J. COMBIN. MATH. COMBIN. COMPUT. 130 (2026) 165–185

Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Combinatorial Press

# An algebraic resolution of the ELSP via group actions in directed Paley graphs

Zhour Oumazouz*

ABSTRACT

We study the Equivalent Local Sequence Problem (ELSP), which consists in recovering an explicit sequence of local complementations that transforms a graph into a locally equivalent one. Focusing on directed Paley graphs, we establish that local complementations commute and induce a free action of an elementary abelian 2-group. The stabilizer condition is reformulated as a system of convolution equations and analyzed through Fourier techniques over finite fields, leading to a proof of stabilizer triviality. As a consequence, each graph in the orbit admits a unique subset encoding, and ELSP reduces to solving a linear inversion problem over $\mathbb{F}_2$. This characterization completely resolves ELSP for directed Paley graphs, provides a polynomial-time inversion algorithm and highlights structural features that may support future developments in cryptographic frameworks and quantum graph-state models.

*Keywords:* local complementation, graph equivalence, ELSP problem, Paley graphs, quadratic residues, complexity

*2020 Mathematics Subject Classification:* 05C25, 05C50, 05C76, 05C90, 15B34, 11T71.

## 1. Introduction

Local complementation is a graph transformation defined by a purely local rule: at a chosen vertex, the adjacency relations inside its neighborhood are toggled. Despite this local definition, iterated applications generate a highly non-trivial dynamical system on the space of graphs. The operation lies at the intersection of algebraic graph theory, group actions, finite field techniques, and computational complexity, and it plays an im-

* Corresponding author.

Received 21 Dec 2025; Revised 21 Jan 2026; Accepted 25 Feb 2026; Published Online 07 Mar 2026.

DOI: 10.61091/jcmcc130-12

portant role in areas such as isotropic systems, quantum graph states, and cryptographic constructions.

The problem of deciding local equivalence between graphs was first introduced by Bouchet, who provided a polynomial-time algorithm to determine whether two simple undirected graphs are locally equivalent [1]. His approach relies on binary matrix techniques and isotropic matroids, yielding a deep structural characterization. However, this framework is essentially existential: it determines whether an equivalence exists, but does not explicitly produce the sequence of local complementations transforming one graph into the other.

This leads to a distinct constructive problem. In this article, we formalize it under the name *Equivalent Local Sequence Problem* (ELSP):

*Given two locally equivalent graphs on the same vertex set, recover an explicit sequence of vertices whose successive local complementations transform one into the other.*

ELSP can be interpreted as an inversion problem in the discrete dynamical system generated by local complementation. Its computational difficulty depends strongly on the algebraic structure of the underlying graph family. While local equivalence has been extensively studied from a structural viewpoint, a complete algebraic resolution of the sequence-recovery problem has not previously been established.

We investigate ELSP in the class of directed Paley graphs, constructed from quadratic residues in finite fields. These graphs possess strong regularity, rich spectral properties, and deep connections with algebraic number theory and cryptography [4, 5, 2]. Despite their rigid algebraic structure, a fundamental question has remained open: does the orbit generated by all sequences of local complementations attain its maximal possible size? Equivalently, do distinct vertex subsets always produce distinct transformed graphs?

The first main contribution of this paper is to answer this question positively for directed Paley graphs with $p \equiv 3 \pmod 4$. We prove that local complementations commute in this setting and generate a free action of an elementary abelian 2-group. By translating the stabilizer condition into convolution equations and analyzing them through Fourier diagonalization over finite fields, we show that the stabilizer is trivial. Consequently, the orbit has maximal size $2^p$, and each locally equivalent graph admits a unique subset representation.

This structural rigidity has decisive algorithmic consequences. Since the group action is free, ELSP reduces to solving a linear inversion problem over $\mathbb{F}_2$. We therefore obtain a fully constructive recovery procedure together with a polynomial complexity bound. In contrast with the general setting-where equivalence may be decidable but sequence recovery remains implicit-the directed Paley case provides an explicit and efficient inversion framework.

It is worth emphasizing that the commutativity phenomenon observed in directed Paley graphs is highly non-generic. In arbitrary tournaments or directed graphs, local complementations typically fail to commute, and the induced action may exhibit nontrivial stabilizers. The fact that, in the Paley setting with $p \equiv 3 \pmod 4$, these operations generate a free elementary abelian 2-group reflects a remarkable algebraic rigidity rooted

in quadratic residue symmetry. This rigidity sharply contrasts with the general behavior of local equivalence in directed graphs and explains why the ELSP problem becomes tractable in this specific algebraic class.

Our previous works investigated algebraic and cryptographic aspects of Paley graphs and local complementations. In particular, [6] studied families of graphs generated by sequences of local complementations, while [4, 5] proposed cryptographic constructions based on related transformation problems. The present article differs both in scope and methodology: we provide a complete algebraic solution of ELSP in the directed Paley setting, establish stabilizer triviality via harmonic analysis, prove maximal orbit size through a spectral non-vanishing argument, and derive an explicit polynomial-time inversion algorithm.

The paper is organized as follows. Section 2 recalls the definition of local complementation and proves commutativity in directed Paley graphs. Section 3 develops the group-action framework, establishes maximal orbit size, and derives the algebraic inversion method. Section 4 presents the recovery algorithm and its complexity analysis. We conclude with structural consequences and perspectives for further research in algebraic graph dynamics and cryptographic applications.

## 2. Local complementation and commutativity

Throughout this article, $\mathbb{F}_p$ denotes the finite field with $p$ elements, and all adjacency-matrix computations are performed over $\mathbb{F}_2$.

