# IISC BANGALORE – EIGENFUNCTIONS SEMINAR NOTES

DOMINIQUE GUILLOT

## 1. Positive definite matrices

Recall that a matrix $A \in \mathbb{C}^{n\times n}$ is *Hermitian* if $A = A^* = \overline{A}^T$. We denote the *spectrum* of $A$ (set of eigenvalues) by $\sigma(A)$, i.e.,

$$\sigma(A) = \{\lambda \in \mathbb{C} : Av = \lambda v \text{ for some } v \in \mathbb{C} \setminus \{\mathbf{0}_{n\times 1}\}\}.$$

For $z, w \in \mathbb{C}^n$, we denote by $\langle z, w\rangle$ their inner product that is conjugate linear in the second argument, i.e.,

$$\langle z, w\rangle = \sum_{k=1}^{n} z_k \overline{w}_k.$$

**Proposition 1.1.** *Let $A \in \mathbb{C}^{n\times n}$ be Hermitian. Then*

(1) *$z^*Az \in \mathbb{R}$ for all $z \in \mathbb{C}^n$.*
(2) *$\sigma(A) \subseteq \mathbb{R}$.*

*Proof.* (1) For $z \in \mathbb{C}^n$, we have

$$z^*Az = \langle Az, z\rangle = \langle z, A^*z\rangle = \langle z, Az\rangle = \overline{\langle Az, z\rangle} = \overline{z^*Az}.$$

Thus, $z^*Az \in \mathbb{R}$.

For (2), let $\lambda \in \sigma(A)$ and let $v \in \mathbb{C}^n \setminus \{\mathbf{0}_{n\times 1}\}$ be such that $Av = \lambda v$. Then

$$\langle Av, v\rangle = \lambda\langle v, v\rangle = \langle v, A^*v\rangle = \langle v, Av\rangle = \overline{\lambda}\langle v, v\rangle.$$

It follows that $\lambda = \overline{\lambda}$ and so $\lambda \in \mathbb{R}$. □

**Definition 1.2.** A Hermitian matrix $A \in \mathbb{C}^{n\times n}$ is said to be *positive definite* (PD) if $x^*Ax > 0$ for all $x \in \mathbb{C}^n \setminus \{\mathbf{0}_{n\times 1}\}$.

Similarly, a matrix is said to be positive semidefinite (PSD) if $x^*Ax \geq 0$ for all $x \in \mathbb{C}^n$.

**Convention:** We say that $x \in \mathbb{R}$ is *positive* if $x > 0$ and *non-negative* if $x \geq 0$.

Positive definite matrices can be recognized in many ways. Recall that a *principal submatrix* of $A$ is a matrix obtained by restricting $A$ to the *same* subset of rows and columns, i.e.,

$$A_{I,I} := (a_{ij})_{i,j\in I}$$

where $I \subseteq \{1, 2, \ldots, n\}$. A *leading principal submatrix* is a principal submatrix for which $I = \{1, 2, \ldots, k\}$ for some $1 \leq k \leq n$. For example, the "$*$ pattern" of the

*Date*: January 22th 2026.

following matrices form a principal and a leading principal submatrix, respectively.

$$\begin{pmatrix} * & + & * & * \\ + & + & + & + \\ * & + & * & * \\ * & + & * & * \end{pmatrix} \qquad \begin{pmatrix} * & * & * & + \\ * & * & * & + \\ * & * & * & + \\ + & + & + & + \end{pmatrix}$$

A *principal minor* is the determinant of a principal submatrix. A *leading principal minor* is the determinant of a leading principal submatrix.

**Theorem 1.1.** *Let $A \in \mathbb{C}^{n\times n}$ be Hermitian. Then the following are equivalent:*

1. *$A$ is positive definite.*
2. *$\sigma(A) \subseteq (0, \infty)$.*
3. *There exists a non-singular matrix $B \in \mathbb{C}^{n\times n}$ such that $A = BB^*$.*
4. *There exists a non-singular Hermitian matrix $C \in \mathbb{C}^{n\times n}$ such that $A = C^2$.*
5. *All principal minors of $A$ are positive.*
6. *All leading principal minors of $A$ are positive.*

The following results will be useful to prove Theorem 1.1. Here and below, for $n \in \mathbb{N}$, we let $[n] := \{1, \dots, n\}$

**Theorem 1.2** (Cauchy–Binet formula)**.** *Let $A \in \mathbb{C}^{n\times m}$ and $B \in \mathbb{C}^{m\times n}$. Then*

$$\det AB = \sum_{\substack{S\subseteq\{1,\dots,m\} \\ |S|=n}} \det A_{[n],S} \det B_{S,[n]}.$$

**Theorem 1.3.** *Let $N = n + m$ and let $A \in \mathbb{C}^{N\times N}$ be written in block form*

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

*where $A_{11} \in \mathbb{C}^{n\times n}$, $A_{12} \in \mathbb{C}^{n\times m}$, $A_{21} \in \mathbb{C}^{m\times n}$, and $A_{22} \in \mathbb{C}^{m\times m}$. If $A_{11}$ is non-singular, then*

$$\det A = \det A_{11} \cdot \det\left(A_{22} - A_{21}A_{11}^{-1}A_{12}\right).$$

*The matrix $A/A_{11} := A_{22} - A_{21}A_{11}^{-1}A_{12}$ is called the Schur complement of $A_{11}$ in $A$.*

*Proof.* We have

$$A = \begin{pmatrix} I_n & \mathbf{0}_{n\times m} \\ A_{21}A_{11}^{-1} & I_m \end{pmatrix} \begin{pmatrix} A_{11} & \mathbf{0}_{n\times m} \\ \mathbf{0}_{m\times n} & A_{22} - A_{21}A_{11}^{-1}A_{12} \end{pmatrix} \begin{pmatrix} I_n & A_{11}^{-1}A_{12} \\ \mathbf{0}_{m\times n} & I_m \end{pmatrix}.$$

The result follows by the multiplicativity property of the determinant. □

*Proof of Theorem 1.1.* (1) $\implies$ (2). Let $A$ be positive definite, let $\lambda \in \sigma(A)$, and let $v \in \mathbb{C}^n$ such that $Av = \lambda v$. Then

$$v^*Av = \lambda\|v\|^2 > 0.$$

Since $v \neq \mathbf{0}_{n\times 1}$, it follows that $\lambda > 0$. Thus $\sigma(A) \subseteq (0, \infty)$.

