On the Strong Regularity of Cubic Paley Graphs for Even Order Finite Fields

Final Paper for MAT-322: Algebraic Graph Theory

John Gouwar

1 Introduction

When I started this project, I wanted to look for strongly regular graphs arising from finite fields. The two examples I initially had of such graphs were the Paley Graphs, and the Clebsch Graph. Both were formed by determining whether or not two vertices shared an edge if they were a particular k-th residue in the field. I noticed that in the case of the Clebsch Graph, $3 \mid |U(\mathbb{F}_{16})|$, and edges were determined by cubic residues. This got me thinking that strongly regular graphs might arise from residues of other divisors of $|U(\mathbb{F}_{16})|$, and even more generally, the divisors of $|U(\mathbb{F}_{2^n})|$. Section 3 details how I went about searching for graphs of this form.

The Paley Graphs, while named for English mathematician Raymond Paley, were not actually subject of any paper that Paley published. Instead, in a seminal paper he was focused on using quadratic residues to construct Hadamard matrices. The canonical definition of these graphs appear with Paley's name almost 30 years after his untimely death. For more information on the history and impact of the Paley Graphs across mathematics, see [1].

The Clebsch Graph is named for Alfred Clebsch, a 19th century mathematician, since the graph can arise from the intersection of 16 lines on a quartic surface named for Clebsch [2]. The Clebsch Graph is strongly regular with parameters (16, 5, 0, 2), and thus is triangle free, which is incredibly rare for strongly regular graphs. It is also possible to embed three copies of the Clebsch Graph in the complete graph on 16 vertices, which along with its triangle free nature, provides an interesting result in Ramsey Theory. Namely, that the Ramsey Number $R(3, 3, 3) = 17$. For more information on this result, see [3].

As a result of my search, I was able to conjecture that whenever 3 was a divisor of $U(\mathbb{F}_{2^n})$, or $2^n \equiv 1 \mod 3$, the graph formed from determining if the difference of two edges was a cubic residue would be strongly regular. I provide a proof of this conjecture, as well as some introduction to and background on the structures that I was studying. Finally, I developed two code bases as part of this project. One written in SageMath for constructing graphs on finite fields, which includes the code necessary to reproduce my experimental results (See Appendix 1). The other is a GAP package for constructing non-commuting graphs of finite groups. This package was developed both as a learning exercise for the GAP language and to aid my research partner, Jasper Egge (See Appendix 2).

2 Background & Definitions

Definition (Graph [4])**.** *A graph Γ is a pair (V, E) of sets satisfying $E \subseteq P_2(V)$, where $P_2(V)$ is the set of all subsets of V with two elements. The elements of V are called vertices and the elements of E are called edges. The set of vertices of a graph $\Gamma = (V, E)$ is often denoted $V(\Gamma)$, the set of edges is denoted $E(\Gamma)$. If $x, y \in V(\Gamma)$ and $\{x, y\} \in E(\Gamma)$, then x and y are said to be adjacent.*

Definition (Graph Automorphism)**.** *Suppose $\Gamma = (V, E)$ is a graph. A graph automorphism on Γ is a bijective function $\varphi : V(\Gamma) \to V(\Gamma)$ such that for all $x, y \in V(\Gamma)$, $\{\varphi(x), \varphi(y)\} \in E(\Gamma)$ if and only if $\{x, y\} \in E(\Gamma)$.*

Fact. *The set of all automorphisms, denoted $Aut(\Gamma)$, form a group which acts on $V(\Gamma)$.*

Definition (Vertex Transitivity)**.** *Suppose $\Gamma = (V, E)$ is a graph. We say that Γ is vertex transitive if for all $x, y \in V(\Gamma)$, there exists $\varphi \in Aut(\Gamma)$ such that $\varphi(x) = y$.*

Definition (Arc Transitivity)**.** *Suppose $\Gamma = (V, E)$ is a graph. We say that Γ is arc transitive if for all $\{x_1, y_1\}, \{x_2, y_2\} \in E(\Gamma)$, there exists $\varphi \in Aut(\Gamma)$ such that $\varphi(x_1) = x_2$ and $\varphi(y_1) = y_2$.*

Definition (Graph Symmetry)**.** *Suppose $\Gamma = (V, E)$ is a graph. Γ is symmetric if and only if it is both vertex and arc transitive.*

Definition (Vertex Neighborhood)**.** *Let $\Gamma = (V, E)$ be a graph and let $x \in V(\Gamma)$. The vertex neighborhood of x, denoted $N(x)$, is $\{y \in V(\Gamma) \mid \{x, y\} \in E(\Gamma)\}$.*