### *2.1. Local complementation*

**Definition 2.1** (Local complementation)**.** Let $G$ be a simple graph (directed or undirected) on $V = \{1, \dots, n\}$ with adjacency matrix $A(G) = (a_{ij}) \in \mathbb{F}_2^{n\times n}$ and $a_{ii} = 0$. For a vertex $v \in V$, the *local complementation* of $G$ at $v$, denoted $G * v$, is the graph with adjacency matrix $A(G * v) = (a_{ij}^{(v)})$ defined by

$$a_{ij}^{(v)} = \begin{cases} a_{ij} + a_{iv}a_{vj}, & i \neq j, \\ 0, & i = j, \end{cases} \qquad \text{in } \mathbb{F}_2.$$

**Remark 2.2.** If $G$ is undirected then $A(G)$ is symmetric, whereas in the directed case no symmetry is assumed. The same algebraic update rule applies in both settings.

**Lemma 2.3** (Involution)**.** *For any graph $G$ and any vertex $v$,*

$$(G * v) * v = G.$$

**Proof.** For $i \neq j$, we have $a_{ij}^{(v)} = a_{ij} + a_{iv}a_{vj}$. Applying the operation again at $v$,

$$a_{ij}^{(v,v)} = a_{ij}^{(v)} + a_{iv}^{(v)}a_{vj}^{(v)}.$$

Local complementation does not change entries incident to $v$, hence $a_{iv}^{(v)} = a_{iv}$ and

$a_{vj}^{(v)} = a_{vj}$. Therefore,

$$a_{ij}^{(v,v)} = a_{ij} + a_{iv}a_{vj} + a_{iv}a_{vj} = a_{ij}.$$

The diagonal stays zero, so $(G * v) * v = G$. □

**Proposition 2.4.** *Local equivalence (generated by local complementations) is an equivalence relation.*

**Proof.** Reflexivity follows from the empty sequence. Symmetry follows from the involution property above. Transitivity follows by concatenating sequences. □

### *2.2. Commutativity of local complementation*

Local complementation is not commutative in general: for distinct vertices $u, v$ one can have

$$G * u * v \neq G * v * u.$$

Indeed, expanding the definition shows that, for $i \neq j$, both $(A(G * u * v))_{ij}$ and $(A(G * v * u))_{ij}$ contain higher-order terms involving $a_{uv}$ and $a_{vu}$; in general these terms differ, so commutativity fails.

### *2.3. Undirected Paley graphs*

Let $p \equiv 1 \ mod\ 4$ be prime, let $V = \mathbb{F}_p$, and let $Q \subset \mathbb{F}_p$ be the set of quadratic residues.

**Definition 2.5** (Undirected Paley graph)**.** The (undirected) Paley graph $P_p$ has vertex set $V$ and

$$x \sim y \iff y - x \in Q \quad (x \neq y).$$

**Proposition 2.6.** *The graph $P_p$ is strongly regular with parameters*

$$\left(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{4}\right).$$

**Proposition 2.7.** *If $G$ is undirected and $u, v$ are non-adjacent, then $G * u * v = G * v * u$. However, for the Paley graph $P_p$ with $p \geq 5$, local complementations do not commute for adjacent vertices $u \sim v$:*

$$P_p * u * v \neq P_p * v * u.$$

**Proof.** In the undirected case, a standard computation shows that the commutator depends on the factor $a_{uv}$; if $a_{uv} = 0$ the difference vanishes for every off-diagonal entry, hence the operations commute. For $P_p$, fix adjacent $u \sim v$. Strong regularity gives $|N(u) \setminus N(v)| = \frac{p-1}{4} \geq 1$. Choose $i \in N(u) \setminus N(v)$. Then $a_{iu} = 1$ and $a_{iv} = 0$, and evaluating the commutator at the entry $(i, v)$ yields a nonzero difference, proving non-commutativity. □

### *2.4. Directed Paley graphs*

Let $p \equiv 3 \pmod 4$ be prime, let $V = \mathbb{F}_p$, and let $Q \subset \mathbb{F}_p$ be the set of quadratic residues.

**Definition 2.8** (Directed Paley graph)**.** The directed Paley graph $P_p$ has vertex set $V$ and

$$x \to y \iff y - x \in Q \quad (x \neq y).$$

**Remark 2.9.** Since $p \equiv 3 \pmod 4$, we have $-1 \notin Q$. Hence for $x \neq y$ exactly one of $y - x$ or $x - y$ is a quadratic residue. Equivalently, for distinct $x, y$,

$$a_{xy} = 1 + a_{yx} \qquad (\text{in } \mathbb{F}_2),$$

so $P_p$ is a tournament and, in particular,

$$a_{uv}a_{vu} = 0 \qquad (u \neq v).$$

**Proposition 2.10** (Commutativity on directed Paley graphs)**.** *In $P_p$, local complementations commute:*

$$P_p * u * v = P_p * v * u \qquad \textit{for all } u, v \in V.$$

**Proof.** In the general expansion of $G*u*v$ versus $G*v*u$, the obstruction terms involve the factor $a_{uv}a_{vu}$. In $P_p$ this product is always zero for $u \neq v$, so the obstruction vanishes and the two compositions agree. □

## 3. The ELSP problem

We progressively translate the stabilizer problem into an algebraic form. First, subsets of vertices are encoded as vectors over $\mathbb{F}_2$. Second, adjacency in Paley graphs is expressed as a translation-invariant function, turning matrix updates into convolution operators. Third, Fourier analysis diagonalizes these operators, converting matrix equations into scalar spectral constraints. This chain of reductions transforms a combinatorial invariance condition into a tractable algebraic system.

### *3.1. Notation*

We fix $p \equiv 3 \pmod 4$ prime and $V = \mathbb{F}_p$.

