ON THE GCD GRAPHS OVER THE POLYNOMIAL RING AND RELATED TOPICS

JÁN MINÁČ, TUNG T. NGUYEN, NGUYễN DUY TÂN

Abstract. Gcd-graphs over the ring of integers modulo n are a natural generalization of unitary Cayley graphs. The study of these graphs has foundations in various mathematical fields, including number theory, ring theory, and representation theory. Using the theory of Ramanujan sums, it is known that these gcd-graphs have integral spectra; i.e., all their eigenvalues are integers. In this work, inspired by the analogy between number fields and function fields, we define and study gcd-graphs over polynomial rings with coefficients in finite fields. We establish some fundamental properties of these graphs, emphasizing their analogy to their counterparts over $\mathbb{Z}$.

Contents

Date: August 1, 2024.

2020 *Mathematics Subject Classification.* Primary 05C25, 05C50, 05C51.

Key words and phrases. Cayley graphs, Gauss sums, Finite fields, Symmetric algebra.

JM is partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) grant R0370A01. He gratefully acknowledges the Western University Faculty of Science Distinguished Professorship 2020-2021. TTN is partially supported by an AMS-Simons Travel Grant. Parts of this work were done while he was a postdoc associate at Western University. He thanks Western University for their hospitality. NDT is partially supported by Vietnam National University, Hanoi (VNU) under the project number QG.23.48.

1. Introduction

Let n be a positive integer. The unitary Cayley graph on the ring of integers modulo n is defined as the Cayley graph $G_n = \mathrm{Cay}(\mathbb{Z}/n, U_n)$ where $\mathbb{Z}/n$ is the ring of integers modulo n and $U_n = (\mathbb{Z}/n)^{\times}$ its unit group. More specifically, G_n is equipped with the following data

(1) The vertex set of G_n is $\mathbb{Z}/n$.

(2) Two vertices $a, b \in V(G_n)$ are adjacent if and only if $a - b \in U_n$.

The unitary Cayley graph G_n was first formally introduced in [17] even though we can trace it back to the work of Evans and Erdős [10]. Due to its elegance and simplicity, the unitary Cayley graph has been further studied and generalized by various works in the literature. For example, [1] studies the unitary Cayley graph of a finite commutative ring. [14] generalizes this study further to finite rings which are not necessarily commutative. In [25], a subset of the authors study various arithmetic and graph-theoretic properties of the p-unitary Cayley graph as defined by [26, 27]. We refer the interested readers to [2, 7, 17, 25] and the references therein for some further topics in this line of research.

As explained in [17, Section 4], a particularly intriguing arithmetical property of G_n is that its spectrum can be described by the theory of circulant matrices and Ramanujan sums. A consequence of this fact is that the unitary Cayley graph has an integral spectrum; i.e., all of its eigenvalues are integers. In [17], the authors note that the unitary Cayley graph is not the sole graph exhibiting an integral spectrum. They identify a closely related family of graphs sharing this characteristic, known as gcd-graphs which we now recall. Let $D = \{d_1, d_2, \ldots, d_k\}$ be a set of proper divisors of n. The gcd-graph $G_n(D)$ is the graph with the following data

(1) The vertex set of $G_n(D)$ is $\mathbb{Z}/n$.

(2) Two vertices $a, b \in G_n$ are adjacent if and only if $\gcd(a - b, n) \in D$.

We remark that the unitary Cayley graph G_n is nothing but $G_n(\{1\})$. It is known that the spectrum of $G_n(D)$ is a summation of various Ramanujan sums (see [17, Section 4]). In particular, all of its eigenvalues are integers. It turns out that, the converse is also true.

Theorem 1.1. *(See* [28, Theorem 7.1]*) A $\mathbb{Z}/n$-circulant graph G is an integral graph if and only if $G = G_n(D)$ for some D.*

Let $\mathbb{F}_q$ be a finite field. As observed by Andre Weil in [29], there is a strong analogy between the ring $\mathbb{Z}$ of integers and the ring $\mathbb{F}_q[x]$ of polynomials with coefficients in $\mathbb{F}_q$ (and more generally, between number fields and function fields). Consequently, it is of reasonable interest to define and investigate gcd-graphs over $\mathbb{F}_q[x]$. Fortunately, the analogous definition of gcd-graphs over $\mathbb{F}_q[x]$ is relatively straightforward. More specifically, let $f \in \mathbb{F}_q[x]$ be a non-zero element in $\mathbb{F}_q[x]$. Let $D = \{f_1, f_2, \ldots, f_k\}$ be a subset of the set of divisors $\mathrm{Div}(f)$ of f; i.e, $f_i \mid f$ for all $1 \leq i \leq k$. Let

$$S_D = \{g \in \mathbb{F}_q[x]/f \,|\, \gcd(g, f) \in D\}.$$

Let $G_f(D)$ be the gcd-Cayley graph $\Gamma(\mathbb{F}_q[x]/f, S_D)$. More precisely

(1) The vertex set of $G_f(D)$ is the finite ring $\mathbb{F}_q[x]/f$.

(2) Two vertices u, v are adjacent if and only if $u - v \in S_D$. In other words, $\gcd(u - v, f) \in D$.

Remark 1.2. In general, the greatest common divisor is only defined up to associates. In our case, however, we can make a canonical choice for the great common divisor by requiring it to be a monic polynomial. Therefore, unless we explicitly state, we will assume throughout this article that all involved polynomials are monic.

Example 1.3. Fig. 1 shows the graph $G_f(D)$ where $f = x(x+1) \in \mathbb{F}_3[x]$ and $D = \{x, x+1\}$. It is a regular graph of degree 4.

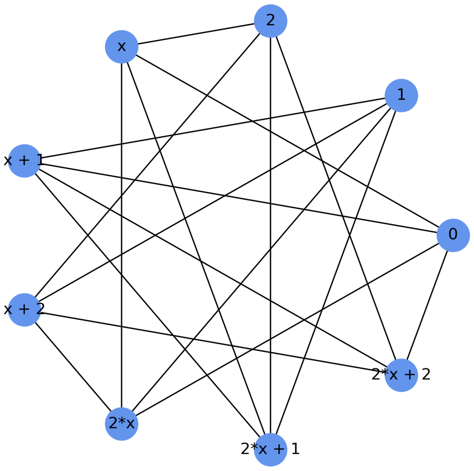

FIGURE 1. The gcd-Cayley graph $G_{x(x+1)}(\{x, x+1\})$

1.1. **Outline.** In this article, we study some foundational properties of gcd-graphs defined over $\mathbb{F}_q[x]$. In Section 2, we recall some standard definitions in graph theory that will be used throughout the article. Section 3 investigates the question of when a gcd-graph is connected and anti-connected. In Section 4, we provide the necessary and sufficient conditions for a gcd-graph to be bipartite. Section 5 explores another graph-theoretic property of gcd-graphs: their prime-property. Although we are not able to provide a complete answer, we present some rather general conditions under which this property holds. Section 6 examines the spectra of gcd-graphs using symmetric algebras and Ramanujan sums. It is quite remarkable that the explicit formulas for these spectra are identical to those that appeared in the number field case. In Section 7, we provide some sufficient conditions for gcd-graphs to be perfect. Finally, in Section 8, we investigate whether a given graph can be realized as an induced subgraph of a gcd-graph. As a by-product, we prove an analogous result to a theorem of Erdős and Evans in the number field case.

1.2. **Code.** The code that we develop to generate gcd-graphs and do experiments on them can be found at [22].

2. Background from graph theory

In this section, we recall some basic concepts in graph theory that we will use throughout this article.

Definition 2.1 (The complete graph K_n)**.** K_n is the graph on n vertices which are pairwisely adjacent.

Definition 2.2 (Tensor product of graphs)**.** Let G, H be two graphs. The tensor product $G \times H$ of G and H (also known as the direct product) is the graph with the following data:

(1) The vertex set of $G \times H$ is the Cartesian product $V(G) \times V(H)$,
(2) Two vertices (g, h) and (g', h') are adjacent in $G \times H$ if and only if $(g, g') \in E(G)$ and $(h, h') \in E(H)$.

Definition 2.3 (Wreath product)**.** Let G, H be two graphs. We define the wreath product of G and H as the graph $G * H$ with the following data

(1) The vertex set of $G * H$ is the Cartesian product $V(G) \times V(H)$,
(2) (g, h) and (g', h') are adjacent in $G * H$ if either $(g, g') \in E(G)$ or $g = g'$ and $(h, h') \in E(H)$.

Definition 2.4 (Graph morphism)**.** Let G_1 and G_2 be two graphs. We define a graph morphism between G_1 and G_2 to be a map from $V(G_1)$ to $V(G_2)$ f that preserves edges. More precisely, if $u, v \in V(G_1)$ are adjacent in G_1, then $f(u), f(v)$ are adjacent in G_2.

Definition 2.5 (Induced subgraph)**.** Let G_1 and G_2 be two graphs. We say that G_1 is an induced subgraph of G_2 if there exists a graph morphism $f : G_1 \to G_2$ such that the following conditions hold

(1) The map $f : V(G_1) \to V(G_2)$ is injective.
(2) For $u, v \in G_1$, u, v are adjacent if and only if $f(u)$ and $f(v)$ are adjacent in G_2.

3. Connectedness of gcd graphs

In this section, we will give the necessary and sufficient conditions for $G_f(D)$ to be connected. Unlike the number field case where these conditions are rather straightforward, the function field case is a bit more complicated. This is partially due to the fact that the unitary Cayley graph on $\mathbb{F}_q[x]/f$ is not always connected. We start our discussion with the following simple observation.

Lemma 3.1. *If $G_f(D)$ is connected then* $\gcd(f_1, \ldots, f_k) = 1$.

Proof. Let $f_0 = \gcd(f_1, \ldots, f_k)$. We observe that if two vertices u and v are adjacent then f_0 divides $u - v$. Now since $G_f(D)$ is connected, there is a path connecting 0 and 1. This implies that f_0 divides $1 - 0 = 1$. Hence $\gcd(f_1, \ldots, f_k) = 1$. □

In the case of $\mathbb{Z}$, the converse of Lemma 3.1 is true as well; i.e. the gcd-graph $G_n(D)$, where $D = \{d_1, d_2, \ldots, d_k\}$ is connected if and only if $\gcd(d_1, d_2, \ldots, d_k) = 1$. In the case of $\mathbb{F}_q[x]$, this condition is not sufficient. For example, let $D = \{1\}$, $\mathbb{F}_q = \mathbb{F}_2, f = x(+1)$. Then $\mathbb{F}_q[x]/f \cong \mathbb{F}_2 \times \mathbb{F}_2$. In this case

$$G_f(\{1\}) \cong K_2 \times K_2,$$

which is not connected (in general, this is the only obstruction where the unitary graph over a commutative ring fails to be connected, see [7] and Proposition 3.3)). In the case of the gcd-graphs, we have the following result.