Definition (Regular Graph)**.** *A graph $\Gamma = (V, E)$ is $k-$regular if and only if for all $x \in V(\Gamma)$, $|N(x)| = k$.*

Definition (Strongly Regular Graph)**.** *Suppose $\Gamma = (V, E)$ is a graph. Γ is a strongly regular graph if and only if there exist parameters r, λ, and μ such that for all $x, y \in V(\Gamma)$:*

- *Γ is r-regular.*
- *If $\{x, y\} \in E(\Gamma)$, then $|N(x) \cap N(y)| = \lambda$.*
- *If $\{x, y\} \notin E(\Gamma)$ and $x \neq y$, then $|N(x) \cap N(y)| = \mu$.*

If so, we say that Γ has parameters (n, r, λ, μ), where $|V(\Gamma)| = n$.

Many strongly regular graphs arise from considering the relation between elements of a finite field.

Definition (Field)**.** *A field is commutative ring such that every non-zero element is a unit.*

Fact. *All fields with a finite number of elements are of order p^n with p prime and $n \in \mathbb{N}$. Up to isomorphism, there is only one field with order p^n, thus we denote this field $\mathbb{F}_{p^n}$.*

Definition (k-th Residues)**.** *Suppose $k \in \mathbb{N}$ with $k \geq 2$, $\mathbb{F}$ is a field, and $a \in \mathbb{F}$. Then a is a k-th residue in $\mathbb{F}$ if and only if there exists $x \in F$ such that $x^k = a$. Residues of low degree have names like polynomials of that degree (e.g. a 2nd residue can also be referred to as a quadratic residue). By convention, 0 is never considered a k-th residue.*

Definition (Characteristic of a Field)**.** *Let $\mathbb{F}$ be a field. The characteristic of $\mathbb{F}$ is the additive order of 1 in the group $(\mathbb{F}, +)$. If the order of 1 is infinite, we say $\mathbb{F}$ has characteristic 0.*

One family of strongly graphs on finite fields are the Paley Graphs.

Definition (Paley Graphs)**.** *Suppose q is a prime power with $q \equiv 1 \mod 4$. We define a graph $P = (V, E)$ such that*

- $V(P) = \mathbb{F}_q$
- $E(P) = \{\{x, y\} \in V(P) \times V(P) \mid x - y$ *is a quadratic residue in* $\mathbb{F}_q\}$.

The Paley Graphs are strongly regular with parameters $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$, and are isomorphic to their complement [4]. For this to be a valid graph $x - y$ must be a quadratic residue if and only if $y - x$ is a quadratic residue. The condition that $q \equiv 1 \mod 4$ ensures this (to see why this is the case, see [4]).

Another famous strongly regular graph arising from a finite field is the Clebsch Graph. While there are multiple ways of defining the Clebsch Graph geometrically, by either connecting maximal distance vertices in the 4-dimensional hypercube graph or contracting maximal distance vertices in the 5-dimensional hypercube graph, the method most similar to the construction of the Paley Graphs is defined below [5].

Definition (Clebsch Graph)**.** *Let $\Gamma = (V, E)$ be a graph. Let $V(\Gamma) = \mathbb{F}_{16}$ and let $\{x, y\} \in E(\Gamma)$ if and only if $x - y$ is a cubic residue in $\mathbb{F}_{16}$. We call this graph the Clebsch Graph.*

One way to interpret the construction of the Clebsch Graph is as a generalization of the Paley Graphs relying on cubic residues, instead of quadratic residues [6].

Definition (Cubic Paley Graph)**.** *Suppose q is a prime power with $q \equiv 1 \mod 3$. We define a graph $G_q^{(3)} = (V, E)$ such that*

- $V(G_q^{(3)}) = \mathbb{F}_q$
- $E(G_q^{(3)}) = \{\{x, y\} \in V(G_q^{(3)}) \times V(G_q^{(3)}) \mid x - y$ *is a cubic residue*$\}$

Using this notation, we can understand the Clebsch Graph as $G_{16}^{(3)}$. I prove in this paper that all Cubic Paley Graphs on even order finite fields are strongly regular.

3 Searching for an Interesting Result

To answer the question that I proposed in Section 1, I developed some code in Python, using SageMath, to generate graphs where the vertices would be elements of $\mathbb{F}_{2^n}$ for $n \in \{4 \dots 14\}$, and two vertices would share an edge if and only if their difference was k-th residue, where k was a specific divisor of $|U(\mathbb{F}_{2^n})|$ (see Appendix 1 for more details). The connected, strongly regular graphs that arose are summarized in Table 1.

