Acta Universitatis Apulensis No. 40/2014
ISSN: 1582-5329 pp. 51-65
http://www.uab.ro/auajournal/ doi: 10.17114/j.aua.2014.40.05

ON CERTAIN INDUCED SUBGRAPHS OF PALEY GRAPHS

R. Atanasov, M. Budden, J. Lambert, K. Murphy, A. Penland

Abstract. Since the advent of Ramsey theory in the 1930's, Paley Graphs have played an important role in the determination of lower bounds for diagonal Ramsey numbers due to their randomness. The construction of Paley graphs (whose vertices are identified with a finite field $\mathbb{F}_q$) leads to several natural induced subgraphs worth considering. In this paper, we consider the subgraphs induced on the squares $\mathbb{F}_q^{\times 2}$ and the subgraphs induced on $\mathbb{F}_q^\times - \mathbb{F}_q^{\times 2}$. We describe their basic properties, demonstrate their utility in simplifying the determination of the clique/independence numbers for Paley graphs, and address the determination of their diameters.

2000 *Mathematics Subject Classification*: Primary 05C30, 11T24; Secondary 05C12, 05C55

Keywords: Jacobi sums, hypergeometric functions.

1. Introduction

Originally defined by Sachs in 1962 [17], the randomness of Paley graphs make them particularly useful in the determination of lower bounds of diagonal Ramsey numbers. To define such graphs, let $q = p^f \equiv 1 \pmod 4$ be a prime power and suppose that $\chi_2 : \mathbb{F}_q^\times \longrightarrow \mathbb{C}^\times$ is the quadratic character of $\mathbb{F}_q^\times$. Denote by $\mathbb{F}_q^{\times 2}$ the kernel of χ_2 (the squares in $\mathbb{F}_q^\times$). Then the Paley graph $G(q)$ is defined as having vertex set $V(G(q)) = \mathbb{F}_q$ and edge set

$$E(G(q)) = \{ab \mid a - b \in \mathbb{F}_q^{\times 2}\}.$$

Note that the assumption $q \equiv 1 \pmod 4$ guarantees that $-1 \in \mathbb{F}_q^{\times 2}$, so that

$$\chi_2(a-b) = \chi_2(b-a).$$

The self-complementary graph $G(q)$ is regular and is easily seen to have size $\frac{q(q-1)}{4}$.

In this article, we focus on certain naturally occurring induced subgraphs of Paley graphs that may also prove useful in Ramsey theory. Namely, consider the subgraphs induced by $\mathbb{F}_q^{\times 2}$ and $\mathbb{F}_q^{\times} - \mathbb{F}_q^{\times 2}$, which we denote by $G_2(q)$ and $\widetilde{G_2(q)}$, respectively. Section 2 describes the main properties of the subgraphs in question, including the relationship between their clique/independence numbers and that of $G(q)$. Of course, the usefulness of these subgraphs in Ramsey theory is dependent upon our ability to compute their clique numbers. In general, this is a very difficult problem, so in Sections 3 and 4 our efforts will focus on a precise enumeration of triangles (K_3-subgraphs) in $G_2(q)$ and $\widetilde{G_2(q)}$ when $p \equiv 1 \pmod 4$ (not just $q = p^f \equiv 1 \pmod 4$). The computation will require us to venture into the realm of hypergeometric functions over finite fields. Our treatment of $G_2(q)$ and $\widetilde{G_2(q)}$ will conclude with section 5, where we consider the diameter of these subgraphs, providing an upper bound in the case of $G_2(q)$, and an exact evaluation in the case of $\widetilde{G_2(q)}$.

2. The Subgraphs $G_2(q)$ and $\widetilde{G_2(q)}$

Since $\chi_2 : \mathbb{F}_q^{\times} \longrightarrow \mathbb{C}^{\times}$ is a character of order 2, it follows that the graphs $G_2(q)$ and $\widetilde{G_2(q)}$ both have order $(q-1)/2$. In order to determine their sizes, consider the following expression:

$$(1 + \chi_2(n)) = \begin{cases} 2 & \text{if } n \in \mathbb{F}_q^{\times 2} \\ 0 & \text{if } n \notin \mathbb{F}_q^{\times 2}. \end{cases} \tag{1}$$

Although we could compute the sizes directly with character sums involving appropriate combinations of the above expression, instead we will first use a character sum to show that these graphs are regular.