Theorem 3.2. *$G_f(D)$ is connected if the following conditions hold*

(1) $\gcd(f_1, f_2, \ldots, f_k) = 1$.

(2) The unitary Cayley graph $G_f(\{1\})$ is connected.

Proof. We need to show that $R = \langle S_D \rangle$ the abelian group generated by S_D. Let $a \in R = \mathbb{F}_q[x]/f$. Because $\gcd(f_1, f_2, \ldots, f_k) = 1$, we can find $a_1, a_2, \ldots, a_k \in R$ such that

$$a = \sum_{i=1}^{k} a_i f_i.$$

Since $G_f(\{1\})$ is connected, for each $1 \leq i \leq d$, we can find 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

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

By definition, $\gcd(s_{ij} f_i, f) = f_i \in D$. This shows that $a \in \langle S_D \rangle$. Since this is true for all a, we conclude that $R = \langle S_D \rangle$. □

We can classify all f such that $G_f(\{1\})$ is not connected.

Proposition 3.3. *(See* [7, Lemma 4.33]*) $G_f(\{1\})$ is not connected if and only if $\mathbb{F}_q = \mathbb{F}_2$ and $x(x+1) \mid f$.*

By Theorem 3.2 and Proposition 3.3, we have the following corollary.

Corollary 3.4. *Suppose that one of the following conditions holds*

(1) $\mathbb{F}_q \neq \mathbb{F}_2$.

(2) $\mathbb{F}_q = \mathbb{F}_2$ and $x(x+1) \nmid f$.

Then $G_f(D)$ is connected if and only if $\gcd(f_1, f_2, \ldots, f_k) = 1$.

We now deal with the case where $G_f(\{1\})$ is not connected. By Proposition 3.3, this implies that $\mathbb{F}_q = \mathbb{F}_2$ and $x(x+1) \mid f$.

Lemma 3.5. *Let g be a divisor of f. Then for every polynomial $h \in \mathbb{F}_q[x]$*

$$\gcd(h, g) = \gcd(\gcd(h, f), g).$$

Proof. Let $m = \gcd(h, f)$. We need to show that $\gcd(h, g) = \gcd(m, g)$. We first claim that $\gcd(h, g) \mid \gcd(m, g)$. By definition, $\gcd(h, g) \mid g$. We also have $\gcd(h, g) \mid \gcd(h, f) = m$. Therefore, $\gcd(h, g) \mid \gcd(m, g)$.

Conversely, we claim that $\gcd(m, g) \mid \gcd(h, g)$. Indeed, we have $\gcd(m, g) \mid g$. Since $m = \gcd(h, f)$, $\gcd(m, g) \mid m \mid h$. We conclude that $\gcd(m, g) \mid \gcd(h, g)$.

In summary, we have $\gcd(m, g) \mid \gcd(h, g)$ and $\gcd(h, g) \mid \gcd(m, g)$. This shows that $\gcd(m, g) = \gcd(h, g)$. □

Proposition 3.6. *Let g be a divisor of f and $\Phi_{f,g}\colon \mathbb{F}_q[x]/f \to \mathbb{F}_q[x]/g$ be the canonical projection map. Let*

$$\overline{D} = \{\gcd(f_i, g) | 1 \leq i \leq k\}.$$

Then $\Phi_{f,g}(S_D) \subseteq S_{\overline{D}}$. Consequently, $\Phi_{f,g}\colon G_f(D) \to G_g(\overline{D})$ is a graph morphism.

Proof. Suppose that $a \in S_D$. Then, there exists i such that $\gcd(a, f) = f_i$. By Lemma 3.5, we know that

$$\gcd(a, g) = \gcd(\gcd(a, f), g) = \gcd(f_i, g).$$

This shows that $a \in S_{\overline{D}}$. We conclude that $\Phi_{f,g}(S_D) \subseteq S_{\overline{D}}$. □

Corollary 3.7. *If $G_f(D)$ is connected then $G_g(\overline{D})$ is connected as well.*

Proof. Let $\bar{a}, \bar{b}$ be two vertices in $G_g(\overline{D})$. Since $\Phi_{f,g}$ is surjective, we can find $a, b \in \mathbb{F}_q[x]/f$ such that $\Phi_{f,g}(a) = \bar{a}, \Phi_{f,g}(b) = \bar{b}$. Since $G_f(D)$ is connected, there is a path P from a to b. By Proposition 3.6, $\Phi_{f,g}(P)$ is a path from $\bar{a}$ to $\bar{b}$. This shows that $G_g(\overline{D})$ is connected as well. □

We are now ready to state our theorem in the case $G_f(\{1\})$ is not connected.

Theorem 3.8. *Suppose that $\mathbb{F}_q = \mathbb{F}_2$ and $x(x+1) \mid f$. Let $\Phi\colon \mathbb{F}_q[x]/f \to \mathbb{F}_q[x]/(x(x+1))$ be the canonical projection map and $\bar{D}$ as described above. Then $G_f(D)$ is connected if and only if*

(1) $\gcd(d_1, d_2, \ldots, d_k) = 1$, *and*

(2) the graph $G_{x(x+1)}(\bar{D})$ is connected. This condition is equivalent to $|\overline{D} \backslash \{x(x+1)\}| \geq 2$.

Proof. By Corollary 3.7, we know that if $G_f(D)$ is connected then (1) and (2) holds. Conversley, let us assume that (1) and (2) both hold. We will show that $G_f(D)$ is connected. This is equivalent to showing that $R := \mathbb{F}_q[x]/f = \langle S_D \rangle$.

The key idea of this proof is similar to the proof for Theorem 3.2. The main difficulty is to deal with the fact that $G_f(\{1\})$ is not connected in this case. We will do this step by step.

We first claim that if $g \in R$ such that $x(x+1) \mid g$ then $g = s_1 + s_2$ where $s_1, s_2 \in R^{\times}$. For an element $s \in R$, s is a unit if and only $\Phi^{\text{ss}}(s) \in (R^{\text{ss}})^{\times}$ where $R^{\text{ss}} = R/J(R)$ is the semisimplification of R (see [7, Proposition 4.30]). Therefore, for this statement, we can assume that $R = R^{\text{ss}}$; namely f is a squarefree polynomial. If we write $f = x(x+1)f_1$ where $\gcd(x(x+1), f_1) = 1$ then we have the isomorphism

$$R \cong \mathbb{F}_2[x]/(x(x+1)) \times \mathbb{F}_2[x]/f_1.$$

Under this isomorphism, g is sent to $(0, g_1)$ where $g_1 \in \mathbb{F}_2[x]/f_1$. Since $F_2[x]/f_1$ is a product of fields of order bigger than 2, every element in it can be written as the sum of two units; say $g_1 = t_1 + t_2$ where $t_1, t_2 \in (\mathbb{F}_2[x]/x(x+1))^{\times}$. We then see that $g = s_1 + s_2$ where $s_1 = (1, t_1)$ and $s_2 = (1, t_2)$. By definition $s_1, s_2 \in R^{\times}$.

We now claim that if $g \in R$ such that $x(x+1) \mid g$ then $g \in \langle S_D \rangle$. Since $\gcd(f_1, f_2, \ldots, f_k) = 1$, we can find $(a_1, a_2, \ldots, a_k)$ such that

$$a_1 f_1 + a_2 f_2 + \cdots + a_k f_k = 1.$$

Multiplying both sides with g, we get $g = \sum_{i=1}^{k} a_i g f_i$. Since $x(x+1) \mid a_i g$, we can write $a_i g = s_{1i} + s_{2i}$ where $s_{1i}, s_{2i} \in R^{\times}$. This shows that

$$g = \sum_{i=1}^{k} (s_{1i} f_i + s_{2i} f_i). \tag{3.1}$$

Since $s_1, s_2 \in R^{\times}$, $s_{1i} f_i, s_{2i} f_i \in S_D$. This shows that $g \in \langle S_D \rangle$.

Finally, let g now be an arbitrary element in R. We claim that $g \in \langle S_D \rangle$. By our assumption, the graph $G_{x(x+1)}(S_{\bar{D}})$ is connected, 0 and $\Phi_{f,x(x+1)}(g)$ are connected by a path. Consequently, we can write

$$g \equiv \sum_i n_i \gcd(h_i, x(x+1)) \pmod{x(x+1)},$$

where $n_i \in \mathbb{Z}$ and $\gcd(h_i, f) \in D$. We can check that over $\mathbb{F}_2[x]$

$$\gcd(h, x(x+1)) \equiv h \pmod{x(x+1)},$$

for all $h \in \mathbb{F}_2[x]$. Therefore, we can write

$$g \equiv \sum_i n_i h_i \pmod{x(x+1)}.$$

By the previous case, we know that $g - \sum_{i=1}^{k} n_i h_i \in \langle S_D \rangle$. This shows that $g \in \langle S_D \rangle$ as well. Since this is true for all g, we conclude that $R = \langle S_D \rangle$. □

Remark 3.9. The proof of Theorem 3.8 also implies that for the case $\mathbb{F}_2[x]$ and $x(x+1) \mid f$, the map $\Phi_{f,g} : \mathbb{F}_2[x]/f \to \mathbb{F}_2[x]/(x(x+1))$ has the property that a and b belong the same connected component in $G_f(D)$ if and only $\Phi_{f,x(x+1)}(a)$ and $\Phi_{f,x(x+1)}(b)$ belong to the same connected component in $G_{x(x+1)}(\overline{D})$. In fact, by Corollary 3.7, if a and b are connected by a path then $\Phi_{f,x(x+1)}(a)$ and $\Phi_{f,x(x+1)}(b)$ are connected by a path. Conversely, if $\Phi_{f,x(x+1)}(a)$ and $\Phi_{f,x(x+1)}(b)$ are connected by a path in $G_{x(x+1)}(\overline{D})$, we can write

$$a - b \equiv \sum_i n_i h_i \pmod{x(x+1)}.$$

where $n_i \in \mathbb{Z}$ and $\gcd(h_1, f) \in D$. Because $x(x+1)R \subseteq \langle S_D \rangle$, we conclude that that $a - b \in \langle S_D \rangle$. By definition, a and b are connected by a path in $G_f(D)$.

We conclude that $G_f(D)$ and $G_{x(x+1)}(\overline{D})$ has the same number of connected component. In particular, the number of connected component in $G_f(D)$ is at most 2.

