The geometric kernel of integral circulant graphs

J.W. Sander

Institut für Mathematik und Angewandte Informatik
Universität Hildesheim
D-31141 Hildesheim, Germany

`sander@imai.uni-hildesheim.de`

Abstract

By a suitable representation in the Euclidean plane, each circulant graph G, i.e. a graph with a circulant adjacency matrix $\mathcal{A}(G)$, reveals its rotational symmetry and, as the drawing's most notable feature, a central hole, the so-called *geometric kernel* of G.

Every integral circulant graph G on n vertices, i.e. satisfying the additional property that all of the eigenvalues of $\mathcal{A}(G)$ are integral, is isomorphic to some graph $\mathrm{ICG}(n, \mathcal{D})$ having vertex set $\mathbb{Z}/n\mathbb{Z}$ and edge set $\{\{a, b\} : a, b \in \mathbb{Z}/n\mathbb{Z},\ \gcd(a - b, n) \in \mathcal{D}\}$ for a uniquely determined set $\mathcal{D}$ of positive divisors of n. A lot of recent research has revolved around the interrelation between graph-theoretical, algebraic and arithmetic properties of such graphs. In this article we examine arithmetic implications imposed on n by a geometric feature, namely the size of the geometric kernel of $\mathrm{ICG}(n, \mathcal{D})$.

Mathematics Subject Classifications: 05C50, 05C62; Secondary 68R10

1 Introduction

A graph G is called *circulant* if G has a circulant adjacency matrix $\mathcal{A}(G)$. *Integral circulant graphs*, i.e. circulant graphs additionally satisfying $\mathrm{Spec}(G) := \mathrm{Spec}(\mathcal{A}(G)) \subseteq \mathbb{Z}$, are fascinating objects since they interconnect graph theory with (linear) algebra and, in particular, number theory. Algebraic properties of these graphs have been studied quite intensely in recent years (see [8, 9, 11] for some results and further references). By the works of So [16] and Klotz and T. Sander [7] each integral circulant graph $\mathrm{ICG}(n, \mathcal{D}) = (V, E)$ is characterised by its order n and a non-empty set $\mathcal{D} \subseteq \mathfrak{D}(n) := \{d > 0 : d \mid n\}$ of positive divisors of n in such a way that $V = \mathbb{Z}/n\mathbb{Z}$ and $E = \{\{a, b\} : a, b \in \mathbb{Z}/n\mathbb{Z},\ \gcd(a - b, n) \in \mathcal{D}\}$. Since graphs usually are assumed to have no loops, we require that $n \notin \mathcal{D}$.

A motivation for investigating spectra of graphs is to find out to which extent the eigenvalues of a graph G characterise G. According to a conjecture of So [16] different integral circulant graphs have different spectra, taking multiplicities of eigenvalues into account. In [6, Corollaries 11.2 and 11.3] this was confirmed by KLIN and KOVÁCS as a consequence of ZIBIN'S conjecture for arbitrary circulant graphs, which in turn follows from work of MUZYCHUK [10] on the structure of Schur rings over cyclic groups. Independently, DOBSON and MORRIS [3] proved TOIDA'S conjecture by using the classification of finite simple groups and deduced ZIBIN'S more general conjecture from it.

As contrasted with those profound tools, T. SANDER and the author (see [15], also for further references) showed that for arbitrary n and so-called *multiplicative divisor sets* $\mathcal{D}$ in particular simple combinatorial arguments can be used to deal with So's conjecture. In [12] the author clarified the interplay between the dimension of the (algebraic) kernel of $\text{ICG}(n, \mathcal{D})$ and the graph itself for all positive integers n and all multiplicative divisor sets $\mathcal{D}$. In [13] the work on the kernel of integral circulant graphs was extended to non-zero eigenvalues.

To complement the knowledge on algebraic features of an integral circulant graph as desribed above, we shall examine a geometric property of $\text{ICG}(n, \mathcal{D})$ by looking at a suitable drawing of the graph and by deducing arithmetic implications imposed on n by the size of a central hole called the *geometric kernel*.

In order to visualise the high degree of rotational symmetry of an (integral) circulant graph G it is appropriate to make a drawing of G by placing its nodes $0, 1, 2, \ldots, n-1$, say, equidistantly along the edge of a circle and connect each pair $a, b \in \{0, 1, 2, \ldots, n-1\} \simeq \mathbb{Z}/n\mathbb{Z}$ of distinct neighbouring nodes by the line segment $\overline{ab}$. A typical example is the drawing of the graph $\text{ICG}(12, \{2, 4\})$ as shown in Figure 1.
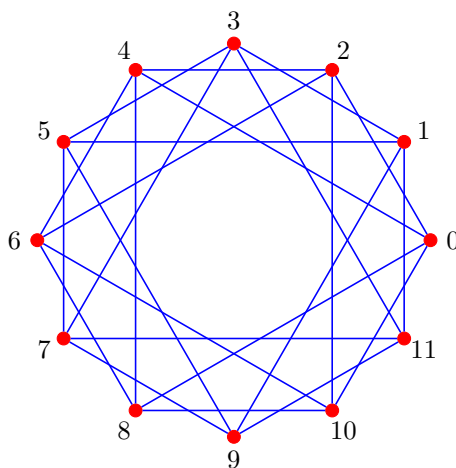

Figure 1: Drawing of the integral circulant graph $\text{ICG}(12, \{2, 4\})$

In [14] we proved that the central hole in the drawing of any circulant graph on $n \geqslant 3$ vertices is a regular n-gon, and we also determined its size. To solve that purely combinatorial problem required little more than some elementary geometric arguments. Quite

differently from that, we shall see that the size of the central hole of an *integral* circulant graph ICG($n, \mathcal{D}$) does provide additional information, namely about the arithmetic nature of n.

Further examples of drawings of integral circulant graphs are displayed in Figure 2. Apart from the beauty of the visualisations of circulant graphs, to a great extent owing
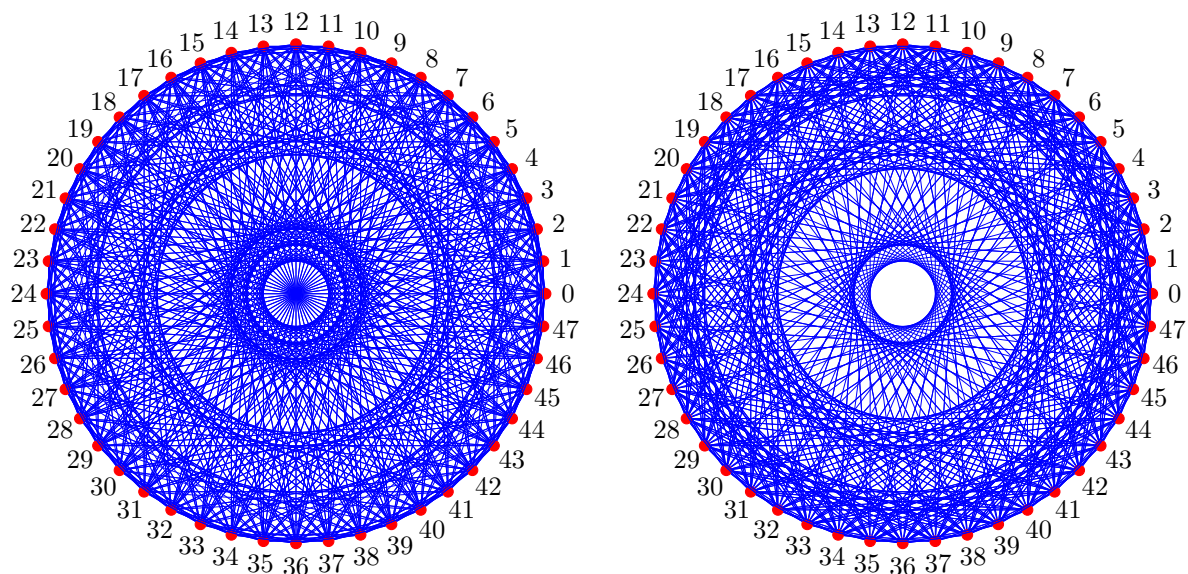

Figure 2: Drawings of ICG($48, \{2, 3, 4, 24\}$) and ICG($48, \{2, 3, 8, 16\}$)

to the high degree of symmetry, one may notice that the drawings of ICG($12, \{2, 4\}$) and ICG($48, \{2, 3, 8, 16\}$) have a hole in their center, but ICG($48, \{2, 3, 4, 24\}$) is without central hole (see Figures 1 and 2). Just like the graph spectrum stores information on the graph, so does the size of the hole in the drawing of an integral circulant graph. In fact, it is related to arithmetic properties of the graph. A trivial example of this is the observation that ICG($n, \mathcal{D}$) is without hole if and only if $\frac{n}{2} \in \mathcal{D}$, which implies that n has to be an even integer. By analogy with the algebraic kernel of such a graph, i.e. the eigenspace of the eigenvalue 0, and its impact on the graph (see [12]), we call the hole of the corresponding drawing the graph's *geometric kernel* – a rigid definition of this concept will be given in the following section.

