CONDENSED RICCI CURVATURE ON PALEY GRAPHS AND THEIR GENERALIZATIONS

VINCENT BONINI, DANIEL CHAMBERLIN, STEPHEN COOK, PARTHIV SEETHARAMAN, AND TRI TRAN

Abstract. We explore properties of generalized Paley graphs and we extend a result of Kim and Praeger [18] by providing a more precise description of the connected components of disconnected generalized Paley graphs. This result leads to a new characterization of when generalized Paley graphs are disconnected. We also provide necessary and sufficient divisibility conditions for the multiplicative group of the prime subfield of certain finite fields to be contained in the multiplicative subgroup of nonzero k-th powers. This latter result plays a crucial role in our development of a sorting algorithm on generalized Paley graphs that exploits the vector space structure of finite fields to partition certain subsets of vertices in a manner that decomposes the induced bipartite subgraph between them into complete balanced bipartite subgraphs. As a consequence, we establish a matching condition between these subsets of vertices that results in an explicit formula for the condensed Ricci curvature on certain Paley graphs and their generalizations.

1. Introduction

Ollivier defined the coarse Ricci curvature of Markov chains on metric spaces in terms of the Wasserstein (or transport) distance of measures in [25, 26], providing a synthetic notion of Ricci curvature and a bridge between Riemannian geometry and probabilistic methods. The investigation of Ollivier's coarse Ricci curvature on graphs presents an interesting avenue for research and offers an accessible framework for quantifying local connectivity of graphs. Consequentially, it has many practical and computational applications in artificial intelligence, network analysis, and data science (cf. [6–8, 11–14, 19]).

Much work has been done on various forms of the coarse Ricci curvature on graphs (cf. [1–3, 5, 9, 10, 15, 17, 21–24, 27]). We consider a modified notion of Ollivier's coarse Ricci curvature on graphs introduced by Lin, Lu, and Yau in [22] that we refer to as the condensed Ricci curvature as in [3]. In particular, we study the condensed Ricci curvature on Paley graphs and their generalizations, which serve as models of pseudo-random graphs that encode algebraic relations between the elements of certain finite fields. Standard (or quadratic) Paley graphs $\mathcal{P}(q, 2)$ are constructed by taking the elements of finite fields of prime power order $q = p^n \equiv 1 \bmod 4$ as vertices and defining edges between vertices that differ by squares or quadratic residues. Generalized Paley graphs $\mathcal{P}(q, k)$ are constructed in a similar manner by taking the elements of finite fields of prime power order $q = p^n \equiv 1 \bmod 2k$ as vertices and defining edges between vertices that differ by higher order k-th powers (see section 2). The connections of Paley graphs and their generalizations to number theory, field theory, and other branches of mathematics adds to their mathematical interest and allows one to apply tools from number theory and algebra in their study.

2020 *Mathematics Subject Classification.* primary 52C99, 53B99; secondary 05C10, 05C81, 05C99.
Key words and phrases. coarse Ricci curvature; Paley graphs.

Generalized Paley graphs $\mathcal{P}(q,k)$ share some of the well-known properties of quadratic Paley graphs. Indeed, they are symmetric and $\frac{q-1}{k}$-regular but unlike quadratic Paley graphs they are not self-complementary and may be disconnected when $k > 2$ (see section 2). Our main results concerning the condensed Ricci curvature on generalized Paley graphs requires an understanding of their connectivity properties. In a study of the automorphism groups of generalized Paley graphs, it was shown in Theorem 2.2 of [18] that a generalized Paley graph $\mathcal{P}(q,k)$ of order $q = p^n$ is connected if and only if k is not a multiple of $(q-1)/(p^a-1)$ for any proper divisor a of n. Moreover, if $\mathcal{P}(q,k)$ is disconnected, then each connected component is isomorphic to the generalized Paley graph $\mathcal{P}(p^a,k')$ where $k' = k(p^a-1)/(q-1) \geq 1$ and a is some proper divisor of n such that $(q-1)/(p^a-1)$ divides k.

From the divisibility conditions in this result of [18], one finds that a generalized Paley graph $\mathcal{P}(q,k)$ is connected if and only if no proper subfield of $\mathbb{F}_q$ contains the multiplicative subgroup of nonzero k-th powers. Hence, although it is not explicitly stated in [18], it is natural to expect that each of the connected components of a disconnected generalized Paley graph $\mathcal{P}(q,k)$ is isomorphic to a generalized Paley graph defined over the smallest subfield of $\mathbb{F}_q$ that contains the subgroup of nonzero k-th powers. Using basic properties of finite fields and finite cyclic groups, we provide a modest extension of this result of [18] by showing that each connected component of a disconnected generalized Paley graph is isomorphic to the generalized Paley graph $\mathcal{P}(p^a,k')$ as described above, where a is in fact the smallest such proper divisor of n, or equivalently, where $\mathbb{F}_{p^a}$ is the smallest subfield of $\mathbb{F}_q$ containing the subgroup of nonzero k-th powers.

Theorem 1.1. *Let $k \geq 2$ and suppose that the generalized Paley graph $\mathcal{P}(q,k)$ of order $q = p^n$ is disconnected. Then each connected component of $\mathcal{P}(q,k)$ is isomorphic to the generalized Paley graph $\mathcal{P}(p^a,k')$ with $k' = k(p^a-1)/(q-1) \geq 1$ where a is the smallest proper divisor of n such that $(q-1)/(p^a-1)$ divides k.*

Now suppose that θ is a primitive element of the finite field $\mathbb{F}_q$ of order $q = p^n$ and let $(\mathbb{F}_q^\times)^k$ denote the multiplicative subgroup of nonzero k-th powers in $\mathbb{F}_q^\times$. Noting that the smallest subfield of $\mathbb{F}_q$ that contains $(\mathbb{F}_q^\times)^k$ is given by the field extension $\mathbb{F}_p(\theta^k)$, it follows that the parameter a in the results of [18] and Theorem 1.1 is precisely the degree of this extension, or equivalently, the degree of the minimal polynomial of θ^k over $\mathbb{F}_p$. As a result of these observations, we have the following reformulation of the findings of [18] and Theorem 1.1, providing a new characterization of when generalized Paley graphs are disconnected.

Theorem 1.2. *Let $k \geq 2$ and suppose that θ is a primitive element of a finite field $\mathbb{F}_q$ of order $q = p^n$ with $q \equiv 1 \bmod 2k$. Then the generalized Paley graph $\mathcal{P}(q,k)$ is disconnected if and only if the field extension $\mathbb{F}_p(\theta^k)$ is a proper subfield of $\mathbb{F}_q$. Furthermore, if $\mathcal{P}(q,k)$ is disconnected, then each connected component is isomorphic to the generalized Paley graph $\mathcal{P}(p^a,k')$ with*

$$k' = \frac{|\mathbb{F}_p(\theta^k)^\times|}{|(\mathbb{F}_q^\times)^k|} \geq 1$$

where $a < n$ is the degree of the extension $\mathbb{F}_p(\theta^k)$ over $\mathbb{F}_p$.

In light of the aforementioned results of [18] and Theorem 1.2, we also provide some cases of interest where we can guarantee that generalized Paley graphs are connected.

Theorem 1.3. *Let $k \geq 2$ and suppose that $q = p^n$ is a prime power such that $q \equiv 1 \bmod 2k$. If $k < p^{\frac{n}{2}} + 1$, then the generalized Paley graph $\mathcal{P}(q,k)$ is connected.*

As a consequence of Theorem 1.3 and a straightforward calculus argument, we obtain the fact that all generalized Paley graphs $\mathcal{P}(q,k)$ of order $q = p^{km}$ are connected.