Remark 3.10. While most of our discussions in this section concern the connectedness of $G_f(D)$, similar statements hold for the anti-connectedness of $G_f(D)$ as well. In fact, the complement of $G_f(D)$ is precisely $G_f(\mathrm{Div}(f) \setminus (D \cup \{f\})$ where $\mathrm{Div}(f)$ is the set of all proper divisors of f.

4. Bipartite property

In this section, we will classify all $G_f(D)$ which is bipartite. We start with the following lemma.

Lemma 4.1. *Suppose that $G_f(D)$ is connected and bipartite.*

(1) Let

$$I = \left\{ \sum_i n_i h_i | n_i \in \mathbb{Z}, h_i \in S_D \textit{ and } \sum_{i=1}^k n_i \equiv 0 \pmod 2 \right\},$$

$$I_1 = \left\{ \sum_i n_i h_i | n_i \in \mathbb{Z}, h_i \in S_D \textit{ and } \sum_{i=1}^k n_i \equiv 1 \pmod 2 \right\},$$

Then I is an subgroup of index 2 in $(R, +)$. Furthermore, I and I_1 are independent set such that $V(G_f(D)) = I \bigsqcup I_1$.

(2) If $G_f(\{1\})$ is connected, then I is an ideal in R as well.

(3) If $G_f(\{1\})$ is not connected, which is equivalent to $x(x+1) \mid f$ and $\mathbb{F}_q = \mathbb{F}_2$ by Proposition 3.3, then $x(x+1)R \subseteq I$.

Proof. (1) Let us consider the first part of this lemma. Because $G_f(D)$ is bipartite, we can write

$$V(G_f(D)) = A \bigsqcup B$$

where A, B are two independent sets in $G_f(D)$. Without loss of generality, we can assume that $0 \in A$. We claim that $A = I$. By the proof of [3, Proposition 2.6], we know that A is a subgroup of $(R, +)$ of index 2. By definition, if $h_i \in S_D$, then $(0, h_i) \in E(G_f(D))$. Because A and B are disjoint independent set in $G_f(D)$, $h_i \in B$. Furthermore, since A is a subgroup of index 2 in R, $h_i + h_j \in A$ for all $h_i, h_j \in S_D$. Consequently, we must have $I \subseteq A$.

By our assumption that $G_f(D)$ is connected we know that $R = \langle S_D \rangle$ and hence $I \cup I_1 = \langle S_D \rangle = R$. From this, we can see that I is a subgroup whose index is at most 2 in R. Additionally, because $I \subseteq A$ and A has index 2 in R, we must have that $I = A$ and $I_1 = B$.

(2) Suppose that $G_f(\{1\})$ is connected. We will show that I is an ideal in R as well. The idea is similar to the proof of Theorem 3.2 so we will be brief. Specifically, we note that for each $s \in R^\times$, $sI = I$. Since $\langle R^\times \rangle = R$, this shows that $aI \subseteq I$ for all $a \in R$. We conclude that I is an ideal in R.

(3) Finally, part (3) follows from Equation Eq. (3.1).

□

Corollary 4.2. *Suppose that either $\mathbb{F}_q \neq \mathbb{F}_2$ or $\gcd(x(x+1), f) = 1$. Then $G_f(D)$ is not a bipartite graph.*

Proof. If $\mathbb{F}_q \neq \mathbb{F}_2$ or $\gcd(x(x+1), f) = 1$, we know that $G_f(\{1\})$ is connected by Proposition 3.3. Furthermore, $\mathbb{F}_q[x]/f$ has no ideal of index 2. By Lemma 4.1, we conclude that $G_f(D)$ is not bipartite. □

We now consider the case $\mathbb{F}_q = \mathbb{F}_2$ and $\gcd(x(x+1), f) \neq 1$. We first consider the following easier case.

Theorem 4.3. *Suppose that f is a polynomial in $\mathbb{F}_2[x]$ such that $\gcd(x(x+1), f) \notin \{1, x(x+1)\}$. Then $G_f(D)$ is bipartite if and only if $\gcd(x(x+1), f) \nmid f_i$ for all $1 \leq i \leq k$.*

Proof. Without loss of generality, we can assume that $x \mid f$ but $x+1 \nmid f$. First, let us assume that $x \nmid f_i$ for all $1 \leq i \leq k$. In this case, we can see that $A = xR$ and $B = 1 + xR$ are independent subsets in $G_f(D)$ such that $V(G_f(D)) = A \bigsqcup B$. This shows that $G_f(D)$ is bipartite.

Conversely, let us assume that $G_f(D)$ is bipartite. We claim that $x \nmid f_i$ for all $1 \leq i \leq k$. Since $x(x+1) \nmid f$, by Theorem 3.2 and Proposition 3.3, we know that $G_f(\{1\})$ is connected. Therefore, by Lemma 4.1, there exists an ideal I of index 2 in R such that I is an independent set in $G_f(D)$. We remark that since the only ideal of index 2 in R is xR, $I = xR$. Because $0 \in I$ and I is independent we must have

$$xR \cap \{f_1, f_2, \ldots, f_k\} = \emptyset.$$

In other words, $x \nmid f_i$ for all $1 \leq i \leq k$. □

Finally, let us consider the trickest case where $x(x+1) \mid f$.

Theorem 4.4. *Suppose that $x(x+1) \mid f$ and that $G_f(D)$ is connected. Let*

$$\overline{D} = \{gcd(f_i, x(x+1)|f_i \in D.\}$$

Then $G_f(D)$ is bipartite if and only if $|\overline{D}| = 2$.

Proof. Suppose that $|\overline{D}| = 2$. We claim that $G_f(D)$ is bipartite. Because $G_f(D)$ is connected, we know by Theorem 3.8 that $|\overline{D} \setminus x(x+1)| \geq 2$. This shows that $\overline{D} \neq \{1, x(x+1)\}$. We can check that $\overline{D}$ must be one of the following sets $\{1, x\}, \{1, x+1\}, \{x, x+1\}$.

First, we consider the case that $\overline{D} = \{1, x+1\}$. In this case $V(G_f(D)) = xR \bigsqcup (1 + xR)$ is a decomposition of $G_f(D)$ into a disjoint union of two independent sets. Similarly, if $\overline{D} = \{1, x\}$ then $V(G_f(D)) = (x+1)R \bigsqcup (1 + (x+1)R)$ is a decomposition of $G_f(D)$ into a disjoint union of two independent sets. Now, suppose that $\overline{D} = \{x, x+1\}$. Let

$$A = \{g \in R | g(0) = g(1)\},$$

and

$$B = \{g \in R | g(0) \neq g(1)\} = x + A.$$

We can check that if $a_1, a_2 \in A$ then $\gcd(a_1 - a_2, x(x+1)) \in \{1, x(x+1)\}$. By definition, $(a_1, a_2) \notin E(G_f(D))$. This shows that A is an independent set in $G_f(B)$. Similarly, B is an independent set in $G_f(D)$ as well. We conclude that $G_f(D)$ is not bipartite.

Conversely, suppose $G_f(D)$ is bipartite. We claim that $|\overline{D}| = 2$. By Lemma 4.1, the subgroup

$$I = \left\{ \sum_i n_i h_i | n_i \in \mathbb{Z}, h_i \in S_D \text{ and } \sum_{i=1} n_i \equiv 0 \pmod 2 \right\},$$

is an independent set in $G_f(D)$. Furthermore, by part (3) of Corollary 3.7, we know that $x(x+1)R \subset I$. Because 0 is not connected to any node in I, we must have $x(x+1)R \cap S_D = \emptyset$. Consequently $x(x+1) \notin \overline{D}$. Suppose to the contrary that $|\overline{D}| \geq 3$. We then have $\overline{D} = \{1, x, x+1\}$. This implies that $G_{x(x+1)}(\overline{D})$ is the complete graph K_4. In K_4, there is a path of length 2 from 0 to any other vertices. From this property, we conclude that for each $g \in R$, we can write

$$g \equiv \gcd(h_1, x(x+1)) + \gcd(h_2, x(x+1)) \pmod{x(x+1)},$$

for some $h_1, h_2 \in S_D$. We then conclude that $g - h_1 - h_2 \in x(x+1)R \subset I$. Since $h_1 + h_2 \in I$, we conclude that $g \in I$ as well. This shows that $I = R$, which is a contradiction. □

Remark 4.5. By an almost identical argument, we can show that the gcd graph $G_n(D)$ over $\mathbb{Z}$ with $D = \{d_1, d_2, \ldots, d_k\}$ and $\gcd(d_1, d_2, \ldots, d_k) = 1$, is bipartite if and only if $2 \mid n$ and $2 \nmid d_i$ for all $1 \leq i \leq k$.

5. Primeness of gcd graphs

For a given graph G, a homogeneous set in G is a set X of vertices of G such that every vertex in $V(G) \setminus X$ is adjacent to either all or none of the vertices in X. A homogenous set X is said to be non-trivial if $2 \leq X < |V(G)|$. The graph G is said to prime if it does not contain any non-trivial homogeneous sets.

The concept of a homogeneous set appears in various branches of mathematics (see [5, 7, 11, 24] for some concrete examples). One of our main motivations comes from the fact that homogeneous sets allow us to decompose a network into a multilevel network of smaller graphs. From both theoretical and computational perspectives, such a decomposition is crucial for understanding the dynamics of multilevel networks (see [4, 12, 16, 24]). In [7], in collaboration with some other graph theorists, we completely classify prime unitary Cayley graphs on finite commutative rings. In this section, we study the problem for the gcd graph $G_f(D)$. We remark that for a graph G, a connected component of G (or of its complement) is a homogeneous set in G. Therefore, while studying the primeness of G, it is safe to assume that G is connected and anti-connected. For this reason, we will assume throughout this section that $G_f(D)$ is both connected and anti-connected (we refer the reader to Section 3 for precise conditions for these properties to hold).

An important property of homogeneous sets is that they are preserved under a graph isomorphism. For this reason, we start our discussion with the following observation.

Proposition 5.1. *Let $a \in (\mathbb{F}_q[t]/f)^{\times}$. Let $m_a : \mathbb{F}_q[x]/f \to \mathbb{F}_q[x]/f$ be the multiplication by a map. Then m_a induces an automorphism on $G_f(D)$.*

Proof. Since $a \in (\mathbb{F}_q[x]/f)^{\times}$, m_a is an automorphism of $(\mathbb{F}_q[x]/f, +)$. Furthermore, m_a preserves S_D; i.e $aS_D = S_D$. As a result, m_a is an automorphism of $G_f(D)$. □

Proposition 5.2. *Assume that $G_f(\{1\})$ is connected. Then, the following conditions are equivalent*

(1) $G_f(D)$ is not a prime graph.
(2) There exists a non-trivial ideal I in $\mathbb{F}_q[x]/f$ such that I is a homogeneous set in $G_f(D)$.

