DIRICHLET CHARACTER DIFFERENCE GRAPHS

M. BUDDEN, N. CALKINS, W. N. HACK, J. LAMBERT and K. THOMPSON

Abstract. We define Dirichlet character difference graphs and describe their basic properties, including the enumeration of triangles. In the case where the modulus is an odd prime, we exploit the spectral properties of such graphs in order to provide meaningful upper bounds for their diameter.

1. Introduction

Upon one’s first encounter with abstract algebra, a theorem which resonates throughout the theory is Cayley’s theorem, which states that every finite group is isomorphic to a subgroup of some symmetric group. The significance of such a result comes from giving all finite groups a common ground by allowing one to focus on groups of permutations. It comes as no surprise that algebraic graph theorists chose the name Cayley graphs to describe graphs which depict groups. More formally, if \( G \) is a group and \( S \) is a subset of \( G \) closed under taking inverses and not containing the identity, then the Cayley graph, \( \text{Cay}(G, S) \), is defined to be the graph with vertex set \( G \) and an edge occurring between the vertices \( g \) and \( h \) if \( hg^{-1} \in S \) \([9]\). Some of the first examples of Cayley graphs that are usually encountered include the class of circulant graphs. A circulant graph, denoted by \( \text{Circ}(m, S) \), uses \( \mathbb{Z}/m\mathbb{Z} \) as the group for a Cayley graph and the generating set \( S \) is chosen amongst the integers in the set \( \{1, 2, \ldots, \lfloor \frac{m}{2} \rfloor \} \) \([2]\).
Alongside the creation of circulant graphs, graph theorists have conceived of generating sets which attract interest and intrigue across multiple disciplines of mathematics. One such generating set is the set of quadratic residues in $\mathbb{Z}/p\mathbb{Z}$ where $p$ is an odd prime with $p \equiv 1 \pmod{4}$. Such graphs involving quadratic residues were first created under a more general setting in 1962 by Sachs [17] and later developed independently in 1963 by Erdős and Rényi [8]. Although these creations came from different schools of thought, the name Paley graphs (named after the mathematician Raymond Paley for his work on Hadamard matrices involving quadratic residues [16]) has been agreed upon across all branches of mathematics.

The general setting for the aforementioned Paley graphs actually takes place with the vertices occurring in the field $\mathbb{F}_q$, where $q$ is a prime power congruent to 1 mod 4, and an edge $ab$ exists in the graph if and only if $a - b$ is a quadratic residue. The self-complementary properties possessed by these Paley graphs play an instrumental role in Ramsey theory. While Greenwood and Gleason [11] found exact values for the Ramsey numbers $R(3, 3)$, $R(3, 4)$, $R(3, 5)$, $R(4, 4)$, and $R(3, 3, 3)$, it was the Paley graphs corresponding to $\mathbb{F}_5$ and $\mathbb{F}_{17}$ that provided the lower bounds for the Ramsey numbers $R(3, 3)$ and $R(4, 4)$, respectively.

Although Paley graphs have caught the eyes of many mathematicians, it was not until 2009 when another generalization came into place, known as the generalized Paley graph [13]. Although the vertices of a generalized Paley graph coincide with those of the Paley graph, the generalized Paley graph takes its generating set forming edges in the graph to come from a subgroup $S$ of the multiplicative group $\mathbb{F}_q^\times$ where $|S| = k$ and $q - 1$ is even. Like its predecessor, these generalized Paley graphs also played a vital role in determining lower bounds for Ramsey numbers. In fact, Su, Li, Luo, and Li [18] used the subgroup of cubic residues in $\mathbb{F}_p^\times$ for prime numbers $p$ of the form $6m + 1$ to produce 16 new lower bounds for Ramsey numbers.

In the spirit of these generalized Paley graphs and the aforementioned circulant graphs, we shall construct Dirichlet character difference graphs, which will arise from characters on $(\mathbb{Z}/m\mathbb{Z})^\times$. In
order to provide a deeper understanding of such graphs, we begin by providing some background information on Dirichlet characters.