- $A(G)$: adjacency matrix of a graph $G$ (over $\mathbb{F}_2$, diagonal 0).
- $c_v(G)$ and $r_v(G)$: the $v$-th column and $v$-th row of $A(G)$, respectively.
- $S \subseteq V$: a subset encoding a (commutative) product of local complementations.
- $s \in \mathbb{F}_2^V$: indicator vector of $S$.
- $f : \mathbb{F}_p \to \{0, 1\}$: Paley indicator $f(t) = \mathbf{1}_Q(t)$ with $f(0) = 0$.
- $g_r(t) = f(t)f(r - t)$: correlation kernel for $r \in \mathbb{F}_p$.
- $T_r$: shift-and-sum operator $(T_r s)(x) = \sum_{t \in \mathbb{F}_p} s(x + t)g_r(t)$.
- $\widehat{h}$: Fourier transform of $h : \mathbb{F}_p \to \mathbb{C}$.

**Definition 3.1** (Local equivalence)**.** Two graphs $G$ and $H$ on the same vertex set are *locally equivalent* if $H$ can be obtained from $G$ by a finite sequence of local complementations.

### *3.2. Problem definition*

Given locally equivalent graphs $G$ and $H$ on the same vertex set, there exists a sequence of vertices $v_0, \ldots, v_k$ such that

$$H = G * v_0 * \cdots * v_k.$$

The *Equivalent Local Sequence Problem (ELSP)* asks to recover such a sequence from $(G, H)$. In general, deciding local equivalence is well understood in the undirected case (e.g., via Bouchet's framework), but producing an explicit sequence is a separate constructive task, and the directed case requires different tools.

**Remark 3.2** (Why orbit size matters)**.** Because local complementations commute on directed Paley graphs, the order of vertices is irrelevant: only the subset $S \subseteq V$ matters. A key structural question is whether different subsets always produce different graphs $P_p * S$. If yes, then every graph locally equivalent to $P_p$ has a unique subset description, turning ELSP into a well-posed inversion problem.

### *3.3. Maximality of the orbit via the stabilizer*

Let $P_p$ be the directed Paley graph on $V = \mathbb{F}_p$.

3.3.1. Group action. For each $v \in V$, define $\tau_v(G) = G * v$ and let

$$\Gamma = \langle \tau_v : v \in V \rangle.$$

Since the $\tau_v$ commute and satisfy $\tau_v^2 = \mathrm{id}$, the group $\Gamma$ is an elementary abelian 2-group. Every element is represented by a unique subset $S \subseteq V$ via

$$\tau_S := \prod_{v \in S} \tau_v, \qquad \text{and we write} \qquad G * S := \tau_S(G).$$

Hence $|\Gamma| = 2^{|V|} = 2^p$ and $\Gamma \cong (\mathbb{Z}_2)^p$.

3.3.2. Orbit and stabilizer. For a graph $G$ define

$$Orb(G) = \{G * S : S \subseteq V\}, \qquad Stab(G) = \{S \subseteq V : G * S = G\}.$$

By the orbit–stabilizer theorem, for any $G$,

$$|Orb(G)| = \frac{|\Gamma|}{|Stab(G)|}.$$

Therefore

$$|Orb(P_p)| \leq 2^p,$$

with equality if and only if $Stab(P_p) = \{\varnothing\}$.

### *3.4. Indicator vectors and convolution operators*

To analyze the stabilizer algebraically, we translate subsets of vertices and adjacency relations into linear objects. The goal of this subsection is to express the stabilizer condition in terms of convolution operators on functions over $\mathbb{F}_p$. Each algebraic object introduced below corresponds directly to a matrix identity coming from the definition of local complementation.

3.4.1. Indicator vectors. A subset $S \subset V$ specifies the vertices at which local complementations are applied. Because local complementations commute in directed Paley graphs, the transformation $P_p * S$ depends only on the subset $S$ and not on the order of operations.

We encode $S$ by its indicator vector

$$s \in \mathbb{F}_2^V, \qquad s_v = \begin{cases} 1 & v \in S, \\ 0 & v \notin S. \end{cases}$$

This encoding reflects the algebraic structure of local complementation. Each vertex contributes a rank–one matrix update $a_v a_v^\top$ to the adjacency matrix, and applying the same vertex twice cancels out. Hence the cumulative effect of a subset $S$ is a binary sum of such updates, so the natural coefficient space is $\mathbb{F}_2$. The unknown vector $s$ therefore parametrizes all possible transformations and represents a candidate stabilizer.

3.4.2. Paley adjacency as a function. The directed Paley graph is translation-invariant: adjacency depends only on vertex differences. Let $Q \subset \mathbb{F}_p$ be the set of quadratic residues and define

$$f(t) = \begin{cases} 1 & t \in Q, \\ 0 & \text{otherwise}, \end{cases} \qquad f(0) = 0.$$

Then the adjacency matrix of $P_p$ satisfies

$$a_{xy} = f(y - x).$$

Thus every adjacency column is a translate of the same quadratic-residue pattern. This replaces matrix indices $(x, y)$ by a function on the additive group $(\mathbb{F}_p, +)$. When substituted into the matrix formula for local complementation, all products of adjacency entries become products of shifted copies of $f$. This translation-invariant description is what forces the appearance of convolution.