Theorem 1.4. *Let $m \geq 1$, $k \geq 2$ and suppose that $q = p^{km}$ is a prime power such that $q \equiv 1 \bmod 2k$. Then the generalized Paley graph $\mathcal{P}(q,k)$ is connected.*

We then turn our attention to the derivation of an explicit formula for the condensed Ricci curvature on Paley graphs and their generalizations. Given a connected, locally finite, undirected, simple graph $G = (V, E)$ with shortest path distance function $\rho : V \times V \to \mathbb{N} \cup \{0\}$ and vertex $v \in V$, let

$$\Gamma(v) = \{w \in V \mid \rho(v,w) = 1\} = \{w \in V \mid vw \in E\}$$

denote the subset of vertices that are adjacent v. Then for any edge $xy \in E$, one can decompose the neighbor sets $\Gamma(x)$ and $\Gamma(y)$ into disjoint unions

$$\Gamma(x) = N_x \cup \nabla_{xy} \cup \{y\} \quad \text{and} \quad \Gamma(y) = N_y \cup \nabla_{xy} \cup \{x\}$$

as in [2], where $\nabla_{xy} = \Gamma(x) \cap \Gamma(y)$ denotes the subset of vertices that are adjacent to both x and y and where

$$N_x = \Gamma(x) \setminus (\nabla_{xy} \cup \{y\}) \quad \text{and} \quad N_y = \Gamma(y) \setminus (\nabla_{xy} \cup \{x\}).$$

Understanding matchings between the neighbor sets N_x and N_y in a graph G is essential to the calculation of the condensed Ricci curvature $\Bbbk(x,y)$ of an edge $xy \in E$. For example, in [3] it is shown that for any edge $xy \in E$ of a strongly regular graph of degree d, the condensed Ricci curvature

$$\Bbbk(x,y) = \frac{1}{d}(2 + |\nabla_{xy}| - (|N_x| - m)) \tag{1.1}$$

where m is the size of a maximum matching $\mathcal{M}$ between N_x and N_y. In general, when a perfect matching exists between the neighbor sets N_x and N_y for every edge $xy \in E$, the graph G is said to satisfying the Global Matching Condition [27]. An explicit formula for the condensed Ricci curvature along edges in graphs that satisfy the Global Matching Condition is established in [27]. We state a combined version of Lemma 6.2 and Theorem 6.3 of [27] below.

Theorem 1.5 ([27])**.** *Let $G = (V, E)$ be a connected, locally finite, undirected, simple graph satisfying the Global Matching Condition. Then G is regular of degree d and the condensed Ricci curvature*

$$\Bbbk(x,y) = \frac{1}{d}(2 + |\nabla_{xy}|)$$

for any edge $xy \in E$.

Our derivation of an explicit formula for the condensed Ricci curvature on generalized Paley graphs relies on establishing the Global Matching Condition and Theorem 1.5. We refer readers to Section 2 of [3] for the precise definition of the condensed Ricci curvature on graphs and our choice of terminology. The main ideas we use to establish the Global Matching Condition were first conceived for the special case of quadratic Paley graphs $\mathcal{P}(q,2)$ of even power order $q = p^{2m}$ in an unpublished student research project [4]. In particular, in [4] the fact that the multiplicative group of the corresponding prime subfield $\mathbb{F}_p^\times$ is contained in the subgroup of nonzero quadratic residues $(\mathbb{F}_q^\times)^2$ led to the idea that the vector space structure of the finite field $\mathbb{F}_q$ could be used to partition (or "sort") the vertices in N_0 and N_1 in a

way that a perfect matching could be easily obtained. Then, by the symmetry of quadratic Paley graphs, there is a perfect matching between the neighbor sets N_x and N_y for every edge $xy \in E$.

We found that the observations of [4] hold more broadly on certain generalized Paley graphs and that the induced bipartite subgraph of edges between vertices in N_x and N_y can actually be decomposed into complete balanced bipartite subgraphs with a "sorting algorithm" (see Section 3). With the aim of generalizing the ideas of [4], we first establish a substantial case where the multiplicative group of the prime subfield $\mathbb{F}_p^\times$ of a finite field $\mathbb{F}_q$ is contained in the subgroup of nonzero k-th powers $(\mathbb{F}_q^\times)^k$.

Theorem 1.6. *Suppose p and k are prime. Then $\mathbb{F}_p^\times \leq (\mathbb{F}_{p^{km}}^\times)^k$ for any positive integer m.*

Moreover, as a simple consequence of basic properties of finite cyclic groups, we have the following necessary and sufficient divisibility conditions for the multiplicative group of the prime subfield to be contained in the subgroup of nonzero k-th powers for the finite fields that serve as vertex sets of generalized Paley graphs.

Theorem 1.7. *Let $k \geq 2$ and suppose that $q = p^n$ is a prime power such that $q \equiv 1 \bmod 2k$. Then $\mathbb{F}_p^\times \leq (\mathbb{F}_q^\times)^k$ if and only if $k \mid \frac{q-1}{p-1}$.*

Furthermore, as a straightforward consequence of Theorem 1.7, we find that if $\mathbb{F}_q$ is a finite field of order $q = p^n \equiv 1 \bmod 2k$ and $k \mid p-1$, then the multiplicative group of the prime subfield is contained in the subgroup of nonzero k-th powers if and only if n is a multiple of k.

Corollary 1.8. *Let $k \geq 2$ and suppose that $q = p^n$ is a prime power such that $q \equiv 1 \bmod 2k$. If $k \mid p-1$, then $\mathbb{F}_p^\times \leq (\mathbb{F}_q^\times)^k$ if and only if $n \equiv 0 \bmod k$.*

With Theorems 1.6 and 1.7 in hand, we then formally develop the sorting algorithm conceived in [4] and use it to establish the Global Matching Condition on connected generalized Paley graphs in which the multiplicative group of the corresponding prime subfield is contained in the subgroup of nonzero k-th powers (see Section 3).

Theorem 1.9. *Let $k \geq 2$ and suppose $\mathcal{P}(q,k)$ is a connected generalized Paley graph of order $q = p^n$. If $\mathbb{F}_p^\times \leq (\mathbb{F}_q^\times)^k$, then $\mathcal{P}(q,k)$ satisfies the Global Matching Condition.*

Due to Theorems 1.4, 1.5, 1.6, and 1.9, we then obtain the following generalization of the unpublished work of [4] on quadratic Paley graphs $\mathcal{P}(q,2)$ of even power order $q = p^{2m}$.

Theorem 1.10. *Let $m \geq 1$ and suppose that $\mathcal{P}(q,k) = (V,E)$ is a generalized Paley graph of order $q = p^{km}$ where k is prime. Then the condensed Ricci curvature*

$$\Bbbk(x,y) = \frac{k}{q-1}(2 + |\nabla_{xy}|)$$

for any edge $xy \in E$.

More generally, as a consequence of Theorems 1.5, 1.7, and 1.9, we obtain the same explicit formula for the condensed Ricci curvature on generalized Paley graphs $\mathcal{P}(q,k)$ of order $q = p^n$ satisfying the divisibility condition $k \mid \frac{q-1}{p-1}$.

Theorem 1.11. *Let $k \geq 2$ and suppose that $\mathcal{P}(q,k) = (V,E)$ is a generalized Paley graph of order $q = p^n$ where $k \mid \frac{q-1}{p-1}$. Then the condensed Ricci curvature*

$$\Bbbk(x,y) = \frac{k}{q-1}(2 + |\nabla_{xy}|)$$

for any edge $xy \in E$.

We would like to point out that the formula for the condensed Ricci curvature in Theorem 1.11 holds for both connected and disconnected generalized Paley graphs. However, in our work we consider these cases separately (see Theorems 3.8 and 3.9) and we recover the same formula for the condensed Ricci curvature by applying our results for connected graphs to the connected components of disconnected generalized Paley graphs. In the special case that the connected components of a disconnected generalized Paley graph are complete graphs, we appeal to the following result stated in [22] and proved in [3].