Suppose that $m$ is a positive integer with $\chi: (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ a character (group homomorphism). We naturally identify $\mathbb{Z}/m\mathbb{Z}$ with the set of least residues $\{0, 1, \ldots, m - 1\}$. A character extended to all of $\mathbb{Z}$ by means of reducing modulo $m$ and requiring $\chi(a) = 0$ whenever $\gcd(a, m) > 1$ is called a Dirichlet character. At times, it will be beneficial to view $\chi$ as a function on $\mathbb{Z}$, but for a majority of this article we shall consider it as just a character of $(\mathbb{Z}/m\mathbb{Z})^\times$. One well-known result in the study of characters is that for any finite abelian group $G$, the character group of $G$, denoted by $\hat{G}$, is isomorphic to $G$ (e.g., see [14, Proposition 4.18]). Let $r_\chi$ denote the order of $\chi: (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ as an element of $(\mathbb{Z}/m\mathbb{Z})^\times$. If we denote the Euler totient function by $\varphi(m)$ (defined as giving the order of $(\mathbb{Z}/m\mathbb{Z})^\times$), then it is understood that $r_\chi$ is a divisor of $\varphi(m)$. Denoting the kernel of $\chi$ by $\text{Ker}(\chi)$, we see that $\chi$ is a $|\text{Ker}(\chi)|$-to-one mapping with $|\text{Ker}(\chi)| = \frac{\varphi(m)}{r_\chi}$. Throughout the remainder of this article, we shall take “character” to mean a character on $(\mathbb{Z}/m\mathbb{Z})^\times$.

With our background on Dirichlet characters complete, we wish to create the appropriately named Dirichlet character difference graphs. For a character $\chi$, we define the graph $\text{Dir}(m, \chi)$ to have vertex set $V(\text{Dir}(m, \chi)) := \mathbb{Z}/m\mathbb{Z}$ and edge set

$$E(\text{Dir}(m, \chi)) := \{ab \mid a - b \in \text{Ker}(\chi) \text{ or } b - a \in \text{Ker}(\chi)\}.$$ 

As a consequence of the definition of the Dirichlet character difference graph $\text{Dir}(m, \chi)$, we find a class of regular Hamiltonian graphs of order $m$. In fact, if $\chi(-1) = 1$, the corresponding Dirichlet character graph is $|\text{Ker}(\chi)|$-regular, while $\chi(-1) = -1$ implies $\text{Dir}(m, \chi)$ is $2|\text{Ker}(\chi)|$-regular. Alongside the aforementioned properties of $\text{Dir}(m, \chi)$, we shall explore the additional contributions Dirichlet characters make to circulant graphs and find an immediate application for $\text{Dir}(m, \chi)$. 
2. Enumeration of Triangles

Following the approach of Maheswari and Lavaku [15], we determine the number of triangles $T(\text{Dir}(m, \chi))$ contained in $\text{Dir}(m, \chi)$ in terms of the number of pairs of consecutive elements in $\text{Ker}(\chi)$, denoted $N(\chi)$. A closed-form for $N(\chi)$ can be achieved for some characters using known evaluations of certain Jacobi sums. In particular, in the case where $m$ is a prime satisfying $m \equiv 1 \pmod{4}$ and $\chi$ is the Legendre symbol (the unique quadratic character) modulo $m$, a closed-form solution can be obtained by combining Maheswari and Lavaku’s result [15] with Aladov’s [1] evaluation of $N(\chi)$. Most recently, a closed-form solution has been given in [6] for $m$ a prime satisfying $m \equiv 1 \pmod{8}$, where $\chi$ is the quartic residue symbol.