If a is any vertex in $G_2(q)$, then the degree of a, denoted $deg(a)$, is given by

$$deg(a) = \frac{1}{4} \sum_{\substack{b \in \mathbb{F}_q^{\times} \\ b \neq a}} (1 + \chi_2(b))(1 + \chi_2(a - b)).$$

Expanding the expression on the right gives four separate sums that can be evaluated using the orthogonality relation

$$\sum_{g \in G} \chi(g) = 0, \tag{2}$$

which holds for any nontrivial character χ of a finite group G. We obtain

$$\sum_{\substack{b\in\mathbb{F}_q^\times\\ b\neq a}} 1 = q-2,$$

$$\sum_{\substack{b\in\mathbb{F}_q^\times\\ b\neq a}} \chi_2(b) = -\chi_2(a) = -1,$$

$$\sum_{\substack{b\in\mathbb{F}_q^\times\\ b\neq a}} \chi_2(a-b) = -\chi_2(a) = -1,$$

$$\sum_{\substack{b\in\mathbb{F}_q^\times\\ b\neq a}} \chi_2(a)\chi_2(a-b) = \sum_{\substack{b\in\mathbb{F}_q^\times\\ b\neq a}} \chi_2(1-ba^{-1}) \quad \text{since } \chi_2(a)=\chi_2(a^{-1})$$

$$= -\chi_2(1) = -1.$$

Thus, the degree of a in $G_2(q)$ is given by $(q-5)/4$ and since this answer is independent of the choice of vertex a, it follows that $G_2(q)$ is regular. Hence, the subgraph $G_2(q)$ has size

$$|E(G_2(q))| = \frac{(q-1)(q-5)}{16}.$$

In a similar manner, we can compute the degree of any vertex a in $\widetilde{G_2(p)}$ with the sum

$$deg(a) = \frac{1}{4}\sum_{\substack{b\in\mathbb{F}_q^\times\\ b\neq a}} (1-\chi_2(b))(1+\chi_2(a-b)).$$

As before, the result is independent of the choice of vertex and is given by $(q-1)/4$. Hence, $\widetilde{G_2(p)}$ is also regular and has size

$$|E(\widetilde{G_2(p)})| = \frac{(q-1)^2}{16}.$$

Thus, we have proved the following theorem.

Theorem 1. *The graphs $G_2(p)$ and $\widetilde{G_2(p)}$ are both regular, having sizes*

$$|E(G_2(q))| = \frac{(q-1)(q-5)}{16} \quad \text{and} \quad |E(\widetilde{G_2(p)})| = \frac{(q-1)^2}{16}.$$

Now we wish to demonstrate the utility of $G_2(q)$ and $\widetilde{G_2(q)}$ in Ramsey theory, but we must first establish some notations. For a graph G, let $\omega(G)$ denote its clique number (order of a maximal complete subgraph), $\alpha(G)$ denotes its independence number (cardinality of a maximal independent vertex set), $\mathcal{K}_n(G)$ denotes the number of K_n-subgraphs of G, and $\mathcal{I}_n(G)$ denotes the number of n-element independent vertex sets. We will prove the following theorem.

Theorem 2. *For $n \geq 2$, the graphs $G(q)$, $G_2(q)$, and $\widetilde{G_2(q)}$ satisfy*

$$\mathcal{K}_{n+1}(G(q)) = \frac{q}{n+1}\mathcal{K}_n(G_2(q)) \quad \text{and} \quad \mathcal{I}_{n+1}(G(q)) = \frac{q}{n+1}\mathcal{I}_n(\widetilde{G_2(q)}).$$

Proof. To prove the first equation, we note that there is a one-to-one correspondence between K_n-subgraphs of $G_2(q)$ and the K_{n+1}-subgraphs of $G(q)$ that contain the vertex 0. Namely, the K_n-subgraph $(a_1, a_2, \ldots, a_n)$ of $G_2(q)$ corresponds to the K_{n+1}-subgraph $(0, a_1, a_2, \ldots, a_n)$ of $G(q)$ containing the vertex 0. Now the affine transformation $f(x) = x + a$ on the vertices of $G(q)$ defines an automorphism, from which we see the number of K_{n+1}-subgraphs of $G(q)$ containing the vertex a is also equal to $\mathcal{K}_n(G_2(q))$. As we consider each one of the q affine transformations of this form, we note that each K_{n+1}-subgraph gets counted $n+1$ times (once for each vertex), resulting in

$$\mathcal{K}_{n+1}(G(q)) = \frac{q}{n+1}\mathcal{K}_n(G_2(q)).$$

The second equation is obtained in a similar manner, so we leave leave the details to the reader.