Theorem 1.12 ([3,22])**.** *A connected, finite, undirected, simple graph $G = (V,E)$ is complete if and only if the condensed Ricci curvature $\Bbbk(x,y) > 1$ for all vertices $x, y \in V$. In particular, if G is a complete graph on n vertices, then $\Bbbk(x,y) = \frac{n}{n-1}$ for all vertices $x, y \in V$.*

Remark 1.13. Generalized Paley graphs $\mathcal{P}(q,k)$ can be defined over finite fields of even order $q = 2^n$ as in [18]. In this case, one requires $q \equiv 1 \bmod k$ rather than requiring $q \equiv 1 \bmod 2k$ as in the case for odd prime powers. Our work applies to generalized Paley graphs of even order, although some our results are trivial when considering finite fields of characteristic 2. However, for simplicity in presentation, we have chosen to focus on generalized Paley graphs of odd order.

This paper is organized as follows: In Section 2 we formally define generalized Paley graphs and we discuss some of their relavant properties. In particular, we extend the results [18] by providing a more precise description of their connected components and we give a new characterization of when generalized Paley graphs are disconnected. In Section 3 we establish results on the containment of the multiplicative group of the prime subfield of a finite field in the subgroup of nonzero k-th powers and we develop the "sorting algorithm", which leads to establishing the Global Matching Condition and our explicit formulas for the condensed Ricci curvature on Paley graphs and their generalizations.

Acknowledgements

This research was generously supported by the William and Linda Frost Fund in the Cal Poly Bailey College of Science and Mathematics. The authors would like to thank the referee for their careful reading of our work and their valuable input and insight. We also extend our gratitude to Professor Eric Brussel and Professor Rob Easton of Cal Poly for many vauble conversations.

2. Generalized Paley Graphs and Their Properties

In this section we introduce the definition of generalized Paley graphs and we discuss some of their relevant properties. Consider the finite field $\mathbb{F}_q$ of order $q = p^n$ and let $\mathbb{F}_q^\times$ denote the multiplicative group of $\mathbb{F}_q$. Then the set of nonzero squares or quadratic residues in $\mathbb{F}_q$ is denoted by

$$(\mathbb{F}_q^\times)^2 = \{\alpha \in \mathbb{F}_q^\times \mid \alpha = \beta^2 \text{ for some } \beta \in \mathbb{F}_q^\times\}.$$

Paley graphs are then constructed by taking the field elements of certain finite fields as vertices and defining edges between those vertices that differ by quadratic residues.

Definition 2.1. Let $q = p^n$ be a prime power such that $q \equiv 1 \bmod 4$. Then the *Paley graph of order* q is defined to be the graph $\mathcal{P}(q) = (V, E)$ with vertex set $V = \mathbb{F}_q$ and edge set $E = \{xy \mid x - y \in (\mathbb{F}_q^\times)^2\}$.

We refer to Paley graphs with edges between vertices that differ by quadratic residues as quadratic Paley graphs. Quadratic Paley graphs are connected, self-complementary, strongly regular graphs with parameters $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ [16]. Naturally, one can generalize the definition of Paley graphs to define edges in terms of higher order powers. For integers $k \geq 2$, we denote the set of nonzero k-th powers in $\mathbb{F}_q$ by

$$(\mathbb{F}_q^\times)^k = \{\alpha \in \mathbb{F}_q^\times \mid \alpha = \beta^k \text{ for some } \beta \in \mathbb{F}_q^\times\}. \tag{2.1}$$

Definition 2.2. Let $k \geq 2$ and suppose $q = p^n$ is a prime power such that $q \equiv 1 \bmod 2k$. Then the *generalized Paley graph of order q with k-th powers* is defined to be the graph $\mathcal{P}(q, k) = (V, E)$ with vertex set $V = \mathbb{F}_q$ and edge set $E = \{xy \mid x - y \in (\mathbb{F}_q^\times)^k\}$.

Note that one can consider $k = 1$ in (2.1) and Definition 2.2. In this case the set of 1-st powers over $\mathbb{F}_q$ is simply the multiplicative group $\mathbb{F}_q^\times$ and therefore $\mathcal{P}(q, 1) = K_q$ is the complete graph on q vertices. For simplicity in our presentation we will sometimes refer to complete graphs as generalized Paley graphs. For $k = 2$ the Paley graphs $\mathcal{P}(q, 2)$ are quadratic Paley graphs as defined in Definition 2.1. It is natural to refer to Paley graphs with $k = 3$ as cubic, $k = 4$ as quartic, $k = 5$ as quintic, and so on. Throughout this work we refer to Paley graphs with edges between vertices that differ by k-th powers simply as generalized Paley graphs or k-Paley graphs.

We also note that the set of nonzero k-th powers of a finite field $\mathbb{F}_q$ form a subgroup of $\mathbb{F}_q^\times$. Moreover, if θ is a generator for the multiplicative cyclic group $\mathbb{F}_q^\times$, then θ^k generates the subgroup $(\mathbb{F}_q^\times)^k$ of k-th powers. Hence, since $|\theta| = q - 1$ and we are considering finite fields $\mathbb{F}_q$ where $k \mid q-1$, it follows that $|\theta^k| = \frac{q-1}{k}$ and therefore $\frac{q-1}{k}$ elements of $\mathbb{F}_q^\times$ are k-th powers, or equivalently, the subgroup of nonzero k-th powers in $\mathbb{F}_q^\times$ has order $\frac{q-1}{k}$.

The condition $q \equiv 1 \bmod 2k$ in Definition 2.2 ensures that $q-1$ is even, so $q = p^n$ must be an odd prime power for the generalized Paley graphs under consideration. It also guarantees that generalized Paley graphs are undirected. In other words, the condition $2k \mid q - 1$ guarantees that if $x - y \in (\mathbb{F}_q^\times)^k$ for some $x, y \in \mathbb{F}_q$, then $y - x \in (\mathbb{F}_q^\times)^k$, or equivalently that $-1 \in (\mathbb{F}_q^\times)^k$. Indeed, if θ is a generator for the multiplicative group $\mathbb{F}_q^\times$, then

$$1 = (\theta^{\frac{q-1}{2}})^2$$

and therefore $\theta^{\frac{q-1}{2}} = -1$. But then since $\frac{q-1}{2k} \in \mathbb{Z}$, it follows that $-1 = (\theta^{\frac{q-1}{2k}})^k \in (\mathbb{F}_q^\times)^k$.

Generalized Paley graphs retain some of the basic properties shared by quadratic Paley graphs. For example, generalized Paley graphs $\mathcal{P}(q, k)$ are symmetric as they are easily seen to be arc-transitive under the subgroup of affine automorphims of the form $x \mapsto ax + b$ where $a \in (\mathbb{F}_q^\times)^k$ and $b \in \mathbb{F}_q$. Moreover, k-Paley graphs are $\frac{q-1}{k}$-regular. For completeness, we record and prove these results in the following propositions.

