J. COMBIN. MATH. COMBIN. COMPUT. 131 (2026) 301–337

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

Combinatorial Press

From normal-matrix factorizations to local complementation sequences

Zhour Oumazouz*

ABSTRACT

We study the Equivalent Local Sequence Problem (ELSP) for simple undirected graphs using Bouchet's isotropic-system formalism and normal matrices over $\mathbb{F}_2$. Although Bouchet's theory characterizes graph local equivalence in polynomial time, converting normal-matrix certificates into explicit graph transformations remains challenging. We introduce the *Normal-Matrix Factorization Problem* (NMFP), which asks whether a normal-matrix witness of local equivalence has a graph-compatible factorization into elementary transformations. Whenever such a factorization exists, an explicit local-complementation sequence can be recovered in polynomial time. Thus, the constructive part of ELSP reduces to NMFP, identifying normal-matrix factorization as its main unresolved algebraic difficulty. We apply this framework to undirected Paley graphs. In contrast to the directed case, whose local-complementation dynamics are abelian and admit linear inversion, the undirected case is noncommutative and has a more intricate stabilizer structure. Using normal matrices, we analyze Paley-graph orbits and stabilizers, derive algebraic constraints on stabilizing transformations, and completely verify the first undirected Paley graph P_5. These results establish NMFP as central to constructive local equivalence and reveal connections among isotropic systems, graph transformations, and algebraic stabilizers.

Keywords: local complementation, graph equivalence, equivalent local sequence problem, paley graphs, quadratic residues, computational complexity

2020 Mathematics Subject Classification: 05C25, 05C50, 05C76, 15B34, 05E18, 11T06.

* Corresponding author.

Received 11 Mar 2026; Revised 10 Jun 2026; Accepted 18 Jun 2026; Published Online 20 Jul 2026.

DOI: 10.61091/jcmcc131-15

1. Introduction

Local complementation (LC) is a graph transformation defined as follows. Given a vertex v of a simple undirected graph G, the graph G*v is obtained by complementing the subgraph induced by the neighborhood $N_G(v)$. Despite its local definition, repeated applications of this operation generate a rich equivalence relation on graphs known as *local equivalence*. This notion occupies a central position in several areas of combinatorics and theoretical computer science, including isotropic-system theory [1], principal pivot transforms [12], binary matrix theory, vertex-minor theory [6], and quantum information theory [5]. More recently, Paley graphs have attracted attention from both algebraic and cryptographic perspectives. Early works explored their use in the design of symmetric-key cryptographic algorithms based on graph-theoretic structures and ASCII encodings [10, 11]. Subsequently, local-complementation dynamics on Paley graphs were investigated in connection with public-key cryptographic constructions and the combinatorial structure of local-equivalence classes [7, 8, 9].

A fundamental theorem of Bouchet [1] provides a complete algebraic characterization of local equivalence through isotropic systems. In this framework, graphs are represented by maximal isotropic subspaces of a finite-dimensional symplectic vector space, while local complementations correspond to particular orthogonal transformations. Bouchet's theory yields a polynomial-time recognition algorithm for deciding whether two graphs are locally equivalent. Consequently, the local-equivalence problem is algorithmically tractable from the perspective of decision.

However, the recognition problem captures only the existence of a transformation. Given two locally equivalent graphs, Bouchet's characterization certifies that they belong to the same local-equivalence class, but it does not directly provide an explicit sequence of local complementations relating them. This observation leads naturally to the following reconstruction problem.

Equivalent Local Sequence Problem (ELSP). Given two locally equivalent graphs on the same vertex set, determine an explicit sequence of vertices

$$(v_1, \dots, v_k),$$

such that

$$H = G * v_1 * \cdots * v_k.$$

The ELSP may be regarded as the search version of the local-equivalence problem. While recognition determines whether a transformation exists, the ELSP seeks an explicit description of such a transformation. Similar distinctions between recognition and reconstruction occur throughout algorithmic algebra and combinatorics, where the existence of a certificate often precedes an understanding of its constructive content.

The purpose of the present work is to investigate how Bouchet's isotropic-system framework may be extended from a recognition theory to a reconstruction theory. More precisely, we study the normal matrices appearing in Bouchet's characterization of local equivalence and analyze their role as algebraic certificates of graph transformations.

A central theme of this paper is the passage from recognition to reconstruction. Bouchet's characterization associates with every pair of locally equivalent graphs a normal matrix witnessing their equivalence. Nevertheless, the existence of such a witness does not by itself provide an explicit transformation sequence. To isolate the additional information required for reconstruction, we introduce the *Normal-Matrix Factorization Problem* (NMFP).

