ON GCD-GRAPHS OVER FINITE RINGS

TUNG T. NGUYEN, NGUYỄN DUY TÂN

ABSTRACT. Gcd-graphs represent an interesting and historically important class of integral graphs. Since the pioneering work of Klotz and Sander, numerous incarnations of these graphs have been explored in the literature. In this article, we define and establish some foundational properties of gcd-graphs defined over a general finite commutative ring. In particular, we investigate the connectivity and diameter of these graphs. Additionally, when the ring is a finite symmetric $\mathbb{Z}/n$-algebra, we give an explicit description of their spectrum using the theory of Ramanujan sums that gives a unified treatment of various results in the literature.

1. INTRODUCTION AND MOTIVATIONS

Gcd-graphs are an interesting and historically important class of integral graphs; i.e., graphs whose eigenvalues are integers. These graphs are first introduced by Klotz and Sander in [5]. To set the context, let us briefly recall the definition of gcd-graphs. Let n be a positive integer and D a subset of proper divisors of n. The gcd-graph $G_n(D)$ is defined as follows: (1) The vertices of $G_n(D)$ are elements of the finite ring $\mathbb{Z}/n$ and (2) two vertices a, b are adjacent if $\gcd(a-b, n) \in D$. Using the theory of Ramanujan sums, one can describe the spectrum of the gcd-graphs $G_n(D)$ explicitly (see [5, Section 4]). More precisely, its eigenvalues are indexed by elements of $\mathbb{Z}/n$; namely $(\lambda_m)_{m \in \mathbb{Z}/n}$ where

$$\lambda_m = \sum_{d \in D} c(m, n/d), \tag{1.1}$$

and

$$c(m, n/d) = \mu(t)\frac{\varphi(n/d)}{\varphi(t)}, \quad \text{where} \quad t = \frac{n/d}{\gcd(n/d, m)}. \tag{1.2}$$

Here μ and φ are respectively the Möbius and Euler totient functions. A direct corollary of this explicit description is that gcd-graphs are integral. In [10], So goes one step further: he shows that gcd-graphs are the only integral circulant graphs. In [7], inspired by the analogy between number fields and function fields, we study gcd-graphs over a polynomial ring with coefficients in a finite field. We show that in this case, there

2020 *Mathematics Subject Classification.* Primary 05C25, 11L05, 13A70, 13M05.

Key words and phrases. Gcd graphs, Finite rings, Ramanujan sums, Integral graphs.

TTN is partially supported by an AMS-Simons Travel Grant. NDT is partially supported by the Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 101.04-2023.21.

is a direct analog of Ramanujan sums that allows us to describe the spectrum of these gcd-graphs by an explicit formula similar to Eq. (1.1). Additionally, in [8], we generalize So's theorem by giving the necessary and sufficient conditions for a Cayley graph over a finite symmetric algebra to be integral. As a by-product of this work, we construct examples of finite symmetric algebras with arithmetic origins.

The goal of this article is to define and study the concept of gcd-graphs over arbitrary finite rings. We hope to unify various constructions in the literature and lay the groundwork for this area of research. In particular, we generalize some existing results in [5, 7, 8, 9] to this general setting.

1.1. **Outline.** In Section 2 we introduce the notion of gcd-graphs over a finite ring which naturally generalizes some previous work in [5, 7]. We also discuss various equivalence conditions for a graph to be a gcd-graph. As a by-product, we describe explicitly the structure of the generating set in a gcd-graph. In Section 3, we investigate the connectivity of a gcd-graph. In particular, we provide a sharp upper bound on the diameter of a gcd-graph which generalizes a theorem of Saxena, Severini, and Shparlinski in [9]. Finally, in Section 4, we describe explicitly the spectrum of a gcd-graph over a finite symmetric algebra. The main result of this section gives a unified treatment for the spectra of various gcd-graphs previously studied in the literature.

2. Gcd-graphs over a finite ring

In this section, we introduce the notion of a gcd-graph defined over a finite ring that unifies the definitions in [5, 7]. Let us first recall the definition of a Cayley graph defined over a finite ring.

Definition 2.1. Let R be a finite ring and $S \subset R \setminus \{0\}$ a symmetric subset. The Cayley graph $\Gamma(R, S)$ is defined as follow

(1) The vertex set of $\Gamma(R, S)$ is R.
(2) Two vertices $x, y \in R$ are adjacent if $x - y \in S$.

In practice, S is often called the generating set for $\Gamma(R, S)$.

As noted in [3, Section 4] and further supported by [7, 8], Cayley graphs defined over a ring exhibit richer structures compared to those defined over abstract abelian groups. This feature arises from the interaction between the additive and multiplicative structures of the ring R. In particular, ideals play a fundamental role in the studying of these graphs.

For a ring that is not necessarily a quotient of a principal ideal domain, the notion of the greatest common divisor is not well defined. As a result, to define gcd-graphs over such a ring, we first need to revisit the definition of the greatest common divisor. We recall that a positive integer n and two integers a, b, $\gcd(a, n) = \gcd(b, n)$ if and only if a and b generate the same ideal in the ring $\mathbb{Z}/n$. This is also equivalent to the condition that $a \equiv ub \pmod{n}$ for some $u \in (\mathbb{Z}/n)^{\times}$. This property generalizes well for Artinian rings, and in particular, to finite rings. More precisely

Lemma 2.2. *(See* [4, Lemma 2.1] *Let R be an Artining ring. If $Ra = Rb$, then there exists $u \in R^{\times}$ such that $b = ua$.*

From this perspective, a crucial observation here is that a generating set S in a finite ring R such as $\mathbb{Z}/n$ or $\mathbb{F}_q[x]$ gives rise to a gcd-graph if and only if S is stable under the action of $R^{\times}$; that is, if $s \in S$, then $us \in S$ for all $u \in R^{\times}$. Motivated by this observation, we introduce the following definition.