Proposition 2.3. *Generalized Paley graphs $\mathcal{P}(q, k) = (V, E)$ of order $q = p^n$ are symmetric.*

Proof. For any edges $x_1y_1, x_2y_2 \in E$, taking

$$a = (y_2 - x_2)(y_1 - x_1)^{-1} \in (\mathbb{F}_q^\times)^k \quad \text{and} \quad b = x_2 - ax_1 \in \mathbb{F}_q^\times,$$

it follows that the automorphism $\phi : V \to V$ defined by $\phi(x) = ax + b$ satisfies $\phi(x_1) = x_2$ and $\phi(y_1) = y_2$. Thus, $\mathcal{P}(q, k)$ is arc-transitive and therefore symmetric. □

Proposition 2.4. *Generalized Paley graphs $\mathcal{P}(q, k) = (V, E)$ of order $q = p^n$ are $\frac{q-1}{k}$-regular.*

Proof. Let θ be a generator for $\mathbb{F}_q^\times$ and suppose $x \in V$. Then for any other vertex $y \in V$, it follows that $y \in \Gamma(x)$ if and only if $y - x \in (\mathbb{F}_q^\times)^k$. Hence, $y \in \Gamma(x)$ if and only if $y = x + (\theta^k)^m$ for some $m \in \mathbb{Z}$. Thus, $y \in \Gamma(x)$ if and only if $y \in x + \langle \theta^k \rangle$, where $x + \langle \theta^k \rangle$ is the additive coset of the subgroup $\langle \theta^k \rangle$ of nonzero k-th powers. Noting that all cosets of $\langle \theta^k \rangle$ have order $|\theta^k| = \frac{q-1}{k}$, we see that $|\Gamma(x)| = \frac{q-1}{k}$. Hence, since x was chosen arbitrarily, it follows that $\mathcal{P}(q, k)$ is $\frac{q-1}{k}$-regular. □

In contrast to the case for quadratic Paley graphs, generalized Paley graphs $\mathcal{P}(q, k)$ are not self-complementary for $k > 2$. This follows directly from the fact that self-complementary graphs with q vertices must have $\frac{q(q-1)}{4}$ edges, that is, half the number of edges as in a complete graph on q vertices. But $\mathcal{P}(q, k)$ is $\frac{q-1}{k}$-regular by Proposition 2.4 and therefore has

$$\frac{1}{2} \cdot q \cdot \frac{q-1}{k} = \frac{q(q-1)}{2k}$$

edges, which is less than $\frac{q(q-1)}{4}$ for $k > 2$. Furthermore, generalized Paley graphs $\mathcal{P}(q, k)$ may not be connected when $k > 2$. However, even when a generalized Paley graph is disconnected, it turns out that each of its connected components is isomorphic to a single generalized Paley graph defined over a proper subfield of $\mathbb{F}_q$. These latter properties are due to Theorem 2.2 of [18]. We restate the relevant portions of this theorem in the context of our work below.

Theorem 2.5 (Theorem 2.2 [18])**.** *For $k \geq 2$, the generalized Paley graph $\mathcal{P}(q, k)$ of order $q = p^n$ is connected if and only if k is not a multiple of $(q-1)/(p^a - 1)$ for any proper divisor a of n. Furthermore, if $\mathcal{P}(q, k)$ is disconnected, then each connected component is isomorphic to the generalized Paley graph $\mathcal{P}(p^a, k')$ with $k' = k(p^a - 1)/(q-1) \geq 1$ where a is some proper divisor of n such that $(q-1)/(p^a - 1)$ divides k.*

As noted in the introduction, the divisibility conditions in Theorem 2.5 imply that a generalized Paley graph $\mathcal{P}(q, k)$ is connected if and only if no proper subfield of $\mathbb{F}_q$ contains the subgroup of nonzero k-th powers. Therefore, it is natural to expect that each of the connected components of a disconnected generalized Paley graph $\mathcal{P}(q, k)$ is isomorphic to a generalized Paley graph defined over the smallest subfield of $\mathbb{F}_q$ that contains the subgroup of nonzero k-th powers.

Now if $q = p^n$ is a prime power such that $q \equiv 1 \bmod 2k$ and b is a proper divisor of n for which $(q-1)/(p^b - 1)$ divides k, then $k = k'(q-1)/(p^b - 1)$ for some $k' \in \mathbb{Z}$ so

$$p^b - 1 = k' \frac{q-1}{k} = 2k' \frac{q-1}{2k}. \tag{2.2}$$

But $\frac{q-1}{2k} \in \mathbb{Z}$ so by (2.2) it follows that $2k' \mid p^b - 1$ and therefore $p^b \equiv 1 \bmod 2k'$. Thus, one obtains a generalized Paley graph $\mathcal{P}(p^b, k')$ over the proper subfield $\mathbb{F}_{p^b}$ of $\mathbb{F}_q$ for every proper divisor b of n for which $(q-1)/(p^b - 1)$ divides k. However, if b is not the smallest such divisor of n, that is if $\mathbb{F}_{p^b}$ is not the smallest subfield of $\mathbb{F}_q$ containing the subgroup of nonzero k-th powers, then it turns out that $\mathcal{P}(p^b, k')$ is also disconnected.

Although it is not explicitly stated in [18], a further analysis shows that each of the connected components of a disconnected generalized Paley graph $\mathcal{P}(q, k)$ is actually isomorphic

to the generalized Paley graph $\mathcal{P}(p^a, k')$ as described in Theorem 2.5 where a is in fact the smallest proper divisor of n such that $(q-1)/(p^a-1)$ divides k, or equivalently, where $\mathbb{F}_{p^a}$ is the smallest subfield of $\mathbb{F}_q$ containing the subgroup of nonzero k-th powers.

Theorem 2.6. *Let $k \geq 2$ and suppose the generalized Paley graph $\mathcal{P}(q,k)$ of order $q = p^n$ is disconnected. Then each connected component of $\mathcal{P}(q,k)$ is isomorphic to the generalized Paley graph $\mathcal{P}(p^a, k')$ with $k' = k(p^a-1)/(q-1) \geq 1$ where a is the smallest proper divisor of n such that $(q-1)/(p^a-1)$ divides k.*

Proof. Suppose that $\mathcal{P}(q,k)$ is disconnected. Then $(q-1)/(p^b-1)$ divides k for some proper divisor b of n by Theorem 2.5. Equivalently, since $k \mid q-1$, we may write this divisibility condition as $\frac{q-1}{k} \mid p^b-1$. Therefore, since $\mathbb{F}_{p^b}^\times$ is cyclic and $|(\mathbb{F}_q^\times)^k| = \frac{q-1}{k}$ divides $|\mathbb{F}_{p^b}^\times| = p^b-1$, it follows that

$$(\mathbb{F}_q^\times)^k \leq \mathbb{F}_{p^b}^\times. \tag{2.3}$$

Let a be the smallest proper divisor of n such that $(q-1)/(p^a-1)$ divides k. If $a < b$, it follows that $(\mathbb{F}_q^\times)^k \leq \mathbb{F}_{p^a}^\times$ as in (2.3) and therefore

$$(\mathbb{F}_q^\times)^k \leq \mathbb{F}_{p^a}^\times \cap \mathbb{F}_{p^b}^\times = \mathbb{F}_{p^d}^\times \tag{2.4}$$

where $d = \gcd(a,b)$. Thus, by Lagrange's theorem, it follows from (2.4) that $\frac{q-1}{k} \mid p^d - 1$, or equivalently $(q-1)/(p^d-1)$ divides k where $d = \gcd(a,b) \leq a$ is a proper divisor of n. But since a is the smallest proper divisor of n such that $(q-1)/(p^a-1)$ divides k, it follows that $a = d$ and therefore $a \mid b$.