Given a normal-matrix witness of local equivalence, the NMFP asks whether this witness admits a graph-compatible factorization into elementary factors corresponding to local complementations and pivot operations. The significance of this problem stems from the fact that a graph-compatible factorization encodes a transformation path between the underlying graphs. Once such a factorization is available, the corresponding sequence of graph operations can be reconstructed explicitly. Moreover, every pivot operation may be replaced by the standard local-complementation identity

$$G \wedge uv = G * u * v * u.$$

Consequently, the recovery of local-complementation sequences reduces to the Normal-Matrix Factorization Problem. From this perspective, the principal unresolved difficulty is no longer the recognition of local equivalence, which is already settled by Bouchet's theory, but rather the existence and computational complexity of graph-compatible factorizations of normal-matrix witnesses.

Beyond this algorithmic aspect, the paper also investigates structural properties of local-complementation dynamics in the particular setting of undirected Paley graphs. For primes $p \equiv 1 \pmod 4$, the Paley graph P_p is the graph on vertex set $mathbbF_p$ in which two vertices x and y are adjacent whenever y-x is a quadratic residue modulo p. Paley graphs form a classical family of highly symmetric Cayley graphs possessing translation invariance, circulant adjacency matrices, and strong regularity properties. These symmetries make them a natural setting for studying local-equivalence phenomena.

In contrast with the directed Paley setting, where local-complementation dynamics exhibit a largely abelian structure and admit linear inversion techniques, the undirected case is substantially more intricate. Local complementations are generally noncommutative, and the associated stabilizer structures become considerably richer. Using the normal-matrix formalism arising from isotropic systems, we derive algebraic equations characterizing stabilizing transformations and reduce the stabilizer problem to systems of equations over $\mathbb{F}_2$.

Main contributions.

- The introduction of the *Normal-Matrix Factorization Problem* (NMFP), which isolates the algebraic obstacle separating Bouchet's recognition theory from the explicit recovery of transformation sequences.
- A reduction of the reconstruction version of the Equivalent Local Sequence Problem to the Normal-Matrix Factorization Problem. In particular, a graph-compatible factorization of a normal-matrix witness determines an explicit local-complementation sequence.

- Explicit formulas describing the action of normal matrices on isotropic representations and the resulting adjacency updates.
- A specialization of the normal-matrix framework to undirected Paley graphs, leading to algebraic equations characterizing stabilizing transformations.
- A complete analysis of the first undirected Paley graph P_5, together with a rigidity conjecture for Paley-graph stabilizers.

Bouchet's isotropic-system theory provides a complete algebraic characterization of local equivalence together with a polynomial-time recognition procedure. The present work does not modify this characterization. Rather, it investigates the additional algebraic structure required to pass from the existence of a normal-matrix witness to the explicit description of a transformation sequence. From this viewpoint, the Normal-Matrix Factorization Problem appears as a natural refinement of Bouchet's framework, situated at the interface between recognition and reconstruction.

Please verify the sections and then ref The paper is organized as follows. Section 2 develops the isotropic framework, introduces the Normal-Matrix Factorization Problem, and establishes the reduction from ELSP recovery to graph-compatible normal-matrix factorization. Section 3 studies stabilizers in the normal-matrix model and develops the corresponding algebraic theory. Section 4 specializes the analysis to undirected Paley graphs and presents the associated structural and computational results.

2. Conditional reconstruction of ELSP via normal-matrix factorization

2.1. *Preliminaries and definitions*

Let $G = (V, E)$ be a simple undirected graph with $|V| = n$. We denote by $A(G) \in \mathbb{F}_2^{n\times n}$ its adjacency matrix, which is symmetric with zero diagonal. All matrix operations are performed over the finite field $\mathbb{F}_2$. Basic algebraic properties of vector spaces over finite fields can be found in standard algebra texts such as [3].

Definition 2.1 (Local Complementation)**.** Let $v \in V$. The local complementation of G at v, denoted $G * v$, is the graph whose adjacency matrix satisfies

$$A(G * v)_{ij} = \begin{cases} A(G)_{ij} + A(G)_{iv}A(G)_{jv}, & i \neq j, \\ 0, & i = j. \end{cases}$$

Equivalently, the subgraph induced by the neighborhood $N(v)$ is replaced by its complement.