The purpose of this paper is to investigate properties of the geometric kernels of integral circulant graphs. In particular, we shall explicitly determine the kernel sizes for *unitary Cayley graphs* ICG($n, \{1\}$) in Section 3. In Section 4 we establish formulae for kernel sizes of graphs ICG($n, \mathcal{D}$) in general and, given n, identify those graphs having largest kernel (depending on the residue class of n mod 12). Finally, Section 5 deals with the average kernel size of graphs ICG($n, \mathcal{D}$) for fixed n.

2 Preliminaries

In order to be able to compare geometric kernels of different circulant graphs we standardised drawings of such graphs in [14], which for integral circulant graphs reads as follows: The **unit circle drawing** $\mathrm{UCD}(n, \mathcal{D}) := \mathrm{UCD}(\mathrm{ICG}(n, \mathcal{D}))$ of $\mathrm{ICG}(n, \mathcal{D})$ is defined as the subset of the complex plane $\mathbb{C}$ characterised by the subsequent construction:

(i) Each vertex $j \in \{0, 1, 2, \ldots, n-1\} \simeq \mathbb{Z}/n\mathbb{Z}$ is represented by the corresponding **corner** $e(\frac{j}{n}) \in \mathbb{C}$ on the unit circle, where $e(x) := e^{2\pi i x}$ for any $x \in \mathbb{R}$.

(ii) If $\{j, k\}$ is an edge, i.e. in case $\gcd(j - k, n) \in \mathcal{D}$, then $\{j, k\}$ is represented by the **thread** $\overline{e(\frac{j}{n})e(\frac{k}{n})}$ defined as the closed line segment between the corners $e(\frac{j}{n})$ and $e(\frac{k}{n})$.

(iii) $\mathrm{UCD}(n, \mathcal{D}) := \mathrm{UCD}(\mathrm{ICG}(n, \mathcal{D})) := \bigcup_{\{j,k\} \in E} \overline{e(\frac{j}{n})e(\frac{k}{n})}$.

Examples of unit circle drawings of some integral circulant graphs are displayed in Figures 1 and 2. Clearly, $\mathrm{UCD}(n, \mathcal{D}) \subseteq P_n$, where $P_n \subseteq \mathbb{C}$ denotes the closed convex regular n-gon formed by the n corners of $\mathrm{UCD}(n, \mathcal{D})$ on the unit circle.

We already observed that $\mathrm{UCD}(n, \mathcal{D})$ contains a thread running through the origin, i.e. through the center of $\mathrm{UCD}(n, \mathcal{D})$, if and only if $\frac{n}{2} \in \mathcal{D}$. In that case $\mathrm{UCD}(n, \mathcal{D})$ has no central hole, and thus we shall require $\frac{n}{2} \notin \mathcal{D}$ in the sequel. Since we assumed from the beginning to consider graphs without loops, we have $n \notin \mathcal{D}$ as well. Therefore, we call a non-empty set $\mathcal{D} \subseteq \mathfrak{D}(n)$ an *appropriate* divisor set of n if $n \notin \mathcal{D}$ and $\frac{n}{2} \notin \mathcal{D}$. All elements of such a set will be called *appropriate divsors* of n, and we define $\mathfrak{D}^*(n) := \mathfrak{D}(n) \setminus \{\frac{n}{2}, n\}$.

Thus $0 \notin \mathrm{UCD}(n, \mathcal{D})$ for appropriate divisor sets $\mathcal{D} \subseteq \mathfrak{D}^*(n)$, and in that case, by using topological terminology, the **geometric kernel** of $\mathrm{ICG}(n, \mathcal{D})$ is defined as the connected component $K_0(n, \mathcal{D}) := K_0(\mathrm{ICG}(n, \mathcal{D}))$, say, of $\mathbb{C} \setminus \mathrm{UCD}(n, \mathcal{D})$ which contains the origin.

By definition, $K_0(n, \mathcal{D})$ is an open set. Since we consider polygons to be closed sets, we introduce the topological closure $\overline{K_0(n, \mathcal{D})} := \overline{K_0(\mathrm{ICG}(n, \mathcal{D}))}$ of $K_0(\mathrm{ICG}(n, \mathcal{D}))$. The following result is the specification of [14, Theorem 3.1] to integral circulant graphs.

Theorem 1 ([14, Theorem 3.1]). *Let $n \geqslant 3$, and let $\varnothing \neq \mathcal{D} \subseteq \mathfrak{D}^*(n)$. Then*

$$m_0 = m_0(n, \mathcal{D}) = m_0(\mathrm{ICG}(n, \mathcal{D})) := \max\{1 \leqslant m < \tfrac{n}{2} : \gcd(m, n) \in \mathcal{D}\} \qquad (1)$$

is well defined, and $\overline{K_0(n, \mathcal{D})}$ is a regular convex n-gon with corners given by the complex points

$$\frac{\cos \frac{\pi m_0}{n}}{\cos \frac{\pi}{n}} \, e\left(\frac{j}{n}\right) \qquad (j = 0, 1, 2, \ldots, n-1) \qquad (2)$$

if m_0 is odd, and with corners

$$\frac{\cos \frac{\pi m_0}{n}}{\cos \frac{\pi}{n}} \, e\left(\frac{1}{n}\left(j + \frac{1}{2}\right)\right) \qquad (j = 0, 1, 2, \ldots, n-1) \qquad (3)$$

if m_0 is even.

All corners of a convex regular polygon P lie on the so-called *circumscribed circle* of P, and we denote its *circumradius* by $\rho(P)$. According to Theorem 1 we define the **kernel radius**

$$\rho_0(n, \mathcal{D}) = \rho_0(\mathrm{ICG}(n, \mathcal{D})) := \rho(\overline{K_0(n, \mathcal{D})})$$

of $\mathrm{ICG}(n, \mathcal{D})$ or $\mathrm{UCD}(\mathrm{ICG}(n, \mathcal{D}))$, respectively, for any $n \geqslant 3$ and every appropriate divisor set $\mathcal{D}$ of n. Moreover, we set $m_0(n, \mathcal{D}) = m_0(\mathrm{ICG}(n, \mathcal{D})) = \frac{n}{2}$ and $\rho_0(n, \mathcal{D}) = \rho_0(\mathrm{ICG}(n, \mathcal{D})) = 0$ for divisor sets with $\frac{n}{2} \in \mathcal{D}$. Clearly, $0 < \rho_0(n, \mathcal{D}) \leqslant 1$ for any integral circulant graph $\mathrm{ICG}(n, \mathcal{D})$ with appropriate divisor set $\mathcal{D}$. As an immediate consequence of Theorem 1 we obtain

Corollary 2. *For $n \geqslant 3$ and $\varnothing \neq \mathcal{D} \subseteq \mathfrak{D}(n)$ we have*

$$\rho_0(n, \mathcal{D}) = \frac{\cos \frac{\pi m_0(n, \mathcal{D})}{n}}{\cos \frac{\pi}{n}}.$$

Remark 3. Given a regular n-gon with *circumradius* ρ_{circ} and *inradius* ρ_{in}, elementary geometry tells us that $\rho_{in} = \rho_{circ} \cdot \cos \frac{\pi}{n}$. By Corollary 2 this implies that the inradius of $\overline{K_0(n, \mathcal{D})}$ equals $\cos \frac{\pi m_0(n, \mathcal{D})}{n}$. Because of this simple relation between the two radii we shall only consider the circumradius $\rho_0(n, \mathcal{D})$ in the sequel.