From the fact that $G(q)$ is self-complementary, we note that

$$\mathcal{K}_n(G(q)) = \mathcal{I}_n(G(q)).$$

Thus, we obtain the following corollary as an immediate consequence of theorem 2.

Corollary 3. *The graphs $G(q)$, $G_2(q)$, and $\widetilde{G_2(q)}$ satisfy*

$$\omega(G_2(q)) + 1 = \omega(G(q)) = \alpha(G(q)) = \alpha(\widetilde{G_2(q)}) + 1.$$

As the determination of clique numbers and independence numbers of graphs is quite difficult in general, the subgraphs we have considered allow us to reduce the problem to graphs with smaller order. Given the ubiquitous role Paley graphs have played in the determination of lower bounds of diagonal Ramsey numbers, it is likely our induced subgraphs can further assist in this process. In the next two sections, our focus will be the determination of $\mathcal{K}_3(G_2(q))$, $\mathcal{K}_3(\widetilde{G_2(q)})$, $\mathcal{I}_3(G_2(q))$, and $\mathcal{I}_3(\widetilde{G_2(q)})$.

3. Hypergeometric Functions and Character Sums

As part of the enumeration of triangles and 3-element independent vertex sets in $G_2(q)$ and $\widetilde{G_2(q)}$, we must first concentrate our efforts on a character sum evaluation that arises as a special value of certain hypergeometric functions over $\mathbb{F}_q$. We will see in the next section the role this character sum will play in computing $\mathcal{K}_3(G_2(q))$ and $\mathcal{K}_3(\widetilde{G_2(q)})$. Following along the lines of classical hypergeometric series, Greene [10] was the first to develop the hypergeometric functions ${}_{n+1}F_n$ over $\mathbb{F}_q$ and to show that they satisfy many analogous transformations to their classical counterparts. In order to define these functions, let $A, B \in \widehat{\mathbb{F}_q^\times}$ (the character group of $\mathbb{F}_q^\times$) and let $J(A,B)$ be the *Jacobi sum*

$$J(A,B) := \sum_{\substack{x \in \mathbb{F}_q^\times \\ x \neq 1}} A(x)B(1-x).$$

Also, define the *binomial coefficient*

$$\binom{A}{B} := \frac{B(-1)}{q} J(A, \overline{B}).$$

Then if $x \in \mathbb{F}_q$ and $A_0, A_1, \ldots, A_n, B_1, \ldots, B_n \in \widehat{\mathbb{F}_q^\times}$, the *hypergeometric function* ${}_{n+1}F_n$ is defined by

$${}_{n+1}F_n\left(\begin{matrix} A_0, A_1, \ldots, A_n \\ B_1, \ldots, B_n \end{matrix} \,\middle|\, x \right) := \frac{q}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_q^\times}} \binom{A_0\chi}{\chi} \binom{A_1\chi}{B_1\chi} \cdots \binom{A_n\chi}{B_n\chi} \chi(x).$$

Besides the connections these functions share with classical hypergeometric series, many authors have investigated them for their arithmetical properties as well as their ties to elliptic curves and modular forms (eg., see [5], [7], [8], [9], [14], [15], and [16]). Our interest in hypergeometric functions comes from their connection with the character sum

$$I(t;p) := \sum_{\substack{x,y \in \mathbb{F}_p^\times \\ x \neq -1, -ty \\ y \neq -1}} \chi_2(x)\chi_2(x+1)\chi_2(y)\chi_2(y+1)\chi_2(x+ty),$$

where $\chi_2 : \mathbb{F}_p^\times \longrightarrow \mathbb{C}^\times$ is the Legendre symbol modulo p. In 1981, Evans, Pulham, and Sheehan [6] conjectured that

$$I(1;p) = \chi_2(2)(4x^2 - p)$$

when $p \equiv 1, 3 \pmod 8$ and $p = x^2 + 2y^2$ for $x, y \in \mathbb{Z}$. The conjecture was proven by Greene and Stanton [11] in 1986 by evaluating the hypergeometric function ${}_3F_2(-1)$ for every prime p. Fundamental to their work was the realization that

$$I(t;p) = p^2 \; {}_3F_2 \left(\begin{array}{c} \chi_2, \chi_2, \chi_2 \\ \quad\;\; \epsilon, \;\; \epsilon \end{array} \middle| -t \right)$$

(cf. Proposition 2.10, [11]). We will need the following lemma, which generalizes the evaluation of $I(t;p)$ to prime powers $q = p^f$, whenever $p \equiv 1 \pmod 4$.