Now let $k'_a = k(p^a-1)/(q-1)$ and $k'_b = k(p^b-1)/(q-1)$. Then

$$k'_b = k\frac{p^b-1}{q-1} = k'_a \frac{q-1}{p^a-1}\frac{p^b-1}{q-1} = k'_a \frac{p^b-1}{p^a-1}$$

and therefore $(p^b-1)/(p^a-1)$ divides k'_b. Hence, since a is a proper divisor of b, it follows from Theorem 2.5 that the generalized Paley graph $\mathcal{P}(p^b, k'_b)$ is disconnected. Thus, in light of Theorem 2.5, the connected components of a disconnected generalized Paley graph $\mathcal{P}(q,k)$ must be isomorphic to the generalized Paley graph $\mathcal{P}(p^a, k')$ with $k' = k(p^a-1)/(q-1) \geq 1$ where a is the smallest proper divisor of n such that $(q-1)/(p^a-1)$ divides k, or equivalently, where $\mathbb{F}_{p^a}$ is the smallest subfield of $\mathbb{F}_q$ containing the subgroup of nonzero k-th powers. □

Now suppose that θ is a primitive element of the finite field $\mathbb{F}_q$ of order $q = p^n$ with $q \equiv 1 \bmod 2k$. Then the smallest subfield of $\mathbb{F}_q$ that contains the subgroup of nonzero k-th powers is given by the field extension $\mathbb{F}_p(\theta^k)$ over $\mathbb{F}_p$. Thus, if the degree of this extension is strictly less than n, say

$$[\mathbb{F}_p(\theta^k) : \mathbb{F}_p] = a < n,$$

it follows that a is a proper divisor of n and that $\mathbb{F}_p(\theta^k) = \mathbb{F}_{p^a}$ is a proper subfield of $\mathbb{F}_q$. Moreover, since $\mathbb{F}_p(\theta^k)$ is the smallest subfield of $\mathbb{F}_q$ that contains the subgroup of nonzero k-th powers, it follows from Lagrange's theorem that a is the smallest proper divisor of n such that $|(\mathbb{F}_q^\times)^k| = \frac{q-1}{k}$ divides $|\mathbb{F}_p(\theta^k)^\times| = p^a-1$, or equivalently, such that $(q-1)/(p^a-1)$ divides k. From these observations we see that the parameter a in the results of [18] and Theorem 1.1 is precisely the degree of the field extension $\mathbb{F}_p(\theta^k)$ over $\mathbb{F}_p$, or equivalently, the degree of the minimal polynomial of θ^k over $\mathbb{F}_p$. Therefore, we have the following reformulation of the results of [18] and Theorem 1.1.

Theorem 2.7. *Let $k \geq 2$ and suppose that θ is a primitive element of a finite field $\mathbb{F}_q$ of order $q = p^n$ with $q \equiv 1 \bmod 2k$. Then the generalized Paley graph $\mathcal{P}(q,k)$ is disconnected if and only if the field extension $\mathbb{F}_p(\theta^k)$ is a proper subfield of $\mathbb{F}_q$. Furthermore, if $\mathcal{P}(q,k)$ is disconnected, then each connected component is isomorphic to the generalized Paley graph $\mathcal{P}(p^a, k')$ with*

$$k' = \frac{|\mathbb{F}_p(\theta^k)^\times|}{|(\mathbb{F}_q^\times)^k|} \geq 1$$

where $a < n$ is the degree of the extension $\mathbb{F}_p(\theta^k)$ over $\mathbb{F}_p$.

With these facts in hand, we focus our attention on connected generalized Paley graphs as our results will easily lend themselves to the connected components of disconnected generalized Paley graphs. One simple case where we can guarantee that generalized Paley graphs are connected is given in the following theorem.

Theorem 2.8. *Let $k \geq 2$ and suppose that $q = p^n$ is a prime power such that $q \equiv 1 \bmod 2k$. If $k < p^{\frac{n}{2}} + 1$, then the generalized Paley graph $\mathcal{P}(q,k)$ of order $q = p^n$ is connected.*

Proof. Suppose that a is a proper divisor of n. Then

$$\frac{p^n - 1}{p^a - 1} \geq \frac{p^n - 1}{p^{\frac{n}{2}} - 1} = p^{\frac{n}{2}} + 1 > k.$$

Hence, k is not a multiple of $(p^n - 1)/(p^a - 1)$ for any proper divisor a of n and therefore $\mathcal{P}(q,k)$ is connected by Theorem 2.5. □

To conclude this section we present another special case where the generalized Paley graphs under consideration are connected. In particular, we show that all generalized Paley graphs $\mathcal{P}(q,k)$ of order $q = p^{km}$ are connected. This result contributes to a complete generalization of the observations outlined in [4] for quadratic Paley graphs $\mathcal{P}(q,2)$ of even power order $q = p^{2m}$.

Theorem 2.9. *Let $m \geq 1$, $k \geq 2$ and suppose that $q = p^{km}$ is a prime power such that $q \equiv 1 \bmod 2k$. Then the generalized Paley graph $\mathcal{P}(q,k)$ of order $q = p^{km}$ is connected.*

Proof. It suffices to show that $km > 2\log_p(k-1)$ since then $p^{\frac{km}{2}} + 1 > k$ and therefore $\mathcal{P}(q,k)$ is connected by Theorem 2.8. To this end, consider the function $f : (1,\infty) \to \mathbb{R}$ defined by

$$f(x) = x - 2\log_2(x-1) = x - \frac{2}{\ln 2}\ln(x-1).$$

Then

$$f'(x) = 1 - \frac{2}{(\ln 2)(x-1)}$$

so f has a single critical point at

$$x^* = \frac{2}{\ln 2} + 1$$

where $f' < 0$ on $(1, x^*)$ and $f' > 0$ on (x^*, ∞). Thus, f is decreasing on $(1, x^*)$ and increasing on (x^*, ∞). Moreover, since

$$f(x^*) = \frac{2}{\ln 2}\left(1 - \ln\left(\frac{2}{\ln 2}\right)\right) + 1 > 0,$$

it follows that f has a positive global minimum at x^*. Hence, $f > 0$ on $(1, \infty)$ and therefore $x > 2\log_2(x-1)$ for all $x \in (1, \infty)$. In particular, since $k \geq 2$ and p is necessarily an odd prime, we see

$$km \geq k > 2\log_2(k-1) > 2\log_p(k-1) \tag{2.5}$$

and the desired result follows. □

3. The Sorting Algorithm and The Global Matching Condition

In this section we establish the Global Matching Condition for certain Paley graphs and their generalizations. As a consequence of Theorem 1.5 of [27] we then obtain an explicit formula for the condensed Ricci curvature along the edges of these graphs. Consider a connected generalized Paley graph $\mathcal{P}(q,k)$ of order $q = p^n$ with vertex set $V = \mathbb{F}_q$ and edge set $E = \{xy \mid x - y \in (\mathbb{F}_q^\times)^k\}$. Due to the symmetry of generalized Paley graphs we may focus on the edge $01 \in E$ and the neighbor sets

$$N_0 = \Gamma(0) \setminus (\nabla_{01} \cup \{1\}) \quad \text{and} \quad N_1 = \Gamma(1) \setminus (\nabla_{01} \cup \{0\})$$

as introduced in Section 1.

Let H denote the induced bipartite subgraph consisting of all edges in E between vertices in N_0 and N_1. Our strategy in establishing the Global Matching Condition on the generalized Paley graphs under consideration is to formally develop and generalize the sorting algorithm that was first conceived in [4] for the special case of quadratic Paley graphs. We then apply this sorting algorithm to decompose the bipartite subgraph H into complete balanced bipartite subgraphs. Then one can pairwise match vertices in these subgraphs to construct a perfect matching between N_0 and N_1 and appeal to the symmetry of generalized Paley graphs to realize a perfect matching between the neighbor sets N_x and N_y for every edge $xy \in E$.

On generalized Paley graphs the containment of the corresponding multiplicative group of the prime subfield in the subgroup of nonzero k-th powers plays a crucial role in the success of the sorting algorithm. With the aim of establishing an important case of this critical component of the sorting algorithm, we first present a special case of Theorem 9.1 in chapter 6, section 9 of [20].

