

THE CLIQUE NUMBER OF THE PALEY GRAPH

ARMANBYEK SOLTANMURAT

ABSTRACT

In this work, we define quadratic residue and its properties. We show Paley graph is strongly regular graph and determine its eigenvalues, the upper bound for its clique number.

Definition 1. *Let q and r be two positive integers with $\gcd(q, r) = 1$, then r is a quadratic residue of q if and only if $x^2 \equiv r \pmod{q}$ has a solution, and r is a quadratic nonresidue of q if and only if $x^2 \equiv r \pmod{q}$ has no solution.*

Lemma 1. *If p is an odd prime, then the numbers $0^2, 1^2, 2^2, \dots, \left[\frac{p-1}{2}\right]^2$ are distinct modulo p .*

Proof. Assume that $x^2 \equiv y^2 \pmod{p}$. Then, we can write

$$(x - y)(x + y) \equiv 0 \pmod{p}.$$

By unique factorization in \mathbb{F}_p , we have either $x - y \equiv 0 \pmod{p}$ or $x + y \equiv 0 \pmod{p}$. This implies $x \equiv y \pmod{p}$ or $x \equiv -y \pmod{p}$. \square

Definition 2. *Let p be an odd prime number. An integer a is a quadratic residue modulo p if it is congruent to a perfect square modulo p , and is a quadratic nonresidue modulo p otherwise. The Legendre symbol is a function of a and p , defined as:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p}, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

Theorem 1. *If p is an odd prime and $a, b \in \mathbb{Z}$, then:*

- (1) $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
- (2) If $p \nmid a$, then $\left(\frac{a^2}{p}\right) = 1$.

- (3) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$: equivalently, $QR \times QR = QR$, $QR \times NR = NR$, $NR \times NR = QR$, where QR denotes a quadratic residue modulo p and NR denotes a quadratic nonresidue modulo p .

Proof. We can prove parts 1 and 2 easily by the definition. In general, we defined a is a quadratic residue (QR) modulo p if and only if

$$\exists c \in \mathbb{F}_p^* \text{ such that } a \equiv c^2 \pmod{p}.$$

To prove part 3, it is trivial that if either or both $p \mid a$ or $p \mid b$. Otherwise, we have to consider the three cases. Let m, n be units (non-zero modulo p).

- (a) $m^2 n^2 \equiv (mn)^2 \pmod{p}$, so the product of two QR's is a QR.
 (b) By part (a), $m^2 r \equiv r^2 \implies r \equiv (nm^{-1})^2 \pmod{p}$, so r is a QR. On the other hand, if r is a nonresidue (NR), then so also is $m^2 r$.
 (c) Let r be a NR. Since $r \not\equiv 0 \pmod{p}$, we have a bijective map

$$\lambda : x \mapsto rx, \quad \mathbb{F}_p^* \rightarrow \mathbb{F}_p^*,$$

where the inverse is $\lambda^{-1}(x) := r^{-1}x$.

For any QR m^2 , part (b) says that $\lambda(m^2) = rn^2$ is a NR. Since (by Lemma 1) the sets of QR's and NR's have equal cardinality, it follows that λ maps the QR's bijectively to the NR's and must therefore map NR's back to QR's.

In particular, if m is a NR, then $\lambda(m) = mn$ is a QR.

□

Theorem 2 (Lagrange). *Let \mathbb{F} be a field, and let $p(x)$ be a non-zero polynomial in $\mathbb{F}[x]$ of degree $n \geq 0$. Then $p(x)$ has at most n roots over \mathbb{F} .*

Proof. We proceed by induction on the degree of the polynomial $p(x)$.

If $n = 0$, then $p(x)$ is a non-zero constant. In this case, $p(x)$ cannot have any roots since no constant polynomial is zero except the zero polynomial. Assume that any polynomial in $\mathbb{F}[x]$ of degree n has at most n roots. Now, consider a polynomial $p(x) \in \mathbb{F}[x]$ of degree $n + 1$.

If $p(x)$ has no roots, the result is trivial. Otherwise, suppose $p(x)$ has at least one root $a \in \mathbb{F}$. By the factorization lemma, there exists a polynomial $q(x) \in \mathbb{F}[x]$ such that

$$p(x) = (x - a) \cdot q(x),$$

where $\deg(q(x)) = n$.

By the induction hypothesis, the polynomial $q(x)$ has at most n roots. Any root of $q(x)$ is also a root of $p(x)$, and if $b \neq a$ is a root of

$p(x)$, then b must also be a root of $q(x)$. Therefore, $p(x)$ has at most $n + 1$ roots.