Definition 2.3. We say that $\Gamma(R, S)$ is a gcd-graph if S is stable under the action of $R^{\times}$.

Remark 2.4. When $S = R^{\times}$, the graph $\Gamma(R, R^{\times})$ is known as a unitary Cayley graph (see [1, 5]). This shows that the unitary Cayley graph over R is a special case of gcd-graphs. Other examples, as explained previously, include the gcd-graphs defined in [5] for the ring $\mathbb{Z}/n$ and the gcd-graphs defined in [7] for the ring $\mathbb{F}_q[x]/f$ where $\mathbb{F}_q$ is a finite field with q elements and f is a non-zero polynomial in $\mathbb{F}_q[x]$.

We provide below the necessary and sufficient conditions for a Cayley graph over R to be a gcd-graph. These conditions are somewhat more explicit than Definition 2.3. Furthermore, together with Corollary 2.7, this description will be important later on when we study the spectrum of these gcd-graphs.

Proposition 2.5. *Let R be a finite commutative ring and S a subset of R. Then the following are equivalent.*

(1) $\Gamma(R, S)$ is a gcd-graph.

(2) There exist distinct nonzero principal ideals $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_k$ such that for each $r \in R$, $r \in S$ if and only if there exists $1 \leq i \leq k$ such that $\mathcal{I}_i = Rr$.

Proof. First, we claim that $(2) \implies (1)$. Clearly, S is symmetric and $0 \notin S$. By definition, we need to show that if $s \in S$ and $u \in R^{\times}$ then $us \in S$. Since $s \in S$, there exists an ideal $\mathcal{I}_i$ with $1 \leq i \leq k$ such that $Rs = \mathcal{I}_k$. Since $u \in R^{\times}$, $\mathcal{I}_k = Rs = Rus$. By (2), this shows that $us \in S$.

Let us show that (1) implies (2) as well. For each $s \in S$, Let $\mathcal{I}_s = Rs$ be the ideal generated by s. Let $\{\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_k\}$ be the set of all $\mathcal{I}_s$. We conclude that for each $s \in S$, $\mathcal{I}_s = \mathcal{I}_i$ for some $1 \leq i \leq k$. Conversely, if $r \in R$ such that $Rr \in \{\mathcal{I}_1, \ldots, \mathcal{I}_k\}$, then $Rr = Rs$ for some $s \in S$. By Lemma 2.2, we know that $r = us$ for some $u \in R^{\times}$. Since $\Gamma(R, S)$ is a gcd-graph, S is stable under the action of $R^{\times}$. This shows that $r \in S$ as well. □

By Proposition 2.5 and to be consistent with the literature, we will denote the gcd-graph $\Gamma(R, S)$ by $G_R(D)$ where $D = \{\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_k\}$. Our next goal is to provide an explicit description of the generating set S for a gcd-graph $\Gamma(R,S)$. To do so, we first recall the following definition from ring theory.

Definition 2.6. Let T be a subset of R. The annihilator ideal $\mathrm{Ann}_R(T)$ is defined as

$$\mathrm{Ann}_R(T) = \{a \in R \mid at = 0 \text{ for all } t \in T\}.$$

With this definition, we can now explicitly describe the generating set S.

Corollary 2.7. *Let $\Gamma(R,S) = G_R(D)$ be a gcd-graph where $D = \{\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_k\}$. Suppose that $\mathcal{I}_i = Rx_i$. Then every element $s \in S$ can be written uniquely in the form $s = \hat{u}x_i$ for some $1 \le i \le k$, $u \in (R/\mathrm{Ann}_R(\mathcal{I}_i))^\times$, and $\hat{u}$ is a lift of u in $R^\times$.*

Proof. By Proposition 2.5, every $s \in S$ can be written in the form $s = \hat{u}x_i$ for some $1 \le i \le k$ and $\hat{u} \in R^\times$. By definition, if $u_1 \equiv u_2 \pmod{\mathcal{I}_i}$ then $u_1 x_i = u_2 x_i$. Therefore, the expression $s = \hat{u}x_i$ only depends on the class of $\hat{u} \in (R/\mathrm{Ann}_R(\mathcal{I}_i))^\times$. □

While the requirement that each $\mathcal{I}_i$ is principal seems quite strict, we will show below that finite rings which are quotients of the ring of integers in a global field have this property. To state and prove this statement, we first fix some notations and set up the background. Let K be a global field. Let $\mathcal{O}_K$ be the integral closure in K of $\mathbb{Z}$ if $\mathrm{char}(K) = 0$ or of $\mathbb{F}_q[t]$ if $\mathrm{char}(K) = p > 0$. Let $\mathfrak{a}$ be a nonzero ideal in $\mathcal{O}_K$.