Lemma 4. *If $q = p^f$, where $p \equiv 1 \pmod 4$ is a prime and if $\chi_2 : \mathbb{F}_q^\times \longrightarrow \mathbb{C}^\times$ is the quadratic character on $\mathbb{F}_q^\times$, then*

$$\sum_{\substack{a,b,c \in F_q^\times \\ a \neq b,c \\ b \neq c}} \chi_2(a)\chi_2(b)\chi_2(c)\chi_2(a-b)\chi_2(b-c)\chi_2(a-c) = (q-1)\left(\pi^{2f} + \overline{\pi}^{2f}\right),$$

where π is a primary prime above p in $\mathbb{Z}[i]$.

Proof. Letting

$$S := \sum_{\substack{a,b,c \in F_q^\times \\ a \neq b,c \\ b \neq c}} \chi_2(a)\chi_2(b)\chi_2(c)\chi_2(a-b)\chi_2(b-c)\chi_2(a-c),$$

begin by making the substitution $x = ac^{-1}$ and $y = bc^{-1}$ (and using the fact that $\chi_2(c) = \chi_2(c^{-1})$), yielding

$$S = \sum_{\substack{x,y,c \in F_q^\times \\ x \neq y,1 \\ y \neq 1}} \chi_2(x)\chi_2(y)\chi_2(x-y)\chi_2(y-1)\chi_2(x-1).$$

Then $S = \sum_{c \in \mathbb{F}_q^\times} C = (q-1)C$, where

$$C := \sum_{\substack{x,y \in F_q^\times \\ x \neq y,1 \\ y \neq 1}} \chi_2(x)\chi_2(y)\chi_2(x-y)\chi_2(x-1)\chi_2(y-1).$$

The sum C is a generalization of the character sum evaluated in [6] and we follow their approach, utilizing a substitution originally implemented by D. Lehmer and E.

Lehmer [13]. Replacing x by $x+1$ and y by $y+1$, we have

$$C = \sum_{\substack{x,y \in F_q^\times \\ x \neq y,-1 \\ y \neq -1}} \chi_2(x+1)\chi_2(y+1)\chi_2(x-y)\chi_2(x)\chi_2(y)$$

$$= \sum_{\substack{x,y \in F_q^\times \\ x \neq y,-1 \\ y \neq -1}} \chi_2((x+1)y^{-1})\chi_2((y+1)x^{-1})\chi_2(x-y).$$

Before we implement the Lehmers' substitution, we must split the sum based upon whether or not the values of x and y satisfy $x+y=-1$. When this condition is met, the contribution of these terms to the overall sum is given by

$$\sum_{\substack{y \in \mathbb{F}_q^\times \\ y \neq -1,-2^{-1}}} \chi_2(-2y-1) = -2.$$

So we have

$$C = -2 + \sum_{\substack{x,y \in \mathbb{F}_q^\times \\ x \neq y,-1,-y-1 \\ y \neq -1}} \chi_2((x+1)y^{-1})\chi_2((y+1)x^{-1})\chi_2(x-y).$$

Now we make the substitution $t=(x+1)y^{-1}$ and $u=(y+1)x^{-1}$ (so that $x=(t+1)(ut-1)^{-1}$ and $y=(u+1)(ut-1)^{-1}$) to obtain

$$C = -2 + \sum_{\substack{t,u \in \mathbb{F}_q^\times \\ t \neq -1,u,u^{-1} \\ u \neq -1}} \chi_2(t)\chi_2(u)\chi_2(u-t)\chi_2(ut-1).$$

Corresponding to the terms we removed from the previous sum, we now reinsert the terms for which $t=-1$ or $u=-1$. Both of these conditions are still not allowed to occur simultaneously, but it is easily checked that each case results in a contribution of -1 to the sum so that we have

$$C = \sum_{\substack{t,u \in \mathbb{F}_q^\times \\ t \neq u,u^{-1}}} \chi_2(t)\chi_2(u)\chi_2(u-t)\chi_2(ut-1).$$