3.4.3. Local interaction kernel. To express the stabilizer condition, fix $r \in \mathbb{F}_p$ and examine the edge $(x, x+r)$. A vertex $v$ modifies this edge under local complementation exactly when both $x$ and $x + r$ are adjacent to $v$. From the matrix rule

$$a_{ij}^{(v)} = a_{ij} + a_{iv} a_{vj},$$

the contribution of $v$ to the edge $(x, x + r)$ is

$$a_{xv} a_{v,x+r} = f(v - x) f(x + r - v).$$

Introduce the relative variable $t = v - x$. Then this expression depends only on $t$:

$$f(v-x)f(x+r-v) = f(t)f(r-t).$$

This motivates the kernel

$$g_r(t) = f(t)f(r-t).$$

The function $g_r$ records exactly which relative positions $t$ allow a vertex to influence edges of difference $r$. It is therefore an algebraic encoding of the local interaction rule induced by quadratic residues.

3.4.4. Convolution operator. If $s$ is the indicator vector of $S$, the total modification of edges of difference $r$ is obtained by summing the contributions of all vertices:

$$(T_r s)(x) = \sum_{t \in V} s(x+t) g_r(t).$$

This quantity measures the net change (modulo 2) of the adjacency entry corresponding to the edge $(x, x+r)$ after applying all local complementations in $S$.

Setting $\tilde{g}_r(u) = g_r(-u)$ and using $u = -t$, we obtain

$$(T_r s)(x) = \sum_{u \in V} s(x-u)\tilde{g}_r(u) = (s * \tilde{g}_r)(x).$$

3.4.5. Stabilizer reformulation. The condition $P_p * S = P_p$ means that every edge difference is unchanged:

$$T_r s(x) = 0 \quad \text{for all } x \in \mathbb{F}_p,\ r \neq 0.$$

Hence stabilizers correspond exactly to vectors lying in

$$\bigcap_{r \neq 0} \ker(T_r).$$

This converts a matrix invariance condition into a system of linear convolution equations.

3.4.6. Stabilizer reduction. Let $s \in \mathbb{F}_2^V$ be the indicator vector of $S$. The stabilizer condition $P_p * S = P_p$ is equivalent to

$$\sum_{v \in V} s_v A_{iv} A_{vj} = 0 \quad \text{for all } i \neq j.$$

Specializing to Paley structure with $A_{xy} = f(y-x)$ and writing $(i,j) = (x, x+r)$ gives

$$\sum_{v \in V} s_v f(v-x) f(x+r-v) = 0.$$

Substituting $t = v - x$ yields

$$\sum_{t \in V} s(x+t) g_r(t) = 0,$$

i.e.

$$T_r s = 0.$$

Thus

$$\mathrm{Stab}(P_p) = \bigcap_{r \neq 0} \ker(T_r).$$

*3.5. Fourier analysis on $\mathbb{F}_p$*

The directed Paley graph is translation-invariant: adjacency depends only on vertex differences. Consequently, the operators describing local complementation are convolution operators on the additive group $(\mathbb{F}_p, +)$.

Fourier characters diagonalize convolution. Passing to the Fourier domain converts convolution equations into pointwise multiplication, allowing stabilizer conditions to be analyzed spectrally. This reduction from matrix algebra to scalar spectral constraints is the key mechanism enabling injectivity proofs.

We diagonalize convolution using Fourier transform.

Let $\omega = e^{2\pi i/p}$ and define additive characters

$$\chi_k(x) = \omega^{kx}.$$

The Fourier transform of $h : \mathbb{F}_p \to \mathbb{C}$ is

$$\hat{h}(k) = \sum_{t \in \mathbb{F}_p} h(t)\omega^{-kt}.$$

Convolution satisfies

$$\widehat{u * v}(k) = \hat{u}(k)\hat{v}(k).$$

Since $T_r s = s * \tilde{g}_r$, taking Fourier transforms gives

$$\widehat{T_r s}(k) = \hat{s}(k)\widehat{\tilde{g}_r}(k).$$

Thus the stabilizer condition is

$$\hat{s}(k)\widehat{\tilde{g}_r}(k) = 0 \quad \text{for all } k, r \neq 0.$$

If for every $k \neq 0$ there exists $r$ with $\widehat{\tilde{g}_r}(k) \neq 0$, then $\hat{s}(k) = 0$ for all $k \neq 0$, forcing $s = 0$.

3.5.1. Non-vanishing spectrum. *Non-vanishing of the quadratic-residue spectrum.* The non-vanishing of the spectrum follows from classical results on quadratic Gauss sums. Let $\eta$ denote the quadratic character on $\mathbb{F}_p^\times$. Writing

$$f(t) = \frac{1 + \eta(t)}{2},$$

its Fourier transform satisfies

$$\widehat{f}(m) = \frac{-1 + \varepsilon\, \eta(m)\, i\sqrt{p}}{2} \quad \text{for } m \neq 0,$$

where $\varepsilon \in \{\pm 1\}$ depends on $p$. In particular,

$$|\widehat{f}(m)| = \frac{\sqrt{p}}{2} \neq 0.$$

This classical computation may be found in standard references on Gauss sums (see, e.g., [3, Chapter 5]). Hence the quadratic-residue spectrum is strictly non-vanishing away from the zero frequency. Define

$$F_k(t) = f(t)\omega^{-kt}.$$

Then

$$\widehat{g}_r(k) = (F_k * f)(r).$$

Taking Fourier transforms,

$$\widehat{F_k * f}(m) = \hat{f}(m+k)\hat{f}(m).$$

Let $\eta$ be the quadratic character and use

$$f(t) = \frac{1+\eta(t)}{2}.$$

The quadratic Gauss sum gives

$$\hat{f}(m) = \frac{-1+\eta(m)\varepsilon i\sqrt{p}}{2}.$$

This never vanishes for $m \neq 0$, so the spectrum is nonzero.