Lemma 2.8. *Let $R = \mathcal{O}_K/\mathfrak{a}$. Then R is a principal ring; i.e., all of its ideals are principal.*

Proof. Let $\mathfrak{a} = \prod_{i=1}^d \mathfrak{p}_i^{e_i}$ be the factorization of $\mathfrak{a}$ into a product of distinct prime ideals. Then

$$R = \mathcal{O}_K/\mathfrak{a} \cong \prod_{i=1}^d \mathcal{O}_K/\mathfrak{p}_i{}^{e_i} \cong \prod_{i=1}^d (\mathcal{O}_K)_{\mathfrak{p}_i}/\mathfrak{p}_i{}^{e_i}.$$

Here $(\mathcal{O}_K)_{\mathfrak{p}_i}$ is the completion of $\mathcal{O}_K$ at $\mathfrak{p}_i$. It is known that $(\mathcal{O}_K)_{\mathfrak{p}_i}$ is a discrete valuation ring, and in particular, a principal ideal domain. This implies that each factor $(\mathcal{O}_K)_{\mathfrak{p}_i}/\mathfrak{p}_i{}^{e_i}$ is a principal ideal ring. Consequently, $\mathcal{O}_K/\mathfrak{a}$ is a principal ideal ring as well. □

Remark 2.9. By [8, Proposition 2.1], if R is a finite ring and $\Gamma(R,S)$ is a gcd-graph, then $\Gamma(R,S)$ is integral. In Section 4, we will provide an explicit description of the spectrum of a gcd-graph when R is a finite symmetric algebra using the theory of generalized Ramanujan sums.

3. Connectivity of gcd-graphs

In this section, we study the connectivity of a gcd-graph $\Gamma(R,S)$. By Proposition 2.5, we can assume that $\Gamma(R,S) = G_R(D)$ where $D = \{\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_k\}$ is a set of principal ideals in R; namely $\mathcal{I}_i = Rx_i$ for some $x_i \in R$. In this setting, the generating set S is precisely the set of s such that $Rs = \mathcal{I}_i$ for some $1 \le i \le k$. Equivalently, there exists $u \in R^\times$ such that $s = ux_i$.

We start with the simplest case which is a direct generalization of [7, Theorem 3.2]. We remark that the proof that we will give is not optimal in the sense that it does not provide a sharp upper bound for the diameter of $G_R(D)$. However, we include it here because it serves as a prototype for our argument in the general case.

Proposition 3.1. *Assume that the unitary Cayley graph G_R is connected. Then $G_R(D)$ is connected if and only if*

$$\mathcal{I}_1 + \cdots + \mathcal{I}_k = R.$$

Here $\mathcal{I}_1 + \cdots + \mathcal{I}_k$ is the sum of these ideals.

Proof. Suppose that $G_R(D)$ is connected. Then S generates R as an abelian group. In particular, we can find $n_1, n_2, \ldots, n_h \in \mathbb{Z}$ and $s_i \in S$ such that

$$1 = n_1 s_1 + n_2 s_2 + \cdots + n_h s_h.$$

Because $Rs_i \in \{\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_k\}$, the above equation shows that $1 \in \mathcal{I}_1 + \mathcal{I}_2 + \cdots + \mathcal{I}_k$. Since this sum is an ideal, we conclude that $\mathcal{I}_1 + \mathcal{I}_2 + \cdots + \mathcal{I}_k = R$.

Conversely, suppose that $\mathcal{I}_1 + \mathcal{I}_2 + \cdots + \mathcal{I}_k = R$. We claim that $G_R(D)$ is connected. Let $a \in R$. By our assumption, we can find $a_1, a_2, \ldots, a_k \in R$ such that $a = \sum_{i=1}^{k} a_i x_i$. Since G_R is connected, for each $1 \leq i \leq k$, we can write $a_i = \sum_{j=1}^{n_i} m_{ij} s_{ij}$, where $m_{ij} \in \mathbb{Z}$ and $s_{ij} \in R^{\times}$. Consequently, we can write

$$a = \sum_{i=1}^{k} \sum_{j=1}^{n_i} m_{ij} s_{ij} x_i.$$

Because $s_{ij} \in R^{\times}$, $s_{ij} x_i \in S$. This shows that a belongs to the abelian group generated by S. Since this is true for all $a \in R$, we conclude that $G_R(D)$ is connected. □

Remark 3.2. We can optimize the proof given in Proposition 3.1 by carefully controlling the number of units s_{ij} that sum up to a_i. By definition, this number is bounded above by the diameter of G_R. The above argument shows that when $G_R(D)$ is connected, its diameter is bounded above by $|D| \text{diag}(G_R)$. We remark that by [1, Theorem 3.1], when G_R is connected, its diameter is at most 3; namely $\text{diag}(G_R) \leq 3$. Consequently, we have a simple estimate $\text{diag}(G_R(D)) \leq 3|D|$. We also note while this upper bound is explicit, it is not optimal in general. We refer to Theorem 3.6 for a better upper bound.

We now modify the above proof to the general case. We start with the following lemma.

Lemma 3.3. *Let R be a finite ring and R' a quotient of R; namely there exists a surjective ring homomorphism $\Phi \colon R \to R'$. Let $D = \{\mathcal{I}_1, \ldots, \mathcal{I}_k\}$ be a set of principal ideals in R and*

$$D' = \{\Phi(\mathcal{I}_1), \ldots, \Phi(\mathcal{I}_k)\},$$

be the image of D in R' (to avoid the tautological case, we adopt the convention of removing $\mathcal{I}_i$ from D' whenever $\Phi(\mathcal{I}_i) = 0$). Then the following statements hold.

(1) $\Phi(\mathcal{I}_i)$ is a principal ideal for each $1 \leq i \leq k$.

(2) Let S' be the generating set in R' associated with D' as described in Proposition 2.5. Then $\Phi(S) \subseteq S'$. Consequently, $\Phi\colon G_R(D) \to G_{R'}(D')$ is a graph morphism.

(3) Suppose that $G_R(D)$ is connected. Then $G_{R'}(D')$ is also connected.