Theorem 1. If $\chi: (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ is a character of order $r\chi$ satisfying $\chi(-1) = 1$, then the number of triangles contained in $\text{Dir}(m, \chi)$ is given by

$$T(\text{Dir}(m, \chi)) = \frac{m\varphi(m)}{6r\chi} N(\chi),$$

where $N(\chi)$ is the number of pairs of consecutive elements in $\text{Ker}(\chi)$. In the case where $\chi(-1) = -1$, we find

$$T(\text{Dir}(m, \chi)) = \frac{m\varphi(m)}{3r\chi} N(\chi).$$

Proof. Our approach mimics that of [15] and [6], but unlike [6], we omit the explicit determination of $N(\chi)$ since the methods employed in such computations are not easily extended to this generalized setting. We begin with the case where $\chi(-1) = 1$ and count the number of fundamental triangles

$$\Delta_1 := \{(0, 1, b) \mid b - 1, b \in \text{Ker}(\chi)\}.$$
It is clear from the definition that

$$|\Delta_1| = N(\chi).$$

For $a \in \text{Ker} (\chi)$, let

$$\Delta_a := \{(0, a, b) \mid b, b - a \in \text{Ker} (\chi)\}.$$  

Applying basic properties of groups, it is easily confirmed that the map $f : \Delta_1 \to \Delta_a$, given by $f((0, 1, b)) = (0, a, ab)$, is a bijection. Thus,

$$|\Delta_1| = |\Delta_a| = N(\chi).$$  

The total number of triangles that contain the vertex 0 may be determined by considering the union

$$\bigcup_{a \in \text{Ker} (\chi)} \Delta_a$$

and noting that each triangle is counted twice since $(0, a, b)$ and $(0, b, a)$ represent the same triangle. Thus,

$$\left| \bigcup_{a \in \text{Ker} (\chi)} \Delta_a \right| = \frac{\phi(m)}{2r_\chi} N(\chi).$$

Finally, $\text{Dir}(m, \chi)$ is regular and each triangle has three vertices, implying that

$$T(\text{Dir}(m, \chi)) = \frac{m\phi(m)}{6r_\chi} N(\chi)$$

gives the total number of triangles in $\text{Dir}(m, \chi)$.

In order to determine the value of $T(\text{Dir}(m, \chi))$ when $\chi(-1) = -1$ observe that only one of $a - b$ and $b - a$ will be in $\text{Ker}(\chi)$ for the edge $ab$ to exist in the graph. In other words, whenever $\chi(-1) = -1$ we form the edge $ab$ if and only if $\chi(a - b) = \pm 1$. Using the fact that the product of two characters of a finite group is also a character and that the only square roots of unity are $\pm 1$, we note that $ab$ is an edge if and only if $a - b \in \text{Ker}(\chi^2)$. Since $\chi^2(-1) = 1$ and $\chi^2$ has order $r_\chi^2 = \frac{r_\chi}{2}$, we find a striking similarity between $\text{Dir}(m, \chi)$ and $\text{Dir}(m, \chi^2)$. In fact, $\text{Dir}(m, \chi)$ is
isomorphic to $\text{Dir}(m, \chi^2)$ whenever $\chi(-1) = -1$, which allows us to deduce the following theorem by applying the proof above to $\chi^2$.

Despite not being able to find a closed-form for $N(\chi)$ that is independent of the choice of $\chi$, we can describe a basic approach used to evaluate $N(\chi)$ for some choices of character. Our approach follows the method described by Andrews in [3, Section 10.1] in the case of the Legendre symbol and [6] in the case of the quartic residue symbol. For any $n \in (\mathbb{Z}/m\mathbb{Z})^\times$, $(\chi(n))^{r_x} = 1$, allowing us to consider the values of $\chi$ as elements in $\mathbb{Z}[\zeta]$, where $\zeta$ is a primitive $r_x$-th root of unity. The polynomial

$$
\psi_{r_x}(x) = \frac{x^{r_x} - 1}{x - 1} = x^{r_x - 1} + x^{r_x - 2} + \cdots + x + 1
$$

has all of the $r_x$-th roots of unity as roots, with the exception of 1. Thus, for $n \in (\mathbb{Z}/m\mathbb{Z})^\times$, we have

$$
\psi_{r_x}(\chi(n)) = \begin{cases} 
  r_x & \text{if } \chi(n) = 1 \\
  0 & \text{if } \chi(n) \neq 1.
\end{cases}
$$