Theorem 3.1 (Theorem 9.1 [20])**.** *Let $\mathbb{F}_p$ denote the field of prime order p and suppose k is prime. Let $\alpha \in \mathbb{F}_p^\times$ and suppose that $\alpha \notin (\mathbb{F}_p^\times)^k$. Then $x^k - \alpha$ is irreducible in $\mathbb{F}_p[x]$.*

For the case of quadratic Paley graphs $\mathcal{P}(q,2)$ of even power order $q = p^{2m}$, it was observed in [4] that the corresponding multiplicative group of the prime subfield $\mathbb{F}_p^\times$ is contained in the subgroup of nonzero quadratic residues $(\mathbb{F}_q^\times)^2$. We appeal to Theorem 3.1 to establish a more general version of this observation.

Theorem 3.2. *Suppose p and k are prime. Then $\mathbb{F}_p^\times \leq (\mathbb{F}_{p^{km}}^\times)^k$ for any positive integer m.*

Proof. Let $\alpha \in \mathbb{F}_p^\times$ and suppose that $\alpha \notin (\mathbb{F}_p^\times)^k$. Then by Theorem 3.1, $f(x) = x^k - \alpha$ is irreducible in $\mathbb{F}_p[x]$. Therefore, if θ is a root of f, then

$$\mathbb{F}_p[x]/\langle x^k - \alpha \rangle \cong \mathbb{F}_p(\theta) \cong \mathbb{F}_{p^k}.$$

Now suppose that $\varphi : \mathbb{F}_p(\theta) \to \mathbb{F}_{p^k}$ is an isomorphism. Noting that $\varphi(\alpha) = \alpha$ since $\alpha \in \mathbb{F}_p$, it follows that

$$\varphi(\theta)^k - \alpha = \varphi(\theta^k) - \varphi(\alpha) = \varphi(\theta^k - \alpha) = \varphi(f(\theta)) = \varphi(0) = 0.$$

Thus, $\alpha = \varphi(\theta)^k \in (\mathbb{F}_{p^k}^\times)^k$ and therefore since $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^{km}}$ for any positive integer m, it follows that $\alpha \in (\mathbb{F}_{p^{km}}^\times)^k$. Hence, $\mathbb{F}_p^\times \leq (\mathbb{F}_{p^{km}}^\times)^k$ as desired. □

Now suppose $\mathbb{F}_q$ is a finite field of order $q = p^n$ such that $q \equiv 1 \bmod 2k$ with $k \geq 2$. As a simple consequence of basic properties of finite cyclic groups, we have the following necessary and sufficient divisibility conditions for the multiplicative group of the prime subfield of $\mathbb{F}_q$ to be contained in the subgroup of nonzero k-th powers.

Theorem 3.3. *Let $k \geq 2$ and suppose that $q = p^n$ is a prime power such that $q \equiv 1 \bmod 2k$. Then $\mathbb{F}_p^\times \leq (\mathbb{F}_q^\times)^k$ if and only if $k \mid \frac{q-1}{p-1}$.*

Proof. Let $\mathbb{F}_q$ be a finite field of order $q = p^n$ such that $q \equiv 1 \bmod 2k$. Then since

$$|\mathbb{F}_p^\times| = p - 1 \quad \text{and} \quad |(\mathbb{F}_q^\times)^k| = \frac{q-1}{k},$$

it follows from properties of finite cyclic groups and Lagrange's theorem that $\mathbb{F}_p^\times \leq (\mathbb{F}_q^\times)^k$ if and only if $p - 1 \mid \frac{q-1}{k}$, or equivalently $k \mid \frac{q-1}{p-1}$. □

Clearly, since we are considering generalized Paley graphs $\mathcal{P}(q, k)$ of order $q = p^n$ where $q \equiv 1 \bmod 2k$, it follows that $k \mid q - 1$. Due to Theorem 3.3, it turns out that when k also divides $p - 1$, the multiplicative group of the corresponding prime subfield $\mathbb{F}_p^\times$ is contained in the subgroup of nonzero k-th powers $(\mathbb{F}_q^\times)^k$ if and only if n is a multiple of k.

Corollary 3.4. *Let $k \geq 2$ and suppose that $q = p^n$ is a prime power such that $q \equiv 1 \bmod 2k$. If $k \mid p - 1$, then $\mathbb{F}_p^\times \leq (\mathbb{F}_q^\times)^k$ if and only if $n \equiv 0 \bmod k$.*

Proof. By Theorem 3.3, $\mathbb{F}_p^\times \leq (\mathbb{F}_q^\times)^k$ if and only if $k \mid \frac{q-1}{p-1}$. Hence, $\mathbb{F}_p^\times \leq (\mathbb{F}_q^\times)^k$ if and only if

$$\frac{q-1}{p-1} = p^{n-1} + p^{n-2} + \cdots + p + 1 \equiv 0 \bmod k. \tag{3.1}$$

But $k \mid p - 1$ so $p \equiv 1 \bmod k$ and therefore

$$\frac{q-1}{p-1} = p^{n-1} + p^{n-2} + \cdots + p + 1 \equiv n \bmod k. \tag{3.2}$$

Hence, by (3.1) and (3.2) it follows that $\mathbb{F}_p^\times \leq (\mathbb{F}_q^\times)^k$ if and only if $n \equiv 0 \bmod k$. □

Now that we have a better understanding of when the multiplicative group of the prime subfield is contained in the subgroup of nonzero k-th powers of a given finite field, we develop the sorting algorithm that we will use to construct a perfect matching between the neighbor sets N_0 and N_1 in a generalized Paley graph. To this end, let θ be a generator of the multiplicative group $\mathbb{F}_q^\times$ of the finite field $\mathbb{F}_q$ of order $q = p^n$. Consider the minimal polynomial $f \in \mathbb{F}_p[x]$ of θ such that

$$\mathbb{F}_q \cong \mathbb{F}_p(\theta) \cong \mathbb{F}_p[x]/\langle f(x) \rangle. \tag{3.3}$$

In light of the isomorphisms in (3.3), it follows that $1, \theta, \theta^2, \ldots, \theta^{n-1}$ is a basis for $\mathbb{F}_q$ as a vector space over $\mathbb{F}_p$ and therefore

$$\mathbb{F}_q = \{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}_p\}. \tag{3.4}$$

Our formalization of the sorting algorithm and substantiation of a perfect matching between the neighbor sets N_0 and N_1 relies on the following fact that was first observed for quadratic Paley graphs in [4].

Lemma 3.5. *Let $\mathcal{P}(q,k)$ be a connected generalized Paley graph of order $q = p^n$ and suppose that θ is a generator of the multiplicative group $\mathbb{F}_q^\times$. Fix $a_1, \ldots, a_{n-1} \in \mathbb{F}_p$ not all zero and set*

$$S = S(a_1, \ldots, a_{n-1}) = \{b + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \mid b \in \mathbb{F}_p\}.$$

Then $|N_0 \cap S| = |N_1 \cap S|$.