Proof. Let us first prove part (1). Suppose that $\mathcal{I}_i = Rx_i$ for each $1 \leq i \leq k$. Since Φ is surjective, we conclude that $\Phi(\mathcal{I}_i) = R'\Phi(x_i)$. This shows that $\Phi(\mathcal{I}_i)$ is a principal ideal generated by $\Phi(x_i)$.

For the second part, we know from Corollary 2.7 that each $s \in S$ can be written in the form $s = ux_i$ for some $u \in R^{\times}$. We then see that $\Phi(s) = \Phi(u)\Phi(x_i)$. Since $\Phi(u) \in (R')^{\times}$, we conclude that $R'\Phi(s) = R'\Phi(x_i)$ and hence $\Phi(s) \in S'$. This shows that $\Phi\colon G_R(D) \to G_{R'}(D')$ is a graph homomorphism.

For the last part, since $\Phi\colon G_R(D) \to G_{R'}(D')$ is a graph homomorphism, Φ maps a walk in $G_R(D)$ to a walk in $G_{R'}(D')$. As a result, if $G_R(D)$ is connected, then $G_{R'}(D')$ is also connected. □

We now deal with the general case. As observed in [1, Theorem 3.1] and [3, Lemma 4.33], the obstruction for G_R to be connected is the existence of multiple local factors of R whose residues are $\mathbb{F}_2$. Let us explain in more detail. By the structure theorem, $R \cong \prod_{i=1}^{d} R_i$ where each R_i is a local ring. For simplicity, let us write $R = R_1 \times R_2$ where R_1 (respectively R_2) consists of local factors whose residue fields are $\mathbb{F}_2$ (respectively $\neq \mathbb{F}_2$). Let $J(R_1)$ be the Jacobson radical of R_1. Because R_1 is a finite product of local rings, $J(R_1)$ is the kernel of the map $R_1 \to R_1/J(R_1) \cong \mathbb{F}_2^r$ where r is the number of local factors whose residue fields are $\mathbb{F}_2$. Keeping the same notations, we have the following lemma.

Lemma 3.4. *(See also* [1, Theorem 3.1]*) Let $(T, \mathfrak{m})$ be a local ring whose residue field $T/\mathfrak{m}$ is not $\mathbb{F}_2$. Then every element in T can be written as the sum of two units.*

Proof. Let $a \in T$ and $\bar{a}$ the image of a in $T/\mathfrak{m}$. Since $T/\mathfrak{m}$ has more than 2 elements, we can write $\bar{a} = \bar{u}_1 + \bar{u}_2$ where $\bar{u}_1, \bar{u}_2 \neq 0$. Consequently, there exist $u_1, u_2 \in T$ and $m \in \mathfrak{m}$ such that $a = u_1 + u_2 + m = u_1 + (u_2 + m)$. By their definition, $u_1, u_2 + m \in T^{\times}$. We conclude that every element in T can be written as a sum of two units. □

Corollary 3.5. *Every element in $J(R_1) \times R_2$ can be written as the sum of two units in R.*

Proof. Let $(m, a) \in J(R_1) \times R_2$. By Lemma 3.4, we can write $a = u_1 + u_2$ where $u_1, u_2 \in R_2^{\times}$. Let 2^w be the characteristics of R_1. We then have

$$(m, a) = (1, u_1) + (2^w - 1 + m, u_2).$$

We remark that $2^w - 1 + m \in R_1^{\times}$ since its image in $R_1/J(R_1) = \mathbb{F}_2^r$ is 1 which is a unit. Consequently, $(2^w - 1 + m, u_2) \in R^{\times}$. We conclude that (m, a) is the sum of two units in R. □

Keeping the same notation as above, we are now ready to state and prove the following theorem which is a direct generalization of [9, Theorem 4].

Theorem 3.6. *Let $\Phi : R \to R_1/J(R_1) = \mathbb{F}_2^r$ be the quotient ring homomorphism described above. Then $G_R(D)$ is connected if and only if the following two conditions hold*

(1) $\mathcal{I}_1 + \mathcal{I}_2 + \cdots + \mathcal{I}_k = R$;

(2) The cubelike graph $G_{\mathbb{F}_2^r}(D')$ is connected where

$$D' = \{\Phi(\mathcal{I}_1), \Phi(\mathcal{I}_2), \ldots, \Phi(\mathcal{I}_k)\}.$$

Furthermore, suppose that the above conditions hold. Let t be the smallest value of t such that there exists $1 \leq i_1 < i_2 < \cdots < i_t \leq k$ such that

$$\mathcal{I}_{i_1} + \mathcal{I}_{i_2} + \cdots + \mathcal{I}_{i_t} = R.$$

Then

$$t \leq \text{diag}(G_R(D)) \leq 2t + \text{diag}(G_{\mathbb{F}_2^r}(D')).$$

Proof. By Lemma 3.3, we know that (1) and (2) are necessary conditions. We will show that they are sufficient as well. In fact, we will simultaneously show that $G_R(D)$ is connected and $\text{diag}(G_R(D)) \leq 2t + \text{diag}(G_{\mathbb{F}_2^r}(D'))$. We remark that since the only unit in $\mathbb{F}_2^r$ is 1, the generating set for $G_{\mathbb{F}_2}(D')$ is precisely the set $S' = \{\Phi(x_1), \Phi(x_2), \ldots, \Phi(x_k)\}$ where $\mathcal{I}_k = Rx_k$. Let $a \in R$ be an arbitrary element in R. We claim that the distance from a to 0 is at most $2t + \text{diag}(G_{\mathbb{F}_2^r}(D'))$. In other words, we need to show that a can be written as the sum of at most $2t + \text{diag}(G_{\mathbb{F}_2^r}(D'))$ elements in S.