Proposition 2.2 (Involution)**.** *For every vertex $v \in V$,*

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

Proof. Applying the defining update twice adds the same rank-one matrix $A(G)_{\cdot v}A(G)_{\cdot v}^{\top}$ twice over $\mathbb{F}_2$, hence it cancels. The diagonal remains zero by definition. □

Definition 2.3 (Local Equivalence)**.** Two graphs G and H on the same vertex set are locally equivalent if there exists a finite sequence $v_1, \dots, v_k$ such that

$$H = G * v_1 * \cdots * v_k.$$

Definition 2.4 (Equivalent Local Sequence Problem (ELSP))**.** Given two simple undirected graphs G and H on the same labeled vertex set V, with the promise that G and H are locally equivalent, determine a sequence of vertices $(v_1, \dots, v_k) \in V^k$ such that $H = G * v_1 * \cdots * v_k$.

The sequence $(v_1, \dots, v_k)$ is called a *local-complementation realization* of the transformation from G to H.

Proposition 2.5 (Stabilizers and non-uniqueness of ELSP solutions)**.** *Let G and H be two locally equivalent graphs. Assume that $H = G * v_1 * \cdots * v_k$, for some sequence of vertices $(v_1, \dots, v_k)$.*

If the LC-stabilizer of H is nontrivial, then the transformation from G to H admits more than one local-complementation realization.

More precisely, for every sequence $(u_1, \dots, u_m) \in \mathrm{Stab}_{LC}(H)$, the concatenated sequence $(v_1, \dots, v_k, u_1, \dots, u_m)$, also transforms G into H.

Proof. Let

$$\sigma = (v_1, \dots, v_k),$$

be a local-complementation realization from G to H, and let

$$\tau = (u_1, \dots, u_m) \in \mathrm{Stab}_{LC}(H).$$

By definition of the stabilizer,

$$H * u_1 * \cdots * u_m = H.$$

Since

$$H = G * v_1 * \cdots * v_k,$$

we obtain

$$G * v_1 * \cdots * v_k * u_1 * \cdots * u_m = H * u_1 * \cdots * u_m = H.$$

Therefore the concatenated sequence

$$(v_1, \dots, v_k, u_1, \dots, u_m),$$

also transforms G into H, proving that it is another realization of the same local-equivalence transformation. □

The previous proposition shows that ELSP is generally not a uniqueness problem. Even when a sequence transforming G into H is known, additional solutions may be obtained by composing with elements of the LC-stabilizer of H. This observation motivates the study of stabilizers developed in Section 3.

2.2. Conditional reconstruction of ELSP via Bouchet's framework: an Isotropic-system formalization

We now present an algebraic formulation of local equivalence based on isotropic systems and normal matrices in the sense of Bouchet. This framework yields a polynomial-time recognition procedure and reduces the constructive version of ELSP to the Normal-Matrix Factorization Problem.

2.2.1. The ambient bilinear space. Let V be a finite vertex set with $|V|= n$. Fixing an ordering of V, we identify $\mathbb{F}_2^V \cong \mathbb{F}_2^n$ and consider

$$\mathcal{K} := \mathbb{F}_2^n \oplus \mathbb{F}_2^n \cong \mathbb{F}_2^{2n}.$$

Write elements of $\mathcal{K}$ as pairs (x, x') with $x, x' \in \mathbb{F}_2^n$. Define the bilinear form $\langle \cdot, \cdot \rangle$ on $\mathcal{K}$ by

$$\langle (x, x'), (y, y') \rangle := x \cdot y' + x' \cdot y,$$

where $\cdot$ denotes the usual dot product on $\mathbb{F}_2^n$. Equivalently,

$$\langle u, v \rangle = u \Lambda v^\top, \qquad \Lambda = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}.$$

Since we work in characteristic 2, we have $\langle u, u \rangle = 0$ for all u, so the form is alternating and nondegenerate.

Definition 2.6 (Isotropic system)**.** (Bouchet[1]). A subspace $W \subseteq \mathcal{K}$ is isotropic if

$$\langle w_1, w_2 \rangle = 0 \quad \text{for all } w_1, w_2 \in W.$$

An isotropic system is an isotropic subspace of dimension n.

2.2.2. Graphs as isotropic systems. Let G be a simple undirected graph on V and let $A = A(G)$. Consider the $n \times 2n$ matrix

$$[\, I_n \mid A \,].$$

Its row space is denoted by

$$W_G := \{\, x[\, I_n \mid A \,] : x \in \mathbb{F}_2^n \,\}.$$

Thus every element of W_G has the form (x, xA).

Proposition 2.7. *For every simple undirected graph G, the subspace W_G is an isotropic system.*

Proof. Since $[I_n|A]$ has rank n, one has $\dim(W_G) = n$.