It follows that

$$
N(\chi) = \frac{1}{r_x^2} \sum_{n-1, n \in (\mathbb{Z}/m\mathbb{Z})^\times} \psi_{r_x}(\chi(n-1)) \psi_{r_x}(\chi(n))
$$

and expanding the product $\psi_{r_x}(\chi(n-1)) \psi_{r_x}(\chi(n))$ yields $r_x^2$ sums of the form

$$
\chi^i(-1) \sum_{n-1, n \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi^i(1 - n) \chi^j(n).
$$

(1)

When the modulus is a prime, $\mathbb{Z}/m\mathbb{Z}$ is a field and we recognize the sums (1) as Jacobi sums (e.g., see [14, Section 4.6]). The reader interested in computing the values of Jacobi sums for specific characters may consult [4] for guidance, although in general, this is a very difficult problem.
3. Diameter and Eigenvalues When the Modulus is Prime

In this section, we set out to provide a meaningful upper bound for the diameter of \( \text{Dir}(m, \chi) \), denoted by \( \text{diam}(\text{Dir}(m, \chi)) \), in the special case when \( m = p \) is an odd prime number. The primary reason for this restriction is that the enumeration of the distinct eigenvalues of \( \text{Dir}(m, \chi) \) is greatly simplified in the prime case. In the case where \( \chi \) is the Legendre symbol with \( \chi(-1) = 1 \), these graphs correspond to the aforementioned Paley graphs, while whenever \( \chi(-1) = -1 \), we find \( \text{Dir}(m, \chi) \) corresponds to the complete graph on \( m \) vertices. In either case, a straightforward computation with the character given by the Legendre symbol shows that

\[
\text{diam}(\text{Dir}(p, \chi)) = \begin{cases} 
2 & \text{if } p \equiv 1 \pmod{4} \\
1 & \text{if } p \equiv 3 \pmod{4}.
\end{cases}
\]

To obtain an upper bound for general \( \text{Dir}(p, \chi) \), we use the well-known property that the number of distinct eigenvalues, denoted \( \Lambda(\text{Dir}(p, \chi)) \), satisfies

\[
(2) \quad \text{diam}(\text{Dir}(p, \chi)) \leq \Lambda(\text{Dir}(p, \chi)) - 1
\]

(for example, see [5, Exercise 11 in Section 6.1] or [7, Section 6.5.2 D10]).

So, we turn our attention to the eigenvalues of \( \text{Dir}(p, \chi) \). They can be computed by noting that \( \text{Dir}(p, \chi) \) is a circulant graph, having circulant adjacency matrix of the form

\[
A = \begin{pmatrix}
  c_0 & c_{p-1} & \cdots & c_1 \\
  c_1 & c_0 & \cdots & c_2 \\
  \vdots & \vdots & \ddots & \vdots \\
  c_{p-1} & c_{p-2} & \cdots & c_0
\end{pmatrix}.
\]
The eigenvalues of such a matrix are given by

$$\lambda_j := c_0 + c_{p-1} \zeta_p^j + \cdots + c_1 \zeta_p^{(p-1)j}, \quad j = 0, 1, \ldots, p - 1,$$

with corresponding eigenvectors

$$v_j := \left(1, \zeta_p^j, \ldots, \zeta_p^{(p-1)j}\right)^T,$$

where $\zeta_p$ is the primitive $p$th root of unity $e^{2\pi i / p}$ [10]. With the required groundwork in place, we transition towards the enumeration of distinct eigenvalues in the case $\chi(-1) = 1$.