These results show that the kernel radius, as well as the corresponding inradius, is a strictly decreasing function with respect to m_0 (in the range $0 < m_0 \leqslant \frac{n}{2}$). Therefore $m_0(n, \mathcal{D})$ as well as $\rho_0(n, \mathcal{D})$ may both serve as measures for the size of the geometric kernel of $\mathrm{ICG}(n, \mathcal{D})$. The following two sections reveal that the size of the geometric kernel, in terms of $m_0(n, \mathcal{D})$ or in terms of the kernel radius $\rho_0(n, \mathcal{D})$, has arithmetic consequences for n.

3   Geometric kernels of unitary Cayley graphs

Let us start with a subclass of integral circulant graphs, namely so-called *unitary Cayley graphs* $\mathcal{X}_n := \mathrm{Cay}(\mathbb{Z}/n\mathbb{Z}, U_n)$, where U_n denotes the group of units in the ring $\mathbb{Z}/n\mathbb{Z}$, i.e. the set of primitive residues mod n. It is well known that the unitary Cayley graph $\mathcal{X}_n$ on n vertices is isomorphic to the special integral circulant graph with the trivial divisor set $\mathcal{D} = \{1\}$ (see [7] for basics of unitary Cayley graphs and their relation to integral circulant graphs). The following result shows two facts in this subclass of integral circulant graphs: The kernel radius of $\mathcal{X}_n$ is minimal for all $n \not\equiv 2 \bmod 4$ and next to minimal for $n \equiv 2 \bmod 4$, i.e. $m_0(\mathcal{X}_n)$ is (almost) maximal, and it determines the residue class of $n \bmod 4$.

Theorem 4. *For a unitary Cayley graph $\mathcal{X}_n$ with $n \geqslant 3$ we have*

$$m_0(\mathcal{X}_n) := m_0(\mathrm{ICG}(n, \{1\})) = \begin{cases} \frac{n-1}{2} & \text{if } n \equiv 1 \bmod 2, \\ \frac{n}{2} - 1 & \text{if } n \equiv 0 \bmod 4, \\ \frac{n}{2} - 2 & \text{if } n \equiv 2 \bmod 4. \end{cases}$$

Proof. By definition we have $m_0(\mathcal{X}_n) = \max\{1 \leqslant m < \frac{n}{2} : \gcd(m, n) = 1\}$. For odd $n = 2q + 1$, say, we obtain $\gcd\left(\frac{n-1}{2}, n\right) = \gcd(q, 2q + 1) = 1$, hence $m_0(\mathcal{X}_n) = \frac{n-1}{2}$. For $n = 4q$, it follows that $\gcd\left(\frac{n}{2} - 1, n\right) = \gcd(2q - 1, 4q) = \gcd(2q - 1, q) = 1$, and therefore $m_0(\mathcal{X}_n) = \frac{n}{2} - 1$. Finally, for $n = 4q + 2$ we have $\gcd\left(\frac{n}{2} - 1, n\right) = \gcd(2q, 4q + 2) = \gcd(2q, 2) = 2$, but $\gcd\left(\frac{n}{2} - 2, n\right) = \gcd(2q - 1, 4q + 2) = \gcd(2q - 1, 4) = 1$, which implies $m_0(\mathcal{X}_n) = \frac{n}{2} - 2$. $\qquad\square$

By a simple monotonicity argument we obtain

Corollary 5. *For $n \geqslant 3$ and any $\mathcal{D} \subseteq \mathfrak{D}^*(n)$ with $1 \in \mathcal{D}$ we have*

$$m_0(n, \mathcal{D}) = m_0(\mathcal{X}_n) = \begin{cases} \frac{n-1}{2} & \text{if } 2 \nmid n, \\ \frac{n}{2} - 1 & \text{if } 4 \mid n. \end{cases}$$

Proof. Clearly, $\mathrm{UCD}(n, \mathcal{D}_1) \subseteq \mathrm{UCD}(n, \mathcal{D}_2)$ for appropriate divisor sets $\mathcal{D}_1 \subseteq \mathcal{D}_2$ of n, which implies $m_0(n, \mathcal{D}_1) \leqslant m_0(n, \mathcal{D}_2)$. Since $1 \in \mathcal{D}$ by assumption, it follows that $m_0(n, \mathcal{D}) \geqslant m_0(\mathcal{X}_n)$. By the definition of appropriate divisor sets $\mathcal{D}$ and according to Theorem 4, we have $m_0(n, \mathcal{D}) \leqslant \frac{n-1}{2} = m_0(\mathcal{X}_n)$ for odd n and $m_0(n, \mathcal{D}) \leqslant \frac{n}{2} - 1 = m_0(\mathcal{X}_n)$ for even n. Hence the result follows. $\qquad\square$

4 The kernel radius of $\mathrm{ICG}(n, \mathcal{D})$ and arithmetic features of n

Now we turn our attention to integral circulant graphs $\mathrm{ICG}(n, \mathcal{D})$ in general, i.e. $n \geqslant 3$ is an arbitrary integer and $\mathcal{D} = \{d_1, d_2, \ldots, d_r\}$, say, is any appropriate divisor set of n.
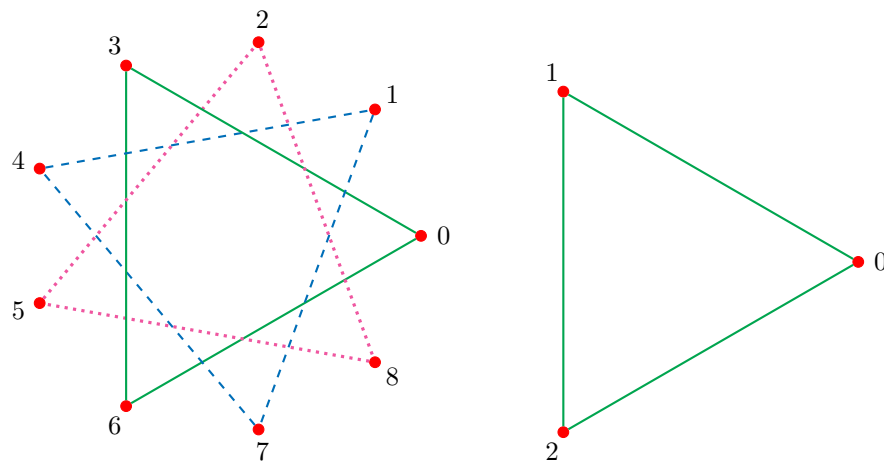

Figure 3: $\mathrm{ICG}(3^2, \{3\})$ with three components, each isomorphic to $\mathrm{ICG}(3, \{1\})$

It is well known that $\mathrm{ICG}(n, \mathcal{D})$ is connected if and only if $g = \gcd(d_1, \ldots, d_r) = 1$ (see [2]). In fact, $\mathrm{ICG}(n, \mathcal{D})$ consists of g isomorphic connected components (see [16]), all of which are isomorphic to $\mathrm{ICG}(\frac{n}{g}, \frac{1}{g}\mathcal{D})$, where $c\mathcal{D}$ denotes elementwise multiplication of $\mathcal{D}$ by

c. Examples are $\mathrm{ICG}(12, \{2, 4\})$ with two components, both isomorphic to $\mathrm{ICG}(6, \{1, 2\})$ (cf. Figure 1), and $\mathrm{ICG}(3^2, \{3\})$ with three components of type $\mathrm{ICG}(3, \{1\})$ in Figure 3.