Field	Residue Power	SRG Parameters
$\mathbb{F}_{16}$	3	(16, 5, 0, 2) Clebsch Graph
$\mathbb{F}_{64}$	3	(64, 21, 8, 6)
$\mathbb{F}_{256}$	3	(256, 85, 24, 30)
$\mathbb{F}_{256}$	5	(256, 51, 2, 12)
$\mathbb{F}_{1024}$	3	(1024, 341, 120, 110)
$\mathbb{F}_{1024}$	11	(1024, 93, 32, 6)
$\mathbb{F}_{4096}$	3	(4096, 1365, 440, 462)
$\mathbb{F}_{4096}$	5	(4096, 819, 194, 156)
$\mathbb{F}_{4096}$	9	(4096, 455, 6, 56)
$\mathbb{F}_{4096}$	13	(4096, 315, 74, 20)
$\mathbb{F}_{16384}$	3	(16384, 5461, 1848, 1806)
$\mathbb{F}_{16384}$	43	(16384, 381, 128, 6)

Table 1: Strongly regular graphs resulting from checking different residues on even order finite fields

From this experiment, I noticed that all fields which had 3 as a divisor of their unit group, or $2^n \equiv 1 \mod 3$, formed a strongly regular graph when two elements shared an edge if and only if their difference was a cubic residue. From here, I set out to determine whether this result had been proven generally. I was unable to find a proof of this, but there was some work into classifying the properties of Cubic Paley Graphs in [6], which is where I discovered the specific definition and notation. Therefore, I took it upon myself to prove the result that all Cubic Paley Graphs on even order finite fields are strongly regular.

4 Properties of Finite Fields and Cubic Residues

Before diving into the proof of strong regularity, it helps to have some idea about the nature of finite fields of even order and cubic residues.

Lemma 1 (Adapted from proof in [7])**.** *Suppose $\mathbb{F}_{p^n}$ is a field of order p^n, with p prime and $n \in \mathbb{N}$. The group of units, $U(\mathbb{F}_{p^n})$, is cyclic.*

Proof. Let $G = U(\mathbb{F}_{p^n})$. Let d be arbitrary such that $d \mid |G|$. Either G has an element of order d, or it does not. Consider the case where there exists $a \in G$ such that $|a| = d$. Let $H = \langle a \rangle$. Notice that for all $b \in H$, $b^d = 1$. Since there are at most d solutions to the polynomial $x^d = 1$ in a field, the elements of H are the only elements such that this is the case. Since H is cyclic, it has $\varphi(d)$ generators (where φ is Euler's totient function), and thus G has $\varphi(d)$ elements of order d.

The Euler Formula tells us that $|G| = \sum_{d||G|} \varphi(d)$. Therefore, for every divisor of $|G|$, including $|G|$ itself, there must be an element of that order, because if there were not, we would have a contradiction of the number of elements in the group with Euler's formula. Therefore, we can conclude that $|G|$ is cyclic, as claimed. □

As a result of this lemma, we can always fix $g \in U(\mathbb{F}_q)$ such that for every $x \in U(\mathbb{F}_q)$ there exists $r \in [1 \ldots q-1]$ such that $x = g^r$.

Lemma 2. *Suppose $\mathbb{F}_{p^n}$ is a field of order p^n, with p prime and $n \in \mathbb{N}$. The characteristic of $\mathbb{F}_{p^n}$ is p.*

Proof. Let $\mathbb{F}_{p^n}$ be a finite field, with p prime and $n \in N$. First, we will show that the characteristic of any finite field is non-zero. Consider the additive subgroup of $(\mathbb{F}_{p^n}, +)$, $\langle 1 \rangle$. Obviously, this group has finite order, since it is the subgroup of $(\mathbb{F}_{p^n}, +)$.

Now, we will show that the characteristic of $\mathbb{F}_{p^n}$ is prime. Assume, for the sake of contradiction, that the characteristic is composite. Let ab be the characteristic of $\mathbb{F}_{p^n}$ with $\underline{a}$ being 1 added a times, and $\underline{b}$ being 1 added b times. We have that $\underline{ab} = 0$ since it is the characteristic. Since a field has no zero divisors, either $\underline{a} = 0$ or $\underline{b} = 0$, and thus either a or b is the characteristic of $\mathbb{F}_{p^n}$. From this contradiction we can conclude that the characteristic must be prime.

Finally, we show that the characteristic $\mathbb{F}_{p^n}$ is p. We again consider the subgroup of $(\mathbb{F}_{p^n}, +)$, $\langle 1 \rangle$. By our previous result, the order of $\langle 1 \rangle$ is prime. By Lagrange's Theorem, the order of $\langle 1 \rangle$ must divide p^n. The only prime which divides p^n is p, therefore the order of $\langle 1 \rangle$ is p, and thus the characteristic of $\mathbb{F}_{p^n}$ is p, as claimed. □

Corollary 1. *In fields of even order,* $1 = -1$.