(2) $\implies$ (3) Since $A$ is Hermitian, it is diagonalizable, i.e., there exists a unitary matrix $U \in \mathbb{C}^{n\times n}$ and a diagonal matrix $D \in \mathbb{R}^{n\times n}$ such that $A = UDU^*$. The diagonal entries of $D = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$ contain the eigenvalues of $A$ and since $\sigma(A) = \{\lambda_1, \dots, \lambda_n\} \subseteq (0, \infty)$, the matrix $D^{1/2} = \operatorname{diag}(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_n})$ is real. Defining $B = UD^{1/2}$, we obtain $A = UD^{1/2}D^{1/2}U^* = BB^*$.

(3) $\implies$ (4) Let $A = BB^*$. Then $z^*Az = z^*BB^*z = (B^*z)^*(B^*z) = \|B^*z\|^2 > 0$ since $B$ (and therefore $B^*$) is non-singular. Therefore $A$ is positive definite and admits an eigendecomposition of the form $A = UDU^*$ where $U$ is unitary and $D$ is diagonal with positive diagonal entries. Let $C = UD^{1/2}U^*$. Using the fact that $U$ is unitary, we obtain $C^2 = UD^{1/2}U^*UD^{1/2}U^* = UDU^* = A$, as desired.
(4) $\implies$ (5) Let $I \subseteq \{1, 2, \ldots, n\}$ with $|I| = k$. Using the Cauchy–Binet formula and the fact that $C$ is Hermitian, we obtain

$$\det A_{I,I} = \sum_{\substack{S \subseteq \{1,2,\ldots,n\} \\ |S|=k}} \det C_{I,S} \det C_{S,I} = \sum_{\substack{S \subseteq \{1,2,\ldots,n\} \\ |S|=k}} |\det C_{I,S}|^2 \geq 0.$$

Since $C$ is non-singular, the matrix $C_{I,S}$ has rank $k$. Letting $S$ be a subset of $k$ linearly independent columns of $C_{I,S}$, we obtain $\det C_{I,S} \neq 0$. Thus $\det A_{I,I} > 0$.

(5) $\implies$ (6) Trivial.

(6) $\implies$ (1) We proceed by induction on $n$. The result trivially holds for $n = 1$. Suppose it holds for matrices of dimension $n-1$ and assume $A$ has dimension $n$. Let $A_k$ denote the $k \times k$ leading principal submatrix of $A$ and let $S_k = A_k/A_1 \in \mathbb{C}^{(k-1)\times(k-1)}$ denote the Schur complement of $A_1$ in $A_k$. We claim that $S_n \in \mathbb{C}^{(n-1)\times(n-1)}$ is positive definite. Indeed, observe that the $(k-1) \times (k-1)$ leading principal submatrix of $S_n$ is $S_k$. By Theorem 1.3, we have

$$0 < \det A_k = a_{11} \det S_k.$$

Thus $\det S_k > 0$ for all $2 \leq k \leq n$. By the induction hypothesis, we conclude that $S_n$ is positive definite.

Now, let $z = (z_1, w)^T \in \mathbb{C}^n \setminus \{\mathbf{0}_{n\times 1}\}$ with $z_1 \in \mathbb{C}$ and $w \in \mathbb{C}^{n-1}$. Write

$$A = \begin{pmatrix} a_{11} & v^* \\ v & B \end{pmatrix}$$

where $v \in \mathbb{C}^{n-1}$ and $B \in \mathbb{C}^{(n-1)\times(n-1)}$. Then

$$\begin{aligned} z^*Az &= a_{11}|z|^2 + 2\Re(\overline{z_1}v^*w) + w^*Bw \\ &= a_{11}\left|z_1 + \frac{1}{a_{11}}v^*w\right|^2 + w^*\left(B - \frac{1}{a_{11}}vv^*\right)w \\ &= a_{11}\left|z_1 + \frac{1}{a_{11}}v^*w\right|^2 + w^*S_nw > 0 \end{aligned}$$

since $S_n$ is positive definite. □

One remarkable property of positive definite matrices is that they are closed under the Hadamard/entrywise product.

**Definition 1.3.** Let $A = (a_{ij}), B = (b_{ij}) \in \mathbb{C}^{m\times n}$. We define their Hadamard (or Schur, or entrywise) product by

$$A \circ B := (a_{ij}b_{ij}).$$

**Theorem 1.4.** *Let $A, B \in \mathbb{C}^{n\times n}$ be positive semidefinite/definite. Then $A \circ B$ is positive semidefinite/definite.*

*Proof.* Suppose first $A$ and $B$ have rank 1, i.e.,

$$A = uu^*$$
$$B = vv^*$$

Then $(A \circ B) = u_i\overline{u_j}v_i\overline{v_j} = (u_iv_i)(\overline{u_jv_j})$. It follows that

$$A \circ B = (u \circ v)(u \circ v)^*$$

is positive semidefinite. For general matrices, write their eigendecompositions:

$$A = \sum_{j=1}^{n} \lambda_j u_j u_j^*, \qquad B = \sum_{k=1}^{n} \mu_k v_k v_k^*$$

and expand $A \circ B$ using bilinearity. It follows immediately that $A \circ B$ is positive semidefinite.

When $A$ and $B$ are positive definite, let $u_j = (u_j^{(1)}, u_j^{(2)}, \ldots, u_j^{(n)})^T$ and define

$$D_j := \operatorname{diag}(u_j^{(1)}, u_j^{(2)}, \ldots, u_j^{(n)}).$$

Then $A \circ B = \sum_{j=1}^{n} \lambda_j D_j B D_j$. It follows easily that $x^T(A \circ B)x > 0$ for any $x \in \mathbb{C}^n \setminus \{\mathbf{0}_{n\times 1}\}$. □

Many other bilinear matrix products preserve matrix positivity. For a general construction of such products, please see [2].

## 2. Entrywise positivity preservers

Given a function $f : \mathbb{C} \to \mathbb{C}$ and a matrix $A = (a_{ij}) \in \mathbb{C}^{n\times n}$, we define

$$f[A] := (f(a_{ij}).$$

The function $f$ is thus applied *entrywise* to the matrix $A$. We are interested in determining which functions $f$ have the property that $f[A]$ is positive semidefinite/definite whenever $A \in \mathbb{P}_n$ (resp. $A \in \mathbb{P}_n^+$). We call such a function an *entrywise positive semidefinite (resp. definite preserver).* The Schur product theorem already provides many examples.

**Notation:**

- For $S \subseteq \mathbb{C}$, we denote by

$$\mathbb{P}_n(S) := \{A \in M_n(S) : A \text{ is psd}\}$$
$$\mathbb{P}_n^+(S) := \{A \in M_n(S) : A \text{ is pd}\}.$$

  When $S = \mathbb{C}$, we write $\mathbb{P}_n$ and $\mathbb{P}_n^+$ instead of $\mathbb{P}_n(\mathbb{C})$ and $\mathbb{P}_n^+(\mathbb{C})$.
- For an integer $k \geq 0$, if $f(z) = z^k$, then we write $f[A] = A^{\circ k}$. We use the convention $0^0 = 1$ when $k = 0$.