Replacing t with tu^{-1}, the sum becomes

$$C = \sum_{\substack{t \in \mathbb{F}_q^\times \\ t \neq 1}} \chi_2(t)\chi_2(1-t) \sum_{\substack{u \in \mathbb{F}_q^\times \\ u^2 \neq t}} \chi_2(u)\chi_2(u^2-t).$$

The inner sum $\phi_2(-t) := \sum \chi_2(u)\chi_2(u^2-t)$ is a generalization of a Jacobsthal sum (which is usually just defined over $\mathbb{F}_p^\times$). We will describe $\phi_2(-t)$ in terms of Jacobi sums following the approach used in Theorem 6.1.14 of [1]. Let $\chi_4 : \mathbb{F}_q^\times \longrightarrow \mathbb{C}^\times$ be a quartic character so that $\chi_4^2 = \chi_2$. Then

$$\begin{aligned}
\phi_2(-t) &= \sum_{\substack{u\in\mathbb{F}_q^\times \\ u^2\neq t}} \chi_2(u)\chi_2(u^2-t) \\
&= \sum_{\substack{u\in\mathbb{F}_q^\times \\ u^2\neq t}} \chi_4(u^2)\chi_4^2(u^2-t) \\
&= \sum_{\substack{v\in\mathbb{F}_q^\times \\ v\neq t}} \chi_4(v)\chi_4^2(v-t)\left(1+\chi_4^2(v)\right).
\end{aligned}$$

Replacing v with tv gives

$$\begin{aligned}
\phi_2(-t) &= \chi_4^3(t) \sum_{\substack{v\in\mathbb{F}_q^\times \\ v\neq 1}} \chi_4(v)\chi_4^3(1-v)\left(1+\chi_4^2(tv)\right) \\
&= \chi_4^3(t) \sum_{\substack{v\in\mathbb{F}_q^\times \\ v\neq 1}} \chi_4(v)\chi_4^2(1-v) + \chi_4(t) \sum_{\substack{v\in\mathbb{F}_q^\times \\ v\neq 1}} \chi_4^3(v)\chi_4^2(1-v) \\
&= \chi_4^3(t)J(\chi_4,\chi_4^2) + \chi_4(t)J(\chi_4^3,\chi_4^2).
\end{aligned}$$

Thus, the sum S becomes

$$S = (q-1)(J(\chi_4,\chi_4^2)^2 + J(\chi_4^3,\chi_4^2)^2).$$

Our result for S is independent of the choice of quartic character since both the Jacobi sum $J(\chi_4,\chi_4^2)$ and its conjugate are present. Without loss of generality, suppose that $\chi_4 = \left(\frac{\cdot}{\pi}\right)_4 \circ N_{\mathbb{F}_q/\mathbb{F}_p}$, where $\left(\frac{\cdot}{\pi}\right)_4$ is the quartic residue character for π, where π is a primary prime above p in $\mathbb{Z}[i]$. By the work of Davenport and Hasse [4],

$$J(\chi_4,\chi_4^2) = -(-J((\cdot/\pi)_4,(\cdot/\pi)_4^2))^f.$$

Finally, by Proposition2 9.9.1 and 9.9.4 of [12], we find that

$$J((\cdot/\pi)_4,(\cdot/\pi)_4^2)) = (-1/\pi)_4 J((\cdot/\pi)_4,(\cdot/\pi_4)) = -\pi,$$

completing the proof of the lemma.

4. Enumeration of Triangles

In order to determine the number of triangles in $G_2(q)$ and $\widetilde{G_2(q)}$ (denoted $T(G_2(q))$ and $T(\widetilde{G_2(q)})$, respectively), we once again exploit the values of the expression (1) and use character sums (cf. [3]). To simplify notation, define

$$C(a) := 1 + \chi_2(a) \qquad \text{and} \qquad \overline{C}(a) := 1 - \chi_2(a).$$

We see that

$$\mathcal{K}_3(G_2(q)) = \frac{1}{384} \sum_{\substack{a,b,c \in \mathbb{F}_q^\times \\ a \neq b,c \\ b \neq c}} C(a)C(b)C(c)C(a-b)C(b-c)C(c-a)$$

and

$$\mathcal{K}_3(\widetilde{G_2(q)}) = \frac{1}{384} \sum_{\substack{a,b,c \in \mathbb{F}_q^\times \\ a \neq b,c \\ b \neq c}} \overline{C}(a)\overline{C}(b)\overline{C}(c)C(a-b)C(b-c)C(c-a).$$

From these sums, we obtain the following theorem.

