length. In doing so, we have described the path lengths and step size counts for which cycles exist, and obtained a formula for the number of Lyndon words on two letters with a given length and letter count.

To illustrate these results consider periodic orbits on the circulant graph $C_{440}(5,14)$ of length l=360 and b-count k=240. The winding number for these orbits is $\omega=9$. From lemma 3 any step sequence w in $\mathbb{W}_2(360,240)$ corresponding to a primitive orbit will have a repetition number q which divides l and k, and is coprime with ω , i.e., $q \in Q = \{1,2,4,8,5,10,20,40\}$. For each q, we can evaluate $|\mathbb{L}_2(360/q,240/q)|$ the number of words where the root is a Lyndon word of length 360/q and b-count 240/q, using theorem 3. To simplify the formulas let $B_t = \binom{360/t}{240/t}$.

$$(34) q = 1 |\mathbb{L}_2(360, 240)| = \frac{1}{360} (B_1 - B_2 - B_3 - B_5 + B_6 + B_{10} + B_{15} - B_{30})$$

(35)
$$q = 2$$
 $|\mathbb{L}_2(180, 120)| = \frac{1}{180} (B_2 - B_4 - B_6 - B_{10} + B_{12} + B_{20} + B_{30} - B_{60})$

(36)
$$q = 4$$
 $|\mathbb{L}_2(90, 60)| = \frac{1}{90} (B_4 - B_8 - B_{12} - B_{20} + B_{24} + B_{40} + B_{60} - B_{120})$

(37)
$$q = 8$$
 $|\mathbb{L}_2(45, 30)| = \frac{1}{45} (B_8 - B_{24} - B_{40} + B_{120})$

(38)
$$q = 5$$
 $|\mathbb{L}_2(72, 48)| = \frac{1}{72} (B_5 - B_{10} - B_{15} + B_{30})$

(39)
$$q = 10$$
 $|\mathbb{L}_2(36, 24)| = \frac{1}{36} (B_{10} - B_{20} - B_{30} + B_{60})$

(40)
$$q = 20$$
 $|\mathbb{L}_2(18, 12)| = \frac{1}{18} (B_{20} - B_{40} - B_{60} + B_{120})$

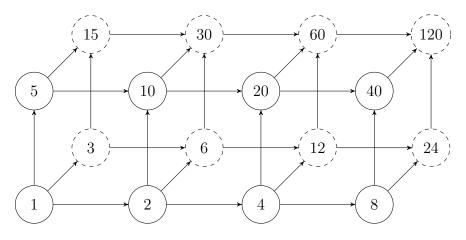
(41)
$$q = 40$$
 $|\mathbb{L}_2(9,6)| = \frac{1}{9} (B_{40} - B_{120})$

To count primitive orbits, each of these quantities is multiplied by n/q (the number of inequivalent starting vertices) and summed, as in the proof of theorem 4. After cancellation, using theorem 5, we see that the number of primitive orbits is,

$$(42) |\mathcal{P}_{360,240}(C_{440}(5,13))| = \frac{440}{360} \left(B_1 - B_3\right) = \frac{440}{360} \left(\binom{360}{240} - \binom{120}{80}\right).$$

The cancellation in theorem 5, is illustrated in figure 5. The figure shows all values of t = qm with $q \in Q$ and m a square-free divisor of gcd(l/q, k/q). The arrows in the figure join

pairs of values that differ by multiplication by a prime. For each t let H_t denote the corners of the hypercube where t is the largest corner. For example, $H_{60} = \{2, 4, 6, 10, 12, 20, 30, 60\}$. The intersection of H_t with Q is the set of values of q which contribute $\pm B_t$ to the sum in theorem 5. The sign $\mu(m)$ depends on the parity of the number of prime factors of m, that is, the graph distance from t to q. Counting points on a cube with this alternating sign results in the alternating sum of binomial coefficients in equation (31), which is nonzero if and only if $|H_t \cap Q| = 1$. In the example this happens twice, when $H_3 \cap Q = \{1\}$ and $H_1 \cap Q = \{1\}$. This condition is equivalent to t being coprime with Q. As m is square-free, the set of contributors $\{1,3\}$ is the set of square-free common divisors of ω, l, k , as in theorem 1.



- Divisors of 120 coprime with $\omega = 9$
- () Divisors of 120 not coprime with $\omega = 9$

FIGURE 5. Divisors t = qm of $\gcd(360, 240) = 120$ with q coprime with the repetition number $\omega = 9$ and m a square-free divisor of $\gcd(360/q, 240/q)$. Arrows show two divisors are related by multiplication by a prime.