A simple geometric consideration reveals that the *incircle radii* of the geometric kernels of $\mathrm{ICG}(n, \mathcal{D})$ and its components $\mathrm{ICG}(\frac{n}{g}, \frac{1}{g}\mathcal{D})$ coincide, while $\rho_0(n, \mathcal{D}) < \rho_0(\frac{n}{g}, \frac{1}{g}\mathcal{D})$ in case $g > 1$ (cf. Remark 3 for details). The corresponding relation between $m_0(n, \mathcal{D})$ and $m_0(\frac{n}{g}, \frac{1}{g}\mathcal{D})$ is provided by formula (ii) of

Proposition 6. *Let $n \geqslant 3$ be an integer, and let $\mathcal{D} = \{d_1, d_2, \ldots, d_r\} \subseteq \mathfrak{D}^*(n)$ with $g := \gcd(d_1, d_2, \ldots, d_r)$. Then we have*

(i) $m_0(n, \mathcal{D}) = \max_{d \in \mathcal{D}} m_0(n, \{d\})$;

(ii) $m_0(n, \mathcal{D}) = g \cdot m_0(\frac{n}{g}, \frac{1}{g}\mathcal{D})$.

Proof. Clearly

$$
\begin{aligned}
\{1 \leqslant m < \tfrac{n}{2} : \ \gcd(m, n) \in \mathcal{D}\} &= \bigcup_{d \in \mathcal{D}} \{1 \leqslant m < \tfrac{n}{2} : \ \gcd(m, n) = d\} \\
&= \bigcup_{d \in \mathcal{D}} \{1 \leqslant m'g < \tfrac{n}{2} : \ \gcd(m'g, \tfrac{n}{g}g) = \tfrac{d}{g}g\} \\
&= \bigcup_{d \in \mathcal{D}} g \cdot \{1 \leqslant m' < \tfrac{n}{2g} : \ \gcd(m', \tfrac{n}{g}) = \tfrac{d}{g}\} \\
&= g \cdot \{1 \leqslant m' < \tfrac{n}{2g} : \ \gcd(m', \tfrac{n}{g}) \in \tfrac{1}{g}\mathcal{D}\}.
\end{aligned}
\tag{4}
$$

Taking maxima on both sides of the first equality implies (i), and taking maxima of the first and the last term in (4) proves (ii). $\qquad \square$

If $n = p \geqslant 3$ is a prime, there is only one possible appropriate divisor set, namely $\mathcal{D} = \{1\}$. This means that $\mathrm{ICG}(p, \mathcal{D}) = \mathcal{X}_p$ (see Theorem 4). For prime powers $n = p^k$, we have

Theorem 7. *Let $p^k \geqslant 3$ be a prime power, and let $\mathcal{D} \subseteq \mathfrak{D}^*(p^k)$ with $\min \mathcal{D} = p^{k_1}$. Then*

$$
m_0(p^k, \mathcal{D}) = \begin{cases} \frac{1}{2}\left(p^k - p^{k_1}\right) & \text{for } p \geqslant 3, \\ 2^{k-1} - 2^{k_1} & \text{for } p = 2. \end{cases}
$$

Proof. Obviously, the greatest common divisor g of the elements of $\mathcal{D}$ satisfies $g = p^{k_1}$. By Proposition 6(ii) we obtain

$$
m_0(p^k, \mathcal{D}) = p^{k_1} m_0(p^{k-k_1}, \tfrac{1}{p^{k_1}}\mathcal{D}),
$$

where $1 \in \frac{1}{p^{k_1}}\mathcal{D}$, $\frac{1}{p^{k_1}}\mathcal{D} \subseteq \mathfrak{D}^*(p^{k-k_1})$ and $k - k_1 \geqslant 2$, since $\mathcal{D} \subseteq \mathfrak{D}^*(p^k)$. In particular $4 \mid p^{k-k_1}$ in case $p = 2$. Thus Corollary 5 yields

$$
m_0(p^k, \mathcal{D}) = p^{k_1} m_0(\mathcal{X}_{p^{k-k_1}}) = \begin{cases} p^{k_1} \cdot \frac{1}{2}\left(p^{k-k_1} - 1\right) & = \frac{1}{2}\left(p^k - p^{k_1}\right) & \text{for } p \geqslant 3, \\ 2^{k_1} \cdot \left(2^{k-k_1-1} - 1\right) & = 2^{k-1} - 2^{k_1} & \text{for } p = 2. \end{cases} \qquad \square
$$

For arbirary integers n and primes p let $e_p(n) \geqslant 0$ denote the order of p in n.

Theorem 8. *Let $n \geqslant 3$ be an arbitrary integer, and let $\mathcal{D} \subseteq \mathfrak{D}^*(n)$. Then*

$$m_0(n, \mathcal{D}) = \frac{1}{2}\Big(n - \min_{d \in \mathcal{D}} \gamma_{n,d}\, d\Big), \tag{5}$$

where

$$\gamma_{n,d} = \begin{cases} 1 & \textit{if } e_2(d) = e_2(n), \\ 4 & \textit{if } e_2(d) = e_2(n) - 1, \\ 2 & \textit{if } e_2(d) \leqslant e_2(n) - 2. \end{cases}$$

Proof. Given any $d \in \mathcal{D}$, it follows from Proposition 6(ii) and Theorem 4 that

$$m_0(n, \{d\}) = d \cdot m_0(\tfrac{n}{d}, \{1\}) = d \cdot m_0(\mathcal{X}_{\frac{n}{d}}) = \begin{cases} d\left(\frac{n}{d} - 1\right)/2 & \textit{if } \frac{n}{d} \equiv 1 \bmod 2, \\ d\left(\frac{n}{2d} - 1\right) & \textit{if } \frac{n}{d} \equiv 0 \bmod 4, \\ d\left(\frac{n}{2d} - 2\right) & \textit{if } \frac{n}{d} \equiv 2 \bmod 4, \end{cases}$$

$$= \tfrac{1}{2}(n - \gamma_{n,d}\, d).$$

Then Proposition 6(i) proves (5). $\qquad\square$

For given n, we shall determine the integral circulant graphs on n vertices having the largest geometric kernel. To this end we define

$$M_0(n) := \min\{m_0(n, \mathcal{D}) : \mathcal{D} \subseteq \mathfrak{D}^*(n),\ \mathcal{D} \neq \varnothing\},$$
$$R_0(n) := \max\{\rho_0(n, \mathcal{D}) : \mathcal{D} \subseteq \mathfrak{D}^*(n),\ \mathcal{D} \neq \varnothing\}.$$

Theorem 9. *Let $n \geqslant 3$ be an integer and $\varnothing \neq \mathcal{D} \subseteq \mathfrak{D}^*(n)$. For n different from a power of 2, we denote by p_1 the smallest odd prime divisor of n. Then*

$$M_0(n) = \begin{cases} \frac{1}{2}(1 - \frac{1}{p_1})n & \textit{if } n \equiv 1 \bmod 2, \\ \frac{1}{2}(1 - \frac{2}{p_1})n & \textit{if } n \equiv j \bmod 12 \textit{ for some } j \in \{0, 2, 6, 10\}, \\ \frac{1}{4}n & \textit{if } n \equiv 4 \bmod 12 \textit{ or } n \equiv 8 \bmod 12, \end{cases} \tag{6}$$

and

$$R_0(n) = \begin{cases} \sin\frac{\pi}{2p_1} / \cos\frac{\pi}{n} & \textit{if } n \equiv 1 \bmod 2, \\ \sin\frac{\pi}{p_1} / \cos\frac{\pi}{n} & \textit{if } n \equiv j \bmod 12 \textit{ for some } j \in \{0, 2, 6, 10\}, \\ \frac{\sqrt{2}}{2} / \cos\frac{\pi}{n} & \textit{if } n \equiv 4 \bmod 12 \textit{ or } n \equiv 8 \bmod 12. \end{cases} \tag{7}$$

The unique singleton divisor sets giving these maximal values of the kernel radius, i.e. the minimal values of $m_0(n, \mathcal{D})$, are $\mathcal{D} = \{\frac{n}{p_1}\}$, $\mathcal{D} = \{\frac{n}{2p_1}\}$, and $\mathcal{D} = \{\frac{n}{4}\}$ according to the three subcases.