**Proposition 2.1.** *Let $f(z) = \sum_{j,k=0}^{\infty} a_{j,k} z^j \overline{z}^k$ where $a_{j,k} \geq 0$. Then $f$ preserves positive semidefiniteness on $\mathbb{P}_n$ for all $n \geq 1$. Moreover, if $a_{j,k} > 0$ for some $(j,k) \neq (0,0)$, then $f$ preserves positive definiteness on $\mathbb{P}_n^+$ for all $n \geq 1$.*

*Proof.* Let $A \in \mathbb{P}_n$. Then $\overline{A} \in \mathbb{P}_n$ as well since for all $z \in \mathbb{C}^n$,

$$z^*\overline{A}z = \sum_{j,k=1}^{n} \overline{a_{ij}} z_i \overline{z_j} = \overline{\sum_{j,k=1}^{n} a_{ij}\overline{z_i}z_j} = \overline{\overline{z}^* A \overline{z}} = \overline{z}^* A \overline{z} \geq 0.$$

By the Schur product theorem, any finite linear combination of the form

$$\sum_{j,k=1}^{N} a_{j,k} z^j \overline{z}^k$$

with $a_{j,k} \geq 0$ preserves positive semidefiniteness. The first part of the result follows from the fact that $\mathbb{P}_n$ is closed upon taking pointwise limits.

If $a_{j,k} > 0$ for some $(j,k) \neq (0,0)$, and if $A \in \mathbb{P}_n^+$, then for any $z \in \mathbb{C}^n \setminus \{\mathbf{0}_{n\times 1}\}$,

$$z^* f[A] z \geq a_{j,k} z^* \left( A^{\circ j} \circ \overline{A}^{\circ k} \right) z > 0.$$

Thus $f[A] \in \mathbb{P}_n^+$. □

Observe that the family of functions identified above preserves positivity for matrices of **all** dimensions $n \geq 1$.

**Theorem 2.1** (Schoenberg (1942), Rudin (1959), Herz (1963), Vasudeva (1979))**.** *Let $0 < \rho \leq \infty$. and let $\Omega = (-\rho, \rho), [0, \rho), (0, \rho)$, or $D(0, \rho)$. Let $f : \Omega \to \mathbb{F}$, where $\mathbb{F} = \mathbb{C}$ if $\Omega \not\subseteq \mathbb{R}$ and $\mathbb{F} = \mathbb{R}$ otherwise. Then the following are equivalent:*

1. *$f[A] := (f(a_{ij})) \in \mathbb{P}_n$ for all $A \in \mathbb{P}_n(\Omega)$, and all $n \geq 1$.*
2. *$f(z) \equiv \sum_{j,k\geq 0} c_{j,k} z^j \overline{z}^k$, where $c_{j,k} \geq 0$ for all integers $j, k \geq 0$.*

*Similarly, the following are equivalent:*
*$f[A] := (f(a_{ij})) \in \mathbb{P}_n^+$ for all $A \in \mathbb{P}_n^+(\Omega)$, and all $n \geq 1$.*
*$f(z) \equiv \sum_{j,k\geq 0} c_{j,k} z^j \overline{z}^k$, where $c_{j,k} \geq 0$ for all integers $j, k \geq 0$ and $a_{j,k} > 0$ for at least one $(j,k) \neq (0,0)$.*

The above characterizes functions that preserve positivity when applied entry-wise to matrices of all dimensions. When the dimension $n$ is fixed, characterizing positivity preservers on $n \times n$ matrices remains a mostly open problem. The $n = 2$ case was addressed by Vasudeva in 1979. The following version was extended to more general subsets of the complex plane.

**Definition 2.2.** We call $\Omega \subseteq \mathbb{C}$ *reflection-symmetric* if $z \in \Omega$ implies $\overline{z} \in \Omega$, and *modulus-closed* if $z \in \Omega$ implies $|z| \in \Omega$. Moreover, if $I := \Omega \cap [0, \infty)$, then we say that $\Omega$ is of

- *pd-type* if for all $z \in \Omega \setminus I$, there exists $\epsilon > 0$ such that $|z| + \epsilon \in I$;
- *psd-type* if for all $z \in \Omega \setminus I$, there exists $\delta > 0$ such that $|z| - \delta \in I$.

**Theorem 2.2** (Vasudeva (1979), Guillot–Gupta–Vishwakarma–Yip (2025))**.** *Let $\Omega \subseteq \mathbb{C}$ be reflection symmetric, modulus-closed, of pd-type, and such that $I := \Omega \cap [0, \infty)$ is an interval. Then the following are equivalent for a function $f : \Omega \to \mathbb{C}$:*

1. *A Hermitian matrix $A \in M_2(\Omega)$ is positive definite if and only if $f[A]$ is positive definite.*
2. *There exist real $\alpha, \beta > 0$ such that the following hold:*
   - *For all $x \in \Omega \cap \mathbb{R}$, $f(x) = \alpha \operatorname{sgn}(x)|x|^\beta$.*
   - *For all $z \in \Omega \setminus \mathbb{R}$, we have*

$$|f(z)| = \alpha |z|^\beta \quad \text{and} \quad f(\overline{z}) = \overline{f(z)}.$$

*The result holds verbatim with "pd-type" replaced by "psd-type" and "definite" by "semidefinite".*

For polynomials and, more generally, sums of powers, more can be said.

**Theorem 2.3** (Belton–Guillot–Khare–Putinar (2016))**.** *Fix $\rho > 0$ and integers $M \geq N \geq 1$, and let $f(z) = \sum_{j=0}^{N-1} c_j z^j + c' z^M$ be a polynomial with real coefficients.*

*Then the following are equivalent.*

(1) *$f[-]$ preserves positivity on $\mathbb{P}_N(\overline{D}(0,\rho))$.*
(2) *The coefficients $c_j$ satisfy either $c_0, \ldots, c_{N-1}, c' \geq 0$, or $c_0, \ldots, c_{N-1} > 0$ and $c' \geq -\mathfrak{C}(\mathbf{c}; z^M; N, \rho)^{-1}$, where $\mathbf{c} := (c_0, \ldots, c_{N-1})$, and*
$$\mathfrak{C}(\mathbf{c}; z^M; N, \rho) := \sum_{j=0}^{N-1} \binom{M}{j}^2 \binom{M-j-1}{N-j-1}^2 \frac{\rho^{M-j}}{c_j}.$$
(3) *$f[-]$ preserves positivity on rank-one matrices in $\mathbb{P}_N((0,\rho))$.*

More generally, the following holds for sums of powers.