Take two vectors in W_G:

$$(x, xA), \qquad (y, yA).$$

Then

$$\langle (x, xA), (y, yA) \rangle = x \cdot (yA) + (xA) \cdot y.$$

Because A is symmetric,

$$x \cdot (yA) = (xA) \cdot y.$$

Hence

$$\langle (x, xA), (y, yA) \rangle = 2(xA) \cdot y = 0 \quad \text{in } \mathbb{F}_2.$$

Therefore W_G is isotropic. □

2.2.3. Normal matrices and orthogonality. We next describe the class of linear transformations preserving isotropic systems.

Definition 2.8 (Normal matrix)**.** A matrix

$$M = \begin{pmatrix} Z & T \\ X & Y \end{pmatrix} \in \mathbb{F}_2^{2n \times 2n},$$

is called *normal* if X, Y, Z, T are diagonal $n \times n$ matrices and

$$YZ + XT = I_n.$$

Proposition 2.9. *If M is normal, then*

$$M \Lambda M^\top = \Lambda.$$

Hence M preserves the bilinear form.

Proof. Let

$$M = \begin{pmatrix} Z & T \\ X & Y \end{pmatrix}.$$

Then

$$M\Lambda = \begin{pmatrix} T & Z \\ Y & X \end{pmatrix},$$

so

$$M \Lambda M^\top = \begin{pmatrix} TZ + ZT & TX + ZY \\ YZ + XT & YX + XY \end{pmatrix}.$$

Since X, Y, Z, T are diagonal matrices, they commute. Over $\mathbb{F}_2$, the condition $YZ + XT = I_n$ gives the off-diagonal blocks, while the diagonal blocks vanish because $TZ + ZT = 0$ and $YX + XY = 0$. Thus

$$M \Lambda M^\top = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} = \Lambda.$$

□

2.2.4. Action on isotropic systems. If $W \subseteq \mathcal{K}$ is a subspace and M is a matrix, define

$$W \cdot M := \{\, wM : w \in W \,\}.$$

Proposition 2.10. *If W is isotropic and M is normal, then $W \cdot M$ is isotropic.*

Proof. For $w_1, w_2 \in W$,

$$\langle w_1 M, w_2 M \rangle = \langle w_1, w_2 \rangle.$$

Since W is isotropic, the claim follows. □

2.2.5. Local complementation as a normal-matrix action. We now relate local complementation to a distinguished normal matrix. Fix a vertex $i \in V$ and let E_i denote the diagonal $n \times n$ matrix with a 1 in position (i,i) and 0 elsewhere. Define

$$M_i^{LC} := \begin{pmatrix} I_n & 0 \\ E_i & I_n \end{pmatrix}.$$

It is normal, since $Z = I_n$, $T = 0$, $X = E_i$, $Y = I_n$ satisfy

$$YZ + XT = I_n.$$

Proposition 2.11 (Rigorous orthogonality of T_i)**.** *The transformation of $\mathcal{K}$ given by right multiplication by M_i^{LC} preserves the bilinear form $\langle \cdot, \cdot \rangle$. Equivalently, the map*

$$T_i : \mathcal{K} \to \mathcal{K}, \qquad T_i(w) = w M_i^{LC},$$

is an isometry of $(\mathcal{K}, \langle \cdot, \cdot \rangle)$.

Proof. This is an immediate consequence of the previous proposition, since M_i^{LC} is normal. Equivalently, one may verify directly that

$$M_i^{LC} \Lambda (M_i^{LC})^\top = \Lambda.$$

□

The following proposition explains how this action corresponds to local complementation of graphs.

Proposition 2.12. *Let G be a simple undirected graph on vertex set V, with adjacency matrix $A = A(G) \in \mathbb{F}_2^{n \times n}$, and let $i \in V$. Define*

$$M_i^{LC} = \begin{pmatrix} I_n & 0 \\ E_i & I_n \end{pmatrix},$$

where E_i is the diagonal matrix whose only nonzero entry is a 1 in position (i,i). Then there exists a (possibly looped) graph $\widetilde{G}$ such that

$$W_G \cdot M_i^{LC} = W_{\widetilde{G}}.$$

Moreover, if $A^\sharp$ denotes the adjacency matrix of $\widetilde{G}$, then

$$A^\sharp = A + AE_iA,$$

and its off-diagonal entries satisfy

$$A^\sharp_{jk} = A_{jk} + A_{ji}A_{ki} \qquad (j \neq k).$$

The off-diagonal part of $A^\sharp$ coincides with the adjacency matrix of the local complementation $G * i$. In particular, if the diagonal of $A^\sharp$ is removed, one obtains the adjacency matrix of $G * i$.