**Lemma 3.3** (Fourier injectivity principle)**.** *Let $T$ be a convolution operator acting on functions $s : \mathbb{F}_p \to \mathbb{F}_2$ with kernel $g$. Assume that its complex Fourier transform satisfies*

$$\widehat{g}(k) \neq 0 \quad \textit{for all } k \neq 0.$$

*Then the only function $s$ satisfying*

$$Ts = 0,$$

*is the zero function.*

**Proof.** Embed $s$ into $\mathbb{C}^{\mathbb{F}_p}$ by viewing its values in $\{0,1\} \subset \mathbb{C}$. Taking Fourier transforms over $\mathbb{C}$ gives

$$\widehat{Ts}(k) = \widehat{s}(k)\widehat{g}(k).$$

If $Ts = 0$, then $\widehat{s}(k)\widehat{g}(k) = 0$ for all $k$. By hypothesis $\widehat{g}(k) \neq 0$ for $k \neq 0$, hence

$$\widehat{s}(k) = 0 \quad \text{for all } k \neq 0.$$

Therefore $s$ is constant. The stabilizer equations preserve the zero diagonal, which forces the constant solution to be 0. Hence $s = 0$. □

3.5.2. Justification of the complex embedding. Although the stabilizer problem is formulated over $\mathbb{F}_2$, we temporarily embed functions $s : \mathbb{F}_p \to \mathbb{F}_2$ into $\mathbb{C}^{\mathbb{F}_p}$ by identifying $\{0,1\} \subset \mathbb{C}$. This embedding is injective, so a function is zero over $\mathbb{F}_2$ if and only if it is zero as a complex-valued function. The Fourier transform is applied over $\mathbb{C}$ purely as an analytic tool to diagonalize convolution. If the Fourier transform of the embedded function vanishes at every frequency, the function itself must vanish identically in $\mathbb{C}$, hence also in $\mathbb{F}_2$. No information is lost in this lifting step; it is a standard technique allowing spectral arguments in characteristic 2 to be handled using complex harmonic analysis.

More precisely, if the Fourier transform of the embedded function vanishes at every frequency, the inversion formula over $\mathbb{C}$ implies that the function itself is identically zero as a complex-valued function. Since the embedding $\{0,1\} \hookrightarrow \mathbb{C}$ is injective, vanishing over $\mathbb{C}$ implies vanishing over $\mathbb{F}_2$. Therefore spectral non-vanishing over $\mathbb{C}$ guarantees injectivity of the original convolution operator defined over $\mathbb{F}_2$.

**Theorem 3.4.** *For $p \equiv 3 \pmod 4$,*

$$Stab(P_p) = \{\emptyset\}.$$

**Proof.** If $s \neq 0$, then $\hat{s}(k) \neq 0$ for some $k$. By spectral non-vanishing there exists $r$ with $\widehat{g_r}(k) \neq 0$, contradicting the stabilizer condition. Hence $s = 0$. □

**Corollary 3.5.**

$$|Orb(P_p)| = 2^p.$$

*Every locally equivalent graph has a unique subset representation.*

**Theorem 3.6** (Unique subset representation)**.** *For directed Paley graphs $P_p$ with $p \equiv 3 \pmod 4$, the orbit map*

$$S \longmapsto P_p * S,$$

*is a bijection between subsets of $V$ and graphs locally equivalent to $P_p$.*

**Proof.** The action group has size $2^p$. By Corollary 3.5, the orbit also has size $2^p$. Hence the action is free and injective. Therefore every locally equivalent graph corresponds to a unique subset. □

*3.6. Algebraic method to solve the ELSP problem*

Let $p \equiv 3 \pmod 4$ be a prime and let $V = \mathbb{F}_p$. Let $P_p$ denote the directed Paley graph on $V$. By Theorem 3.6, the map

$$S \longmapsto P_p * S,$$

is bijective on the orbit of $P_p$. Hence every graph $H$ locally equivalent to $P_p$ admits a unique subset $S \subseteq V$ such that

$$H = P_p * S.$$

The ELSP problem reduces to recovering this subset $S$.

We encode $S$ by its indicator vector

$$s = (s_v)_{v\in V} \in \mathbb{F}_2^V, \qquad s_v = \begin{cases} 1 & v \in S, \\ 0 & v \notin S. \end{cases}$$

3.6.1. Justification of the linearisation. The key idea of this section is that, in the commutative Paley setting, iterated local complementations behave additively at the matrix level. Because the operations commute and are involutions, the effect of applying a subset of vertices depends only on the subset itself and not on the order. This converts a nonlinear graph transformation problem into a linear algebraic problem over $\mathbb{F}_2$, which is the fundamental reason ELSP becomes tractable.

Throughout this subsection all matrices are over $\mathbb{F}_2$ and have zero diagonal.

For any graph $G$ on $V$, let

$$A(G) = (a_{ij})_{i,j\in V},$$

denote its adjacency matrix. For $v \in V$, define the column vector

$$a_v(G) \in \mathbb{F}_2^V, \qquad (a_v(G))_i = a_{iv}.$$

**Lemma 3.7** (Local complementation as a rank–one update)**.** *Let $G$ be a directed graph and $v \in V$. Then for $i \neq j$,*

$$A(G * v)_{ij} = A(G)_{ij} + A(G)_{iv}A(G)_{jv}.$$

*Equivalently, off the diagonal,*

$$A(G * v) = A(G) + a_v(G)a_v(G)^\top.$$

**Proof.** This is Definition 2.1 written in matrix form. For $i \neq j$,

$$a_{ij}^{(v)} = a_{ij} + a_{iv}a_{vj} = a_{ij} + (a_v)_i(a_v)_j.$$

□

**Lemma 3.8** (Effect on columns)**.** *Let $u \neq v$. Then the $u$-th column transforms as*

$$a_u(G * v) = a_u(G) + A(G)_{uv}\, a_v(G).$$

**Proof.** For $x \neq u$,

$$A(G * v)_{xu} = A(G)_{xu} + A(G)_{xv}A(G)_{uv}.$$

This is exactly the stated vector identity. □

**Structural observation.** The invariance of columns relies on a fundamental property of directed Paley graphs: for distinct vertices $u, v$ exactly one of $a_{uv}$ or $a_{vu}$ equals 1. Consequently,

$$a_{uv}a_{vu} = 0.$$

This tournament asymmetry prevents a vertex $v \neq u$ from simultaneously interacting with both orientations of edges incident to $u$. Therefore, rank–one updates induced by local complementation at vertices different from $u$ cannot alter the column indexed by $u$.