Proof. First note that $x \in \Gamma(0)$ if and only if $x \in (\mathbb{F}_q^\times)^k$ if and only if $x + 1 \in \Gamma(1)$ and therefore

$$|\Gamma(0) \cap S| = |\Gamma(1) \cap S|. \tag{3.5}$$

Now since $a_1, \ldots, a_{n-1} \in \mathbb{F}_p$ are not all zero, it follows that

$$\{0\} \cap S = \varnothing \quad \text{and} \quad \{1\} \cap S = \varnothing.$$

Moreover, since

$$\Gamma(0) = \{1\} \cup N_0 \cup \nabla_{01} \quad \text{and} \quad \Gamma(1) = \{0\} \cup N_1 \cup \nabla_{01}$$

are disjoint unions, it follows that

$$|\Gamma(0) \cap S| = |N_0 \cap S| + |\nabla_{01} \cap S| \tag{3.6}$$

and

$$|\Gamma(1) \cap S| = |N_1 \cap S| + |\nabla_{01} \cap S|. \tag{3.7}$$

Thus, by (3.5) we may equate equations (3.6) and (3.7) to find $|N_0 \cap S| = |N_1 \cap S|$. □

Lemma 3.5 provides an avenue for partitioning the neighbor sets N_0 and N_1 of a generalized Paley graph $\mathcal{P}(q,k)$ by grouping vertices (or elements) in N_0 and N_1 with the same coefficients of $\theta, \ldots, \theta^{n-1}$. In particular, when the nonzero elements of the prime subfield are all k-th powers, we can partition the induced bipartite subgraph H consisting of all edges in E between N_0 and N_1 into complete balanced bipartite subgraphs. By matching vertices in each of these complete subgraphs in pairwise fashion, we obtain a perfect matching between N_0 and N_1, which by symmetry shows that the generalized Paley graphs under consideration satisfy the Global Matching Condition. This approach is based on ideas from [4] where the argument was outlined for quadratic Paley graphs of even power order $q = p^{2m}$.

Theorem 3.6. *Let $k \geq 2$ and suppose $\mathcal{P}(q,k)$ is a connected generalized Paley graph of order $q = p^n$. If $\mathbb{F}_p^\times \leq (\mathbb{F}_q^\times)^k$, then $\mathcal{P}(q,k)$ satisfies the Global Matching Condition.*

Proof. By symmetry it suffices to consider the edge $01 \in E$ and to show that there is a perfect matching between N_0 and N_1. As in Lemma 3.5, fix $a_1, \ldots, a_{n-1} \in \mathbb{F}_p$ not all zero and set

$$S(a_1, \ldots, a_{n-1}) = \{b + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \mid b \in \mathbb{F}_p\}.$$

Then for any $\alpha \in N_0 \cap S(a_1, \ldots, a_{n-1})$, $\beta \in N_1 \cap S(a_1, \ldots, a_{n-1})$, it follows that

$$\alpha - \beta \in \mathbb{F}_p^\times \leq (\mathbb{F}_q^\times)^k.$$

Hence, $\alpha\beta \in E$ and therefore the bipartite subgraph $H(a_1, \ldots, a_{n-1})$ consisting of all edges in E between $N_0 \cap S(a_1, \ldots, a_{n-1})$ and $N_1 \cap S(a_1, \ldots, a_{n-1})$ is complete. In light of Lemma 3.5, it follows that that the complete bipartite subgraph $H(a_1, \ldots, a_{n-1})$ is balanced. Thus, we can match vertices in $H(a_1, \ldots, a_{n-1})$ in a pairwise fashion to obtain a perfect matching between $N_0 \cap S(a_1, \ldots, a_{n-1})$ and $N_1 \cap S(a_1, \ldots, a_{n-1})$.

Now let $a = (a_1, \dots, a_{n-1}) \in \mathbb{F}_p^{n-1}$ be a multi-index for $a_1, \dots, a_{n-1} \in \mathbb{F}_p$ so that $S(a) = S(a_1, \dots, a_{n-1})$. Set $\mathcal{S} = \{S(a) \mid a \neq 0 \in \mathbb{F}_p^{n-1}\}$ and let $\mathcal{J}$ be a multi-indexing set for $\mathcal{S}$. Noting that $\mathbb{F}_p^\times \leq (\mathbb{F}_q^\times)^k$ implies $\mathbb{F}_p \subseteq \{0\} \cup \{1\} \cup \nabla_{01}$, it follows that

$$\bigcup_{a \in \mathcal{J}} N_0 \cap S(a) = N_0 \cap \bigcup_{a \in \mathcal{J}} S(a) = N_0 \cap (\mathbb{F}_q \setminus \mathbb{F}_p) = N_0 \tag{3.8}$$

and similarly

$$\bigcup_{a \in \mathcal{J}} N_1 \cap S(a) = N_1. \tag{3.9}$$

Therefore, since the sets $S(a) = S(a_1, \dots, a_{n-1})$ are disjoint for each distinct choice of $a = (a_1, \dots, a_{n-1}) \in \mathcal{J}$, it follows from (3.8) and (3.9) that the bipartite subgraph H between N_0 and N_1 can be partitioned into complete balanced bipartite subgraphs $H(a) = H(a_1, \dots, a_{n-1})$ consisting of all edges in E between $N_0 \cap S(a)$ and $N_1 \cap S(a)$. Thus, since each subgraph $H(a)$ admits a perfect matching, it follows that there is a perfect matching between N_0 and N_1 and therefore $\mathcal{P}(q, k)$ satisfies the Global Matching Condition by symmetry. □

Due to Theorems 1.5, 2.9, 3.2, and 3.6, we obtain the following full generalization of the unpublished work of [4] on quadratic Paley graphs $\mathcal{P}(q, 2)$ of even power order $q = p^{2m}$.

Theorem 3.7. *Let $m \geq 1$ and suppose that $\mathcal{P}(q, k) = (V, E)$ is a generalized Paley graph of order $q = p^{km}$ where k is prime. Then the condensed Ricci curvature*

$$\Bbbk(x, y) = \frac{k}{q-1}(2 + |\nabla_{xy}|)$$

for any edge $xy \in E$.

Proof. First note that since $\mathcal{P}(q, k)$ is a generalized Paley graph of order $q = p^{km}$ with $k \geq 2$, it follows that $\mathcal{P}(q, k)$ is connected by Theorem 2.9. Moreover, since k is prime it follows that $\mathbb{F}_p^\times \leq (\mathbb{F}_q^\times)^k$ by Theorem 3.2. Hence, from Theorem 3.6 we see that $\mathcal{P}(q, k)$ satisfies the Global Matching Condition so that the condensed Ricci curvature

$$\Bbbk(x, y) = \frac{k}{q-1}(2 + |\nabla_{xy}|)$$

for any edge $xy \in E$ by Theorem 1.5. □

Furthermore, as a consequence of Theorems 1.5, 3.3, and 3.6, we obtain the same explicit formula for the condensed Ricci curvature on a large class of connected generalized Paley graphs.

Theorem 3.8. *Let $k \geq 2$ and suppose that $\mathcal{P}(q, k) = (V, E)$ is a connected generalized Paley graph of order $q = p^n$ where $k \mid \frac{q-1}{p-1}$. Then the condensed Ricci curvature*

$$\Bbbk(x, y) = \frac{k}{q-1}(2 + |\nabla_{xy}|)$$

for any edge $xy \in E$.

Proof. Since $k \mid \frac{q-1}{p-1}$ it follows that $\mathbb{F}_p^\times \leq (\mathbb{F}_q^\times)^k$ from Theorem 3.3. Hence, $\mathcal{P}(q, k)$ satisfies the Global Matching Condition by Theorem 3.6. Therefore, since $\mathcal{P}(q, k)$ is connected, it follows from Theorem 1.5 that the condensed Ricci curvature

$$\Bbbk(x, y) = \frac{k}{q-1}(2 + |\nabla_{xy}|)$$

for any edge $xy \in E$. □

On the other hand, when a generalized Paley graph $\mathcal{P}(q,k)$ with $k \mid \frac{q-1}{p-1}$ is disconnected, our work can be adapted to its connected components to recover the same formula as in Theorem 3.8 for the condensed Ricci curvature.

Theorem 3.9. *Let $k \geq 2$ and suppose that $\mathcal{P}(q,k) = (V,E)$ is a disconnected generalized Paley graph order $q = p^n$ where $k \mid \frac{q-1}{p-1}$. Then the condensed Ricci curvature*

$$\Bbbk(x,y) = \frac{k}{q-1}(2 + |\nabla_{xy}|)$$

for any edge $xy \in E$.