Proof. Clearly (2) implies (1). Let us now prove (1) implies (2). The proof that we discuss here is quite similar to the one that we gave for [7, Theorem 4.1] and Theorem 3.2. Because $G_f(D)$

is not prime, we can find a maximal homogenous set H containing 0. By [7, Theorem 3.4], we know that H is a subgroup of $\mathbb{F}_q[x]/f$. We claim that it is an ideal as well. By Proposition 5.1, we conclude that $aH = H$ for all $a \in (\mathbb{F}_q[x]/f)^{\times}$. Furthermore, since $G_f(\{1\})$ is connected, $aH \subset H$ for all $a \in \mathbb{F}_q[x]/f$ as well. This shows that H is an ideal in $\mathbb{F}_q[x]/f$. □

By Proposition 5.2, in order to study the prime property of $G_f(D)$, it is essentially equivalent to classify g such that the ideal generated by g is a homogenous set in $G_f(D)$. In order to do so, we first introduce the following lemmas.

Lemma 5.3. *Let $a, b, c \in \mathbb{F}_q[x]$ such that $\gcd(a,b) = \gcd(b,c) = m$ and $c \mid f$. Then, there exists $t \in \mathbb{F}_q[x]$ such that*

$$\gcd(a - bt, f) = c.$$

Proof. By replacing a, b, c, f by $\frac{a}{m}, \frac{b}{m}, \frac{c}{m}, \frac{f}{m}$, we can assume that $m = 1$. Because $\gcd(b,c) = 1$, we can find t_1 such that $c \mid a - bt_1$. Let us write $a - bt_1 = a_1 c$. We will look for $t = t_1 + ct_2$ such that the condition $\gcd(a - bt, f) = c$ holds. By our choices of t_1, t_2, this is equivalent to

$$c = \gcd(a - b(t_1 + ct_2), f) = \gcd(a_1 c - bt_2 c, f) = c \gcd(a_1 - b_1 t_2, \frac{f}{c}).$$

We remark that the relation $a - bt_1 = a_1 c$ and the fact that $\gcd(a,b) = 1$ imply that $\gcd(a_1, b) = 1$. By the Chinese remained theorem, we can find t_2 such that $\gcd(a_1 - b_1 t_2, \frac{f}{c}) = 1$.

□

Lemma 5.4. *Let g be a divisor of f. Let I_g be the ideal in $R = \mathbb{F}_q[x]/f$ generated by g. The induced graph on I_g is isomorphic to $G_{f/g}(D_g)$ where*

$$D_g = \left\{ \frac{f_i}{g} | f_i \in D, g \mid f_i \right\}.$$

Proof. Every element in I_g can be written in the form gm for a unique $m \in \mathbb{F}_q[x]/(f/g)$. Therefore we have a natural map $I_g \to \mathbb{F}_q[x]/(f/g)$ sending $gm \mapsto m$. Furthermore, for two elements $ga, gb \in I_g$, we have

$$\gcd(ga - gb, f) = g \gcd(a - b, \frac{f}{g}).$$

Therefore, we see that $\gcd(ga - gb, f) \in D$ if and only $\gcd(a - b, \frac{f}{g}) \in D_g$. From this, we conclude that the induced graph on I_g is naturally isomorphic to $G_{f/g}(D_g)$. □

Theorem 5.5. *Let $g \mid f$ be a divisor of f and I the ideal in $\mathbb{F}_q[x]/f$ generated by g. Let*

$$D_1 = \{f_i \in D | g \nmid f_i\}, \quad D_2 = \{f_i \in D | g \mid f_i\}.$$

As in Proposition 3.6 let

$$\overline{D_1} = \{\gcd(f_i, g) | f_i \in D_1\}, \quad \widetilde{D_2} = \left\{ \frac{f_i}{g} | f_i \in D_2 \right\}.$$

Then, the following statements are equivalent

(1) I is a homogeneous set in $G_f(D)$.

(2) $\Phi_{f,g}^{-1}(\overline{D_1}) \cap Div(f) = D_1$ where $\Phi_{f,g} : \mathbb{F}_q[x]/f \to \mathbb{F}_q[x]/g$ is the canonical projection map.

Furthermore, if one of the above equivalent conditions holds, $G_f(D)$ is isomorphic to the wreath product $G_g(D_1) * G_{f/g}(\widetilde{D_2})$.

Proof. First, let us show that (2) implies (1). In other words, suppose that g satisfies the condition that $\Phi_{f,g}^{-1}(\overline{D_1}) \cap \text{Div}(f) = D_1$. We claim that the ideal I generated by g is a homogeneous set in $G_f(D)$. In fact, let $a \notin I$ be an arbitrary element in $\mathbb{F}_q[x]/f$ and suppose that a is adjacent to an element in I. By a translation, we can assume that a is adjacent to 0 in $G_f(D)$. We claim that a is adjacent to all elements in I as well. Let gt be an element in I. We need to show that

$$gcd(a - gt, f) \in D.$$

Since $(a, 0) \in E(G_f(D))$ we know that $\gcd(a, f) \in D$. Because $a \notin I$, we know further that $\gcd(a, f) \in D_1$. Additionally, by Lemma 3.5, we must have $\gcd(a, g) = \gcd(\gcd(a, f), g) \in \overline{D_1}$. By Lemma 3.5, we conclude that $\gcd(a, g) \in \overline{D_1}$. Again, by Lemma 3.5, we have

$$\gcd(\gcd(a - gt, f), g) = \gcd(a - gt, g) = \gcd(a, g) \in \overline{D_1}.$$

Because $D_1 = \Phi_{f,g}^{-1}(\overline{D_1}) \cap \text{Div}(f)$, this shows that $\gcd(a-gt, f) \in D_1$ and hence $\gcd(a-gt, f) \in D$ as required.

Conversely, we claim that (1) implies (2). Suppose that I is a homogeneous set in $G_f(D)$. We need to show that $D_1 = \Phi_{f,g}^{-1}(\overline{D_1}) \cap \text{Div}(f)$. By Proposition 3.6, we always have $D_1 \subset \Phi_{f,g}^{-1}(D_1) \cap \text{Div}(f)$. Therefore, it is sufficient to show that $\Phi_{f,g}^{-1}(\overline{D_1}) \cap \text{Div}(f) \subset D_1$. Let $h \in \Phi_{f,g}^{-1}(D_1) \cap \text{Div}(f)$. By definition, there exists $f_i \in D_1$ such that

$$\gcd(h, g) = \gcd(f_i, g).$$

By Lemma 5.3, we can find $t \in \mathbb{F}_q[x]$ such that

$$\gcd(h - gt, f) = f_i.$$

This shows that $(h, gt) \in E(G_f(D))$. Since I is homogenous and $h \notin I$, we conclude that $(h, 0) \in E(G_f(D))$ as well. By definition, $\gcd(h, f) \in D$. Since $h \mid f$, we conclude that $h \in D$ and hence $h \in D_1$.

□

In general, it seems unclear how to check the conditions mentioned in Theorem 5.5 explicitly. We discuss here a particular case when this can be done.

Proposition 5.6. *Let f, g, I be as in Theorem 5.5 . Assume further that $f_i \nmid f_j$ for all $i \neq j$ and $\gcd(f_1, f_2, \ldots, f_k) = 1$. Then I is a homogenous set in $G_f(D)$ if and only if the following conditions hold*

(1) For each $1 \leq i \leq k$, $f_i \mid g$ for all i.

(2) Furthermore,

$$rad\left(\frac{g}{f_i}\right) = rad\left(\frac{f}{f_i}\right).$$

In particular, if f is squarefree then $f = g$.

Proof. Let us first assume that I is homogenous. Let $g_i = \gcd(f_i, g)$. We claim that if $f_i \in D_1$ then $g_i = f_i$ and hence $f_i \mid g$. In fact, we have $\gcd(g_i, g) = g_i = \gcd(f_i, g)$. This shows that $g_i \in \Phi_{f,g}^{-1}(\overline{D_1}) \cap \mathrm{Div}(f) = D_1$ (by Theorem 5.5). Since $f_i \nmid f_j$ for all $i \neq j$, we must have $f_i = g_i$ and hence $f_i \mid g$. By our assumption, $\gcd(f_1, f_2, \ldots, f_k) = 1$, and hence we must have $D_1 \neq \emptyset$. If $D_2 \neq \emptyset$ then for each $f_1 \in D_1$ and $f_2 \in D_2$, we have $f_1 \mid g \mid f_2$ which is a contradiction. Therefore, we must have $D_2 = \emptyset$. In summary, we just prove that $f_i \mid g$ for all $1 \leq i \leq k$. We now show that

$$\mathrm{rad}\left(\frac{g}{f_i}\right) = \mathrm{rad}\left(\frac{f}{f_i}\right).$$

Suppose this is not the case. We can find a non-constant irreducible polynomial h of such that $\gcd(h, \frac{g}{f_i}) = 1$ and $h | \frac{f}{f_i}$. We then see that $\gcd(hf_i, g) = f_i = \gcd(f_i, g)$. This implies that $hf_i \in D$. Since $f_i \mid hf_i$ and $f_i \neq hf_i$, this leads to a contradiction.

Let us now show the converse. By Theorem 5.5, we need to show that if $h \in \Phi_{f,g}^{-1}(\overline{D_1}) \cap \mathrm{Div}(f)$ then $h \in D_1$. Since $h \in \Phi_{f,g}^{-1}(\overline{D_1})$ we can find $f_i \in D_1$ such that $\gcd(h, g) = \gcd(f_i, g) = f_i$. Let us write $h = f_i h_1$ with $\gcd(h_1, \frac{g}{f_i}) = 1$. By our assumption that $\mathrm{rad}\left(\frac{g}{f_i}\right) = \mathrm{rad}\left(\frac{f}{f_i}\right)$, we must have $\gcd(h_1, \frac{f}{f_i}) = 1$ as well. Since $h_1 \mid \frac{f}{f_i}$, we must have $h_1 = 1$ and hence $h = f_i$. □

Corollary 5.7. *Let that f be a squarefree polynomial. Suppose that $G_f(\{1\})$ is connected. Let $D = \{f_1, f_2, \ldots, f_k\}$ be a subset of Div(f) such that the following conditions hold*

(1) $f_i \nmid f_j$ for all $i \neq j$.

(2) $G_f(D)$ is connected and anti-connected.

Then $G_f(D)$ is prime.

Proof. Suppose that $G_f(D)$ is not prime. By Proposition 5.2, there exists a proper divisor $g \mid f$ such that the ideal I generated by g is homogeneous. By Proposition 5.6, we must have $g = f$ which is a contradiction. □

Remark 5.8. Everything we do in this section applies to gcd-graphs over $\mathbb{Z}$ as well. To the best of our knowledge, even over $\mathbb{Z}$, this topic has not been explored in the literature.