**Theorem 2.4** (Khare–Tao (2021))**.** *Fix an integer $N > 0$ and real powers $n_0 < \cdots < n_{N-1} < M$. Also fix real scalars $\rho > 0$ and $c_{n_0}, \ldots, c_{n_{N-1}}, c'$, and define*
$$f(x) := \sum_{j=0}^{N-1} c_{n_j} x^{n_j} + c' x^M .$$
*Then the following are equivalent:*

(1) *The entrywise map $f[-]$ preserves positivity on rank-one matrices in $\mathbb{P}_N((0,\rho))$.*
(2) *Either all $c_{n_j}, c' > 0$; or $c_{n_j} > 0$ for all $j$ and*
$$c' > -\mathcal{C}^{-1},$$
*where*
$$\mathcal{C} = \sum_{j=0}^{N-1} \frac{V(n_j)^2}{V(n)^2} \rho^{M-n_j} c_{n_j}.$$
*Here $n := (n_0, \ldots, n_{N-1})$, $n_j := (n_0, \ldots, n_{j-1}, n_{j+1}, \ldots, n_{N-1}, M)$, and for any tuple $(t_0, \ldots, t_{k-1})$ the Vandermonde determinant is defined by*
$$V(t_0, \ldots, t_{k-1}) := \prod_{0 \leq i < j \leq k-1} (t_j - t_i).$$

*Furthermore, if we assume that $n_j \in \mathbb{Z}_{\geq 0} \cup [\mathbb{N} - 2, \infty)$ for all $j$, then the two conditions (1), (2) are further equivalent to:*

(3) *The entrywise map $f[-]$ preserves positivity on $\mathbb{P}_N([0,\rho])$.*

## 3. Finite fields

Let $p$ be a prime number. For any $q = p^k$, we denote the unique finite field with $q$ elements by $\mathbb{F}_q$. We let $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$.

### 3.1. Elementary results about finite fields.

**Proposition 3.1.** *Let $q = p^k$. Then*

(1) *Every element $x \in \mathbb{F}_q$ satisfies $x^q - x = 0$.*
(2) *$\mathbb{F}_q^*$ forms a cyclic group.*
(3) *For any $x, y \in \mathbb{F}_q$, we have*
$$(x+y)^p = x^p + y^p.$$

*Proof.* (1) Let $n := q-1$. Since $\mathbb{F}_q^*$ forms a group, by Lagrange's theorem, we have $x^{q-1} = 1$ for all $x \in \mathbb{F}_q$. It follows that $x^q = x$ for all $x \in \mathbb{F}_q$.

(2) For each positive divisor of $n$, let

$$a_d := \#\{x \in \mathbb{F}_q^* : x^d = 1\}$$
$$N(d) := \#\{x \in \mathbb{F}_q^* : \mathrm{ord}(x) = d\},$$

where $\mathrm{ord}(x)$ denotes the order of $x$. Every element whose order divides $d$ is a solution of $x^d = 1$, and every solution of $x^d = 1$ has order dividing $d$. Hence,

$$a_d = \sum_{e|d} N(e).$$

Since $x^d - 1$ has at most $d$ roots in $\mathbb{F}_q$, we have $a_d \leq d$ for every $d|n$. For $d = n$, every element of $\mathbb{F}_q^*$ satisfies $x^n - 1 = x^{q-1} - 1 = 0$. Thus $a_n = n$ and so

$$n = a_n = \sum_{d|n} N(d).$$

Using Möbius inversion, we obtain

$$N(n) = \sum_{d|n} \mu(d) a_{n/d}.$$

From the bound $a_{n/d} \leq n/d$, we conclude that

$$N(n) \geq \sum_{d|n} \mu(d) \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d} = \phi(n),$$

where $\phi$ is Euler's function and where we used the identity $n \sum_{d|n} \frac{\mu(d)}{d} = \phi(n)$. In particular,

$$N(n) \geq \phi(n) \geq 1.$$

Thus $\mathbb{F}_q^*$ has an element of order $n$ and is therefore cyclic.

(3) Using binomial expansion,

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{n-k}.$$

For any $1 \leq k \leq p-1$, the prime factorization of $k!(p-k)!$ only contains prime strictly smaller than $p$. Thus, $p$ divides $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ and the result follows. □

**Proposition 3.2.** *Let $q = p^k$ and let $1 \leq n \leq q-1$. Then the monomial $f(x) = x^n$ is injective (and therefore bijective) on $\mathbb{F}_q$ if and only if* $\gcd(n, q-1) = 1$.

*Proof.* Since $f(0) = 0$ and $f(x) \neq 0$ for $x \neq 0$, it suffices to prove the result on $\mathbb{F}_q^*$.

($\Leftarrow$) Suppose $\gcd(n, q-1) = 1$. Using Proposition 3.1(2), let $g$ be a generator of the cyclic group $\mathbb{F}_q^*$. Since $\gcd(n, q-1) = 1$, there exists $1 \leq m \leq q-2$ such that $nm \equiv 1 \pmod{q-1}$. Thus, $(x^n)^m = x^{mn} = x$ for all $x \in \mathbb{F}_q^*$. The map $f$ thus has inverse $f(x) = x^m$ and so $f$ is injective.

($\Rightarrow$) Suppose now $\gcd(n, q-1) = d > 1$ and let $t := (q-1)/d$. Consider the element $h = g^t \in \mathbb{F}_q^*$. Since $g$ is a generator, the order of $h$ is $d$. Therefore $h \neq 1$, but

$$h^n = g^{tn} = g^{\frac{q-1}{d} n} = \left(g^{q-1}\right)^{n/d} = 1.$$

This proves $f$ is not injective. □

Letting $q = p^k$, we define

$$\sigma_j(x) = x^{p^j} \qquad (j = 0, 1, \ldots, k-1).$$

As a consequence of Proposition 3.1(3) and of Proposition 3.2, the functions $\sigma_0, \sigma_1, \ldots, \sigma_{k-1}$ are automorphisms of $\mathbb{F}_q$, i.e., they are bijective and satisfy

$$\sigma_j(x+y) = \sigma_j(x) + \sigma_j(y)$$
$$\sigma_j(xy) = \sigma_j(x)\sigma_j(y).$$

In particular, $\sigma_1(x) = x^p$ is the *Frobenius automorphism* of $\mathbb{F}_q$.