This completes the induction and proves the theorem. \square

Theorem 3 (Euler's criterion). *If p is an odd prime, then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Proof. If $p \mid a$, both sides are trivially zero.

If a is a quadratic residue, then $a \equiv b^2$ for some $b \in \mathbb{F}_p^*$, so

$$a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Little Theorem.

Now consider the equation

$$y^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

By Lagrange's Theorem, this equation has at most $\frac{p-1}{2}$ solutions. However, all $\frac{p-1}{2}$ quadratic residues (Lemma 1) are already solutions! Hence, a is a quadratic residue if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Finally, observe that Fermat's Little Theorem can be factored (uniquely modulo p) as

$$0 \equiv a^{p-1} - 1 \equiv \left(a^{\frac{p-1}{2}} - 1\right) \left(a^{\frac{p-1}{2}} + 1\right) \pmod{p}.$$

We conclude that a is a non-residue if and only if

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

\square

One of the nice applications of Euler's criterion is that we can determine when -1 is a quadratic residue.

Theorem 4. *If p is an odd prime, then -1 is a quadratic residue (QR) if and only if $p \equiv 1 \pmod{4}$. Indeed,*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

We introduced the definitions and theorems regarding quadratic residues. Now, we are ready to define what is Paley graph.

Definition 3. Let q be a prime power such that $q \equiv 1 \pmod{4}$. The graph $P = (V, E)$, where

$$V(P) = \mathbb{F}_q \quad \text{and} \quad E(P) = \{\{x, y\} : x, y \in \mathbb{F}_q, x - y \in (\mathbb{F}_q^*)^2\},$$

is called the Paley graph of order q .

Definition 4. A graph G is called k -regular if all the vertices of G have the same degree k . Let G be a k -regular graph with n vertices. If there exist two integers λ and μ such that:

- every two adjacent vertices have λ common neighbors, and
- every two non-adjacent vertices have μ common neighbors,

then G is called a strongly regular graph with parameters (n, k, λ, μ) and is denoted by $\text{srg}(n, k, \lambda, \mu)$.

Definition 5. Let $G = (V, E)$ and $G' = (V', E')$ be two graphs. G is isomorphic to G' if there exists a bijection $f : V \rightarrow V'$ such that $xy \in E$ if and only if $f(x)f(y) \in E'$. We denote this by $G \cong G'$.

Definition 6. A graph G is called self-complementary if it is isomorphic to its complement.

Theorem 5. Let P be the Paley graph of order $q = p^n$. Then P is a self-complementary graph.

Proof. Let r be a quadratic nonresidue modulo q . Define the function $f : V(P) \rightarrow V(P)$ by $f(x) = rx$.

To show that f is well-defined, observe that

$$\{x, y\} \in E(P) \iff (x - y) \in (\mathbb{F}_{p^n}^*)^2.$$

Substituting $f(x)$ and $f(y)$, we have

$$f(x) - f(y) = r(x - y).$$

Since r is a quadratic nonresidue, $r(x - y) \notin (\mathbb{F}_{p^n}^*)^2$, and thus

$$\{f(x), f(y)\} \notin E(P).$$

Therefore, the function f preserves adjacency and is well-defined.

Next, we prove that f is a bijection.

1. Injectivity: Suppose $f(x) = f(y)$. Then

$$rx = ry \implies r(x - y) = 0.$$

Since $r \neq 0$, it follows that $x - y = 0$, and hence $x = y$.

2. Surjectivity: Since $\gcd(r, q) = 1$, there exist integers $a, b \in \mathbb{Z}$ such that

$$1 = qa + rb \implies rb \equiv 1 \pmod{q}.$$

Thus, for any $x \in V(P)$, we can write

$$f(bx) = r(bx) = x.$$

This shows that f is surjective.

Since f is both injective and surjective, it is a bijection. □

Theorem 6. *Let P be the Paley graph of order $q = p^n$. Then P is a strongly regular graph with parameters $\text{srg}(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$.*

Proof. In the first, we prove that each vertex has degree $\frac{q-1}{2}$. Let $x \in V(P)$ and define its neighbor $N(x) = \{z \in V(P) : x - z = s \in (\mathbb{F}_{p^n}^*)^2\}$. If $x - z_1 = s$ and $x - z_2 = s$, then $z_1 = x - s = z_2$. So for all $s \in (\mathbb{F}_{p^n}^*)^2$, there exists a unique $z \in V(P)$ such that $x - z = s$. Thus, there exists a one-to-one correspondence between the elements of $N(x)$ and the elements of $(\mathbb{F}_{p^n}^*)^2$. Therefore, all vertices have the same degree $d(x) = |N(x)| = |(\mathbb{F}_{p^n}^*)^2|$. By Lemma 1, $|(\mathbb{F}_{p^n}^*)^2| = \frac{q-1}{2}$.