Remark 5.9. The proof of Proposition 5.6 relies crucially on the divisibility relationship between f_i and f_j. It seems important to study this relationship systematically. We are studying this problem in a work in progress (see [21]).

6. Spectrum of gcd graphs

The spectrum of gcd-graphs over $\mathbb{Z}$ is described by the theory of Ramanujan sums (see [17, Section 4]), which in turn is a special case of Gauss sums (see [20]). As explained in [6], these sums are precisely values of Fekete polynomials at certain n-roots of unity. One might wonder whether such a similar statement for the spectrum of gcd-graphs holds in the context of function fields. It turns out that the answer is yes as we will explain in this section.

6.1. **Symmetric algebras.** A key point in the theory of $\mathbb{Z}/n$-circulant graph is the fact that the character group of $\mathbb{Z}/n$ is isomorphic to $\mathbb{Z}/n$

$$\mathbb{Z}/n \cong \mathrm{Hom}(\mathbb{Z}/n, \mathbb{C}^\times).$$

This isomorphism can be obtained as follows. Fix a primitive n-root of unity ζ_n in $\mathbb{C}$. Let $\chi_1 : \mathbb{Z}/n \to \mathbb{C}^\times$ be the character defined by $\chi_1(m) = \zeta_n^m$ for all $m \in \mathbb{Z}/n$. For each $a \in \mathbb{Z}/n$, let $\chi_a = \chi_1^a$ be the character of $\mathbb{Z}/n$ defined by $\chi_a(b) = \zeta_n^{ab} = \chi_1^a(b)$. The following proposition is standard.

Proposition 6.1. *The map $a \mapsto \chi_1^a$ gives an isomorphism between $\mathbb{Z}/n$ and Hom$(\mathbb{Z}/n, \mathbb{C}^\times)$.*

In summary, once we fix a primitive n-root of unity, the isomorphism $\mathbb{Z}/n \cong \mathrm{Hom}(\mathbb{Z}/n, \mathbb{C}^\times)$ is obtained via the multiplicative structure on $\mathbb{Z}/n$. We will use a similar approach in the function field case. We first recall the following definition.

Definition 6.2. (See [19, Page 66-67]) Let A be a finite dimensional commutative $\mathbb{F}_q$-algebra. A is said to be a symmetric $\mathbb{F}_q$-algebra if there exists an $\mathbb{F}_q$-linear functional $\lambda : A \to \mathbb{F}_q$ such that the kernel of λ contains no nonzero ideal of A. We call λ a non-degenerate linear function on A.

Example 6.3. Let $\mathbb{F}_{q^r}$ be a finite extension of $\mathbb{F}_q$. Then, $\mathbb{F}_{q^r}$ equipped with the canonical trace map $\mathrm{Tr} : \mathbb{F}_{q^r} \to \mathbb{F}_q$ is a symmetric $\mathbb{F}_q$-algebra.

The following lemma is rather standard.

Lemma 6.4. *Suppose that A is a symmetric $\mathbb{F}_{q^r}$-algebra with a $\mathbb{F}_{q^r}$-linear functional $\lambda : A \to \mathbb{F}_{q^r}$. Then A is a symmetric $\mathbb{F}_q$-algebra where the linear functional is the composition of λ and Tr : $\mathbb{F}_{q^r} \to \mathbb{F}_q$.*

Proposition 6.5. *Let A be a symmetric finite dimensional $\mathbb{F}_q$-algebra and $\lambda : A \to \mathbb{F}_q$ an associated non-degenerate $\mathbb{F}_q$-linear functional. For each $a \in A$, let $\lambda_a : A \to \mathbb{F}_q$ be the $\mathbb{F}_q$-linear map defined by $\lambda_a(b) = \lambda(ab)$. Let Φ be the map $A \to Hom_{\mathbb{F}_q}(A, \mathbb{F}_q)$ sending $a \mapsto \lambda_a$. Then Φ is an isomorphism.*

Proof. Since λ is non-degenerate, Φ is injective. Furthermore, because A is finite dimensional over $\mathbb{F}_q$, $\dim(A) = \dim(\mathrm{Hom}_{\mathbb{F}_q}(A, \mathbb{F}_q))$. Since Φ is $\mathbb{F}_q$-linear, it must be an isomorphism. □

Fix a primitive p-root of unity $\zeta_p \in \mathbb{C}^\times$. Then, $\mathbb{F}_p$ is (non)-cannonically a group of $\mathbb{C}^\times$. If A is an $\mathbb{F}_q$-algebra, then $(A, +)$ is a direct sum of several copies of $\mathbb{F}_p$. Therefore

$$\mathrm{Hom}((A, +), \mathbb{C}^\times) \cong \mathrm{Hom}_{\mathbb{F}_p}(A, \mathbb{F}_p).$$

By Proposition 6.5 we have the following corollary, which is a direct analog of Proposition 6.1.

Corollary 6.6. *Let A be a symmetric $\mathbb{F}_p$-algebra together with a non-degenerate functional $\lambda : A \to \mathbb{F}_p$. For each $a \in A$, let $\lambda_a : A \to \mathbb{C}^\times$ defined by $\lambda_a(b) = \zeta_p^{\lambda(ab)}$. Then $\lambda \in$ Hom$((A, +), \mathbb{C}^\times)$. Furthermore, the map $a \mapsto \lambda_a$ gives an isomorphism between A and Hom$((A, +), \mathbb{C}^\times)$.*

We will now focus on the case $A = \mathbb{F}_q[x]/f$. We will show that it is a symmetric $\mathbb{F}_q$-algebra (and hence a symmetric $\mathbb{F}_p$-algebra as explained in Lemma 6.4). We will show this by constructing an explicit $\mathbb{F}_q$-linear functional on A. We learned about this construction in [18]. Every element g in $\mathbb{F}_q[x]/f$ can be written uniquely in the form

$$g = a_0(g) + a_1(g) + \ldots + a_{n-1}(g)x^{n-1}.$$

We define $\psi : \mathbb{F}_q[x]/f \to \mathbb{F}_q$ by

$$\psi(g) = a_{n-1}(g).$$

Proposition 6.7. *Suppose $g \in \mathbb{F}_q[x]/f$ such that $\psi(hg) = 0$ for all $h \in \mathbb{F}_q[x]/f$. Then $g = 0$ in $\mathbb{F}_q[x]/f$.*

Proof. Let us write $g = a_0(g) + a_1(g) + \ldots + a_{n-1}(g)x^{n-1}$. We will prove by induction that $a_{n-k}(g) = 0$ for $1 \leq k \leq n$. In fact, since $\psi(g) = 0$, we know that $a_{n-1}(g) = 0$. Consequently, the statement is true for $k = 1$. Let us assume that it has been for all $1 \leq k \leq m < n$. We claim that it is also true for $m+1$, namely $a_{n-m-1}(g) = 0$ as well. In fact, we have

$$\begin{aligned} x^{m-1}g &= x^{m-1}a_0(g) + \ldots + a_{n-m-1}(g)x^{n-1} + a_{n-m}(g)x^n + \ldots + a_{n-1}(g)x^{m+n-2} \\ &= a_0(g) + \ldots + a_{n-m-1}(g)x^{n-1}. \end{aligned}$$

Consequently

$$a_{n-m-1}(g) = \psi(x^{m-1}g) = 0.$$

By the induction principle, we conclude that $a_{n-k} = 0$ for all $1 \leq k \leq n$.

□

Corollary 6.8. *ψ is a non-degenerate $\mathbb{F}_q$-linear functional on $\mathbb{F}_q[x]/f$. Consequently, $\mathbb{F}_q[x]/f$ is a symmetric $\mathbb{F}_q$-algebra.*

By Lemma 6.4, under the composition $\mathbb{F}_q[x]/f \xrightarrow{\psi} \mathbb{F}_q \xrightarrow{Tr} \mathbb{F}_p$ where Tr is the trace map, $\mathbb{F}_q[x]/f$ becomes a symmetric $\mathbb{F}_p$-algebra. By Corollary 6.6, we have the following proposition.

Proposition 6.9. *There exists a bijection*

$$Hom((\mathbb{F}_q[x]/f, +), \mathbb{C}^\times) \longleftrightarrow \{\psi_a\}$$

where

$$\psi_a : \mathbb{F}_q[x]/f \to \mathbb{C}^\times$$

is given by

$$\psi_a(b) = \zeta_p^{Tr(\psi(ab))}, \forall b \in \mathbb{F}_q[x]/f.$$

We remark that over $\mathbb{Z}$, if ζ_n is a prime n-root of unity, then for each divisor $m \mid n$, $\zeta_n^{\frac{n}{m}}$ is a primitive m-root of unity. An analogous statement holds for $\mathbb{F}_q[x]$ as well.

Proposition 6.10. *Let $f \in \mathbb{F}_q[x]$ and $\psi : \mathbb{F}_q[x]/f \to \mathbb{F}_q$ be a non-degenerate linear functional. Let g be a divisor of f and $\psi_g : \mathbb{F}_q[x]/g \to \mathbb{F}_q$ be the function defined by*

$$\psi_g(a) = \psi\left(\frac{f}{g}a\right).$$

Then ψ_g is a non-degenerate linear functional on $\mathbb{F}_q[x]/g$.

Proof. It is clear from the definition that ψ_g is $\mathbb{F}_q$-linear. We only need to show that it is non-degenrate. In fact, suppose to the contrary that the kernel of ψ_g contains a non-zero ideal I in $\mathbb{F}_q[x]/g$. Since $\mathbb{F}_q[x]$ is a PID, I must be of the form $I = \langle h \rangle$ for some $h|g$. We then see that $\langle h\frac{f}{g}\rangle$ belongs to the kernel of ψ. Because ψ is non-degenerate, this implies that $h\frac{f}{g} = 0$ in $\mathbb{F}_q[x]/f$. In other words, $g|h$ or equivalently $h = 0$ in $\mathbb{F}_q[x]/g$. This shows that $I = 0$, which is a contradiction. □

6.2. **Ramanujan sums over $\mathbb{F}_q[x]$.** We now introduce the definition of Ramanujan sum over $\mathbb{F}_q[x]$.

Definition 6.11. (Ramanujan sums over $\mathbb{F}_q[x]$) Let $f, g \in \mathbb{F}_q[x]$ be monic polynomials. The Ramanujan sum $c(g, f)$ is defined as

$$c(g,f) = \sum_{a \in (\mathbb{F}_q[x]/f)^\times} \zeta_p^{\mathrm{Tr}(\psi(ga))}.$$

Remark 6.12. We remark also that at first glance, $c(g, f)$ depends on the choice of ψ. However, as we explain in what follows, it does not. This is similar to the case over $\mathbb{Z}$: Ramanujan sums do not depend on the choice of a primitive n-root of unity. In fact, we will show that there is an explicit formula for $c(g, f)$ similar to the case of Ramanujan sum over $\mathbb{Z}$.