**Proposition 3.3.** *Let $q = p^k$. Then the functions $\sigma_0, \sigma_1, \ldots, \sigma_{k-1}$ are precisely the automorphisms of $\mathbb{F}_q$.*

*Proof.* Let $\sigma$ be an automorphism of $\mathbb{F}_q$. Since $\sigma(0) = 0$ and $\sigma(1) = 1$, it follows that $\sigma(a) = a$ for all $a \in \mathbb{F}_p \subseteq \mathbb{F}_q$. Now, let $g$ be a generator of $\mathbb{F}_q^*$. The minimal polynomial $p \in \mathbb{F}_p[x]$ of $g$ over $\mathbb{F}_p$ has degree $k$. Observe that for any $0 \leq j \leq k-1$,

$$0 = \sigma_j(p(g)) = p(\sigma_j(g)).$$

Thus, $\sigma_j(g)$ is a root of $p$. Since the degree of $p$ is $k$, its roots are precisely $\sigma_0(g), \ldots, \sigma_{k-1}(g)$. The same calculation shows that $0 = \sigma(p(g)) = p(\sigma(g))$. Thus $\sigma(g)$ is a root of $p$. As a result, there exists $0 \leq j \leq k-1$ such that $\sigma(g) = \sigma_j(g)$. Since $g$ is a generator and $\sigma$ is an automorphism, it follows immediately that $\sigma = \sigma_j$. □

3.2. **Positive elements in $\mathbb{F}_q$.** We define the set of *positive elements* of the finite field $\mathbb{F}_q$ to be its non-zero squares:

$$\mathbb{F}_q^+ := \{x \in \mathbb{F}_q : x = y^2 \text{ for some } y \in \mathbb{F}_q^*\}.$$

Similarly, we define its *negative elements* to be

$$\mathbb{F}_q^- := \mathbb{F}_q^* \setminus \mathbb{F}_q^+.$$

**Proposition 3.4.** *Let $q = p^k$. Then*

(1) $|\mathbb{F}_q^+| = q - 1$ *if $q$ is even.*
(2) $|\mathbb{F}_q^+| = \frac{q-1}{2}$ *if $q$ is odd.*

*Proof.* When $q$ is even, the Frobenius automorphism $\phi_1(x) = x^2$ is bijective and so every non-zero element of $\mathbb{F}_q$ is a square. Thus $|F_q^+| = q - 1$.

When $q$ is odd, we have $-1 \neq 1$ and the map $f(x) = x^2$ satisfies $f(x) = f(-x)$. Moreover, for any $a \in \mathbb{F}_q$, the polynomial $x^2 - a$ has at most two roots. It follows that the map $f$ is 2-to-1 on $\mathbb{F}_q^*$ and so $|\mathbb{F}_q^+| = |f(\mathbb{F}_q^*)| = \frac{q-1}{2}$. □

When $q$ is even, every non-zero element in $\mathbb{F}_q$ is positive. In particular, $-1 = 1$ is positive. We now examine when $-1$ is a square in $\mathbb{F}_q$ for $q$ odd.

**Proposition 3.5.** *Let $q = p^k$ be odd. Then*

(1) $-1 \notin \mathbb{F}_q^+$ *if* $q \equiv 3 \pmod 4$.
(2) $-1 \in \mathbb{F}_q^+$ *if* $q \equiv 1 \pmod 4$.

*Proof.* Suppose $-1 \in \mathbb{F}_q^+$, say $-1 = y^2$. Then $y^4 = 1$ and so $4|q-1$. This is impossible when $q \equiv 3 \pmod 4$. On the other hand, if $q \equiv 1 \pmod 4$, then $4|q-1$. Since $\mathbb{F}_q^*$ is cyclic and 4 divides its order, $\mathbb{F}_q^*$ admits an element $y$ of order 4. Letting $x = y^2$, we have $x \neq 1$ and $x^2 = 1$. Thus $x = -1 = y^2$ and $-1 \in \mathbb{F}_q^+$. □

### 3.3. **Paley (di)graphs.**

3.3.1. *Definition and strong regularity.* To any finite field $\mathbb{F}_q$, we associate a graph $P(q) = (V, E)$ where $V = \mathbb{F}_q$ and where $(x, y) \in E$ if and only if $y - x \in \mathbb{F}_q^+$. When $q \equiv 1 \pmod 4$, by Proposition 3.5, we have $x - y \in \mathbb{F}_q^+$ if and only if $y - x \in \mathbb{F}_q^+$. We therefore think of the Paley graph as an undirected graph. When $q \equiv 3 \pmod 4$, the graph is directed.

When $q \equiv 1 \pmod 4$, we denote the neighborhood of $u \in P(q)$ by

$$N(u) := \{v \in \mathbb{F}_q : u - v \in \mathbb{F}_q^+\}.$$

When $q \equiv 3 \pmod 4$, we define the in and out neighborhoods of $u \in \mathbb{F}_q$ by

$$N_{\text{out}}(u) = \{v \in \mathbb{F}_q : v - u \in \mathbb{F}_q^+\}$$
$$N_{\text{in}}(u) = \{v \in \mathbb{F}_q^+ : u - v \in \mathbb{F}_q^+\}.$$

A useful tool to study the structure of $P(q)$ is the *quadratic character* of $\mathbb{F}_q$, defined by

$$\eta(x) := \begin{cases} 1 & \text{if } x \in \mathbb{F}_q^+ \\ 0 & \text{if } x = 0 \\ -1 & \text{if } x \in \mathbb{F}_q^-. \end{cases} \tag{3.1}$$

**Proposition 3.6.** *The quadratic chatacter satisfies:*

1. *$\eta(xy) = \eta(x)\eta(y)$ for all $x, y \in \mathbb{F}_q$ (multiplicativity).*
2. *If $q$ is odd, then for any $a, b \in \mathbb{F}_q$ with $a \neq 0$, we have*

$$\sum_{x \in \mathbb{F}_q} \eta(ax + b) = 0.$$

*Proof.* (1) The result is clear if $x, y \in \mathbb{F}_q^+$ or if $x$ or $y$ equals 0. Now, suppose $x \in \mathbb{F}_q^+$ and $y \in \mathbb{F}_q^-$. If $xy = z^2$ for some $z \in \mathbb{F}_q^*$, then $y = x^{-1}z^2 \in \mathbb{F}_q^+$, a contradiction. Therefore $xy \in \mathbb{F}_q^-$ and $-1 = \eta(xy) = \eta(x)\eta(y)$. Now, fix $\omega \in \mathbb{F}_q^-$. By the above, $\omega x \in \mathbb{F}_q^-$ for all $x \in \mathbb{F}_q^+$. Since the map $f(x) = \omega x$ is injective, we conclude that $\mathbb{F}_q^- = \{\omega x : x \in \mathbb{F}_q^+\}$. Now, let $x, y \in \mathbb{F}_q^-$, say $x = \omega a$ and $y = \omega b$ for $a, b \in \mathbb{F}_q^+$. Then $xy = \omega^2 ab \in \mathbb{F}_q^+$ and therefore $\eta(xy) = 1 = \eta(x)\eta(y)$.