Secondly, we prove that every two adjacent vertices have $\frac{q-5}{4}$ common neighbors and every two non-adjacent vertices have $\frac{q-1}{4}$ common neighbors. Consider two adjacent vertices x and y in P . Let the difference between x and y be a quadratic residue, i.e.,

$$x - y = a^2.$$

Let z be a common neighbor of both x and y . Then we have:

$$x - z = b^2 \quad \text{and} \quad y - z = c^2.$$

To count the number of common neighbors of x and y we count the different solutions for z . We can get that $(b-c)(b+c) = a^2$. Let $b-c = t$ then $b+c = t^{-1}a^2$. This gives us

$$b = \frac{t + t^{-1}a^2}{2}, \quad c = \frac{t^{-1}a^2 - t}{2}.$$

We consider different cases for t :

- (1) If $t = t$, then $t = 0$ and $c = 0$.
- (2) If $t = -t$, then $t = 0$ and $c = 0$.
- (3) If $t = -a^2t^{-1}$, then $t = \pm ia$, and $b = 0$.
- (4) If $t = a^2t^{-1}$, then $t = \pm a$ and $c = 0$.

In all these four cases, we can see that $c^2 = 0$ or $b^2 = 0$ which cannot be since $b, c \in \mathbb{F}_q^*$. Hence, we exclude these five solutions which are $t = 0, \pm ia, \pm a$ from the set \mathbb{F}_q . Now if we substitute $-t, -a^2t^{-1}, a^2t^{-1}$ instead of t on c then it does not contribute distinct solutions. The squares of substitutions on c have the same value. Hence, we divide

$q - 5$ solutions by 4. Hence, the number of different solutions for the pairs (b, c) is $\frac{q-5}{4}$.

We now count the number of common neighbors of nonadjacent x and y .

$$x - y = r, r \notin (\mathbb{F}_q^*)^2.$$

Similarly, we can get

$$b = \frac{t + t^{-1}r}{2}, \quad c = \frac{t^{-1}r - t}{2}.$$

We skip the solution $t = rt^{-1}$ and $t = -rt^{-1}$ which is impossible because we get $r = t^2$ and $r = -t^2$ contradicts that $r \notin (\mathbb{F}_q^*)^2$. Therefore, we only exclude $t = 0$ from the set \mathbb{F}_q and divide by 4 in the same way. Hence, the number of different solutions of pairs (b, c) is $\frac{q-1}{4}$.

In the result, Paley graph P is a strongly regular graph with parameters $\text{srg}(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$. □

Theorem 7. *Let G be a connected strongly regular graph with parameters (n, d, a, b) . Then its eigenvalues are d with multiplicity 1, and*

$$\lambda_{\pm} = \frac{a - b \pm \sqrt{(a - b)^2 + 4(d - b)}}{2}$$

with multiplicities

$$m_{\pm} = \frac{1}{2} \left(n - 1 \mp \frac{2d + (n - 1)(a - b)}{\sqrt{(a - b)^2 + 4(d - b)}} \right).$$

The Paley graphs are connected because if there is non-adjacent x and y then x and y have at least common neighbor z as $\frac{q-1}{4} \geq 1$. So there exists a path xe_1ze_2y . Using the theorem we can determine the eigenvalues of Paley graph.

Theorem 8. *The eigenvalues of Paley graph are*

$$\lambda_0 = \frac{q-1}{2} \quad (\text{with multiplicity } 1),$$

$$\lambda_{\pm} = -\frac{1}{2} \pm \frac{\sqrt{q}}{2} \quad (\text{each with multiplicity } \frac{q-1}{2}).$$

We give an upper bound for the clique number of Paley graph.

Theorem 9. *Let q be a prime power such that $q \equiv 1 \pmod{4}$ and P be Paley graph order of q . Then $\omega(P) \leq \sqrt{q}$*

Proof. Let $N = \omega(P)$, and let $C = \{v_1, v_2, \dots, v_N\} \subseteq \mathbb{F}_q$ be a clique of the maximum size in P . Let g be a primitive root of \mathbb{F}_q^* , and consider the set

$$W = \{v_i + gv_j : 1 \leq i, j \leq N\}.$$

If $v_i + gv_j = v_{i'} + gv_{j'}$, then $v_i - v_{i'} = g(v_{j'} - v_j)$, which is impossible unless $i = i'$ and $j = j'$. Thus, each element of W is distinct. This implies that $|W| = N^2 \leq q$, i.e.,

$$N \leq \sqrt{q}.$$

□