Theorem 5. *If $q = p^f$ and $p \equiv 1 \pmod 4$, then the number of triangles in $G_2(q)$ and $\widetilde{G_2(q)}$ are given by*

$$\mathcal{K}_3(G_2(q)) = \frac{q-1}{384}((q-2)(q-3) - 15(q-5) + 2Re(\pi^{2f}))$$

and

$$\mathcal{K}_3(\widetilde{G_2(q)}) = \frac{q-1}{384}((q-2)(q-3) - 3(q-1) - 2Re(\pi^{2f})),$$

where π is a primary prime above p in $\mathbb{Z}[i]$.

Proof. Expanding the products in each of the above sums yields 64 character sums of the form

$$\sum_{\substack{a,b,c \in \mathbb{F}_q^\times \\ a \neq b,c \\ b \neq c}} \chi_2^{\alpha_1}(a)\chi_2^{\alpha_2}(b)\chi_2^{\alpha_3}(c)\chi_2^{\alpha_4}(a-b)\chi_2^{\alpha_5}(b-c)\chi_2^{\alpha_6}(c-a),$$

where $\alpha_i \in \{0, 1\}$. Although we omit most of the technical details of the computations of the 64 sums, we state the results based upon the number of nonidentity terms in each sum (that is, the number of $\alpha_i = 1$). The only sum containing 0 nonidentity terms is

$$\sum_{\substack{a,b,c\in\mathbb{F}_q^\times \\ a\neq b,c \\ b\neq c}} 1 = (q-1)(q-2)(q-3).$$

From the orthogonality relation (2), it is easily checked that all of the sums containing only 1 nonidentity term sum to 0. Continuing in this manner, of the 15 sums which contain exactly 2 nonidentity terms, 12 sum to $-(q-1)(q-3)$ and 3 sum to $2(q-1)$. The sums containing exactly 3 nonidentity terms all sum to 0 while for those containing exactly 4 nonidentity terms, 12 sum to $2(q-1)$ and 3 sum to $-(q-1)(q-3)$. The sums containing exactly 5 nonidentity terms all sum to 0 and the case in which all of the nonidentity terms appear falls back to the sum evaluated in Lemma 4. The theorem follows from these evaluations along with careful regard to signs in the case of $\widetilde{G_2(q)}$.

This result along with Theorem 2 implies the following corollary, which is a generalized version of Theorem 1 in Evans, Pulham and Sheehan's paper [6]. Their result provides an enumeration of K_4-subgraphs in $G(p)$, and although their answer appears different from ours, one can verify that the two solutions agree.

Corollary 6. *The number of complete subgraphs of order* 4 *in the Paley graph* $G(q)$*, where* $q = p^f$ *and* $p \equiv 1 \pmod 4$*, is given by*

$$\mathcal{K}_4(G(q)) = \frac{q(q-1)}{1536}((q-2)(q-3) - 15(q-5) + 2Re(\pi^{2f})),$$

where π *is a primary prime above* p *in* $\mathbb{Z}[i]$.

Using a similar approach to the one used in Theorem 5, we may determine the number of independent sets of order 3 in $G_2(q)$ and $\widetilde{G_2(q)}$ using the sums

$$\mathcal{I}_3(G_2(q)) = \frac{1}{384} \sum_{\substack{a,b,c\in\mathbb{F}_q^\times \\ a\neq b,c \\ b\neq c}} C(a)C(b)C(c)\overline{C}(a-b)\overline{C}(b-c)\overline{C}(c-a)$$

and

$$\mathcal{I}_3(\widetilde{G_2(q)}) = \frac{1}{384} \sum_{\substack{a,b,c\in\mathbb{F}_q^\times \\ a\neq b,c \\ b\neq c}} \overline{C}(a)\overline{C}(b)\overline{C}(c)\overline{C}(a-b)\overline{C}(b-c)\overline{C}(c-a).$$

This gives us the following theorem.