**Lemma 2.** If $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ is a character of order $r_{\chi}$ that satisfies $\chi(-1) = 1$, then the graph $\text{Dir}(p, \chi)$ has $r_{\chi} + 1$ distinct eigenvalues.

**Proof.** The eigenvalue $\lambda_0$ has multiplicity 1 and simply counts the number of vertices that are adjacent to the vertex 0. Namely, we have

$$\lambda_0 = \frac{p - 1}{r_{\chi}}.$$

In order to determine the other distinct eigenvalues, we identify the remaining values of $j$ with elements in $(\mathbb{Z}/p\mathbb{Z})^\times$, since this realization enables us to use properties of the Galois group

$$\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \{\sigma_j : \mathbb{Q}(\zeta_p) \to \mathbb{Q}(\zeta_p) \mid \sigma_j(\zeta_p) = \zeta_p^j, \ j \in (\mathbb{Z}/p\mathbb{Z})^\times\}.$$

Letting $a_1, a_2, \ldots, a_k$ be the distinct elements in $\text{Ker}(\chi)$, we have that

$$\lambda_1 = \zeta_p^{a_1} + \zeta_p^{a_2} + \cdots + \zeta_p^{a_k}.$$

From the isomorphism

$$\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times,$$
we see that $\lambda_1$ is a primitive element for the unique subfield $K_{r\chi}$ of $\mathbb{Q}(\zeta_p)$ of degree $r\chi$ over $\mathbb{Q}$. The action of the automorphism $\sigma_j$ is given by

$$\sigma_j(\lambda_1) = \lambda_j,$$

and it follows that $\lambda_j$ is distinct for indices that are distinct coset representatives of

$$(\mathbb{Z}/p\mathbb{Z})^\times / \ker(\chi) \cong \text{Gal}(\mathbb{Q}(\zeta_p)/K_{r\chi}).$$

So, from $j \in (\mathbb{Z}/p\mathbb{Z})^\times$, we obtain $r\chi$ distinct eigenvalues corresponding to these distinct coset representatives. □

**Lemma 3.** If $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ is a character of order $r\chi$ that satisfies $\chi(-1) = -1$, then the graph $\text{Dir}(p, \chi)$ has $r\chi^2 + 1$ distinct eigenvalues.

**Proof.** We simply apply the previous lemma to the character $\chi^2$ using the identity $r\chi = 2r\chi^2$ to obtain the desired result. □

From Lemmas 2 and 3 and the inequality (2) mentioned at the beginning of this section, we obtain the following upper bound for the diameter of $\text{Dir}(p, \chi)$.

**Theorem 4.** If $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ is a character of order $r\chi$, then

$$\text{diam}(\text{Dir}(p, \chi)) \leq \begin{cases} r\chi & \text{if } \chi(-1) = 1 \\ \frac{r\chi}{2} & \text{if } \chi(-1) = -1. \end{cases}$$

When encountering any upper bound for the diameter on a class of graphs, the main cause for concern is whether or not the upper bound is tight. We shall alleviate those concerns by giving an example where the upper bound obtained from Theorem 4 actually equals the diameter of a given Dirichlet character graph.
Example 5. We may form a character on \((\mathbb{Z}/257\mathbb{Z})^\times\) using the 128\(^{th}\) power residue symbol defined on \((\mathbb{Z}[\zeta]/\pi\mathbb{Z}[\zeta])^\times\), where \(\zeta\) is a primitive 128\(^{th}\) root of unity and \(\pi\) is any prime above 257 in \(\mathbb{Z}[\zeta]\). This character naturally extends to a character of order 128 on \((\mathbb{Z}/257\mathbb{Z})^\times\), which we denote by \(\chi_{128}\). We find that \(\text{Ker}(\chi_{128}) = \{\pm 1\}\). Applying Theorem 4 to \(\text{Dir}(257, \chi_{128})\), we obtain the upper bound

\[
\text{diam}(\text{Dir}(257, \chi_{128})) \leq 128.
\]

However, \(\text{Dir}(257, \chi_{128})\) is isomorphic to the cycle \(C_{257}\). Since \(C_{257}\) has a diameter of 128, we see that our upper bound is the diameter in this case. This helps establish that the bound given in Theorem 4 is tight.