Since $G_{\mathbb{F}_2}(D')$ is connected, we can write $\Phi(a) = \sum_{i=1}^k n_i \Phi(x_i)$ where $n_i \in \{0, 1\}$ and $\sum_{i=1}^k n_i \leq \text{diag}(G_{\mathbb{F}_2^r})(D')$. Let $b := a - \sum_{i=1}^k n_i x_i \in J(R_1) \times R_2$. By our assumption $\mathcal{I}_{i_1} + \mathcal{I}_{i_2} + \cdots + \mathcal{I}_{i_t} = R$, we can write $1 = \sum_{m=1}^t a_i x_{i_m}$. As a result, we can write $b = \sum_{m=1}^t (ba_i) x_{i_m}$. By Corollary 3.5, for each $1 \leq i \leq t$, we can write (ba_i) as a the sum of two units in R. This shows that b can be written as a sum of at most $2t$ elements in S. Consequently, a can be written as a sum of at most $2t + \text{diag}(G_{\mathbb{F}_2^r}(D'))$ elements in S. Since this is true for all $a \in R$, we conclude that

$$\text{diag}(G_R(D)) \leq 2t + \text{diag}(G_{\mathbb{F}_2^r}(D')).$$

The lower bound $t \leq \text{diag}(G_R(D))$ follows from a similar argument. □

Remark 3.7. The proof for Theorem 3.6 shows $G_R(D)$ and $G_{\mathbb{F}_2^r}(D')$ have the same number of connected components.

In the special case where $R = \mathbb{Z}/n$, our theorem recovers the following estimate in [9, Theorem 3.1].

Corollary 3.8. *Suppose that $r \leq 1$. Then $G_R(D)$ is connected if and only if $\mathcal{I}_1 + \mathcal{I}_2 + \ldots + \mathcal{I}_k = R$. Furthermore, let t be the smallest value of t such that there exists $1 \leq i_1 < i_2 < \cdots < i_t \leq k$ such that*

$$\mathcal{I}_{i_1} + \mathcal{I}_{i_2} + \cdots + \mathcal{I}_{i_t} = R.$$

We then have $\operatorname{diag}(G_R(D)) \leq 2t + 1$.

Proof. If $\mathcal{I}_1 + \mathcal{I}_2 + \ldots + \mathcal{I}_k = R$ then $D' \neq \emptyset$. Since $r \leq 1$, this shows that $G_{\mathbb{F}_2^r}(D')$ is connected and its diameter is at most 1. Theorem 3.6 then shows that $\operatorname{diag}(G_R(D)) \leq 2t + 1$. □

Remark 3.9. In [2], the authors determine the maximum diameter in the family of gcd-graphs over $\mathbb{Z}/n$ for fixed n. It would be interesting to study the same problem for gcd-graphs over an arbitrary ring.

4. Spectrum of $G_R(D)$.

In this section, we describe the spectrum of a gcd-graph $G_R(D)$ over a finite symmetric $\mathbb{Z}/n$ algebra. We first recall this definition.

Definition 4.1. Let R be a finite $\mathbb{Z}/n$-algebra. We say that R is symmetric if there exists a $\mathbb{Z}/n$-linear functional $\psi\colon R \to \mathbb{Z}/n$ such that the kernel of ψ does not contain any non-zero ideal in R.

For the rest of this article, we will assume that R is a finite symmetric $\mathbb{Z}/n$-algebra equipped with a fixed linear functional $\psi\colon R \to \mathbb{Z}/n$. Character theory for the additive group structure of R is quite simple. More specifically, by [8, Propsition 2.3], for each character $\widehat{\psi} \in \operatorname{Hom}(R, \mathbb{C}^\times)$ of R, there exists a unique element $r \in R$ such that for all $t \in R$

$$\widehat{\psi}(t) = \zeta_n^{\psi_r(t)} = \zeta_n^{\psi(rt)}.$$

Here $\zeta_n \in \mathbb{C}$ is a fixed primitive n-root of unity. Let us recall the following standard lemma which we will need later on.

Lemma 4.2. *Let G be an abelian group and $\widehat{\psi}\colon G \to \mathbb{C}^\times$ be a nontrivial character of G. Then $\sum_{g \in G} \widehat{\psi}(g) = 0$.*

Let $x \in R$ and $\psi_x\colon R/\operatorname{Ann}_R(x) \to \mathbb{Z}/n$ be the linear functional defined by

$$\psi_x(\bar{a}) = \psi(ax),$$

here $\bar{a} \in R/\operatorname{Ann}_R(x)$ and a is any lift of $\bar{a}$ in R. We can see that this map is well-defined. Furthermore, we have the following.

Lemma 4.3. *ψ_x is a non-degenerate linear function on $R/\operatorname{Ann}_R(x)$. Consequently, $R/\operatorname{Ann}_R(x)$ is a symmetric $\mathbb{Z}/n$-algebra.*

Proof. Let $R' = R/\operatorname{Ann}_R(x)$. Suppose that ψ_x is degenerate. Then, there exists $b' \in R'$ such that $b' \neq 0$ and $R'b' \subset \ker(\psi_x)$. Let b be a lift of b' to R. Then, by the definition of ψ_x we have $\psi(xbR) = 0$. This implies that the $\ker(\psi)$ contains the ideal Rbx. Since ψ is non-degenerate, $bx = 0$ and hence $b \in \operatorname{Ann}_R(x)$. This would imply that $b' = 0$, which is a contradiction. □