Proof. Fields of even order are of the form $\mathbb{F}_{2^n}$, and thus by Lemma 2, have a characteristic of 2. Therefore $1 + 1 = 0$; thus 1 is its own additive inverse, or $1 = -1$, as claimed. □

Corollary 2. *For all* x, y *in fields of even order, the following are equivalent:*

1. $x - y$
2. $x + y$
3. $y + x$
4. $y - x$

Proof. $\underline{1 \implies 2}$ Notice that,

$$\begin{aligned} x - y &= x + (-1)y, \\ &= x + (1)y, && \text{(By Corollary 1)} \\ &= x + y. \end{aligned}$$

$\underline{2 \implies 3}$ This follows from the fact that addition in a field is commutative.
$\underline{3 \implies 4}$ Apply the reverse argument as $1 \implies 2$.
$\underline{4 \implies 1}$ Apply the reverse argument as $3 \implies 4$, addition in a field is commutative, apply the reverse argument as $1 \implies 2$. □

The previous corollary ensures that $x - y$ is a kth residue if and only if $y - x$ is a kth residue.

Lemma 3. *Let* $\mathbb{F}_q$ *be a field of order* q*, with* $q \equiv 1 \mod 3$*. Let* g *be a generator of* $U(\mathbb{F}_q)$ *and let* $a = g^r$ *with* $a \neq 0$*. Then* a *is a cubic residue if and only if* $3 \mid r$*.*

Proof. If a is a cubic residue, we can fix $x \in \mathbb{F}_q$ such that $x^3 = a$. Let $x = g^u$. Then $g^{3u} = g^r$. Thus $3u \equiv r \mod q - 1$, which has a solution if and only if $\gcd(3, q-1) \mid r$, and since $q \equiv 1 \mod 3$, $\gcd(3, q-1) = 3$. If $3 \mid r$, then we can fix $x \in \mathbb{F}_q$ such that $x = g^{\frac{r}{3}}$. Notice that $x^3 = g^r = a$, and thus a is a cubic residue. □

Lemma 4. *Let* $\mathbb{F}_q$ *be a field of even order* q *such that* $q \equiv 1 \mod 3$*, then* $\mathbb{F}_q$ *has* $\frac{q-1}{3}$ *cubic residues*
.

Proof. Fix g to be a generator of $U(\mathbb{F}_q)$. Therefore, every element of $U(\mathbb{F}_q)$ can be written as g^n with $n \in [0 \dots q-2]$. Since g^n is a cubic residue if and only if $3 \mid n$ by the previous lemma and there are $\frac{q-1}{3}$ values of n for which this is the case, we can conclude that there are $\frac{q-1}{3}$ cubic residues in $\mathbb{F}_q$. □

Lemma 5. *In an even order field, every non-zero element is a quadratic residue.*

Proof. Let $\mathbb{F}_{2^n}$ be an arbitrary field of even order. Suppose $a \in \mathbb{F}_{2^n}$ is arbitrary such that $a \neq 0$. Since $U(\mathbb{F}_{2^n})$ is a group under multiplication of order $2^n - 1$,

$$\begin{aligned} a^{2^n} &= a^{2^n-1}a, \\ &= 1 \cdot a, \\ &= a. \end{aligned}$$

Therefore it follows that,

$$\begin{aligned} a &= a^{2n}, \\ &= (a^{2^{n-1}})^2, \end{aligned}$$

and thus a is a quadratic residue. □

5 Properties of $G_{2^n}^{(3)}$

Lemma 6. *Suppose $a, b, c \in \mathbb{Z}$ such that $a \mid b$ and $a \nmid c$, then $a \nmid (b + c)$.*

Proof. Let a, b, and c be as stated in the claim. Assume, for the sake of contradiction, that $a \mid (b+c)$. Since $a \mid b$, we can fix $k \in Z$ such that $b = ka$. Since $a \mid (b + c)$, we can fix ℓ such that $b + c = \ell a$. Notice that,

$$\begin{aligned} b + c &= \ell a, \\ ka + c &= \ell a, \\ c &= \ell a - ka, \\ &= (\ell - k)a, \end{aligned}$$

therefore $a \mid c$, which is a contradiction. Therefore we can conclude that $a \nmid (b+c)$, as claimed. □

Lemma 7 (Adapted from proof about symmetry of Paley Graphs in [4])**.** *Suppose $n \in \mathbb{N}$ such that $2^n \equiv 1 \mod 3$ and consider $\varphi : V(G_{2^n}^{(3)}) \to V(G_{2^n}^{(3)})$ defined $\varphi(x) = ax + b$ with $a, b \in \mathbb{F}_{2^n}$ and a a cubic residue. Then φ is an automorphism of $G_{2^n}^{(3)}$.*

Proof. We will show φ to be a bijection which preserves edges and non-edges.