Proof. Theorem 8 implies that

$$M_0(n) = \min_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \mathcal{D} \neq \varnothing}} \tfrac{1}{2}\Big(n - \min_{d \in \mathcal{D}} \gamma_{n,d}\, d\Big) = \tfrac{1}{2}\Big(n - \max_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \mathcal{D} \neq \varnothing}} \min_{d \in \mathcal{D}} \gamma_{n,d}\, d\Big)$$
$$= \tfrac{1}{2}\Big(n - \max_{d \in \mathfrak{D}^*(n)} \gamma_{n,d}\, d\Big) = \tfrac{1}{2}\Big(n - \max_{\substack{d \mid n \\ d < \frac{n}{2}}} \gamma_{n,d}\, d\Big). \tag{8}$$

In case $n \equiv 1 \bmod 2$, we have $\gamma_{n,d} = 1$, thus $\max_{d|n,\, d<\frac{n}{2}} \gamma_{n,d}\, d = \max_{d|n,\, d<\frac{n}{2}} d = \frac{n}{p_1}$, which by use of (8) verifies (6) and also shows that $\mathcal{D} = \{\frac{n}{p_1}\}$ is the unique corresponding singleton divisor set for odd n.

We continue with the case $n \equiv 0 \bmod 12$. It follows that $3 \mid n$, hence $p_1 = 3$. Theorem 8 implies that

$$\gamma_{n,d}\, d = \begin{cases} d & \text{if } e_2(d) = e_2(n), \\ 4d & \text{if } e_2(d) = e_2(n) - 1, \\ 2d & \text{if } e_2(d) \leqslant e_2(n) - 2, \end{cases} \tag{9}$$

where the maximal appropriate divisor d equals $\frac{n}{3}$, $\frac{n}{2\cdot3}$ or $\frac{n}{2\cdot2}$ according to the three sub-cases. Therefore, $\gamma_{n,d}\, d$ equals $\frac{n}{3}$, $\frac{2n}{3}$ or $\frac{n}{2}$ accordingly. This implies that $\max \gamma_{n,d}\, d = \frac{2n}{3}$, which by (8) confirms (6) for $12 \mid n$. The case $n \equiv 6 \bmod 12$ gives the same result be the same argument, where the third subcase in (9) does not occur, since here $4 \nmid n$. The identical reasoning works for $n \equiv 2 \bmod 12$ and $n \equiv 10 \bmod 12$ (again $4 \nmid n$), but now $3 \nmid n$ and consequently 3 has to be replaced by the smallest odd prime divisor p_1 of n.

We are left with the cases $n \equiv 4 \bmod 12$ and $n \equiv 8 \bmod 12$, thus $4 \mid n$ but $3 \nmid n$. Hence either n is a power of 2 or $p_1 \geqslant 5$. Under these conditions $\max \gamma_{n,d}\, d$ is obtained by the third subcase in (9) with $d = \frac{n}{2\cdot2}$, and this completes the proof of (6).

Finally, (7) is an immediate consequence of Corollary 2 and (6), applying the trigonometric identity $\cos(\frac{\pi}{2} - x) = \sin x$ and $\cos \frac{\pi}{4} = \frac{\sqrt{2}}{2}$. $\qquad \square$

As a first consequence of Theorem 9 we obtain that the kernel radii of integral circulant graphs are uniformly bounded by $\frac{\sqrt{3}}{2} + \mathrm{O}(\frac{1}{n^2})$.

Corollary 10. *Let $n \geqslant 3$ be an integer. Then*

(i) $M_0(n) \geqslant \frac{1}{6}n$ with equality if and only if $6 \mid n$;

(ii) $R_0(n) < \frac{\sqrt{3}}{2} + \frac{5}{n^2}$.

Proof. We observe that $p_1 = 3$ yields the smallest possible value $\frac{1}{6}n$ of $M_0(n)$ in (the second subcase of) (6). This requires $3 \mid n$, thus $n \equiv 0 \bmod 12$ or $n \equiv 6 \bmod 12$, which confirms (i).

Since trivially $R_0(n) \leqslant 1$ and the right-hand side of (ii) is greater than 1 for $n \leqslant 6$, we may assume that $n > 6$. Looking at the Taylor expansion of cosine one easily verifies that in this range

$$\left(\cos \frac{\pi}{n}\right)^{-1} < 1 + \frac{10}{\sqrt{3}\, n^2}.$$

By (i) and Corollary 2 it follows that

$$R_0(n) = \frac{\cos \frac{\pi M_0(n)}{n}}{\cos \frac{\pi}{n}} < \left(1 + \frac{10}{\sqrt{3}n^2}\right) \cos \frac{\pi}{6} = \frac{\sqrt{3}}{2} + \frac{5}{n^2}. \qquad \square$$

Theorem 9 also implies that the sizes of geometric kernels of certain integral circulant graphs $\mathrm{ICG}(n, \mathcal{D})$ all by themselves reveal information about the residue class of n mod 12 and the smallest odd prime divisor of n. Notice, however, that there is no such information in case n is divisible by 4.

Corollary 11. *Let $n \geqslant 18$ be an integer and $\varnothing \neq \mathcal{D} \subseteq \mathfrak{D}^*(n)$.*

(i) If $m_0(n, \mathcal{D}) < \frac{1}{3}n$ or if $\rho_0(n, \mathcal{D}) \geqslant \frac{1}{2}(1 + \frac{5}{n^2})$, then n is even.

(ii) If $m_0(n, \mathcal{D}) < \frac{1}{4}n$ or if $\rho_0(n, \mathcal{D}) \geqslant \frac{\sqrt{2}}{2}(1 + \frac{5}{n^2})$, then $n \equiv 2 \mod 4$ or $12 \mid n$.

(iii) For odd n the smallest prime divisor p_1 of n satisfies

$$p_1 \leqslant \min\left\{\frac{1}{1 - \frac{2m_0(n, \mathcal{D})}{n}}, \frac{\pi}{2\rho_0(n, \mathcal{D})}\left(1 + \frac{5}{n^2}\right)\right\} < \frac{8}{5\rho_0(n, \mathcal{D})}.$$

(iv) For $n \equiv 2 \mod 4$ the smallest odd prime divisor p_1 of n satisfies

$$p_1 \leqslant \min\left\{\frac{2}{1 - \frac{2m_0(n, \mathcal{D})}{n}}, \frac{\pi}{\rho_0(n, \mathcal{D})}\left(1 + \frac{5}{n^2}\right)\right\} < \frac{16}{5\rho_0(n, \mathcal{D})}.$$

Proof. The Taylor expansion of cosine gives that for $n \geqslant 18$

$$\left(\cos\frac{\pi}{n}\right)^{-1} < 1 + \frac{5}{n^2}. \tag{10}$$

For odd n with smallest prime factor p_1, Theorem 9 implies that

$$m_0(n, \mathcal{D}) \geqslant M_0(n) = \frac{1}{2}\left(1 - \frac{1}{p_1}\right)n \geqslant \frac{1}{2}\left(1 - \frac{1}{3}\right)n = \frac{1}{3}n$$

and, by virtue of (10), that

$$\rho_0(n, \mathcal{D}) \leqslant R_0(n) = \frac{\sin\frac{\pi}{2p_1}}{\cos\frac{\pi}{n}} \leqslant \frac{\sin\frac{\pi}{6}}{\cos\frac{\pi}{n}} < \frac{1}{2}\left(1 + \frac{5}{n^2}\right).$$

These inequalities prove (i).