Theorem 7. *The number of independent sets of order* 3 *in* $G_2(q)$ *and* $\widetilde{G_2(q)}$*, where* $q = p^f$ *and* $p \equiv 1 \pmod 4$*, are given by*

$$\mathcal{I}_3(G_2(q)) = \frac{q-1}{384}((q-2)(q-3) - 3(q-1) - 2Re(\pi^{2f}))$$

and

$$\mathcal{I}_3(\widetilde{G_2(q)}) = \frac{q-1}{384}((q-2)(q-3) - 15(q-5) + 2Re(\pi^{2f})),$$

where π *is a primary prime above* p *in* $\mathbb{Z}[i]$*.*

Of course, the self-complementary nature of Paley graphs means that

$$\mathcal{K}_n(G(q)) = \mathcal{I}_n(G(q)),$$

so we do not need to appeal to the previous theorem to determine

$$\mathcal{I}_4(G(q)) = \frac{q(q-1)}{1536}((q-2)(q-3) - 15(p-5) + 2Re(\pi^{2f}))$$

where $q = p^f$ and π is a primary prime above p in $\mathbb{Z}[i]$.

5. Distance in $G_2(q)$ and $\widetilde{G_2(q)}$

Now we conclude our analysis of $G_2(q)$ and $\widetilde{G_2(q)}$ by considering their diameters. Recall that the diameter of a graph G is the maximum of all distances $d(u, v)$ where u and v are vertices in G. It is a straight-forward exercise to prove that $diam(G(q)) = 2$. We'll begin by considering $G_2(q)$.

Theorem 8. *If* $q \equiv 1 \pmod 4$ *is a power of a prime with* $q > 9$*, then the induced subgraph* $G_2(q)$ *has diameter*

$$diam(G_2(q)) \leq 3.$$

Proof. For $q = 5$ and $q = 9$, it is easily verified that $G_2(q)$ is disconnected, and hence, the diameters of these graphs are infinite. Now assume $q > 9$ and suppose that $a, b \in \mathbb{F}_q^{\times 2}$ are two vertices with distance $d(a, b) > 2$ (including the possibility that a and b are in different connected components of $G_2(q)$). Let $N(a)$ (respectively $N(b)$) be the set of all vertices that are adjacent to a (respectively, b). We have already noted that $N(a)$ and $N(b)$ each have cardinality $\frac{q-5}{4}$. Since we are assuming $d(a, b) > 2$, we see that $N(a) \cap N(b) = \emptyset$. Note also that

$$N(a) \cup \{a\} \cup N(b) \cup \{b\} = V(G_2(q)).$$

If any member of $N(a)$ is adjacent to any member of $N(b)$, then $d(a,b) = 3$. Otherwise, we find that both $N(a) \cup \{a\}$ and $N(b) \cup \{b\}$ are isomorphic to $K_{(q-1)/4}$. In this case, the clique number $\omega(G(q))$ of $G(q)$ satisfies

$$\omega(G(q)) \geq \frac{q-1}{4}.$$

However, it is well-known (for example, see [2]) that

$$\omega(G(q)) \leq \sqrt{q}.$$

So, the only way that two vertices in $G_2(q)$ can have a distance of more than 3 is if q satisfies

$$\frac{q-1}{4} \leq \sqrt{q}.$$

This can only happen for values of $q \leq 17$. The remaining values of q that we have neglected are $q = 13$ and $q = 17$. By constructing the corresponding graphs, one can check directly that $diam(G_2(13)) = 3$ and $diam(G_2(17)) = 2$.

Although we have not proved it here, numerical evidence suggests that

$$diam(G_2(q)) = 2$$

whenever $q > 13$. However, in the case of the graph $\widetilde{G_2(q)}$, we can be more precise about the determination of diameters.

Theorem 9. *If $q \equiv 1 \pmod 4$ is a power of a prime with $q > 5$, then the induced subgraph $\widetilde{G_2(q)}$ has diameter 2.*

Proof. It is easily observed that $diam(\widetilde{G_2(5)}) = 1$ and that $\widetilde{G_2(q)}$ is not complete when $q > 5$, hence $diam(\widetilde{G_2(q)}) > 1$. Let $a, b \in \mathbb{F}_q^\times - \mathbb{F}_q^{\times 2}$ be nonadjacent vertices in $\widetilde{G_2(q)}$. We have already seen that a (and b) is adjacent to $(q-1)/2$ vertices. Since

$$2\left(\frac{q-1}{4}\right) > \frac{q-5}{4},$$

it follows that a and b must have at least one neighbor in common. Thus, $d(a,b) = 2$.