Remark 6.13. Ramanujan sums are a special case of Gauss sums as defined and studied in [20, Definition 1]. In fact, they are Gauss sums for the principal Dirichlet characters on $\mathbb{F}_q[x]/f$. It would be rather interesting if we can define a Fekete polynomials for these principal Dirichlet characters (the case over $\mathbb{Z}$ was studied in [6]).

We first recall the following standard lemma in group theory.

Lemma 6.14. *Let $\chi : G \to \mathbb{C}^\times$ be a non-trivial character. Then*

$$\sum_{g \in G} \chi(g) = 0.$$

Proof. Since χ is non-trivial, there exists $h \in G$ such that $\chi(h) \neq 1$. We then have

$$\sum_{g \in G} \chi(g) = \sum_{h \in G} \chi(hg) = \chi(h) \sum_{g \in G} \chi(g).$$

Because $\chi(h) \neq 1$, we must have $\sum_{g \in G} \chi(g) = 0$. □

Proposition 6.15. *For each $f \in \mathbb{F}_q[x]$*

$$c(1, f) = \mu(f),$$

where μ is the Mobius function on $\mathbb{F}_q[x]$.

Proof. If $f = \prod_{i=1}^d f_i^{\alpha_i}$ where $\alpha_i \in \mathbb{N}$ and f_i are irreducible, then by [20, Satz 1] we have

$$c(1, f) = \prod_{i=1}^d c(1, f_i^{\alpha_i}).$$

Therefore, it is enough to consider the case $f = f_1^{a_1}$ where f_1 is irreducible. We have

$$c(1,f) = \sum_{a \in (\mathbb{F}_q[x]/f)^\times} \zeta_p^{\mathrm{Tr}(\psi(a))} \tag{6.1}$$

$$= \sum_{a \in \mathbb{F}_q[x]/f} \zeta_p^{\mathrm{Tr}(\psi(a))} - \sum_{a \in \mathbb{F}_q[x]/f_1^{a_1-1}} \zeta_p^{\mathrm{Tr}(\psi(f_1 a))} \tag{6.2}$$

By Lemma 6.14

$$\sum_{a \in \mathbb{F}_q[x]/f} \zeta_p^{\mathrm{Tr}(\psi(a))} = 0.$$

Similarly, if $a_1 \geq 2$ then by Lemma 6.14 and Proposition 6.10

$$\sum_{a \in \mathbb{F}_q[x]/f_1^{a_1-1}} \zeta_p^{\mathrm{Tr}(\psi(f_1 a))} = 0.$$

On the other hand if $a_1 = 1$ then $\sum_{a \in \mathbb{F}_q[x]/f_1^{a_1-1}} \zeta_p^{\mathrm{Tr}(\psi(f_1 a))} = -1$. We conclude that

$$c(1,f) = c(1, f_1^{a_1}) = \mu(f_1^{a_1}) = \mu(f).$$

□

Theorem 6.16. *Let $f, g \in \mathbb{F}_q[x]$ be monic polynomials. Then (compare with* [17, Equation 9]*)*

$$c(g,f) = \mu(t)\frac{\varphi(f)}{\varphi(t)}, \quad \textit{where} \quad t = \frac{f}{\gcd(f,g)}.$$

6.3. **Spectrum of $G_f(D)$.** Let G be an abelian group and S a symmetric subset of G such that $0 \notin S$. The adjacency matrix of the Cayley graph $\Gamma(G,S)$ is a G-circulant matrix. By the G-circulant theorem, the spectrum of $\Gamma(G,S)$ is the collection of the sums $\sum_{s \in S} \chi(s)$, where χ runs over the set of all characters of G (see [13, Section 1.2]). When $G = \mathbb{F}_q[x]/f$, we know by Proposition 6.9 that the character of G is parameterized by G itself. Consequently, we have the following proposition.

Proposition 6.17. *Let S be a subset of $\mathbb{F}_q[x]$. Then the spectrum of the Cayley graph $\Gamma(\mathbb{F}_q[x]/f, S)$ is given by the set*

$$\left\{ \sum_{s \in S} \zeta_p^{Tr(\psi(gs))} \right\}_{g \in \mathbb{F}_q[x]/f}.$$

Let us now focus on the case of gcd-graphs; i.e, $S = S_D$. We have the following lemma.

Lemma 6.18. *Let $h \mid f$ be a monic divisor of f. Then for each $g \in \mathbb{F}_q[x]$*

$$\sum_{a \in \mathbb{F}_q[x]/f, \gcd(a,f)=h} \zeta_p^{Tr(\psi(ag))} = c\left(g, \frac{f}{h}\right).$$

Proof. For $a \in \mathbb{F}_q[x]$, $\gcd(a,f) = h$ if and only if $a = hb$ where $\gcd(b, \frac{f}{h}) = 1$. Therefore, the above sum can be rewritten as

$$\sum_{b \in \mathbb{F}_q[x]/(f/h), \gcd(a, f/h)=1} \zeta_p^{\mathrm{Tr}(\psi(bgh))} = \sum_{b \in \mathbb{F}_q[x]/(f/h), \gcd(b, f/h)=1} \zeta_p^{\mathrm{Tr}(\psi_h(bg))}.$$

Here $\psi_h : \mathbb{F}_q[x]/(f/h) \to \mathbb{F}_q$ is the functional given by $\psi_h(x) = \psi(hx)$. By Proposition 6.10, ψ_h is a non-generate linear functional on $\mathbb{F}_q[x]/(f/g)$. Therefore, we conclude that

$$\sum_{a \in \mathbb{F}_q[x]/f, \gcd(a,f)=h} \zeta_p^{\mathrm{Tr}(\psi(ag))} = \sum_{b \in \mathbb{F}_q[x]/(f/h), \gcd(b, f/h)=1} \zeta_p^{\mathrm{Tr}(\psi_h(bg))} = c\left(g, \frac{f}{h}\right).$$

□

By Proposition 6.17 and Lemma 6.18, we have the following theorem.

Theorem 6.19. *Let f be a monic polynomial and $D = \{f_1, f_2, \ldots, f_k\}$ where $f_i \mid f$. Then, the spectrum of $S_f(D)$ is given by the set*

$$\left\{\sum_{i=1}^{k} c\left(g, \frac{f}{f_i}\right)\right\}_{g \in \mathbb{F}_q[x]/f}.$$

Corollary 6.20. *All eigenvalues of the gcd-graph $G_f(D)$ are integers.*

As we discussed in the introduction, it is known that a $\mathbb{Z}/n$-circulant graph has an integral spectrum if and only if it is a gcd-graph (see [28, Theorem 7.1]). One may ask whether the same statement is true for graphs associated with $\mathbb{F}_q[x]/f$. The answer is no in general. In fact, we have the following general observation.

Proposition 6.21. *Let S be a symmetric subset of $\mathbb{F}_q[x]/f$ such that $0 \notin S$. Suppose further that $\mathbb{F}_p^\times S = S$. Then, the Cayley graph $\Gamma(\mathbb{F}_q[x]/f, S)$ has an integral spectrum.*

Proof. We define the following equivalence relation on $\mathbb{F}_q[x]/f$. For $u, v \in \mathbb{F}_q[x]/f$, we say that $u \sim v$ if $a = kb$ where $k \in \mathbb{F}_p^\times$. By Proposition 6.17, it is enough to show that for each $g \in \mathbb{F}_q[x]/f$, $\sum_{s \in S} \zeta_p^{\mathrm{Tr}(\psi(gs))} \in \mathbb{Z}$. Because $\mathbb{F}_p^\times S = S$, this sum can be written as

$$\sum_{[s] \in S/\sim} \left(\sum_{k \in \mathbb{F}_p^\times} \zeta_p^{\mathrm{Tr}(\psi(gks))}\right) = \sum_{[s] \in S/\sim} \left(\sum_{k \in \mathbb{F}_p^\times} (\zeta_p^{\mathrm{Tr}(\psi(gs))})^k\right).$$

We know that

$$\sum_{k \in \mathbb{F}_p^\times} (\zeta_p^{\mathrm{Tr}(\psi(gs))})^k = \begin{cases} -1 & \text{if } \mathrm{Tr}(\psi(gs)) \neq 0 \\ p-1 & \text{if } \mathrm{Tr}(\psi(gs)) = 0. \end{cases}$$

This shows that $\sum_{s \in S} \zeta_p^{\mathrm{Tr}(\psi(gs))} \in \mathbb{Z}$ for each $g \in \mathbb{F}_q[x]/f$. □

Remark 6.22. Let $\mathbb{F}_q$ be a finite field such that $\mathbb{F}_q \neq \mathbb{F}_p$. Let $f = x$. In this case $\mathbb{F}_q[x]/f \cong \mathbb{F}_q$. Let V be proper $\mathbb{F}_p$-subspace of $\mathbb{F}_q$ and $S = V \setminus \{0\}$. Then by Proposition 6.21, $\Gamma(\mathbb{F}_q[x]/f, S)$ has an integral spectrum even though it is not a gcd-graph.

We wonder whether the converse of Proposition 6.21 holds (perhaps, under some mild assumptions).

7. Perfect gcd-graphs

A graph G is said to be perfect if, for every induced subgraph H of G, the chromatic number of H equals the size of its maximum clique. Perfect graphs play a fundamental role in the study of graph coloring and cliques. They encompass several important families of graphs and provide a unified framework for results relating to colorings and cliques within these families. Moreover, many central problems in combinatorics can be rephrased as questions about whether certain associated graphs are perfect (see [8, 9, 23]). For these reasons, it seems interesting to study whether $G_f(D)$ is perfect.

In [1, Theorem 9.5], the authors classify all perfect unitary Cayley graphs associated with finite commutative rings. Specifically, for a ring $R = R_1 \times R_2 \times \ldots \times R_t$ where R_i are finite local rings, the unitary Cayley graph on R is perfect if and only if one of the following conditions hold

(1) The residue field of R_1 is 2. In this case, G_R is bipartite and hence perfect.
(2) R is either a local ring or a product of two local rings; i.e, $t \leq 2$.

A direct consequence of [1, Theorem 9.5] for the unitary Cayley graph over $\mathbb{Z}$ is the following.

Corollary 7.1. *The unitary Cayley graph on $\mathbb{Z}/N$ is perfect if and only if one of the following conditions hold*

(1) $2 \mid N$.
(2) $\omega(N) \leq 2$ *where* $\omega(N)$ *is the number of distinct irreducible factors of* N.