By (i) we know that n is even under any of the two assumptions of (ii). If such an even integer satisfies $n \not\equiv 2 \mod 4$ and $12 \nmid n$, i.e. $n \equiv 4 \mod 12$ or $n \equiv 8 \mod 12$, then Theorem 9 implies $m_0(n, \mathcal{D}) \geqslant M_0(n) = \frac{1}{4}n$ and, again using (10),

$$\rho_0(n, \mathcal{D}) \leqslant R_0(n) = \frac{\sqrt{2}}{2\cos\frac{\pi}{n}} < \frac{\sqrt{2}}{2}\left(1 + \frac{5}{n^2}\right).$$

These inequalities confirm (ii).

For an odd n with smallest prime factor p_1 it follows from (6) that $m_0(n, \mathcal{D}) \geqslant M_0(n) = \frac{1}{2}(1 - \frac{1}{p_1})n$, and by (7), (10) and $\sin x \leqslant x$ that

$$\rho_0(n, \mathcal{D}) \leqslant R_0(n) = \frac{\sin\frac{\pi}{2p_1}}{\cos\frac{\pi}{n}} < \frac{\pi}{2p_1}\left(1 + \frac{5}{n^2}\right) < \frac{8}{5p_1}.$$

These inequalities imply (iii). With respect to (iv) we similarly obtain that $m_0(n, \mathcal{D}) \geqslant M_0(n) = \frac{1}{2}(1 - \frac{2}{p_1})n$ and that

$$\rho_0(n, \mathcal{D}) \leqslant R_0(n) = \frac{\sin\frac{\pi}{p_1}}{\cos\frac{\pi}{n}} < \frac{\pi}{p_1}\left(1 + \frac{5}{n^2}\right) < \frac{16}{5p_1}. \qquad \square$$

5 The kernel radius on average

Given a positive integer n the kernel radii $\rho_0(n, \mathcal{D})$ may vary quite a lot for different divisor sets $\mathcal{D}$. Therefore, we finally address the problem of the kernel radius on average.

The number of divisor sets $\mathcal{D}$ of n naturally depends on the number of positive divisors of n, denoted by $\tau(n)$. The divisor function $\tau(n)$ is well studied in number theory. While it possesses the useful arithmetic property of being *multiplicative*, i.e. $\tau(m \cdot n) = \tau(m) \cdot \tau(n)$ for all coprime m and n, its growth behaviour is rather erratic: $\tau(p) = 2$ for all primes p, but $\tau(n)$ tends to infinity on certain subsequences of (highly composite) positive integers n. This is expressed by saying that $\tau(n)$ does not have a *normal order*, i.e. there is no function $f(n)$ satisfying "reasonable" smoothness criteria, e.g. monotonicity, such that $(1 - \varepsilon)f(n) < \tau(n) < (1 + \varepsilon)f(n)$ for any $\varepsilon > 0$ and almost all n (cf. [4, Chapter 4.4] or [5, Chapters 22.11 and 22.13]). However, $\log \tau(n)$ does have a normal order (see Proposition 12).

Although we have infinitely many of them, primes are "rare" among the positive integers. Using elementary combinatorial arguments much weaker than the *prime number theorem* (cf. [1] or [5, Theorem 6] the claim can be made precise by the statement that the relative frequency of primes among positive integers below a bound N tends to 0:

$$\lim_{N \to \infty} \frac{|\{p \leqslant N : \ p \text{ prime}\}|}{|\{1, 2, 3, \dots, N\}|} = \lim_{N \to \infty} \frac{|\{p \leqslant N : \ p \text{ prime}\}|}{N} = 0. \tag{11}$$

More generally, given any increasing sequence $(a_n)_{n=1,2,3,\dots}$ of positive integers such that $\lim_{N \to \infty} \frac{|\{a_n \leqslant N : \ n=1,2,3,\dots\}|}{N} = \alpha$ exists, α is called the *asymptotic density* of the sequence. Clearly, $0 \leqslant \alpha \leqslant 1$. In particular the sequence of primes has asymptotic density 0 by (11). Any statement which is true for all positive integers in a sequence of asymptotic density 1 is said to hold for *almost all* positive integers. In this case the so-called *exceptional set* of positive integers, i.e. those for which the statement does not hold, has asymptotic density 0.

Since the irregular oscillation of the divisor function will have consequences in our setting, we record the well-known correlating properties of $\tau(n)$ in

Proposition 12 (cf. [1, Theorem 13.12] or [5, Theorem 432]). *Given any $\varepsilon > 0$, we have*

$$(\log n)^{\log 2 - \varepsilon} < \tau(n) < (\log n)^{\log 2 + \varepsilon}$$

for almost all positive integers n, where $\log$ *denotes the natural logarithm.*

In order to apply results on $\tau(n)$ for our purposes, we define for $n \geqslant 3$

$$\tau^*(n) := \begin{cases} \tau(n) - 1 & \text{if } n \text{ is odd,} \\ \tau(n) - 2 & \text{if } n \text{ is even.} \end{cases}$$

Clearly $\tau^*(n) = |\mathfrak{D}^*(n)|$. Consequently,

$$|\{\mathcal{D} \subseteq \mathfrak{D}^*(n) : \ \mathcal{D} \neq \varnothing\}| = 2^{\tau^*(n)} - 1. \tag{12}$$

Given any fixed $n \geqslant 3$, this implies that

$$\overline{m_0(n)} := \frac{1}{2^{\tau^*(n)} - 1} \sum_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \mathcal{D} \neq \varnothing}} m_0(n, \mathcal{D})$$

is the arithmetic mean of $m_0(n, \mathcal{D})$ over all non-empty $\mathcal{D} \subseteq \mathfrak{D}^*(n)$. By definition we have $0 < m_0(n, \mathcal{D}) < \frac{n}{2}$ for all n and $\mathcal{D}$, so trivially

$$0 < \frac{\overline{m_0(n)}}{n} < \frac{1}{2} \qquad (n \geqslant 3).$$

Before we prove in Theorem 15 below that $\frac{\overline{m_0(n)}}{n}$ usually lies arbitrarily close to $\frac{1}{2}$ for sufficiently large n, let us look at some exceptional integers n.

Example 13. Consider $n = 3p$ for primes $p \geqslant 5$. The appropriate divisors of n are $1, 3, p$. Hence $\tau^*(n) = 3$, and we have $2^{\tau^*(n)} - 1 = 7$ appropriate divisor sets, namely four with least element 1, two with least element 3 and one with least element p. Since n is odd, all $\gamma_{n,d} = 1$ in Theorem 8. Consequently we obtain by (5) that

$$\frac{\overline{m_0(3p)}}{3p} = \frac{1}{7 \cdot 3p \cdot 2}\big(4 \cdot (3p - 1) + 2 \cdot (3p - 3) + (3p - p)\big) = \frac{1}{2} - \frac{5}{21p} - \frac{1}{42} < \frac{1}{2} - \frac{1}{42}.$$

This shows that the sequence $\big(\frac{\overline{m_0(3p)}}{3p}\big)_{p=5,7,11,13,\dots}$ stays away from $\frac{1}{2}$ for primes $p \to \infty$.