Remark 4.4. It is not true that if R is a finite symmetric algebra, then $R/\mathcal{I}$ is a symmetric algebra for all ideals $\mathcal{I}$ of R. Let us provide a concrete example (see Corollary 4.7 for a more general statement). Let p be a prime number. We claim that $R = \mathbb{F}_p[x,y]/(x^2,y^2)$ is a symmetric algebra. In fact, every element in $r \in R$ can be written in the form

$$r = a_0 + a_1x + a_2y + a_3xy.$$

We define a linear functional $\psi\colon R \to \mathbb{F}_p$ by $\psi(r) = a_3$. We can check that this is a non-degenerate $\mathbb{F}_p$-linear functional on R. On the other hand, the quotient $\mathbb{F}_p[x,y]/(xy)^2$ of R is not a symmetric $\mathbb{F}_p$-algebra. In fact, suppose that $\sigma\colon \mathbb{F}_p[x,y]/(xy)^2 \to \mathbb{F}_p$ is a $\mathbb{F}_p$-linear functional on $\mathbb{F}_p[x,y]/(xy)^2$. If $\sigma(x) = \sigma(y) = 0$ then $\ker(\sigma)$ contains the ideal (x,y). Otherwise, $\ker(\sigma)$ contains the non-zero ideal generated by $\sigma(x)y - \sigma(y)x$. This shows that, in all cases, σ is degenerate.

We also remark that the construction of the symmetric algebra mentioned in Remark 4.4 could be generalized. We have the following observation.

Proposition 4.5. *Let R be a finite symmetric $\mathbb{Z}/n$-algebra. Let $f \in R[x]$ be a monic polynomial of degree n. Then $R[x]/f$ is also a finite symmetric $\mathbb{Z}/n$-algebra.*

Proof. Let $\psi\colon R \to \mathbb{Z}/n$ be a $\mathbb{Z}/n$-linear functional on R. We will now define a non-degenerate $\mathbb{Z}/n$-linear functional on $R[x]/f$. Each element of $R[x]/f$ can be written uniquely as

$$g = a_{n-1}x^{n-1} + \cdots + a_1x + a_0.$$

This shows that $R[x]/f$ is a finite ring of order $|R|^n$. We define $\widehat{\psi} : R[x]/f \to \mathbb{Z}/n$ by the rule $\widehat{\psi}(g) = \psi(a_{n-1})$. By an identical argument as the proof of [7, Proposition 6.7], we can see that $\widehat{\psi}$ is non-degenerate. We conclude that $R[x]/f$ is a finite symmetric $\mathbb{Z}/n$-algebra. □

Remark 4.6. We recall that a Galois ring is a ring of the form $R = \mathbb{Z}[x]/(p^n, f(x)) = (\mathbb{Z}/p^n)[x]/f(x)$ where f is a monic polynomial. Proposition 4.5 shows that Galois rings are finite symmetric $\mathbb{Z}/p^n$-algebras.

Another corollary of Proposition 4.5 is the following.

Corollary 4.7. *Every finite commutative ring is a quotient of a finite symmetric algebra.*

Proof. Let T be a commutative ring and n the characteristic of T. Since T is finite, there exists $\alpha_1, \alpha_2, \ldots, \alpha_k$ such that T is generated by $\alpha_1, \alpha_2, \ldots, \alpha_k$; namely $T = \mathbb{Z}/n[\alpha_1, \alpha_2, \ldots, \alpha_k]$.

Let us prove by induction that $\mathbb{Z}/n[\alpha_1, \alpha_2, \ldots, \alpha_i]$ is a quotient of a finite symmetric $\mathbb{Z}/n$-algebra for each $0 \leq i \leq k$. If $i = 0$ then $T = \mathbb{Z}/n$ which is a symmetric algebra. Suppose that $\mathbb{Z}/n[\alpha_1, \alpha_2, \ldots, \alpha_i]$ is a quotient of a symmetric algebra, say R. We claim that $\mathbb{Z}/n[\alpha_1, \alpha_2, \ldots, \alpha_{i+1}] = \mathbb{Z}/n[\alpha_1, \alpha_2, \ldots, \alpha_i][\alpha_{i+1}]$ is a quotient of a symmetric algebra as well. Since T is finite, there exists a monic polynomial $f \in \mathbb{Z}/n[\alpha_1, \alpha_2, \ldots, \alpha_i][x]$ such that $f(a_{i+1}) = 0$. Let $\widehat{f}$ be a lift of f to R. Then we have the following quotient maps

$$R[x]/\widehat{f} \to \mathbb{Z}/n[\alpha_1, \alpha_2, \alpha_i][x]/f \to \mathbb{Z}/n[\alpha_1, \alpha_2, \ldots, \alpha_i][\alpha_{i+1}].$$

By Proposition 4.5, $R[x]/\widehat{f}$ is a finite symmetric $\mathbb{Z}/n$- algebra. This shows that the inductive statement holds for $i+1$. By the principle of mathematical induction, T is a quotient of a finite symmetric $\mathbb{Z}/n$-algebra. □

We now define generalized Ramanujan sum.

Definition 4.8. Let $g \in R$. The generalized Ramanujan sum $c(g, R)$ is defined as follows

$$c(g, R) = c_{\psi}(g, R) = \sum_{a \in R^{\times}} \zeta_n^{\psi(ga)}.$$

Our goal is to give an explicit description for $c(g, R)$. In particular, we will show that $c(g, R)$ does not depend on the choice of ψ as long as ψ is non-degenerate. Similar to the case with Ramanujan sums over $\mathbb{Z}$ as described in Eq. (1.2), doing so would require some generalization of the Möbius and Euler totient functions. The definition for the Euler function $\varphi(\mathcal{I})$ is quite straightforward.