**Lemma 3.9** (Column invariance under commuting local complementations)**.** *Let $G$ be a graph in which local complementations commute pairwise. Fix $u \in V$. For any subset $S \subseteq V \setminus \{u\}$, the $u$-th column of the adjacency matrix is invariant:*

$$a_u(G * S) = a_u(G).$$

**Proof.** Let $u \notin S$. Since local complementations commute, we may apply them in arbitrary order. It suffices to show that for every $v \neq u$, the operation $*v$ does not alter the column indexed by $u$.

By Definition 2.1, for $x \neq u$,

$$A(G * v)_{x,u} = A(G)_{x,u} + A(G)_{x,v}A(G)_{u,v}.$$

Thus the entry $(x, u)$ changes if and only if

$$A(G)_{x,v}A(G)_{u,v} = 1.$$

In a directed Paley graph, for distinct vertices $u, v$ exactly one of $A(G)_{u,v}$ or $A(G)_{v,u}$ equals 1, hence

$$A(G)_{u,v}A(G)_{v,u} = 0.$$

This tournament asymmetry implies that no vertex $v \neq u$ can create symmetric interactions simultaneously affecting both orientations incident to $u$. Consequently, no operation $*v$ with $v \neq u$ modifies the $u$-th column.

Since $u \notin S$, the operation $*u$ is never applied. Therefore the $u$-th column remains unchanged throughout the sequence, proving the result. □

**Proposition 3.10** (Additivity of commuting local complementations)**.** *Assume local complementations commute pairwise in $G$:*

$$(G * u) * v = (G * v) * u \qquad \forall u, v \in V.$$

*Then for every subset $S \subseteq V$,*

$$A(G * S) = A(G) + \sum_{v \in S} a_v(G)a_v(G)^\top \quad \textit{(off-diagonal)}.$$

*Consequently, if $H = G * S$ then*

$$A(H) + A(G) = \sum_{v \in S} a_v(G)a_v(G)^\top.$$

**Proof.** We prove the identity by induction on $|S|$.

If $S = \varnothing$, the statement is trivial.

Assume the formula holds for a subset $S'$. Let $S = S' \cup \{u\}$ and write $G' = G * S'$. By the induction hypothesis,

$$A(G') = A(G) + \sum_{v \in S'} a_v(G) a_v(G)^\top.$$

Applying local complementation at $u$ yields

$$A(G' * u) = A(G') + a_u(G') a_u(G')^\top.$$

By Lemma 3.9, column $u$ is invariant under all operations in $S'$, hence

$$a_u(G') = a_u(G).$$

Substituting gives

$$A(G * S) = A(G) + \sum_{v \in S'} a_v(G) a_v(G)^\top + a_u(G) a_u(G)^\top.$$

This is exactly the desired identity for $S$. □

**Remark on diagonal entries.** All equalities above are interpreted off the diagonal, since adjacency matrices are required to have zero diagonal throughout the paper. Rank–one updates may introduce diagonal terms, but these are systematically discarded by definition of local complementation.

**Independence of updates.** The commutativity assumption ensures that each rank–one update $a_v a_v^\top$ contributes linearly and independently in $\mathbb{F}_2$. No cross-terms appear because applying the same vertex twice cancels out, and applying different vertices in any order yields the same cumulative sum. This algebraic rigidity is what allows the nonlinear graph dynamics to collapse into a linear superposition principle.

**Corollary 3.11** (Linearisation for directed Paley graphs)**.** *Let $G = P_p$. Let $H = P_p * S$ with indicator vector $s$. Let*

$$A = A(P_p), \qquad B = A(H), \qquad D = A + B.$$

*Let $f : \mathbb{F}_p \to \mathbb{F}_2$ be the Paley indicator function*

$$f(t) = \begin{cases} 1 & t \in Q, \\ 0 & t \notin Q, \end{cases} \qquad f(0) = 0,$$

*where $Q$ is the set of quadratic residues in $\mathbb{F}_p$.*

*For $r \in \mathbb{F}_p^*$ define*

$$g_r(t) = f(t) f(r - t).$$

*Then for every $x \in \mathbb{F}_p$ and $r \neq 0$,*

$$D_{x,x+r} = \sum_{t \in \mathbb{F}_p} s(x+t)\, g_r(t).$$

*Equivalently,*

$$D_r(x) = (T_r s)(x),$$

*where*

$$(T_r s)(x) = \sum_{t \in \mathbb{F}_p} s(x+t) g_r(t).$$

**Proof.** Local complementations commute in directed Paley graphs, so the additivity proposition applies. Hence

$$D = \sum_{v \in S} a_v a_v^\top,$$

off-diagonal. Using $A_{xy} = f(y-x)$ and the change of variables $t = v - x$ yields the convolution identity. □

3.6.2. Linear inversion formulation. By Corollary 3.11, for every $r \neq 0$,

$$D_r = T_r s.$$

Thus ELSP reduces to solving a linear system over $\mathbb{F}_2$.