Proof. From Theorems 2.5 and 2.6, it follows that each of the connected components of $\mathcal{P}(q,k)$ is isomorphic to the generalized Paley graph $\mathcal{P}(p^a,k')$ with $k' = k(p^a-1)/(q-1) \geq 1$ where a is the smallest proper divisor of n such that $(q-1)/(p^a-1)$ divides k. Recalling that the divisibility condition $k \mid \frac{q-1}{p-1}$ is equivalent to $p-1 \mid \frac{q-1}{k}$, it follows that

$$p-1 \mid \frac{q-1}{k} = \frac{p^a-1}{k'} = |(\mathbb{F}_{p^a}^{\times})^{k'}|$$

and therefore $\mathbb{F}_p^{\times} \leq (\mathbb{F}_{p^a}^{\times})^{k'}$ since $(\mathbb{F}_{p^a}^{\times})^{k'}$ is a finite cyclic group. So for $k' > 1$, applying Theorems 3.6 and 1.5 to the connected components of $\mathcal{P}(q,k)$ and noting the fact that $k' = k(p^a-1)/(q-1)$, we see that the condensed Ricci curvature

$$\Bbbk(x,y) = \frac{k'}{p^a-1}(2 + |\nabla_{xy}|) = \frac{k}{q-1}(2 + |\nabla_{xy}|)$$

for any edge $xy \in E$.

In the special case that $k' = 1$, we recall that the subgroup of 1-st powers over $\mathbb{F}_{p^a}$ is simply the multiplicative group $\mathbb{F}_{p^a}^{\times}$. Therefore, each connected component of the disconnected generalized Paley graph $\mathcal{P}(q,k)$ is isomorphic to the complete graph $\mathcal{P}(p^a,1) = K_{p^a}$ on p^a vertices. Thus, since the complete graph K_{p^a} on p^a vertices is regular of degree p^a-1, it follows for any edge $xy \in E$ that $\nabla_{xy} = K_{p^a} \setminus (\{x\} \cup \{y\})$. Hence, $|\nabla_{xy}| = p^a - 2$ and by Theorem 1.12 we recover the formula

$$\Bbbk(x,y) = \frac{p^a}{p^a-1} = \frac{1}{p^a-1}(2 + |\nabla_{xy}|) = \frac{k}{q-1}(2 + |\nabla_{xy}|)$$

for the condensed Ricci curvature of any edge $xy \in E$. □

References

[1] Frank Bauer, Jürgen Jost, and Shiping Liu. Ollivier-Ricci curvature and the spectrum of the normalized graph Laplace operator. *Math. Res. Lett.*, 19(6):1185–1205, 2012.

[2] Bhaswar B. Bhattacharya and Sumit Mukherjee. Exact and asymptotic results on coarse Ricci curvature of graphs. *Discrete Mathematics*, 338(1):23–42, 2015.

[3] Vincent Bonini, Conor Carroll, Uyen Dinh, Sydney Dye, Joshua Frederick, and Erin Pearse. Condensed Ricci curvature of complete and strongly regular graphs. *Involve*, 13(4), 2020.

[4] Vincent Bonini, Shiaohan Liu, Caroline Semmens, and Tyler Tran. Condensed Ricci curvature on Paley graphs. 2021, Unpublished Student Research Project.

[5] David Bourne, David Cushing, Shiping Liu, Florentin Münch, and Norbert Peyerimhoff. Ollivier–Ricci idleness functions of graphs. *SIAM Journal on Discrete Mathematics*, 32, 2017.

[6] M. M. Bronstein, B. P. Chamberlain, F. Di Giovanni, X. Dong, and J. Topping. Understanding over-squashing and bottlenecks on graphs via curvature. *International Conference on Learning Representations 2022*.

[7] K.L.H. Carpenter, S. Nadeem, A.K. Simhal, and et al. Measuring robustness of brain networks in autism spectrum disorder with Ricci curvature. *Sci. Rep.*, 10(10819), 2020.

[8] H. Chen, Z. Li, S. Pan, J. Wu, P. Zhang, and C. Zhou. CurvDrop: A Ricci curvature based approach to prevent graph neural networks from over-smoothing and over-squashing. *Proceedings of the ACM Web Conference 2023*, pages 221–230.

[9] David Cushing, Supanat Kamtue, J. Koolen, Shiping Liu, Florentin Münch, and Norbert Peyerimhoff. Rigidity of the Bonnet-Myers inequality for graphs with respect to Ollivier Ricci curvature. *Advances in Mathematics*, 369, 2020.

[10] David Cushing, Shiping Liu, and Norbert Peyerimhoff. Bakry-Émery curvature functions of graphs. *Canadian Journal of Mathematics*, 2016.

[11] J. Gao, Y.-Y. Lin, F. Luo, and C.-C. Ni. Community detection on networks with Ricci flow. *Sci. Rep.*, 9(1):1–12, 2019.

[12] T. Georgiou, E. Reznik, R. Sandhu, and et al. Graph curvature for differentiating cancer networks. *Sci. Rep.*, 5(12323), 2015.

[13] X. Gu, J. Gao, Y.-Y. Lin, and C.-C. Ni. Network alignment by discrete Oliivier-Ricci flow. *Proceedings of the 26th International Symposium on Graph Drawing and Network Visualization*, pages 447–462, 2018.

[14] N. Ho, K. D. Nguyen, K. N. Nguyen, T. M. Nguyen, V. P. Nguyen, and H. Nong. Revisiting over-smoothing and over-squashing using Ollivier's Ricci curvature. *International Conference on Machine Learning 2022*.

[15] Xueping Huang, Shiping Liu, and Qing Xia. Bounding the diameter and eigenvalues of amply regular graphs via Lin-Lu-Yau curvature. *Combinatorica*, 2024.

[16] Gareth A. Jones. Paley and the Paley graphs. *Isomorphisms, symmetry and computations in algebraic graph theory, Springer Proc. Math. Stat.*, 305:155–183, 2020.

[17] Jürgen Jost and Shiping Liu. Ollivier's Ricci curvature, local clustering and curvature-dimension inequalities on graphs. *Discrete & Computational Geometry*, 51(2):300–322, 2014.

[18] Tian Khoon Kim and Cheryl E. Praeger. On generalised Paley graphs and their automorphism groups. *Michigan Mathematical Journal*, 58(1):293–308, 2009.

[19] X. Lai, S. Bai, and Y. Lin. Normalized discrete Ricci flow used in community detection. *Physica A*, 597(127251), 2022.

[20] Serge Lang. *Algebra*. Springer, 3rd edition, 2002.

[21] X. Li and S. Liu. Lin–Lu–Yau curvature and diameter of amply regular graphs. *Journal of University of Science and Technology of China*, 51(12):889–893, 2021.

[22] Yong Lin, Linyuan Lu, and S.-T. Yau. Ricci curvature of graphs. *Tohoku Mathematical Journal, Second Series*, 63(4):605–627, 2011.

[23] Yong Lin, Linyuan Lu, and S.-T. Yau. Ricci-flat graphs with girth at least five. *Comm. Anal. Geom.*, 22(4):671–687, 2014.

[24] Florentin Münch and Radosław K. Wojciechowski. Ollivier Ricci curvature for general graph Laplacians: heat equation, Laplacian comparison, non-explosion and diameter bounds. *Adv. Math.*, 356:106759, 2019.

[25] Yann Ollivier. Ricci curvature of Markov chains on metric spaces. *Journal of Functional Analysis*, 256(3):810–864, 2009.

[26] Yann Ollivier. A survey of Ricci curvature for metric spaces and Markov chains. *Probabilistic approach to geometry*, 57:343–381, 2010.

[27] Jonathan DH Smith. Ricci curvature, circulants, and a matching condition. *Discrete Mathematics*, 329:88–98, 2014.