Definition 4.9. Let T be a finite ring. The Euler number of T is defined as

$$\varphi(T) = |T^{\times}|,$$

where $T^{\times}$ is the set of invertible elements in T.

The definition of the Möbius function $\mu(T)$ is a little more complicated. First, we recall that by the structure theorem for Artinian rings, the finite ring T is isomorphic to a finite product of local rings $T \cong \prod_{i=1}^{d} R_i$. The following definition is inspired by the classical Möbius function.

Definition 4.10.

$$\mu(T) = \begin{cases} 1, & \text{if } |T| = 1, \\ 0, & \text{if there exists } 1 \leq i \leq d \text{ such that } R_i \text{ is not a field,} \\ (-1)^d, & \text{otherwise.} \end{cases}$$

Example 4.11. Let us consider the case R is a finite quotient of the ring of integers in a global field; i.e, $R = \mathcal{O}_K/\mathfrak{a}$ where $\mathfrak{a}$ is a non-zero ideal in $\mathcal{O}_K$. Suppose that $\mathfrak{a} = \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$

is the factorization of $\mathfrak{a}$ into a product of prime ideals, then

$$\mathcal{O}_K/\mathfrak{a} \cong \prod_{i=1}^{d} \mathcal{O}_K/\mathfrak{p}_i^{e_i}.$$

By definition, $\mu(\mathcal{O}_K/\mathfrak{a}) = 0$ if there exists $1 \leq i \leq d$ such that $e_i > 1$. Otherwise, $\mu(\mathcal{O}_K/\mathfrak{a}) = (-1)^d$. With this interpretation, we can see the $\mu(\mathcal{O}_K/\mathfrak{a})$ is a direct generalization of the classical Möbius function.

We discuss a simple property for the behavior of the Euler and Möbius functions with respect to direct products.

Lemma 4.12. *Let R be a finite ring. Suppose that $R = R_1 \times R_2$. Then $\mu(R) = \mu(R_1)\mu(R_2)$ and $\varphi(R) = \varphi(R_1)\varphi(R_2)$.*

Proof. Both statements follow directly from the definition of μ and φ. □

With these preparations, we can now calculate the generalized Ramanujan sum $c(g, R)$. We first calculate the Ramanujan sum $c(g, R)$ when $g = 1$.

Proposition 4.13. $c(1, R) = \mu(R)$.

Proof. By the structure theorem, R is isomorphic to a product of local rings; i.e., $R \cong \prod_{i=1}^{d} R_i$, where R_i is a local ring. Let ψ_i be the linear functional on R_i induced by ψ. Since ψ is non-degenrate, ψ_i is non-degenerate as well. Furthermore, by [6, Satz1] we have $c_\psi(1, R) = \prod_{i=1}^{d} c_{\psi_i}(1, R_i)$. Together with Lemma 4.12 about the multiplicative property of the Möbius function under direct products, it is sufficient to prove the statement when R is a local ring. Namely, we need to show that if R is a local ring then

$$c_\psi(1, R) = \begin{cases} 0, & \text{if } R \text{ is not a field,} \\ -1 & \text{otherwise.} \end{cases}$$

Let $\mathfrak{m}$ be the maximal ideal of R and $\widehat{\psi} = \zeta_n^{\psi}$ be the chacteracter of R associated with ψ. Because $R^\times = R \setminus \mathfrak{m}$, we have

$$c_\psi(1, R) = \sum_{a \in R^\times} \widehat{\psi}(a) = \sum_{a \in R} \widehat{\psi}(a) - \sum_{a \in \mathfrak{m}} \widehat{\psi}(a). \tag{4.1}$$

Since $\widehat{\psi}$ is a nontrivial character of R, we know that $\sum_{a \in R} \widehat{\psi}(a) = 0$. Additionally, because $\mathfrak{m}$ is an additive subgroup of R, the restriction of $\widehat{\psi}$ to $\mathfrak{m}$ is a character of $\mathfrak{m}$ (considered as an abstract abelian group). Since ψ is non-degenerate, the restriction of $\widehat{\psi}$ to $\mathfrak{m}$ is a non-trivial character unless $\mathfrak{m} = 0$. By Lemma 4.2, we conclude that

$$\sum_{a \in \mathfrak{m}} \widehat{\psi}(a) = \begin{cases} 0, & \text{if } \mathfrak{m} \neq 0 \\ 1 & \text{otherwise.} \end{cases}$$

By Eq. (4.1), we conclude that if R is a local ring then

$$c_\psi(1,R) = \begin{cases} 0, & \text{if } R \text{ is not a field,} \\ -1 & \text{otherwise.} \end{cases}$$

□

We now consider the general case.

Theorem 4.14.

$$c(g,R) = \frac{\varphi(R)}{\varphi(R/\mathrm{Ann}_R(g))} c(1, R/\mathrm{Ann}_R(g)) = \frac{\varphi(R)}{\varphi(R/\mathrm{Ann}_R(g))} \mu(R/\mathrm{Ann}_R(g)).$$

Proof. By definition $c(g,R) = \sum_{a \in R^\times} \zeta_n^{\psi(ga)}$. We remark that if $a - b \in \mathrm{Ann}_R(g)$ then $ga = gb$ and hence $\psi(ga) = \psi(gb)$. We also note that since the reduction map $\Phi : R^\times \to (R/\mathrm{Ann}_R(g))^\times$ is a surjective group homomorphism, each $u \in (R/\mathrm{Ann}_R(g))^\times$ has exactly $\frac{\varphi(R)}{\varphi(R/\mathrm{Ann}_R(g))}$ lifts to $R^\times$. Therefore

$$c(g,R) = \frac{\varphi(R)}{\varphi(R/\mathrm{Ann}_R(g))} \sum_{a \in (R/\mathrm{Ann}_R(g))^\times} \zeta_n^{\psi(ga)} = \frac{\varphi(R)}{\varphi(R/\mathrm{Ann}_R(g))} \sum_{a \in (R/\mathrm{Ann}_R(g))^\times} \zeta_n^{\psi_g(a)}.$$