3.6.3. Recovery algorithm. For each $(x, r)$ with $r \neq 0$, the equation

$$D_r(x) = \sum_{t \in \mathbb{F}_p} s(x+t) g_r(t),$$

is linear in $s$.

Define the row vector

$$m_{(x,r)}(v) = g_r(v-x), \qquad v \in V.$$

Then

$$\sum_{v \in V} m_{(x,r)}(v) s_v = D_r(x).$$

**Algorithm**

1. Compute $D = A + B$.
2. Initialize empty matrix $M$ and vector $d$.
3. For $r = 1, \ldots, p-1$:
   (i) For all $x \in \mathbb{F}_p$:
      i. append row $m_{(x,r)}$ to $M$
      ii. append $D_r(x)$ to $d$
      iii. if $\operatorname{rank}(M) = p$, stop
4. Solve $Ms = d$ over $\mathbb{F}_2$.
5. Output $S = \{v \in V : s_v = 1\}$.

**Detailed example: inversion for $p = 7$.** Let $V = \mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. The quadratic residues modulo 7 are

$$Q = \{1, 2, 4\}.$$

Thus the Paley adjacency function is

$$f(t) = \begin{cases} 1 & t \in \{1, 2, 4\}, \\ 0 & \text{otherwise}, \end{cases} \qquad f(0) = 0.$$

Assume the unknown subset is

$$S = \{1, 4\}.$$

Its indicator vector is

$$s = (0, 1, 0, 0, 1, 0, 0).$$

We simulate the inversion procedure and show how $s$ is recovered from linear equations.
*Step 1: compute $g_1(t)$.*
For $r = 1$,

$$g_1(t) = f(t)f(1 - t).$$

We compute it for all $t \in \mathbb{F}_7$:

| $t$ | $f(t)$ | $f(1-t)$ | $g_1(t)$ |
|---|---|---|---|
| 0 | 0 | $f(1) = 1$ | 0 |
| 1 | 1 | $f(0) = 0$ | 0 |
| 2 | 1 | $f(6) = 0$ | 0 |
| 3 | 0 | $f(5) = 0$ | 0 |
| 4 | 1 | $f(4) = 1$ | 1 |
| 5 | 0 | $f(3) = 0$ | 0 |
| 6 | 0 | $f(2) = 1$ | 0 |

Thus

$$g_1(t) = 1 \iff t = 4.$$

*Step 2: build equations from $D_1(x) = (T_1 s)(x)$.*
Recall

$$(T_1 s)(x) = \sum_{t \in \mathbb{F}_7} s(x + t) g_1(t).$$

Since $g_1(t)$ is nonzero only at $t = 4$, this simplifies to

$$(T_1 s)(x) = s(x + 4).$$

Hence

$$D_1(x) = s(x + 4).$$

We now write the equations:

$$D_1(0) = s(4),$$
$$D_1(1) = s(5),$$
$$D_1(2) = s(6),$$
$$D_1(3) = s(0),$$
$$D_1(4) = s(1),$$
$$D_1(5) = s(2),$$
$$D_1(6) = s(3).$$

From the observed graph difference $D$, suppose we measure

$$D_1 = (1, 0, 0, 0, 1, 0, 0).$$

Then we immediately recover

$$s = (0, 1, 0, 0, 1, 0, 0).$$

Thus

$$S = \{1, 4\}.$$

*Interpretation.*

This example illustrates the general mechanism of the inversion algorithm. Each operator $T_r$ acts as a structured linear transform built from shifted quadratic-residue correlations. For small primes these operators often reduce to cyclic shifts, making inversion transparent.

For larger primes the matrices behave pseudorandomly, which explains the rapid rank saturation observed in practice and the effectiveness of Gaussian elimination.

## 4. Complexity analysis of the ELSP inversion

We analyze the computational complexity of recovering the subset $S \subset V$ from a graph

$$H = P_p * S,$$

under the algebraic inversion framework developed above. All computations are performed over the finite field $\mathbb{F}_2$. We measure complexity in bit operations in the standard RAM model, where arithmetic in $\mathbb{F}_2$ costs constant time.

Let $p$ denote the number of vertices. The unknown vector $s \in \mathbb{F}_2^p$ represents the indicator of $S$.

### *4.1. Phase 1: difference matrix computation*

Let $A$ and $B$ be the adjacency matrices of $P_p$ and $H$. The difference matrix

$$D = A + B,$$

is computed entrywise in $\mathbb{F}_2$. Since each matrix contains $p^2$ entries, this phase requires

$$T_1(p) = \Theta(p^2),$$

bit operations and $\Theta(p^2)$ memory. This cost is optimal because the input size itself is $\Theta(p^2)$.

### *4.2. Phase 2: equation generation*

Each pair $(x, r)$ with $r \neq 0$ yields a linear equation

$$D_r(x) = (T_r s)(x) = \sum_{t \in \mathbb{F}_p} s(x+t) g_r(t).$$

There are at most $p(p-1) = \Theta(p^2)$ candidate equations. Constructing a single row requires evaluating a convolution of length $p$, hence

$$T_2(p) = \Theta(p^3).$$

This phase is dominated by arithmetic in $\mathbb{F}_2$ and involves no matrix inversion. The convolution kernels $g_r$ can be precomputed once in $\Theta(p^2)$ time and reused, which does not change the asymptotic bound.

### *4.3. Phase 3: incremental rank construction*

Rows are appended until a full-rank linear system is obtained. Let $M$ denote the current matrix with width $p$. Maintaining row-echelon form under incremental Gaussian elimination costs $O(p^2)$ operations per appended row in the worst case.