Proposition 14. *Let $n \geqslant 3$ and let $1 = d_1 < d_2 < \dots < d_{\tau^*(n)} < \frac{n}{2}$ be all of the appropriate divisors of n. Then we have*

$$\frac{2^{\tau^*(n)}}{2^{\tau^*(n)} - 1} \sum_{i=1}^{\tau^*(n)} \frac{d_i}{2^i} \quad \leqslant \quad \frac{n}{2} - \overline{m_0(n)} \quad \leqslant \quad 4 \cdot \frac{2^{\tau^*(n)}}{2^{\tau^*(n)} - 1} \sum_{i=1}^{\tau^*(n)} \frac{d_i}{2^i}. \qquad (13)$$

Proof. We have by Theorem 8 and (12) that

$$\overline{m_0(n)} = \frac{1}{2^{\tau^*(n)} - 1} \sum_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \mathcal{D} \neq \varnothing}} \frac{1}{2}\bigg(n - \min_{d \in \mathcal{D}} \gamma_{n,d}\, d\bigg) = \frac{n}{2} - \frac{1}{2^{\tau^*(n)} - 1} \sum_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \mathcal{D} \neq \varnothing}} \min_{d \in \mathcal{D}} \gamma_{n,d}\, d.$$

Since $1 \leqslant \gamma_{n,d} \leqslant 4$, it follows that

$$\frac{1}{2^{\tau^*(n)} - 1} \sum_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \mathcal{D} \neq \varnothing}} \min_{d \in \mathcal{D}} d \leqslant \frac{n}{2} - \overline{m_0(n)} \leqslant \frac{1}{2^{\tau^*(n)} - 1} \sum_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \mathcal{D} \neq \varnothing}} 4 \cdot \min_{d \in \mathcal{D}} d. \qquad (14)$$

We have

$$\sum_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \mathcal{D} \neq \varnothing}} \min_{d \in \mathcal{D}} d = \sum_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \mathcal{D} \neq \varnothing}} \min \mathcal{D} = \sum_{i=1}^{\tau^*(n)} \sum_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \min \mathcal{D} = d_i}} \min \mathcal{D}$$

$$= \sum_{i=1}^{\tau^*(n)} d_i \big|\{\mathcal{D} \subseteq \mathfrak{D}^*(n) : \min \mathcal{D} = d_i\}\big| = \sum_{i=1}^{\tau^*(n)} d_i 2^{\tau^*(n) - i}.$$

Integrating this identity in (14) yields (13). $\qquad \square$

Example 13 shows that there are infinitely many, i.e. arbitrarily large n satisfying $\frac{\overline{m_0(n)}}{n} < \frac{1}{2} - \frac{1}{42}$. This reveals that the next result cannot hold for more than almost all integers n.

Theorem 15. *For any $\varepsilon > 0$ and almost all $n \geqslant 3$ we have*

$$\frac{1}{2} - 2^{-(\log n)^{\log 2 - \varepsilon}} < \frac{\overline{m_0(n)}}{n} < \frac{1}{2}. \tag{15}$$

Remark 16.

(i) Clearly, any function of type n^κ with (small) real $\kappa > 0$ is growing faster than any function of type $(\log n)^K$ with (large) K if $n \to \infty$. Functions of type $C^{(\log n)^\delta}$ with real $C > 1$ and $0 < \delta < 1$ are lying inbetween these two classes of functions and belong to the standard fine-tuning accessories of analytic number theory to compare and classify the growth of arithmetic functions.

(ii) Theorem 15 certainly implies that given any $\varepsilon > 0$ the set $\{n \geqslant 3 : \frac{1}{2} - \varepsilon < \frac{\overline{m_0(n)}}{n} < \frac{1}{2}\}$ has asymptotic density one. However our statement about the set of integers $n \geqslant 3$ satisfying (15) is much stronger, since it tells us that $\frac{1}{2} - \varepsilon < \frac{\overline{m_0(n)}}{n} < \frac{1}{2}$ still holds for almost all n even if we shrink the interval in the specified manner with increasing n.

Proof of Theorem 15. Let $1 = d_1 < d_2 < \ldots < d_{\tau^*(n)} < \ldots < d_{\tau(n)} = n$ be all positive divisors of n, the first $\tau^*(n)$ of them being the appropriate ones. By Proposition 14 we know that

$$\frac{\overline{m_0(n)}}{n} > \frac{1}{2} - \frac{2^{\tau^*(n)}}{2^{\tau^*(n)} - 1} \cdot \frac{4}{n} \sum_{i=1}^{\tau^*(n)} \frac{d_i}{2^i} \geqslant \frac{1}{2} - \frac{8}{n} \sum_{i=1}^{\tau^*(n)} \frac{d_i}{2^i} \tag{16}$$

for all $n \geqslant 3$. We have $d \mid n$ for some $d < \sqrt{n}$ if and only if $\frac{n}{d} \mid n$ with $\frac{n}{d} > \sqrt{n}$, giving an even number of divisors of n. There is an additional divisor $\sqrt{n}$ if n happens to be a square, and $\tau(n)$ is odd exactly in this special situation. If n is not a square, i.e. $\tau(n)$ is even, the smallest divisor $d > \sqrt{n}$ of n is $d_{\frac{\tau(n)}{2}+1}$. If n is a square, i.e. $\tau(n)$ is odd, the smallest divisor $d > \sqrt{n}$ of n is $d_{\frac{\tau(n)+1}{2}+1}$. Combining the two cases, $d = d_{\lceil \frac{\tau(n)}{2} \rceil + 1}$ is the smallest divisor $d > \sqrt{n}$ of any $n \geqslant 3$. Since $d_i < \frac{n}{2}$ for $i \leqslant \tau^*(n)$, we obtain

$$\sum_{i=1}^{\tau^*(n)} \frac{d_i}{2^i} = \sum_{\substack{i=1 \\ d_i \leqslant \sqrt{n}}}^{\tau^*(n)} \frac{d_i}{2^i} + \sum_{\substack{i=1 \\ d_i > \sqrt{n}}}^{\tau^*(n)} \frac{d_i}{2^i} < \sqrt{n} \sum_{i=1}^{\tau^*(n)} \frac{1}{2^i} + \frac{n}{2} \sum_{i=\lceil \frac{\tau(n)}{2} \rceil + 1}^{\tau^*(n)} \frac{1}{2^i}$$

$$< \sqrt{n} \sum_{i=1}^{\infty} \frac{1}{2^i} + \frac{n}{2} \sum_{i=\lceil \frac{\tau(n)}{2} \rceil + 1}^{\infty} \frac{1}{2^i} = \sqrt{n} + \frac{n}{2} \cdot 2^{-\lceil \frac{\tau(n)}{2} \rceil} < \sqrt{n} + \frac{n}{2^{\frac{\tau(n)}{2}+1}} \tag{17}$$

for all $n \geqslant 3$. Then (16) and Proposition 12 finally imply that

$$\frac{1}{2} - \frac{\overline{m_0(n)}}{n} < \frac{8}{\sqrt{n}} + 2^{-\frac{\tau(n)}{2}+2}$$

$$< \frac{8}{\sqrt{n}} + 2^{-\frac{1}{2}(\log n)^{\log 2 - \frac{\varepsilon}{2}}+2} = 2^{-\frac{\log n}{2\log 2}+3} + 2^{-\frac{1}{2}(\log n)^{\log 2 - \frac{\varepsilon}{2}}+2} < 2^{-(\log n)^{\log 2 - \varepsilon}}$$

for almost all n, where the last inequality can be verified for all sufficiently large n by careful comparison of the three exponents. This completes the proof of our theorem. $\quad\square$

By analogy with the definition of $\overline{m_0(n)}$ let

$$\overline{\rho_0(n)} := \frac{1}{2^{\tau^*(n)} - 1} \sum_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \mathcal{D} \neq \varnothing}} \rho_0(n, \mathcal{D})$$

for any fixed $n \geqslant 3$, i.e. the average of all kernel radii. Since $0 < \rho_0(n, \mathcal{D}) \leqslant 1$ for all $n \geqslant 3$ and all divisor sets $\mathcal{D}$ of n, we trivially have $0 < \overline{\rho_0(n)} \leqslant 1$ $(n \geqslant 3)$.