To demonstrate counting all primitive periodic orbits of a fixed length consider $C_{21}(4, 10)$ with l=15. The lattice of allowed winding numbers and b-counts $S_{21}(4, 10)$ is shown in figure 6. The figure also illustrates the bounds on the winding number $la/n \le \omega \le lb/n$. For instance, counting orbits of length l=15, we have $2.86 \le \omega \le 7.14$. The only valid winding numbers are those divisible by $\gcd(4, 10) = 2$, which is reflected in the proof of theorem 2 since $k_3 = 1/2$ and $k_5 = 15/2$ and $k_7 = 29/2$ which are not integers so the corresponding binomial coefficients are omitted. Similarly, when $\omega = 4$ or 6, note that m=2 has l/m=15/2 and m=3 has $k_6/m=11/3$. Therefore,

(43)
$$|\mathcal{P}_{15}(C_{21}(4,10))| = \frac{21}{15} \sum_{\omega=3}^{7} \sum_{m|\omega} \mu(m) \binom{15/m}{(21\omega - 60)/(6m)}$$

$$=\frac{21}{15}\left(\binom{15}{4}+\binom{15}{11}\right)$$

$$= 3822.$$

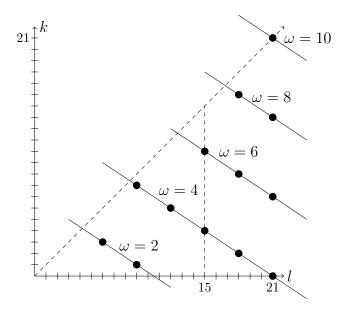


FIGURE 6. The lattice $S_{21}(4, 10)$.

Acknowledgments. TH would like to thank Lauren Engelthaler, and Isaac Hellerman for helpful suggestions.

References

- [1] E. Akkermans, A. Comtet, J. Desbois, G. Montambaux, and C. Texier. Spectral determinant on quantum graphs. *Ann. Phys.*, 284:10–51, 2000.
- [2] R. Band, J. M. Harrison, and C. H. Joyner. Finite pseudo orbit expansions for spectral quantities of quantum graphs. J. Phys. A: Math. Theor., 45:325204, 2012.
- [3] R. Band, J.M. Harrison, and M. Sepanski. Lyndon word decompositions and pseudo orbits on q-nary graphs. *J. Math. Anal. Appl.*, 470:135–144, 2019.
- [4] G. Berkolaiko and P. Kuchment. *Introduction to Quantum Graphs*, volume 186 of *Mathematical Surveys and Monographs*. Amer. Math. Soc., Providence, RI, 2013.
- [5] J. Bolte and J. M. Harrison. Spectral statistics for the dirac operator on graphs. J. Phys. A: Math. Gen., 36:2747–2769, 2003.
- [6] J. Bolte and Endres S. The trace formula for quantum graphs with general self adjoint boundary conditions. Ann. Henri Poincaré, 10:189–223, 2009.
- [7] L. Engelthaler, I. Hellerman, and T. Hudgins. A combinatorial approach to counting primitive periodic and primitive pseudo orbits on circulant graphs, 2021. Preprint at https://arxiv.org/abs/2107. 13051.
- [8] J. M. Harrison and T. Hudgins. Complete dynamical evaluation of the characteristic polynomial of binary quantum graphs. J. Phys. A: Math. Theor., 55:425202, 2022.
- [9] J. M. Harrison and T. Hudgins. Periodic-orbit evaluation of a spectral statistic of quantum graphs without the semiclassical limit. *EPL*, 138:30002, 2022.
- [10] J. M. Harrison and E. Swindle. Spectral properties of quantum curculant graphs. *J. Phys. A: Math. Theor.*, 52:28101, 2019.
- [11] K. Hashimoto. Zeta functions of finite graphs and representation of p-adic groups. Adv. Studies Pure Math, 15:211–280, 1989.
- [12] V. Kostrykin, J. Potthoff, and R. Schrader. Heat kernels on metric graphs and a trace formula. In *Contemp. Math.*, volume 447, pages 175–198, Providence, RI, 2007. AMS.
- [13] T. Kottos and U. Smilansky. Quantum chaos on graphs. Phys. Rev. Lett., 79:4794, 1997.
- [14] T. Kottos and U. Smilansky. Periodic orbit theory and spectral statistics for quantum graphs. *Ann. Phys.*, 274:76–124, 1999.

- [15] P. Kuchment. Quantum graphs I: Some basic structures. Waves Random Media, 14:S107–S128, 2004.
- [16] P. Kurasov. Graph Laplacians and toplogy. Ark. Mat., 46:95–111, 2008.
- [17] P. Kurasov. Spectral Geometry of Graphs, volume 293 of Operator Theory: Advances and Applications. Birkhäuser, Berlin, 2024.
- [18] R. C. Lyndon. On burnside's problem. Trans. Amer. Math. Soc., 77:202–215, 1954.
- [19] J. Marklof and A. Strömbergsson. Diameters of random circulant graphs. Combinatorica, 33:429–466, 2013.
- [20] P. T. Meijer. Connectivities and diameters of circulant graphs. Master's thesis, Simon Fraser University, 1991. Available at https://api.semanticscholar.org/CorpusID:28325039.
- [21] J. P. Roth. Le spectre du laplacien sur un graphe théorie du potentiel. In *Lecture Notes in Mathematics*, volume 1096, pages 521–539, Berlin, 1983. Springer.
- [22] H. M. Stark and A. A. Terras. Zeta functions of finite graphs and coverings. Adv. Math., 121:142–165, 1996.
- [23] T. Sunada. L-functions in geometry and some applications. In *Curvature and topology of Riemannian manifolds, Lecture Notes in Math.*, volume 1201, pages 266–284, Berlin, 1986. Springer.

Department of Mathematics, Baylor University, 1410 S. 4th Street, Waco, 76706, TX, USA

Email address: isaac_echols1@baylor.edu, jon_harrison@baylor.edu

Department of Mathematics, 405 Snow Hall, 1460 Jayhawk Blvd., Lawrence, 66045, KS, USA

Email address: thudgins@ku.edu