Let $x_1, x_2 \in V(G_{2^n}^{(3)})$ be arbitrary such that $\varphi(x_1) = \varphi(x_2)$. Therefore, $\varphi(x_1) - \varphi(x_2) = 0$, and thus $ax_1 + b - ax_2 + b = 0$. Simplifying the previous expression yields that, $a(x_1 - x_2) = 0$. Since a is a cubic residue, $a \neq 0$, thus $x_1 - x_2 = 0$, and thus $x_1 = x_2$. Therefore, φ is injective. Now, consider $a^{-1}x_1 - a^{-1}b \in V(\Gamma)$. Notice that,

$$\begin{aligned} \varphi(a^{-1}x_1 - a^{-1}b) &= a(a^{-1}x_1 - a^{-1}b) + b, \\ &= x_1. \end{aligned}$$

Since x_1 was arbitrary, φ is surjective.

Let $\{x, y\} \in E(\Gamma)$ be arbitrary. It follows from the definition that $x - y$ is a cubic residue. Thus, we can fix $c_1 \in \mathbb{F}_{2^n}$ such that $(c_1)^3 = x - y$. Notice that,

$$\begin{aligned} \varphi(x) - \varphi(y) &= (ax + b) - (ay + b), \\ &= a(x - y). \end{aligned}$$

Since a is a cubic residue, we can fix $c_2 \in V(\Gamma)$ such that $(c_2)^3 = a$. Notice that,

$$\begin{aligned} (c_1 c_2)^3 &= (c_1)^3 (c_2)^3 \\ &= (x - y)a, \end{aligned}$$

thus, $\varphi(x) - \varphi(y)$ is a cubic residue, and thus $\{\varphi(x), \varphi(y)\} \in E(G_{2^n}^{(3)})\}$.

Now let $\{x, y\} \notin E(G_{2^n}^{(3)})$ arbitrary and let g be a generator of $U(\mathbb{F}_{2^n})$. Fix r such that $g^r = x - y$ and fix t such that $g^t = a$. Since $\{x, y\} \notin E(G_{2^n}^{(3)})$, $x - y$ is not a cubic residue, and thus $3 \nmid r$ by Lemma 3. Notice that,

$$\begin{aligned} \varphi(x) - \varphi(y) &= (ax + b) - (ay + b), \\ &= a(x - y), \\ &= ag^r, \\ &= g^t g^r, \\ &= g^{t+r}, \end{aligned}$$

By Lemma 6, $3 \nmid t + r$, thus $\varphi(x) - \varphi(y)$ is not a cubic residue by a Lemma 3, and thus $\{\varphi(x), \varphi(y)\} \notin E(G_{2^n}^{(3)})$.

Therefore, we have shown φ to be a bijection which preserves both edges and non-edges, and thus have show it to be an automorphism of $G_{2^n}^{(3)}$. □

Lemma 8. *Suppose $n \in \mathbb{N}$ such that $2^n \equiv 1 \mod 3$ and consider $\psi : V(G_{2^n}^{(3)}) \to V(G_{2^n}^{(3)})$ defined $\psi(x) = x^2$. ψ is an automorphism of $G_{2^n}^{(3)}$.*

Proof. Notice that the image of ψ is 0 and all of the quadratic residues. By Lemma 5, every non-zero element of an even order field is a quadratic residue. Therefore, for each $a \in \mathbb{F}_q$, there exists $x \in \mathbb{F}_q$ such that $x^2 = a$, and thus ψ is surjective. A surjection between finite sets of the same size is also a bijection, and thus ψ is a bijection.

Let $\{x, y\} \in E(G_{2^n}^{(3)})$; therefore $x - y$ is a cubic residue. Therefore, we can fix $c \in F_{2^n}$ such that $c^3 = x - y$. Notice that,

$$\begin{aligned} \psi(x) - \psi(y) &= x^2 - y^2, \\ &= (x - y)(x + y), \\ &= (x - y)(x - y), && \text{(By Corollary 1)} \\ &= (x - y)^2, \\ &= (c^3)^2, \\ &= (c^2)^3, \end{aligned}$$

thus $\psi(x) - \psi(y)$ is a cubic residue, and thus $\{\psi(x), \psi(y)\} \in E(G_{2^n}^{(3)})$.