Over the polynomial ring $\mathbb{F}_q[x]$, we have an analogous statement.

Corollary 7.2. *The unitary Cayley graph $G_f(\{1\})$ on $\mathbb{F}_q[x]/f$ is perfect if and only if one of the following conditions hold*

(1) $\mathbb{F}_q = \mathbb{F}_2$ *and* $gcd(f, x(x+1)) \neq 1$.
(2) $\omega(f) \leq 2$ *where* $\omega(f)$ *is the number of distinct irreducible factors of* f.

We will use Corollary 7.2 together with patterns of $G_f(D)$ discovered through our experiments in Sagemath and the Python package Networkx in order to find some sufficient conditions for $G_f(D)$ to be *non-perfect.* In particular, we will exploit the fact that certain induced subgraphs of $G_f(D)$ are naturally isomorphic to the unitary Cayley graphs on some quotient rings of $R = \mathbb{F}_q[x]/f$. More precisely, by Lemma 5.4, we have the following observation.

Proposition 7.3. *Suppose $g \in D$ such that $g \nmid f_i$ for all i such that $f_i \neq g$. Then the induced graph on I_g is naturally isomorphic to the unitary Cayley graph $G_{f/g}(\{1\})$. Furthermore, if $\omega(f/g) \geq 3$ and $\mathbb{F}_q \neq \mathbb{F}_2$, then $G_{f/g}(D)$ is not perfect and hence $G_f(D)$ is not perfect.*

We discuss a case where we can apply Proposition 7.3 rather directly.

Proposition 7.4. *Let $f \in \mathbb{F}_q[x]$ and $S_D = \{f_1, f_2, \ldots, f_k\}$ be a subset of divisors of f. Suppose that the following conditions hold*

(1) $\deg(f_i) \geq 1$.

(2) f_i's are pairwisely relatively prime; i.e, $\gcd(f_i, f_j) = 1$ *for all* $i \neq j$.

(3) $k \geq 3$.

(4) $\mathbb{F}_q \neq \mathbb{F}_2$.

Then $G_f(D)$ *is not a perfect graph.*

Proof. If $k \geq 4$ then

$$\omega(f/f_1) \geq \omega(f_2) + \omega(f_3) + \omega(f_4) \geq 3.$$

By applying Proposition 7.3 for $g = f_1$, we conclude that $G_f(D)$ is not perfect. Let us assume now that $k = 3$. By the same argument, it is enough to consider the case $\omega(f_1) = \omega(f_2) = \omega(f_3) = 1$. Furthermore, if $f \neq f_1f_2f_3$, then there exists an index $i \in \{1, 2, 3\}$ such that $\omega(f/f_i) \geq 3$. As a result, $G_f(D)$ is not perfect by Proposition 7.3. Let us now consider the case $f = f_1f_2f_3$. In this case

$$\mathbb{F}_q[x]/f \cong \mathbb{F}_q[x]/f_1 \times \mathbb{F}_q[x]/f_2 \times \mathbb{F}_q[x]/f_3.$$

Under this isomorphism, we can identify $V(G_f(D))$ as the set of all triples (a_1, a_2, a_3) where $a_i \in \mathbb{F}_q[x]/f_i$ for $1 \leq i \leq 3$. Furthermore, two vertices (a_1, a_2, a_3) and (b_1, b_2, b_3) are adjacent if and only if there exists an index $i \in \{1, 2, 3\}$ such that $a_i = b_i$ and $(a_j - b_i) \in (\mathbb{F}_q[x]/f_j)^\times$ if $j \neq i$. Using Sagemath, we can find the following induced 5-cycle in $G_f(D)$

$$(0, 0, 0) \to (\alpha, \alpha, 0) \to (1, \alpha, 1) \to (1, 1, \alpha) \to (\alpha, 1, 0),$$

where $\alpha \in \mathbb{F}_q \setminus \{0, 1\}$. This show that $G_f(D)$ is not perfect. □

The case $k = 2$ is a bit more challenging. After some experiments with Sagemath, we found the following statement.

Proposition 7.5. *Let* $f \in \mathbb{F}_q[x]$ *and* $S_D = \{f_1, f_2\}$ *be a subset of divisors of* f *such that* $\gcd(f_1, f_2) = 1$. *Suppose that the following conditions hold*

(1) $\mathbb{F}_q \neq \mathbb{F}_2$.

(2) $\omega(f_1) \geq 2$, $\omega(f_2) \geq 1$.

Then, $G_f(D)$ *is not perfect.*

Proof. Let us assume to the contrary that $G_f(D)$ is perfect. Since $\gcd(f_1, f_2) = 1$, we have $f_1f_2 \mid f$ and hence

$$\omega(f) \geq \omega(f_1) + \omega(f_2).$$

If $\omega(f) > \omega(f_1) + \omega(f_2)$ then $\omega(f/f_2) > \omega(f_1) \geq 2$. By Proposition 7.3, we know $G_f(D)$ is not perfect. Therefore, we must have $\omega(f) = \omega(f_1) + \omega(f_2)$.

Let $g = f_1f_2$. By Proposition 5.6, the ideal generated by g is a homogeneous set in $G_f(D)$ and furthermore $G_f(D)$ is isomorphic to the wreath product $G_g(\{f_1, f_2\}) * G_{f/g}(\emptyset)$. Since $G_f(D)$ is perfect, $G_g(\{f_1, f_2\})$ is perfect as well. Because $\omega(f_1) \geq 2$, we can find $h_1, h_2 \in \mathbb{F}_q[x]$ such that $f_1 = h_1h_2$ and $\gcd(h_1, h_2) = 1$. By the Chinese remainder theorem

$$\mathbb{F}_q[x]/g \cong \mathbb{F}_q[x]/h_1 \times \mathbb{F}_q[x]/h_2 \times \mathbb{F}_q[x]/f_2.$$

Under this isomorphism, we can identify $\mathbb{F}_q[x]/g$ with the set of tuples (a_1, a_2, a_3) such that $a_1 \in \mathbb{F}_q[x]/h_1, a_2 \in \mathbb{F}_q[x]/h_2, a_3 \in \mathbb{F}_q[x]/f_2$. Furthermore, two vertices (a_1, a_2, a_3) and (b_1, b_2, b_3) are adjacent if and only if one the following conditions happen

(1) $a_1 = b_1, a_2 = b_2$ and $a_3 - b_3 \in (\mathbb{F}_q[x]/f_2)^\times$.

(2) $a_3 = b_3$ and $a_i - b_i \in (\mathbb{F}_q[x]/h_i)^\times$ for $i \in \{1, 2\}$.

Using Sagemath, we can find the following 7-cycle in $G_g(\{f_1, f_2\})$

$$(0,0,0) \to (1,1,0) \to (\alpha,0,0) \to (\alpha,0,1) \to (0,1,1) \to (\alpha,\alpha,1) \to (0,0,1),$$

where $\alpha \in \mathbb{F}_q \setminus \{0,1\}$. We conclude that $G_g(\{f_1, f_2\})$ is not a perfect graph, which is a contradiction. □

Remark 7.6. Curious readers might wonder why we choose a 7-cycle in the proof of Proposition 7.5 instead of choosing a 5-cycle as in the proof of Proposition 7.4. The reason is that when $\omega(f_1) = 2, \omega(f_2) = 1$ and $f = f_1 f_2$, our code cannot find 5-cycle in $G_f(D)$. It seems interesting to investigate whether this is always the case.

Remark 7.7. The only remaining case that we miss is when $\omega(f_1) = \omega(f_2) = 1$. We distinguish the following cases.

(1) If $f = f_1 f_2$ where both f_1, f_2 are irreducible then $G_f(D)$ is isomorphic to the complement of $G_f(\{1\})$ which is perfect by Corollary 7.2. Therefore, $G_f(D)$ is perfect as well.

(2) On the other hand, if either f_1 or f_2 is reducible, our code can always find a 7-cycle in $G_f(D)$. Unfortunately, we cannot find a universal pattern in this case. It would be quite interesting to solve this puzzle completely.

8. Induced subgraphs of gcd-graphs

A theorem of Erdős and Evans (see [10])says that every graph G is an induced subgraph of the unitary Cayley graph on $\mathbb{Z}/n$ for some squarefree n. Using this result, it is shown in [15] that for a given finite graph G and a finite field F, G is an induced subgraph of the unitary graph of a matrix algebra $M_d(F)$ for some value of d (they also provide some precise upper-bound on d when G is the complete graph K_m). In light of these results, it seems interesting to ask whether a graph G can be realized as an induced subgraph of $G_f(D)$ for some choice of f, D and $\mathbb{F}_q$. Under some rather mild conditions, the answer is yes as we will show below. First, we introduce the following observation.

Lemma 8.1. *If G is an induced subgraph of H, then G is also an induced subgraph of the product $H \times K_{|G|}$ where $K_{|G|}$ is the complete graph on $|G|$-nodes.*

Proof. Let $f\colon G \to H$ be a graph morphism that makes G into an induced subgraph of H. Let us index $V(G) = \{v_1, v_2, \ldots, v_{|G|}\}$. Let $\hat{f}\colon G \to H \times K_{|G|}$ be the map defined by

$$\hat{f}(v_i) = (f(v_i), i).$$

We can see that $\hat{f}$ is a graph morphism which turns G into an induced subgraph of $H \times K_{|G|}$. □

We are now ready to prove an analog of Erdős-Evans's theorem in the function fields case.

Proposition 8.2. *Let G be a fixed graph and q a fixed prime power. There exists a positive integer r such that for each $d \geq r$, we can find $F_d \in \mathbb{F}_q[x]$ satisfying the following conditions*

(1) $\omega(F_d) = d$,

(2) G is an induced subgraph of the unitary Cayley graph $G_{F_d}(\{1\})$.

Proof. By Erdős and Evans's theorem [10], there exists a squarefree integer $n \in \mathbb{N}$ such that G is an induced subgraph of the unitary graph G_n on $\mathbb{Z}/n$. Let $r = \omega(n)$; i.e, $n = p_1p_2 \ldots p_r$ be the prime factorization of n. Then

$$G_n \cong \prod_{i=1}^{r} G_{p_i} \cong \prod_{i=1}^{r} K_{p_i}.$$

For each $i \in \mathbb{N}$ and $m_i \in \mathbb{N}$, there exists a polynomial h_i of degree m_i such that h_i is irreducible over $\mathbb{F}_q[x]$. We then see that $G_{h_i}(\{1\})$ is isomorphic to the complete graph $K_{q^{m_i}}$. Let us choose m_i so that $q^{m_i} > n$ for all i. For each $d \geq r$, let $F_d = h_1h_2 \ldots h_d$. We then have

$$G_{F_d}(\{1\}) \cong \prod_{i=1}^{d} G_{h_i}(\{1\}) \cong \prod_{i=1}^{d} K_{q^{m_i}}.$$

Since $q^{m_i} > n$, we know that G_n is an induced subgraph of $G_{F_r}(\{1\})$. By Lemma 8.1 , G is an induced subgraph of $G_{F_d}(\{1\})$ as well.