6. Conclusion

Our results which connect the clique and independence numbers of $G_2(q)$ and $\widetilde{G_2(q)}$ with that of the Paley graph $G(q)$ may serve as a useful tool in Ramsey theory. Although these graphs are "natural" subgraphs of $G(q)$ to consider, additional assumptions allow other subgraphs to be considered as well. For example, if one assumes $q \equiv 1 \pmod{m}$, then one may consider the subgraph of $G(q)$ induced on the m^{th} power residues in $\mathbb{F}_p^{\times}$. Such graphs may also prove useful, but computations similar to those contained here will be significantly more difficult. We reserve such subgraphs for future inquiry.

References

[1] B. Berndt, R. Evans, K. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, Inc., New York, 1998.

[2] B. Bollobás, *Random Graphs*, Cambridge University Press, 2001.

[3] M. Budden, N. Calkins, N. Hack, J. Lambert, K. Thompson, *Enumeration of Triangles in Quaritc Residue Graphs*, INTEGERS 11 (2011), #A48.

[4] H. Davenport, H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. 172 (1934), 151-182.

[5] R. Evans, J. Greene, *Evaluations of Hypergeometric Functions over Finite Fields*, Hiroshima Math. J. 39 (2009), 217-235.

[6] R. Evans, J. Pulham, J. Sheehan, *On the Number of Complete Subgraphs Contained in Certain Graphs*, J. Combin. Theory Ser. B 30 (1981), 364-371.

[7] S. Frechette, K. Ono, M. Papanikolas, *Gaussian Hypergeometric Functions and Traces of Hecke Operators*, Int. Math. Res. Notices 60 (2004), 3233-3262.

[8] J. Fuselier, *Hypergeometric Functions over Finite Fields and Relations to Modular Forms and Elliptic Curves*, dissertation, Texas A&M University, 2007.

[9] J. Fuselier, *Hypergeometric Functions over $\mathbb{F}_p$ and Relations to Elliptic Curves and Modular Forms*, Proc. Amer. Math. Soc. 138 (2010), 109-123.

[10] J. Greene, *Hypergeometric Functions over Finite Fields*, Trans. Amer. Math. Soc. 301 (1987), 77-101.

[11] J. Greene, D. Stanton, *A Character Sum Evaluation and Gaussian Hypergeometric Series*, J. Number Theory 23 (1986), 136-148.

[12] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, 2^{nd} edition, Springer-Verlag, 1990.

[13] D. Lehmer, E. Lehmer, *On the Cubes of Kloosterman Sums*, Acta Arith. 6 (1960), 15-22.

[14] C. Lennon, *Trace Formulas for Hecke Operators, Gaussian Hypergeometric Functions, and the Modularity of a Threefold*, J. Number Theory 131 (2011), 2320-2351.

[15] C. Lennon, *Gaussian Hypergeometric Evaluations of Traces of Frobenius for Elliptic Curves*, preprint.

[16] K. Ono, *Values of Gaussian Hypergeometric Series*, Trans. Amer. Math. Soc. 350, No. 3 (1998), 1205-1223.

[17] H. Sachs, *Über Selbstkomplementäre Graphen*, Publicationes Math. 9 (1962), 270-288.

Risto Atanasov
Department of Mathematics and Computer Science
Western Carolina University
Cullowhee, NC 28723
email: *ratanasov@email.wcu.edu*

Mark Budden
Department of Mathematics and Computer Science
Western Carolina University
Cullowhee, NC 28723
email: *mrbudden@email.wcu.edu*

Joshua Lambert
Department of Mathematics
Armstrong Atlantic State University
11935 Abercorn St.
Savannah, GA 31419
email: *Joshua.Lambert@armstrong.edu*

Kyle Murphy
Department of Mathematics and Computer Science
Western Carolina University
Cullowhee, NC 28723
email: *ksmurphy1@catamount.wcu.edu*

Andrew Penland
Department of Mathematics

Mailstop 3368
Texas A&M University
College Station, TX 77843-3368
email: *apenland@math.tamu.edu*