Let $\{x, y\} \notin E(\Gamma)$. Let g be a generator of $U(\mathbb{F}_{2^n})$ and fix r such that $g^r = x - y$. Since $\{x, y\} \notin E(G_{2^n}^{(3)})$, $x - y$ is not a cubic residue. By a Lemma 3, $3 \nmid r$. Notice that,

$$\begin{aligned}
\psi(x) - \psi(y) &= x^2 - y^2 \\
&= (x + y)(x - y) \\
&= (x - y)^2 && \text{(by Corollary 2)} \\
&= (g^r)^2 \\
&= (g^{2r})
\end{aligned}$$

Since $3 \nmid r$, $3 \nmid 2r$, thus $\psi(x) - \psi(y)$ is not a cubic residue by Lemma 3, and thus $\{\psi(x), \psi(y)\} \notin E(G_{2^n}^{(3)})$.

Since ψ is a bijection from $V(G_{2^n}^{(3)}) \to V(G_{2^n}^{(3)})$ that preserves edges and non-edges, ψ is an automorphism of $G_{2^n}^{(3)}$, as claimed. □

Theorem 1 (Adapted from a proof about symmetry of Paley Graphs in [4])**.** *Suppose $n \in \mathbb{N}$ such that $2^n \equiv 1 \mod 3$. $G_{2^n}^{(3)}$ is symmetric.*

Proof. For arbitrary $x, y \in V(G_{2^n}^{(3)})$, consider the automorphism φ from Lemma 6 with $a = 1$ and $b = y - x$. Notice that by Lemma 6 φ is an automorphism with $\varphi(x) = y$. Therefore, $Aut(\Gamma)$ acts transitively on the vertices. Consider two arbitrary edges, $\{x_1, y_1\}, \{x_2, y_2\}$. Let φ be as defined in Lemma 7 with $a = (x_2 - y_2)(x_1 - y_1)^{-1}$ and $b = x_2 - ax_1$. Notice that by Lemma 7 φ is an automorphism with $\varphi(x_1) = x_2$ and $\varphi(y_1) = y_2$. Therefore $Aut(G_{2^n}^{(3)})$ acts arc-transitively on $G_{2^n}^{(3)}$. This completes the proof. □

Theorem 2. *Suppose $n \in \mathbb{N}$ such that $2^n \equiv 1 \mod 3$. The complement of $G_{2^n}^{(3)}$ is arc transitive.*

Proof. Let g be a generator of $U(\mathbb{F}_{2^n})$, let $\{x, y\} \notin E(G_{2^n}^{(3)})$. Fix r such that $g^r = x - y$. We consider two classes of non-cubic residues, those where $r \equiv 1 \mod 3$ and those where $r \equiv 2 \mod 3$. We will refer to these as type I and type II respectively.

Notice that, if $x - y$ is type I, then $(x - y)^{-1}$ is type II and vice versa. This follows from the fact that if $(x - y) = g^r$ and $(x - y)^{-1} = g^t$, then $(x - y)(x - y)^{-1} = g^{r+t} = 1$, and thus $3 \mid (r + t)$ by Lemma 3, since 1 is a cubic residue.

Let $\{x_1, y_1\}, \{x_2, y_2\} \notin E(G_{2^n}^{(3)})$ of the with $x_1 - y_1$ and $x_2 - y_2$ of the same type. Consider the previously defined automorphism φ with $a = (x_2 - y_2)(x_1 - y_1)^{-1}$ and $b = x_2 - ax_1$. We know a is a cubic residue by our observation from the previous paragraph, and thus φ is an automorphism of $G_{2^n}^{(3)}$. Notice that $\varphi(x_1) = x_2$ and $\varphi(y_1) = y_2$, and thus φ acts transitively on non-edges whose vertex difference is of the same type.

Now consider $\{x, y\} \notin E(G_{2^n}^{(3)})$ with $x - y$ a type I non-cubic residue. Let $x - y = g^r$. Then,

$$\begin{aligned}
\psi(x) &= x^2, \\
\psi(y) &= y^2, \\
x^2 - y^2 &= (x - y)^2, && \text{(by Corollary 2)} \\
&= (g^r)^2, \\
&= g^{2r}.
\end{aligned}$$

Now, if $3|(r-1)$, then $3|(2r-2)$, and thus $\{\psi(x), \psi(y)\}$ is a non-edge with $\psi(x) - \psi(y)$ a type II non-cubic residue.