(2) Since the map $x \mapsto ax + b$ is a bijection, the result follows from Proposition 3.4. □

**Proposition 3.7.** *Let $q \equiv 1 \pmod 4$. Then*

1. *For any $u \in P(q)$, the number of neighbors of $u$ is $\frac{q-1}{2}$.*
2. *For any two distinct adjacent vertices $u, v \in \mathbb{F}_q$, we have $|N(u) \cap N(v)| = \frac{q-5}{4}$.*
3. *For any two distinct non-adjacent vertices $u, v \in \mathbb{F}_q$, we have $|N(u) \cap N(v)| = \frac{q-1}{4}$.*
4. *$P(q)$ is isomorphic to its complement.*
5. *$P(q)$ has diameter 2.*

*Proof.* (1) For any fixed $u \in \mathbb{F}_q$, the map $x \mapsto u - x$ is a bijection of $\mathbb{F}_q$ onto itself. It follows that $|N(u)| = \frac{q-1}{2}$.

To prove (2) and (3), let $u, v \in \mathbb{F}_q$ be distinct. Observe that

$$\begin{aligned}|N(u) \cap N(v)| &= \sum_{x \in \mathbb{F}_q \setminus \{u,v\}} \frac{\eta(x-u)+1}{2} \frac{\eta(x-v)+1}{2} \\ &= \frac{1}{4} \sum_{x \in \mathbb{F}_q \setminus \{u,v\}} \eta(x-u)\eta(x-v) + \frac{1}{4} \sum_{x \in \mathbb{F}_q \setminus \{u,v\}} \eta(x-u) \\ &+ \frac{1}{4} \sum_{x \in \mathbb{F}_q \setminus \{u,v\}} \eta(x-v) + \frac{1}{4} \sum_{x \in \mathbb{F}_q \setminus \{u,v\}} 1.\end{aligned}$$

We evaluate each term. First, setting $y = x - u$, we obtain:

$$S_1 := \sum_{x \in \mathbb{F}_q \setminus \{u,v\}} \eta(x-u)\eta(x-v) = \sum_{y \in \mathbb{F}_q \setminus \{0, v-u\}} \eta(y)\eta(y+u-v).$$

Since $\eta(y) = \eta(y^{-1})$ for all $y \in \mathbb{F}_q^*$, using the multiplicativity of the quadratic character (Proposition 3.6(1)), we obtain

$$S_1 = \sum_{y \in \mathbb{F}_q \setminus \{0, v-u\}} \eta(y^{-1})\eta(y+u-v) = \sum_{y \in \mathbb{F}_q \setminus \{0, v-u\}} \eta(1 + y^{-1}(u-v)).$$

Finally, replacing $y^{-1}$ by $y$, we obtain

$$S_1 = \sum_{y \in \mathbb{F}_q \setminus \{0, (v-u)^{-1}\}} \eta(1 + y(u-v)).$$

When $y = 0$, we have $\eta(1 + y(u-v)) = 1$ and when $y = (v-u)^{-1}$ we have $\eta(1 + y(u-v)) = 0$. Thus,

$$S_1 = -1 + \sum_{y \in \mathbb{F}_q} \eta(1 + y(u-v)) = -1$$

where we used Proposition 3.6(2) in the last equality.

For the second term, we have

$$\sum_{x \in \mathbb{F}_q \setminus \{u,v\}} \eta(x-u) = -\eta(v-u) + \sum_{x \in \mathbb{F}_q} \eta(x-u) = -\eta(v-u)$$

where we used Proposition 3.6(2) again for the last equality. The same calculation shows that

$$\sum_{x \in \mathbb{F}_q \setminus \{u,v\}} \eta(x-v) = -\eta(u-v).$$

Combining all the above, we obtain

$$\begin{aligned}|N(u) \cap N(v)| &= \frac{-1 - 2 \cdot \eta(u-v) + q - 2}{4} \\ &= \begin{cases} \frac{q-5}{4} & \text{if } \eta(u-v) = 1 \\ \frac{q-1}{4} & \text{if } \eta(u-v) = -1 \end{cases} = \begin{cases} \frac{q-5}{4} & \text{if } u \text{ and } v \text{ are adjacent} \\ \frac{q-1}{4} & \text{if } u \text{ and } v \text{ are not adjacent.} \end{cases}\end{aligned}$$

To prove (4), fix $\omega \in \mathbb{F}_q^-$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$ be given by $f(x) = \omega x$. Then $f$ is a bijection and

$$f(x) - f(y) \in \mathbb{F}_q^+ \iff \omega(x-y) \in \mathbb{F}_q^+ \iff x - y \in \mathbb{F}_q^-.$$

The function $f$ thus provides an isomorphism between the complement of $P(q)$ and $P(q)$.

Finally, (5) follows immediately from the fact that $N(u) \cap N(v) \neq \emptyset$ for any two distinct $u, v \in \mathbb{F}_q$. □

A similar result holds when $q \equiv 3 \pmod 4$.

**Proposition 3.8.** *Let $q \equiv 3 \pmod 4$. Then*

1. *$P(q)$ is a tournament (i.e., an orientation of the complete graph on $\mathbb{F}_q$).*
2. *For any $u \in \mathbb{F}_q$, we have $|N_{in}(u)| = |N_{out}(u)| = \frac{q-1}{2}$.*
3. *For any edge $(u, v)$ in $P(q)$, the number of two steps walks from $u$ to $v$ is $\frac{q-3}{4}$.*
4. *For any edge $(u, v)$ in $P(q)$, the number of two steps walks from $v$ to $u$ is $\frac{q+1}{4}$.*
5. *$P(q)$ is isomorphic to its complement (obtained by reversing all edges).*
6. *$P(q)$ has directed diameter 2.*

*Proof.* (1) For any distinct $u, v \in \mathbb{F}_q$, since $-1 \notin \mathbb{F}_q^+$ (Proposition 3.5), we have either $u - v \in \mathbb{F}_q^+$ or $v - u \in \mathbb{F}_q^+$. The graph $P(q)$ is therefore a tournament.

(2) This follows from the fact that $f(x) = x - u$ and $g(x) = u - x$ are bijections.