By Lemma 4.3, ψ_g is a non-degenerate linear functional on $R/\mathrm{Ann}_R(g)$. By Proposition 4.13, we know that

$$\sum_{a \in (R/Ann_R(g))^\times} \zeta_n^{\psi_g(a)} = \mu(R/\mathrm{Ann}_R(g)).$$

We conclude that

$$c(g,R) = \frac{\varphi(R)}{\varphi(R/\mathrm{Ann}_R(g))} \mu(R/\mathrm{Ann}_R(g)).$$

□

We can now describe explicitly the spectrum of a gcd-graph.

Theorem 4.15. *Let $G_R(D)$ be a gcd-graph with $D = \{\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_k\}$ and $\mathcal{I}_i = Rx_i$ is a principal ideal. Then, the spectrum of $G_D(D)$ is the multiset $\{\lambda_g\}_{g \in R}$ where*

$$\lambda_g = \sum_{i=1}^{k} c(g, R/\mathrm{Ann}_R(x_i)).$$

Here $c(g, R/\mathrm{Ann}_R(x_i))$ is the Ramanujan sum with an explicit formula given in Theorem 4.14.

Proof. Let S be the generating set associated with D as described in Proposition 2.5. By the circulant diagonalization theorem, the spectrum of $G_R(D) = \Gamma(R,S)$ is the multiset $\{\lambda_g\}_{g \in R}$ where

$$\lambda_g = \sum_{s \in S} \zeta_n^{\psi(gs)} = \sum_{i=1}^{k} \left[\sum_{s, Rs = \mathcal{I}_i} \zeta_n^{\psi(gs)} \right].$$

We remark that by Corollary 2.7, if $s \in R$ such that $Rs = \mathcal{I}_i = Rx_i$ then s has a unique representation of the form $s = \hat{u}x_i$ where $u \in (R/\mathrm{Ann}_R(x_i))^{\times}$ and $\hat{u}$ is a fixed lift of u to $R^{\times}$. With this presentation, we can write

$$\sum_{s, Rs=\mathcal{I}_i} \zeta_n^{\psi(gs)} = \sum_{u \in (R/Ann_R(x_i))^{\times}} \zeta_n^{\psi(gux_i)} = \sum_{u \in (R/Ann_R(x_i))^{\times}} \zeta_n^{\psi_{x_i}(gu)} = c(g, R/\mathrm{Ann}_R(x_i)).$$

Here we recall that ψ_{x_i} is the induced linear functional on $R/\mathrm{Ann}_R(x_i)$. We conclude that $\lambda_g = \sum_{i=1}^{k} c(g, R/\mathrm{Ann}_R(x_i))$. □

Corollary 4.16. *Suppose that $g' = ug$ for some $u \in R^{\times}$. Then $\lambda_g = \lambda_{g'}$.*

Acknowledgements

We thank the Department of Mathematics and Computer Science at Lake Forest College for their generous financial support through an Overleaf subscription. We also thank Ján Mináč for his constant encouragement and support.

References

1. Reza Akhtar, Megan Boggess, Tiffany Jackson-Henderson, Isidora Jiménez, Rachel Karpman, Amanda Kinzel, and Dan Pritikin, *On the unitary Cayley graph of a finite ring*, Electron. J. Combin. **16** (2009), no. 1, Research Paper 117, 13 pages.
2. Milan Bašić, Aleksandar Ilić, and Aleksandar Stamenković, *Maximal diameter of integral circulant graphs*, Information and Computation **301** (2024), 105208.
3. Maria Chudnovsky, Michal Cizek, Logan Crew, Ján Mináč, Tung T. Nguyen, Sophie Spirkl, and Nguyên Duy Tân, *On prime Cayley graphs*, arXiv preprint arXiv:2401.06062 (2024).
4. Irving Kaplansky, *Elementary divisors and modules*, Transactions of the American Mathematical Society **66** (1949), no. 2, 464–491.
5. Walter Klotz and Torsten Sander, *Some properties of unitary Cayley graphs*, The electronic journal of combinatorics (2007), R45–R45.
6. Erich Lamprecht, *Allgemeine theorie der Gaußschen Summen in endlichen kommutativen Ringen*, Mathematische Nachrichten **9** (1953), no. 3, 149–196.
7. Ján Mináč, Tung T Nguyen, and Nguyen Duy Tân, *On the gcd graphs over polynomial rings*, arXiv preprint arXiv:2409.01929 (2024).
8. Tung T Nguyen and Nguyen Duy Tân, *Integral cayley graphs over a finite symmetric algebra*, arXiv preprint arXiv:2411.00307 (2024).
9. Nitin Saxena, Simone Severini, and Igor E Shparlinski, *Parameters of integral circulant graphs and periodic quantum dynamics*, International Journal of Quantum Information **5** (2007), no. 03, 417–430.
10. Wasin So, *Integral circulant graphs*, Discrete Mathematics **306** (2006), no. 1, 153–158.

Department of Mathematics and Computer Science, Lake Forest College, Lake Forest, Illinois, USA
Email address: tnguyen@lakeforest.edu

Faculty Mathematics and Informatics, Hanoi University of Science and Technology, 1 Dai Co Viet Road, Hanoi, Vietnam
Email address: tan.nguyenduy@hust.edu.vn