Since φ acts transitively on non-edges of the same type, and ψ takes edges of one type to another, by composing them, we can take any non-edge to any other non-edge. Therefore, the complement of $G_{2^n}^{(3)}$ is arc transitive, as claimed. □

Theorem 3. *Suppose $n \in \mathbb{N}$ such that $2^n \equiv 1 \mod 3$. $G_{2^n}^{(3)}$ is a strongly regular graph.*

Proof. First, we show that $G_{2^n}^{(3)}$ is regular. Let x in $V(G_{2^n}^{(3)})$ be arbitrary. Notice that, $N(x) = \{y \in V(G_{2^n}^{(3)}) \mid x - y \text{ is a cubic residue}\}$. Let c be an arbitrary cubic residue. Notice that if $x - y_1 = c = x - y_2$, then $y_1 = x - c = y_2$. Therefore, for every cubic residue there is a unique element y of $V(G_{2^n}^{(3)})$ such that $x - y = c$, so for all $x \in V(G_{2^n}^{(3)})$, $|N(x)|$ is equal to the number of cubic residues, which is $\frac{2^n-1}{3}$ by Lemma 4. (I did not really understand your comment here as to what I was lacking)

Next, we will show the existence of a λ value. Fix $\{x_1, y_1\} \in E(G_{2^n}^{(3)})$ and consider the set $A = \{z \in V(G_{2^n}^{(3)}) \mid \{z, x_1\} \text{ and } \{y_1, z\} \text{ are edges}\}$. Let $\lambda = |A|$. Consider arbitrary edge, $\{x, y\}$. By Theorem 1, we can fix an automorphism, θ, such that $\theta(x_1) = x$ and $\theta(y_1) = y$. Let $z \in V(G_{2^n}^{(3)})$ be arbitrary. Since θ is an automorphism, $\theta(z)$ is adjacent to both x and y if and only if $z \in A$. Therefore, θ is a bijection between A and the set of elements adjacent to both x and y under θ. Therefore, there are also λ elements adjacent to both x and y, and since x and y were arbitrary, this guarantees the existence of a universal λ value. Finally, we will show the existence of a μ value. Fix $x_2, y_2 \in V(G_{2^n}^{(3)})$ such that $\{x_2, y_2\} \notin E(G_{2^n}^{(3)})$ and consider the set $B = \{z \in V(G_{2^n}^{(3)}) \mid \{x_2, z\} \text{ and } \{z, y_2\} \text{ are edges}\}$. Let $\mu = |B|$. Consider arbitrary $x, y \in V(G_{2^n}^{(3)})$ such that $\{x, y\} \notin E(G_{2^n}^{(3)})$. By Theorem 2, we can fix an automorphism, γ, such that $\gamma(x_2) = x$ and $\gamma(y_2) = y$. Let $z \in V(G_{2^n}^{(3)})$ be arbitrary. Since γ is an automorphism, $\gamma(z)$ is adjacent x and y if and only if z is adjacent to x_2 and y_2. Therefore, γ is a bijection between B and the set of elements adjacent to both x and y, and since x and y were arbitrary, this guarantees the existence of a universal μ value.

Since we have shown the existence of r, λ, and μ values, we can conclude that $G_{2^n}^{(3)}$ is strongly regular, as claimed. □

6 Conclusion

This project taught me how to use computational tools to develop conjectures about algebraic structures, and then attempt to formally prove those conjectures. The computational aspects of the project do not actually serve as part of the proof or result, like in the case of the Four Color Theorem or the classification of self-complementary strongly regular graphs, but simply guided my thinking and allowed me to find a problem I would want to solve. Technically speaking, I could have presented all of the results in this paper without writing one line of code; however, without the code I generated, I would not have known what conditions to look for to guarantee the construction of a strongly regular graph. Therefore, the code I wrote was invaluable to me in proving these results, because without it, I would not have had any idea that there was a result to prove.

This project also allowed me to become familiar with two of the most important libraries/languages for combinatorial algebra, namely SageMath and GAP. I have often found that the best way to learn a new programming language or extensive library is not to simply read through an arbitrary tutorial, but instead to apply the language or library to a task or problem that interests you.

Because this project was entirely directed by my interests, I was able to stay interested with the process of learning these frameworks, since the reward was developing a solution to a problem that is actually intriguing to me.

Finally, this project allowed me to experience, if even for a short amount of time, what research in algebraic graph theory, and combinatorial algebra more generally, is like (especially on the computational side). I am certain that I would like to pursue a PhD somewhere on the boundary of computer science and mathematics, but what field that will be in exactly is still up in the air. Therefore, being exposed to research in a variety of fields will not only help develop my skills as a researcher, but also expose me to possible areas of postgraduate study.

7 Acknowledgments

I would like to thank my research partner, Jasper Egge, for providing critiques and feedback on my work throughout the entire process. Furthermore, he's the reason I decided to learn GAP, which I will certainly use again at some point in my life.

I would like to thank my research adviser, Professor Chris French, for his continued support on this project. He has helped me edit this paper, as well as helping me find the direction of my research into this topic.

8 Appendix 1: Using FiniteFieldGraphs Python Code for Developing Conjectures

The table in section 3 from which I developed the conjecture that lead to the ultimate result presented in this paper was developed with the help of python code using the SageMath package to generate the graphs described. I present both the way of reproducing my results, and an introduction to the code so that others may use it to develop new conjectures.