(3) The calculation is similar to the one in Proposition 3.7. For distinct $u, v \in \mathbb{F}_q$, the number of two step wals from $u$ to $v$ is given by

$$\sum_{x \in \mathbb{F}_q \setminus \{u,v\}} \frac{\eta(x-u)+1}{2} \frac{\eta(v-x)+1}{2}.$$

We have

$$\begin{aligned}
&\sum_{x \in \mathbb{F}_q \setminus \{u,v\}} \eta(x-u)\eta(v-x) = \sum_{y \in \mathbb{F}_q \setminus \{0, v-u\}} \eta(y)\eta(v-u-y) \\
&= \sum_{y \in \mathbb{F}_q \setminus \{0, v-u\}} \eta(y^{-1}(v-u)-1) = \sum_{y \in \mathbb{F}_q \setminus \{0, (v-u)^{-1}\}} \eta(y(v-u)-1) \\
&= 1 + \sum_{y \in \mathbb{F}_q} \eta(y(v-u)-1) = 1.
\end{aligned}$$

Also,

$$\sum_{x \in \mathbb{F}_q \setminus \{u,v\}} \eta(x-u) = -\eta(v-u) + \sum_{x \in \mathbb{F}_q} \eta(x-u) = -\eta(v-u)$$

and

$$\sum_{x \in \mathbb{F}_q \setminus \{u,v\}} \eta(v-x) = -\eta(v-u) + \sum_{x \in \mathbb{F}_q} \eta(v-x) = -\eta(v-u).$$

Combining all the above, the number of 2 step walks is

$$\frac{1 - 2\eta(v-u) + q - 2}{4}.$$

When $(u, v)$ is an edge in $P(q)$, we have $\eta(v-u) = 1$ and the number of two walks from $u$ to $v$ is $\frac{q-3}{4}$. Counting the number of walks from $v$ to $u$ is equivalent to counting the number of walks from $u$ to $v$ assuming $\eta(v-u) = -1$. We therefore obtain $\frac{q+1}{4}$ such walks.

For (5), the map $f(x) = -x$ provides an isomorphism between $P(q)$ and its complement. (6) follows from (3) and (4). □

3.3.2. *Multiplicative characters and Weil's bound.* In order to calculate the number of common neighbors of vertices in the Paley graph, we used above sums involving the quadratic character. For the common neighbors of two vertices, we were able to evaluate these sums exactly. For more than 2 vertices, it becomes very tricky to evaluate such sums. However, the *Weil character bound* provides a useful estimate. This deep result applies to any (additive or multiplicative character) of finite fields.

**Definition 3.9.** Let $G$ be finite abelian group (written multiplicatively). A *character* of $G$ is a homomorphism from $G$ into the multiplicative group $U$ of complex numbers of modulus 1.

In other words, a character of $G$ is a map $\chi : G \to U$ such that $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$. The set of characters forms a group under multiplication: $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$. The *order* of a character $\chi$ is its order in that group.

Characters of the group $(\mathbb{F}_q, +)$ are called *additive characters*, while those of the group $(\mathbb{F}_q^*, \cdot)$ are called *multiplicative character*. Notice that the quadratic character $\eta$ (Equation (3.1)) is a multuplicative character of order 2.

**Theorem 3.2** (Weil bound)**.** *Let $\psi$ be a multiplicative character of order $m > 1$ and let $f \in \mathbb{F}_q[x]$ be a monic polynomial of positive degree that is not an $m$-th power of a polynomial. Let $d$ be the number of distinct roots of $f$ in its splitting field over $\mathbb{F}_q$. Then for every $a \in \mathbb{F}_q$, we have*

$$\left| \sum_{c \in \mathbb{F}_q} \psi(af(c)) \right| \leq (d-1)\sqrt{q}.$$

Using Weil's bound, we can estimate the number of common neighbors of three or more vertices in the Paley graph $P(q)$ – see [1, Lemma 2.18]

3.3.3. *Spectrum and clique number bound.* Recall that a set of vertices $S$ in a graph $G$ forms an *independent set* (or coclique) if no two vertices in $S$ are adjacent in $G$. The *independence number* of $G$, denoted $\alpha(G)$, is the largest possible size of an independent set in $G$.

In contrast, a subset of vertices $S$ in a graph $G$ forms a *clique* of all pairs of vertices in $S$ are adjacent in $G$. The *clique number* of $G$, denoted $\omega(G)$ is the largest possible size of a clique in $G$.

**Theorem 3.3** (Hoffman bound)**.** *Let $G$ be an undirected $d$-regular graph on $n$ vertices, and let the eigenvalues of its adjacency matrix $A$ be*

$$d = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n = \lambda_{\min}.$$

*If $\alpha(G)$ denotes the independence number of $G$, then*

$$\alpha(G) \leq \frac{-\lambda_{\min}}{d - \lambda_{\min}}\, n.$$

*Proof.* Since $G$ is $d$ regular, $A\mathbf{1}_{n\times 1} = d\mathbf{1}_{n\times 1}$. Thus $\lambda = d$ is an eigenvalue of $A$. By the Perron–Frobenius theorem, $d = \lambda_1$ is the largest eigenvalue of $A$. It follows that $A$ and $\mathbf{1}_{n\times n}$ have a common basis of eigenvectors, consisting of $v_1 := \mathbf{1}_{n\times 1}$ and

$n-1$ vectors $v_2, \ldots, v_n$ orthogonal to $\mathbf{1}_{n\times 1}$. Letting $B := A - \frac{d-\lambda_n}{n}\mathbf{1}_{n\times n}$, observe that

$$Bv_1 = \lambda_n v_1, \qquad Bv_i = \lambda_i v_i \qquad (i = 2, \ldots, n).$$

The smallest eigenvalue of $B$ is therefore $\lambda_n$ and it follows that the matrix

$$M := B - \lambda_n I_n = A - \frac{d-\lambda_n}{n}\mathbf{1}_{n\times n} - \lambda_n I_n$$

is positive semidefinite. Now, let $S$ be an independent set of vertices in $G$ of size $\alpha := \alpha(G)$. Since $M$ is positive semidefinite, so is the principal submatrix

$$M_{S,S} = -\frac{d-\lambda_n}{n}\mathbf{1}_{\alpha\times\alpha} - \lambda_n I_\alpha.$$

Since

$$M_{S,S}\mathbf{1}_{\alpha\times 1} = \left(-\alpha\frac{d-\lambda_n}{n} - \lambda_n\right)\mathbf{1}_{\alpha\times 1},$$

we conclude that

$$-\alpha\frac{d-\lambda_n}{n} - \lambda_n \geq 0.$$

Re-organizing, we obtain:

$$\alpha \leq \frac{-\lambda_n}{d-\lambda_n}n.$$

□

When $q \equiv 1 \pmod 4$, we can use the Hoffman bound to estimate the independence number of $P(q)$. Since $P(q)$ is self-complementary, that also immediately gives a bound on the clique number of $P(q)$. We begin by identifying the possible eigenvalues of $P(q)$.