Corollary 17. *For any $\varepsilon > 0$ and almost all $n \geqslant 3$ we have $0 < \overline{\rho_0(n)} < 2^{-(\log n)^{\log 2 - \varepsilon}}$.*

Proof. Let $\varepsilon > 0$ be given. According to Theorem 15

$$\frac{n}{2} - \frac{n}{2^{(\log n)^{\log 2 - \frac{\varepsilon}{4}}}} < \overline{m_0(n)} < \frac{n}{2} \tag{18}$$

for almost all n. Let $n \geqslant 3$ be any integer satisfying (18), and let $\Delta_\varepsilon(n)$ denote the set of all non-empty divisor sets $\mathcal{D} \subseteq \mathfrak{D}^*(n)$ such that

$$m_0(n, \mathcal{D}) < \frac{n}{2} - \frac{n}{2^{(\log n)^{\log 2 - \frac{\varepsilon}{2}}}}. \tag{19}$$

Since $m_0(n, \mathcal{D}) < \frac{n}{2}$ by definition, we obtain

$$\overline{m_0(n)} = \frac{1}{2^{\tau^*(n)} - 1} \sum_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \mathcal{D} \neq \varnothing}} m_0(n, \mathcal{D}) =$$

$$= \frac{1}{2^{\tau^*(n)} - 1} \left(\sum_{\mathcal{D} \in \Delta_\varepsilon(n)} m_0(n, \mathcal{D}) + \sum_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \mathcal{D} \neq \varnothing,\, \mathcal{D} \notin \Delta_\varepsilon(n)}} m_0(n, \mathcal{D}) \right)$$

$$< \frac{1}{2^{\tau^*(n)} - 1} \left(|\Delta_\varepsilon(n)| \left(\frac{n}{2} - \frac{n}{2^{(\log n)^{\log 2 - \frac{\varepsilon}{2}}}} \right) + \left(2^{\tau^*(n)} - 1 - |\Delta_\varepsilon(n)| \right) \frac{n}{2} \right)$$

$$= \frac{n}{2} - \frac{n}{(2^{\tau^*(n)} - 1) \cdot 2^{(\log n)^{\log 2 - \frac{\varepsilon}{2}}}} |\Delta_\varepsilon(n)|.$$

Together with the lower bound in (18) it follows that

$$|\Delta_\varepsilon(n)| < (2^{\tau^*(n)} - 1) \cdot 2^{(\log n)^{\log 2 - \frac{\varepsilon}{2}} - (\log n)^{\log 2 - \frac{\varepsilon}{4}}} < (2^{\tau^*(n)} - 1) \cdot 2^{-(\log n)^{\log 2 - \frac{\varepsilon}{2}}},$$

if n is sufficiently large. This, Corollary 2, (19) and basic properties of cosine and sine imply for sufficiently large n satisfying (18), i.e. for almost all n, that

$$0 < \overline{\rho_0(n)} = \frac{1}{2^{\tau^*(n)} - 1} \sum_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \mathcal{D} \neq \varnothing}} \frac{\cos \frac{\pi m_0(n, \mathcal{D})}{n}}{\cos \frac{\pi}{n}}$$

$$= \frac{1}{(2^{\tau^*(n)} - 1) \cos \frac{\pi}{n}} \left(\sum_{\mathcal{D} \in \Delta_\varepsilon(n)} \cos \frac{\pi m_0(n, \mathcal{D})}{n} + \sum_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \mathcal{D} \neq \varnothing, \, \mathcal{D} \notin \Delta_\varepsilon(n)}} \cos \frac{\pi m_0(n, \mathcal{D})}{n} \right)$$

$$\leqslant \frac{1}{(2^{\tau^*(n)} - 1) \cos \frac{\pi}{n}} \left(\sum_{\mathcal{D} \in \Delta_\varepsilon(n)} 1 + \sum_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \mathcal{D} \neq \varnothing, \, \mathcal{D} \notin \Delta_\varepsilon(n)}} \cos \left(\frac{\pi}{n} \left(\frac{n}{2} - \frac{n}{2^{(\log n)^{\log 2 - \frac{\varepsilon}{2}}}} \right) \right) \right)$$

$$\leqslant \frac{1}{(2^{\tau^*(n)} - 1) \cos \frac{\pi}{n}} \left(|\Delta_\varepsilon(n)| + \sum_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(n) \\ \mathcal{D} \neq \varnothing}} \cos \left(\frac{\pi}{2} - \frac{\pi}{2^{(\log n)^{\log 2 - \frac{\varepsilon}{2}}}} \right) \right)$$

$$< \frac{1}{\cos \frac{\pi}{n}} \left(2^{-(\log n)^{\log 2 - \frac{\varepsilon}{2}}} + \sin \frac{\pi}{2^{(\log n)^{\log 2 - \frac{\varepsilon}{2}}}} \right)$$

$$< 2 \cdot \left(2^{-(\log n)^{\log 2 - \frac{\varepsilon}{2}}} + \frac{2\pi}{2^{(\log n)^{\log 2 - \frac{\varepsilon}{2}}}} \right)$$

$$< 2^{-(\log n)^{\log 2 - \varepsilon}}. \qquad \qquad \square$$

In continuation of Example 13 the following shows that Corollary 17 cannot hold for more than almost all n.

Example 18. For all $n = 3p$ with a prime $p \geqslant 5$, thus $\tau^*(n) = 3$, we have by Corollary 2 and Theorem 8 that

$$\overline{\rho_0(3p)} = \frac{1}{2^{\tau^*(3p)} - 1} \sum_{\substack{\mathcal{D} \subseteq \mathfrak{D}^*(3p) \\ \mathcal{D} \neq \varnothing}} \rho_0(3p, \mathcal{D})$$

$$> \frac{1}{7} \cdot \rho_0(3p, \{p\}) = \frac{1}{7} \cdot \frac{\cos \frac{\pi m_0(3p, \{p\})}{3p}}{\cos \frac{\pi}{3p}}$$

$$> \frac{1}{7} \cdot \cos \frac{\pi \cdot \frac{1}{2}(3p - p)}{3p} = \frac{1}{7} \cdot \cos \frac{\pi}{3} = \frac{1}{14}.$$

Acknowledgements

References

[1] T. M. Apostol. Introduction to Analytic Number Theory. Springer Verlag, Berlin-Heidelberg-New York, 1976.

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

[3] E. Dobson and J. Morris. Toida's conjecture is true. *Electronic J. Combinatorics*, 9:#R35, 2002.

[4] R. R. Hall and G. Tenenbaum. Divisors. Cambridge University Press, 1988.

[5] G. H. Hardy and E. M. Wright. An Introduction to the Theory of Numbers. 6th ed., Oxford University Press, 2011.

[6] M. Klin and I. Kovács. Automorphism groups of rational circulant graphs. *Electronic J. Combinatorics*, 19:#P35, 2012.

[7] W. Klotz and T. Sander. Some properties of unitary Cayley graphs. *Electronic J. Combinatorics*, 14:#R45, 2007.

[8] T. A. Le and J. W. Sander. Convolutions of Ramanujan sums and integral circulant graphs. *Int. J. Number Theory*, 8:1777–1788, 2012.

[9] T. A. Le and J. W. Sander. Extremal energies of integral circulant graphs via multiplicativity, *Linear Algebra Appl.*, 437:1408–1421, 2012.

[10] M. E. Muzychuk. On the structure of basic sets of Schur rings over cyclic groups. *J. Algebra*, 169:655–678, 1994.

[11] J. W. Sander. Integral circulant Ramanujan graphs via multiplicativity and ultrafriable integers. *Linear Algebra Appl.*, 477:21–41, 2015.

[12] J. W. Sander. On the kernel of integral circulant graphs. *Linear Algebra Appl.*, 549:79–85, 2018.

[13] J. W. Sander. Structural properties and formulae of the spectra of integral circulant graphs, *Acta Arith.*, 184:297–315, 2018.

[14] J. W. Sander. Holes in lace doilies: The geometric kernel of circulant graphs. *Elemente Math.*, electr. publ. https://doi.org/10.4171/EM/435 (to appear in print), 2021.

[15] J. W. Sander and T. Sander. On So's conjecture for integral circulant graphs. *Appl. Anal. Discrete Math.*, 9:59–72, 2015.

[16] W. So. Integral circulant graphs. *Discrete Math.*, 306:153–158, 2005.