To reproduce my results simply run the command `sage -python gcg_experiment.py`. You will be prompted to input a starting power of 2 (I used 4), and an ending power of two (I used 14). You will also be prompted to give an output file, which can either be a text file, or nothing if you would like to have the results sent to the console. For each divisor d of $U(\mathbb{F}_{2^n})$, the program will construct a graph with $\mathbb{F}_{2^n}$ as the vertex set, and determine whether two vertices share an edge if their difference is a d-residue. It will then check if the graph is connected, and then if it is strongly regular. The output will be of the form, "GF(2^n), Residue Power: d", followed either by "is not connected", "SRG: False", or the actual strongly regular graph parameters. The program runs in parallel, and generates as many sub-processes as it can, so it will consume the vast majority of your CPU power while it is running.

To produce programs that construct and analyze graphs on finite fields, I have created the `FiniteFieldGraph` graph class. To construct an instance of the class simply provide the desired order of the field and a function that takes two field elements and returns true if there should be an edge between them, and false otherwise. This will construct an object which contains the field, the field's order, the relation used, and the actual graph object as members. Accessing the graph member from the object allows for the use of SageMath's graph algorithms for analysis of the properties of the graph, and the other members are kept for the purpose of relating a graph to the field and relation that it was constructed from.

Everything else I developed was to aid in the development of the `gcg_experiment.py` program. For more information about the rest of the code developed, see `https://github.com/GouwarPower/FiniteFieldGraphs`.

9 Appendix 2: NCGraph, A GAP Package for Generating Non-commuting Graphs of Finite Groups

Before delving into the specifics of the package, I will first define a non-commuting graph of a finite group.

Definition. *Suppose that G is a finite group. Let $\Gamma = (V, E)$ with $V = G \setminus Z(G)$, where $Z(G)$ is the center of G, and $E = \{\{x, y\} \in P_2(G) \mid xy \neq yx\}$. We remove the center, since elements of the center commute with all elements of the group and thus would be isolated points on the graph.*

I developed NCGraph to help my research partner, Jasper Egge, develop conjectures about non-commuting graphs on small groups. It originally started as a simple GAP script to generate the adjacency matrices of these graphs directly, without relying on GAP's builtin package for graph theory, GRAPE. However, this left something to be desired, since GRAPE implements are large number of graph theoretic algorithms, such as computing a graph's automorphism group. Therefore, I re-implemented the script so that it would first generate a GRAPE non-commuting graph, then generate an adjacency for the graph. Both of these scripts also contained a way to loop through all of GAP's "Small Groups" in a range of orders, generate their non-commuting graphs, and write the results to a file or console. I realized that the functionality of generating the non-commuting graphs and adjacency matrices could be useful beyond the one application I developed it for, and thus I decided to replicate the functionality in a GAP package that could be reused by anyone who wanted to study these graphs.

NCGraph is a small package, with only 3 functions. `RemoveCenter(G)` takes a group `G`, and returns a list of the non-central elements of the group. `NonCommutingGraph(G)` takes a group `G` and generates a GRAPE graph object that represents the non-commuting graph of that group. `AdjacencyMatrix(G)` takes a GRAPE graph object `G` and returns the adjacency matrix of that graph.

For more information or to install the package, go to `https://github.com/GouwarPower/NCGraph`
For an example of the package in action, go to
`https://github.com/GouwarPower/SmallGroupsNonCommutingGraphs`

References

[1] G. A. Jones, "Paley and the paley graphs," in *International workshop on Isomorphisms, Symmetry and Computations in Algebraic Graph Theory*, pp. 155–183, Springer, 2016.

[2] J. J. Seidel, "Strongly regular graphs with (1, 1, 0) adjacency matrix having eigenvalue 3," in *Geometry and Combinatorics*, pp. 26–43, Elsevier, 1991.

[3] R. E. Greenwood and A. M. Gleason, "Combinatorial relations and chromatic graphs," *Canadian Journal of Mathematics*, vol. 7, pp. 1–7, 1955.

[4] A. N. Elsawy, "Paley graphs and their generalizations," *arXiv preprint arXiv:1203.1818*, 2012.

[5] F. De Clerck, "Constructions and characterizations of (semi) partial geometries," *Summer School on Finite Geometries, Potenza*, pp. 2–13, 1997.

[6] W. Ananchuen, "On the adjacency properties of generalized paley graphs," *Australasian Journal of Combinatorics*, vol. 24, pp. 129–148, 2001.

[7] B. Conrad, "Finite multiplicative subgroups of a field," in *Class Notes For Math 210B: Algebra*, Stanford University.