4. Applications

Perhaps the most alluring application of Dirichlet character difference graphs follows in the footsteps of its predecessors, Paley graphs. In the spirit of Paley graphs, Dirichlet character difference graphs can use the consecutive pairs of elements in the kernel of the given character to provide us with some insight into the size of a clique in the corresponding graph.

Although determining the clique number of \(\text{Dir}(m, \chi)\) can be difficult in general, there is a particular subgraph that can assist in the process. Define the set

\[
B := \{x \in \text{Ker}(\chi) \mid x - 1 \in \text{Ker}(\chi)\}
\]

and let \(\langle B \rangle\) denote the subgraph of \(\text{Dir}(p, \chi)\) induced by \(B\). Then we have the following relationship between the clique numbers of the two graphs.

Theorem 6. If \(\chi : (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow \mathbb{C}^\times\) is a Dirichlet character, then

\[
\omega(\text{Dir}(p, \chi)) = \omega(\langle B \rangle) + 2.
\]
Proof. Let \((a_1, a_2, \ldots, a_q)\) be a clique of order \(q\) in \(\text{Dir}(p, \chi)\). By symmetry, there must also be a clique that contains the vertex 0, which we denote by \((0, b_1, b_2, \ldots, b_{q-1})\). As \(b_1\) is adjacent to 0, we find that \(b_1^{-1} \in \text{Ker}(\chi)\), from which it follows that \((0, 1, b_1^{-1}b_2, \ldots, b_1^{-1}b_{q-1})\) is a clique in \(\text{Dir}(p, \chi)\). Thus, \((b_1^{-1}b_2, \ldots, b_1^{-1}b_{q-1})\) is a clique of order \(q - 2\) in \(\langle B \rangle\). On the other hand, suppose \((c_1, c_2, \ldots, c_k)\) is a clique in \(\langle B \rangle\). By the definition of \(B\), it follows that \((0, 1, c_1, \ldots, c_k)\) is a clique of order \(k + 2\) in \(\text{Dir}(p, \chi)\). Hence, we obtain the statement of the theorem. \(\square\)

It is our hope that in simplifying the computation of the clique number of \(\text{Dir}(m, \chi)\), future work with these graphs will result in new lower bounds for Ramsey numbers.

Acknowledgment. The authors would like to thank the anonymous referee for helpful suggestions that improved the composition of this paper.

1. Aladov N.S., *Sur la distribution des résidus quadratiques et non-quadratiques d’un nombre premier \(p\) dans la suite \(1, 2, \ldots, p – 1\)*, Recueil Math. 18 (1896), 61–75.


M. Budden, Department of Mathematics and Computer Science, Western Carolina University, Cullowhee, NC 28723, e-mail: mrbudden@email.wcu.edu

N. Calkins, Department of Mathematics, Louisiana State University, 303 Lockett Hall, Baton Rouge, LA 70803, e-mail: ncalki1@lsu.edu

W. N. Hack, Department of Mathematics, Armstrong Atlantic State University, 11935 Abercorn St., Savannah, GA 31419, e-mail: wh3022@students.armstrong.edu

J. Lambert, Department of Mathematics, Armstrong Atlantic State University, 11935 Abercorn St., Savannah, GA 31419, e-mail: Joshua.Lambert@armstrong.edu

K. Thompson, Department of Mathematics, Armstrong Atlantic State University, 11935 Abercorn St., Savannah, GA 31419, e-mail: sue144@hotmail.com