□

Corollary 8.3. *Let G be a fixed graph and k a fixed positive integer. Then, there exist a polynomial f and a subset $D = \{f_1, f_2, \ldots, f_k\}$ of divisors of f such that G is an induced subgraph of $G_f(D)$.*

Proof. Let h_0 be an arbitrary polynomial in $\mathbb{F}_q[x]$. By Proposition 8.2, there exists a positive integer $d \geq k$ and a polynomial h of the form $h = h_1h_2 \ldots h_d$ such that G is an induced subgraph of $G_h(\{1\})$. Let us choose $f = h_0h$ and

$$\{f_1, f_2, \ldots, f_k\} = \{h_1, h_2, \ldots, h_k\}.$$

Let I be the ideal generated by h_0 in $\mathbb{F}_q[x]/f$. By Lemma 5.4 the induced graph on I is naturally isomorphic to the unitary Cayley graph $G_h(\{1\})$. This shows that G is an induced subgraph of $G_f(D)$. □

One may wonder whether the following stronger form of Corollary 8.3 holds. Let G be a fixed graph and $f_1, f_2, \ldots, f_k$ fixed polynomials. Does there exist a polynomial f such that

(1) $f_i \mid f$ for all $1 \leq i \leq k$.

(2) G is an induced subgraph of $G_f(D)$ where $D = \{f_1, f_2, \ldots, f_k\}$.

In general, the answer is no. There seem to be some subtle constraints. We discuss here a particle one. Let $g = \operatorname{lcm}(f_1, f_2, \ldots, f_k)$ and assume further that $g \neq f_i$ for all $1 \leq i \leq k$. If such f exists, then $g \mid f$ and there is a canonical map

$$\Phi : \mathbb{F}_q[x]/f \to \mathbb{F}_q[x]/g.$$

If we take a subset $S \subset \mathbb{F}_q[x]/f$ such that $|S| > |\mathbb{F}_q[x]/g|$, then there exists $a, b \in S$ such that $a \neq b$ and $\Phi(a) = \Phi(b)$. Consequently, $\Phi(a - b) = 0$ or $g \mid a - b$. By definition, $(a, b) \notin E(G_f(D))$. Consequently, we have the following upper bound for the clique number of $G_f(D)$

$$\omega(G_f(D)) \leq |\mathbb{F}_q[x]/g|.$$

This shows that if $\omega(G) > |\mathbb{F}_q[x]/g|$ then G cannot be an induced subgraph of $G_f(D)$.

We can overcome the constraint by enlarging the base field $\mathbb{F}_q$.

Proposition 8.4. *Let G be a fixed graph. Let $f_1, f_2, \ldots, f_k$ be fixed polynomials in $\mathbb{F}_q[x]$. Then, there exist a finite extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ and a polynomial $f \in \mathbb{F}_{q^m}[x]$ such that*

1. *$f_i \mid f$ for all $1 \leq i \leq k$.*
2. *G is an induced subgraph of $G_f(D)$ where $D = \{f_1, f_2, \ldots, f_k\}$ and we consider f as an element of $\mathbb{F}_{q^m}[x]$.*

Proof. By Erdős and Evans's theorem, there exists a squarefree number n such that G is an induced subgraph of the unitary Cayley graph G_n. Suppose that $r = \omega(n)$ and $n = p_1p_2 \ldots p_r$ be the prime factorization of n. Then, as explained in the proof of Proposition 8.2, $G_n \cong \prod_{i=1}^r K_{p_i}$. Our goal is to show that we can find $\mathbb{F}_{q^m}$ and f such that G_n is an induced subgraph of $G_f(D)$ where we consider f as an element in $\mathbb{F}_{q^m}[x]$.

Let m be a positive integer such that $q^m > n$ and $g = \mathrm{lcm}(f_1, f_2, \ldots, f_k) \in \mathbb{F}_q[x]$. By Galois theory, there exists a polynomial $h \in \mathbb{F}_q[x]$ with at least r distinct irreducible factors and $\gcd(h, g) = 1$. Let $f = hg$. Let I be the ideal in $\mathbb{F}_{q^m}[x]/f$ generated by f_1. Then, by Lemma 5.4, the induced subgraph on I is isomorphic to the unitary Cayley graph $G_{\bar{f}}(\{1\})$ where $\bar{f} = f/f_1$. Suppose that $\bar{f} = g_1^{a_1} g_2^{a_2} \ldots g_t^{a_t}$ be the factorization of f/f_1 over $\mathbb{F}_{q^m}[x]$. Then, by the choice of f, $t \geq r$. By the Chinese remainder theorem, we know that $\mathbb{F}_{q^m}^t$ is a subring of $\mathbb{F}_{q^m}[x]/\bar{f}$. Therefore, $G_{\mathbb{F}_{q^m}^t} = \prod_{i=1}^t K_{q^m}$ is an induced subgraph of $G_{\bar{f}}(\{1\})$. Since $t \geq r$ and $q^m \geq n$, by Lemma 8.1 G_n is an induced subgraph of $G_{\mathbb{F}_{q^m}^t}$. Consequently, G_n is an induced subgraph of $G_f(D)$ as well. □

Acknowledgements

We thank Professor Torsten Sander for the enlightening correspondence about gcd-graphs. We also thank Minh-Tam Trinh for several helpful discussions on Gauss and Ramanujan sums over function fields.

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 and Aleksandar Ilić, *Polynomials of unitary Cayley graphs*, Filomat **29** (2015), no. 9, 2079–2086.
3. Arindam Biswas, *On a cheeger type inequality in Cayley graphs of finite groups*, European Journal of Combinatorics **81** (2019), 298–308.
4. Stefano Boccaletti, Ginestra Bianconi, Regino Criado, Charo I Del Genio, Jesús Gómez-Gardenes, Miguel Romance, Irene Sendina-Nadal, Zhen Wang, and Massimiliano Zanin, *The structure and dynamics of multilayer networks*, Physics reports **544** (2014), no. 1, 1–122.
5. Andreas Brandstädt, Van Bang Le, and Jeremy P Spinrad, *Graph classes: a survey*, SIAM Monographs on Discrete Mathematics and Applications, 1999.

6. Shiva Chidambaram, Ján Minac, Tung T. Nguyen, and Nguyen Duy Tan, *Fekete polynomials of principal Dirichlet characters*, The Journal of Experimental Mathematics (2024).
7. 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).
8. Vaŝek Chvátal and Claude Berge, *Topics on perfect graphs*, Elsevier, 1984.
9. Robert P Dilworth, *A decomposition theorem for partially ordered sets*, Classic papers in combinatorics (1987), 139–144.
10. Paul Erdös and Anthony B Evans, *Representations of graphs and orthogonal Latin square graphs*, Journal of Graph Theory **13** (1989), no. 5, 593–595.
11. Tibor Gallai, *Transitiv orientierbare graphen*, Acta Mathematica Hungarica **18** (1967), no. 1-2, 25–66.
12. Priya B Jain, Tung T. Nguyen, Ján Mináč, Lyle E Muller, and Roberto C Budzinski, *Composed solutions of synchronized patterns in multiplex networks of Kuramoto oscillators*, Chaos: An Interdisciplinary Journal of Nonlinear Science **33** (2023), no. 10.
13. Shigeru Kanemitsu and Michel Waldschmidt, *Matrices of finite abelian groups, finite fourier transform and codes*, Proc. 6th China-Japan Sem. Number Theory, World Sci. London-Singapore-New Jersey (2013), 90–106.
14. Dariush Kiani and Mohsen Molla Haji Aghaei, *On the unitary Cayley graph of a ring*, The electronic journal of combinatorics (2012), P10–P10.
15. Dariush Kiani and Mohsen Mollahajiaghaei, *On the unitary Cayley graphs of matrix algebras*, Linear Algebra and its Applications **466** (2015), 421–428.
16. M. Kivelä, A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, and M. A. Porter, *Multilayer networks*, Journal of Complex Networks **2** (2014), no. 3, 203–271.
17. Walter Klotz and Torsten Sander, *Some properties of unitary Cayley graphs*, The electronic journal of combinatorics (2007), R45–R45.
18. E Kowalski, *Exponential sums over finite fields, i: elementary methods*, preparation; available at www. math. ethz. ch/˜ kowalski/exp-sums. pdf (2018).
19. T. Y. Lam, *Lectures on modules and rings*, Graduate Texts in Mathematics, vol. 189, Springer-Verlag, New York, 1999.
20. Erich Lamprecht, *Allgemeine theorie der gaußschen summen in endlichen kommutativen ringen*, Mathematische Nachrichten **9** (1953), no. 3, 149–196.
21. Jonathan Merzel, Ján Minac, Tung T. Nguyen, and Nguyen Duy Tan, *On divisor graphs and related topics*, in preparation (2024).
22. Ján Minac, Tung T. Nguyen, and Nguyen Duy Tan, *Gcd-graphs over function fields*, `https://github.com/tungprime/gcd_graphs`, 2024.
23. Leon Mirsky, *A dual of dilworth's decomposition theorem*, The American Mathematical Monthly **78** (1971), no. 8, 876–877.
24. Tung T. Nguyen, Roberto C Budzinski, Federico W Pasini, Robin Delabays, Ján Mináč, and Lyle E Muller, *Broadcasting solutions on networked systems of phase oscillators*, Chaos, Solitons & Fractals **168** (2023), 113166.
25. Tung T. Nguyen and Nguyen Duy Tân, *On certain properties of the p-unitary Cayley graph over a finite ring*, arXiv preprint arXiv:2403.05635 (2024).
26. Ricardo A Podestá and Denis E Videla, *Spectral properties of generalized Paley graphs and their associated irreducible cyclic codes*, arXiv preprint arXiv:1908.08097 (2019).
27. ———, *The waring's problem over finite fields through generalized Paley graphs*, Discrete Mathematics **344** (2021), no. 5, 112324.
28. Wasin So, *Integral circulant graphs*, Discrete Mathematics **306** (2006), no. 1, 153–158.
29. André Weil, *Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques*, Revue Scient **77** (1939), 104–106.

Department of Mathematics, Western University, London, Ontario, Canada N6A 5B7
Email address: minac@uwo.ca

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

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