Recall that a graph $G$ with $n$ vertices is strongly regular if:

- every vertex has degree $d$;
- every two adjacent vertices have $\lambda$ common neighbors;
- every two non-adjacent vertices have $\mu$ common neighbors.

In that case, we say $G$ is strongly regular with parameters $(n, d, \lambda, \mu)$. By Proposition 3.7, when $q \equiv 1 \pmod 4$, the graph $P(q)$ is strongly regular with parameters $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$.

**Proposition 3.10.** *Let $G$ be a simple $(n, d, \lambda, \mu)$ strongly regular graph. Then the adjacency matrix $A$ of $G$ satisfies:*

$$A^2 + (\mu - d)I_n + (\mu - \lambda)A + \mu\mathbf{1}_{n\times n} = \mathbf{0}_{n\times n}.$$

*Proof.* Observe that the $(i, j)$th entry of $A^2$ counts the number of walks from $i$ to $j$. Then $i = j$, there are $d$ such walks. When $i \neq j$ the number of walks is $\lambda$ when $(i, j)$ are adjacent and $\mu$ otherwise. It follows that

$$A^2 = dI_n + \lambda A + \mu(\mathbf{1}_{n\times n} - A - I_n).$$

□

**Corollary 3.11.** *Let $G$ be a simple connected $(n, d, \lambda, \mu)$ strongly regular graph. Then $d$ is an eigenvalue of the adjacency matrix of $G$ and the following are the only two possible other eigenvalues:*

$$\theta_\pm = \frac{1}{2}\left((\lambda - \mu) \pm \sqrt{(\lambda-\mu)^2 + 4(d-\mu)}\right),$$

*The multiplicity of $d$ is 1 and the multiplicity of $\theta_+$ and $\theta_-$ are:*

$$m_+ = \frac{-d-(n-1)\theta_-}{\theta_+ - \theta_-}, \qquad m_- = \frac{-d-(n-1)\theta_+}{\theta_- - \theta_+}.$$

*Moreover, unless $G$ is the empty graph or the complete graph, the adjacency matrix of $G$ has precisely three distinct eigenvalues.*

*Proof.* Let $A$ be the adjacency matrix of $G$. Then $A\mathbf{1}_{n\times 1} = d\mathbf{1}_{n\times 1}$ since $G$ is $d$-regular. Thus, $d$ is an eigenvalue of $G$.

Let $v \in \mathbb{R}^n$ be any eigenvector of $A$ orthogonal to $\mathbf{1}_{n\times 1}$, say, $Av = \theta v$. Then we have

$$A^2 v + (\mu - d)v + (\mu - \lambda)Av = \mathbf{0}_{n\times 1} = \left(\theta^2 + (\mu-\lambda)\theta + (\mu - d)\right) v = \mathbf{0}_{n\times 1}.$$

Thus,

$$\theta^2 + (\mu - \lambda)\theta + (\mu - d) = 0 \tag{3.4}$$

and so the possible eigenvalues of $G$ are $d$, $\theta_+$, and $\theta_-$.

For the multiplicities, by the Perron–Frobenius theorem, the multiplicity of the $d$ eigenvalue is 1. Thus,

$$1 + m_+ + m_- = n.$$

Moreover,

$$0 = \operatorname{tr}(A) = d + m_+\theta_+ + m_-\theta_-.$$

The multiplicities follow by solving these two equations for $m_+$ and $m_-$. □

Using the above, we can now give a bound on the clique number of the Paley graph $P(q)$.

**Theorem 3.5.** *The clique number of the Paley graph $P(q)$ satisfies:*

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

*Proof.* For the Paley graph $P(q)$, we have $d = \frac{q-1}{2}$, $\lambda = \frac{q-5}{4}$, and $\mu = \frac{q-1}{4}$. Thus, by Corollary 3.11,

$$\begin{aligned}
\lambda_{\min} = \theta_- &= \frac{1}{2}\left((\lambda-\mu) - \sqrt{(\lambda-\mu)^2 + 4(d-\mu)}\right) \\
&= \frac{1}{2}\left(-1 - \sqrt{1 + 4\frac{q-1}{4}}\right) \\
&= \frac{1}{2}\left(-1 - \sqrt{q}\right).
\end{aligned}$$

Therefore, using the Hoffman bound, we obtain:

$$\begin{aligned}
\alpha(P(q)) &\leq \frac{\frac{1}{2}(1+\sqrt{q})}{\frac{q-1}{2} + \frac{1}{2}(1+\sqrt{q})} q \\
&= \frac{1+\sqrt{q}}{q+\sqrt{q}} q \\
&= \frac{1}{\sqrt{q}} q = \sqrt{q}.
\end{aligned}$$

We therefore have $\alpha(P(q)) \leq \sqrt{q}$. Using the fact that $P(q)$ is self-complementary (Proposition 3.7(4)), we conclude that $\omega(P(q)) \leq \sqrt{q}$ as claimed. □

In the case where $q$ is a perfect square, we can show that the bound obtained above is tight.

**Corollary 3.12.** *Let $q = r^2$. Then the clique number of the Paley graph $P(q)$ is $\omega(P(q)) = \sqrt{q} = r$.*

*Proof.* Notice that $\mathbb{F}_r$ is a subfield of $\mathbb{F}_q$. We claim that $\mathbb{F}_r$ is in fact a clique in $\mathbb{F}_q$, i.e., every nonzero element of $\mathbb{F}_r$ is a square in $\mathbb{F}_q$. Indeed, observe $x \in \mathbb{F}_q^+$ if and only if

$$x^{\frac{r^2-1}{2}} = 1.$$

Now, every element in $x \in \mathbb{F}_r$ satisfies $x^{r-1} = 1$. Since

$$\frac{r^2-1}{2} = \frac{(r-1)(r+1)}{2}$$

it follows that $x^{\frac{r^2-1}{2}} = 1$, i.e., $x \in \mathbb{F}_q^+$. □

## References

[1] Dominique Guillot, Himanshu Gupta, Prateek Kumar Vishwakarma, and Chi Hoi Yip. Positivity preservers over finite fields. *Journal of Algebra*, 2025.

[2] Dominique Guillot, Javad Mashreghi, and Prateek Kumar Vishwakarma. Sharp lower bounds for generalized operator products. *arXiv preprint arXiv:2601.00409*, 2026.