Since at most $\Theta(p^2)$ rows are tested, the total cost of rank maintenance is

$$T_3(p) = O(p^4).$$

This phase dominates the total running time. It corresponds to solving a sequence of linear independence tests in $\mathbb{F}_2^p$. The bound is worst-case; in practice, rank saturation typically occurs after $O(p)$ rows because the operators $T_r$ behave pseudorandomly. However, we state the conservative bound.

Memory usage in this phase is $O(p^2)$ bits to store the evolving matrix.

### *4.4. Phase 4: final linear solve*

Once a full-rank $p \times p$ subsystem is extracted, solving

$$Ms = d,$$

by Gaussian elimination costs

$$T_4(p) = \Theta(p^3).$$

This is asymptotically smaller than the rank-construction phase and does not affect the overall complexity. The $O(p^4)$ bound represents a conservative worst-case estimate. In

practice, numerical experiments indicate that rank saturation typically occurs after $O(p)$ rows, suggesting an effective running time closer to $O(p^3)$. The higher bound is stated to guarantee correctness under all inputs.

### *4.5. Total complexity*

The dominant term is $T_3(p)$, yielding

$$T(p) = O(p^4).$$

Thus the ELSP inversion for directed Paley graphs is polynomial in the graph size. The algorithm requires $O(p^2)$ memory and $O(p^4)$ time.

**Expected complexity refinement.** Although the worst-case bound is $O(p^4)$ due to incremental rank maintenance, the operators $T_r$ exhibit strong pseudorandom behavior arising from quadratic-residue correlations. Empirically, full rank is typically achieved after $O(p)$ independent rows, reducing the effective complexity of the inversion stage to $O(p^3)$ in practice. A randomized row-selection strategy or block elimination technique would therefore yield an expected cubic-time implementation while preserving correctness.

**Structured and spectral acceleration.** The worst-case bound $O(p^4)$ arises from conservative incremental rank maintenance. Since each operator $T_r$ is a convolution operator diagonalizable via Fourier transform, the inversion problem admits an equivalent spectral formulation. This opens the possibility of structured elimination schemes or block-Gaussian techniques that reduce the deterministic complexity to $O(p^3)$.

Moreover, randomized row-selection strategies suggest that full rank is typically achieved after $O(p)$ independent equations, yielding an expected cubic running time in practice. Thus, while the quartic bound guarantees correctness in all cases, practical implementations are expected to operate in near-cubic time.

### *4.6. Comparison with brute-force search*

A naive exhaustive search over all subsets $S \subset V$ requires

$$O(2^p \cdot p^2),$$

operations, since each candidate must be verified by recomputing the transformed adjacency matrix. This is exponential in $p$.

The algebraic inversion replaces an exponential search by a polynomial-time linear algebra problem. The reduction from exponential to polynomial complexity is a direct consequence of the structural injectivity proved in Section 3.

### *4.7. Structural interpretation*

The complexity bound reflects a deeper structural fact: ELSP becomes tractable because the group action generated by local complementations is free and admits a linear encoding. The inversion algorithm is not merely a computational shortcut; it is a manifestation of

algebraic rigidity. Without trivial stabilizer and spectral non-vanishing, the problem would revert to exponential search.

This explains why ELSP remains difficult in general graph classes while becoming polynomial in the directed Paley setting.

**Practical behavior.** Although the worst-case bound is $O(p^4)$, numerical experiments suggest that the matrices generated by the operators $T_r$ behave similarly to random binary matrices. In practice, full rank is typically reached after $O(p)$ rows, leading to an effective running time closer to $O(p^3)$.

## 5. Conclusion

We solved the Equivalent Local Sequence Problem for directed Paley graphs using an algebraic framework that combines group actions, convolution operators, and Fourier analysis over finite fields. Pairwise commutativity of local complementation induces an elementary abelian 2-group action whose stabilizer was shown to be trivial via spectral analysis of quadratic correlations. This yields maximal orbit size and a unique subset representation for every locally equivalent graph. ELSP therefore reduces to a linear inversion problem over $\mathbb{F}_2$, for which we provided a constructive recovery algorithm with polynomial complexity.

## Cryptographic implications

From a cryptographic perspective, the triviality of the stabilizer and the resulting polynomial time inversion algorithm imply that directed Paley graphs are unsuitable as a hard instance family for ELSP-based public-key constructions. The algebraic rigidity that enables efficient inversion simultaneously prevents the problem from providing computational hardness in this structured setting. This observation suggests that potential cryptographic applications must rely on graph families lacking such spectral rigidity. These results clarify the algebraic structure underlying local equivalence in directed Paley graphs and highlight the role of harmonic analysis in graph transformation problems.

## References

[1] A. Bouchet. An efficient algorithm to recognize locally equivalent graphs. *Combinatorica*, 11:315–329, 1991. https://doi.org/10.1007/BF01275668.

[2] J. Javelle. *Cryptographie Quantique: Protocoles Et Graphes*. PhD thesis, Université de Grenoble, 2014.

[3] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 1997.

[4] Z. Oumazouz. Novel public-key cryptosystem based on the problem of performing a sequence of local complementations on the Paley graphs. *International Journal of Mathematics and Computer Science*, 17(3):1451–1461, 2022.

[5] Z. Oumazouz. A proposed public-key cryptosystem constructed using Paley graphs. *International Journal of Mathematics and Computer Science*, 20(2):465–468, 2025. https://doi.org/10.69793/ijmcs/02.2025/zhour.

[6] Z. Oumazouz. On the classification of graphs induced by a sequence of local complementations of Paley graphs. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 126:29–72, 2025. https://doi.org/10.61091/jcmcc126-03.

Zhour Oumazouz
FST Mohammedia, Hassan II University, Casablanca, Morocco
E-mail oumazouzzhour@gmail.com