Proof. By definition,

$$W_G = \mathrm{RowSpace}\,([\,I_n \mid A\,]) \subseteq \mathbb{F}_2^n \oplus \mathbb{F}_2^n.$$

Therefore

$$W_G \cdot M_i^{LC} = \mathrm{RowSpace}\left([\,I_n \mid A\,]M_i^{LC}\right).$$

A direct block multiplication gives

$$[\,I_n \mid A\,]\begin{pmatrix} I_n & 0 \\ E_i & I_n \end{pmatrix} = [\,I_n + AE_i \mid A\,].$$

Set

$$N := I_n + AE_i.$$

We first show that N is invertible and that $N^{-1} = N$.

Since E_i has a single nonzero diagonal entry at (i,i), the matrix AE_i has only one possibly nonzero column, namely the ith column, and

$$(AE_i)_{jk} = A_{ji}\delta_{ik}.$$

In particular,

$$(AE_i)_{ik} = A_{ii}\delta_{ik} = 0,$$

because $A_{ii} = 0$ for a simple graph. Hence, for all j,k,

$$\left((AE_i)^2\right)_{jk} = \sum_{\ell=1}^{n}(AE_i)_{j\ell}(AE_i)_{\ell k} = (AE_i)_{ji}(AE_i)_{ik} = 0.$$

Thus $(AE_i)^2 = 0$, and since the field is $\mathbb{F}_2$,

$$N^2 = (I_n + AE_i)^2 = I_n + 2AE_i + (AE_i)^2 = I_n.$$

Therefore N is invertible and $N^{-1} = N$.

Since N is invertible, left multiplication by N^{-1} preserves the row space. Hence

$$\mathrm{RowSpace}\,([\,I_n + AE_i \mid A\,]) = \mathrm{RowSpace}\left(N^{-1}[\,I_n + AE_i \mid A\,]\right).$$

Using $N^{-1} = N$, we obtain

$$N^{-1}[\, I_n + AE_i \mid A\,] = [\, I_n \mid N^{-1}A\,] = [\, I_n \mid (I_n + AE_i)A\,].$$

Thus

$$W_G \cdot M_i^{LC} = \mathrm{RowSpace}\left([\, I_n \mid A^\sharp\,]\right), \qquad A^\sharp := (I_n + AE_i)A = A + AE_iA.$$

We now compute the entries of $A^\sharp$. For $j, k \in V$,

$$(AE_iA)_{jk} = \sum_{r,s=1}^{n} A_{jr}(E_i)_{rs}A_{sk}.$$

Since E_i vanishes except at (i, i), the only surviving term is $r = s = i$, and so

$$(AE_iA)_{jk} = A_{ji}A_{ik}.$$

Therefore

$$A^\sharp_{jk} = A_{jk} + A_{ji}A_{ik}.$$

Because A is symmetric, $A_{ik} = A_{ki}$, so for $j \neq k$,

$$A^\sharp_{jk} = A_{jk} + A_{ji}A_{ki},$$

which is exactly the local-complementation update formula at the vertex i.

For the diagonal entries, we have

$$A^\sharp_{jj} = A_{jj} + A_{ji}A_{ij} = 0 + A_{ji}^2 = A_{ji},$$

since $A_{jj} = 0$ and $x^2 = x$ in $\mathbb{F}_2$. Thus $A^\sharp$ may have nonzero diagonal entries, and hence corresponds to a looped graph.

Since $A^\sharp$ is symmetric, it defines a (possibly looped) graph $\widetilde{G}$, and we set

$$W_{\widetilde{G}} := \mathrm{RowSpace}\left([\, I_n \mid A^\sharp\,]\right).$$

Therefore,

$$W_G \cdot M_i^{LC} = W_{\widetilde{G}}.$$

Finally, define a matrix $\widetilde{A}$ by removing the diagonal of $A^\sharp$:

$$\widetilde{A}_{jk} = \begin{cases} A^\sharp_{jk}, & j \neq k, \\ 0, & j = k. \end{cases}$$

Then $\widetilde{A}$ is symmetric with zero diagonal, and for $j \neq k$,

$$\widetilde{A}_{jk} = A_{jk} + A_{ji}A_{ki}.$$

Hence $\widetilde{A}$ is exactly the adjacency matrix of the simple graph $G * i$.

This proves the result. $\square$

Remark 2.13. Proposition 2.11 shows that the action of the elementary normal matrix M_i^{LC} naturally produces a symmetric matrix $A^\sharp = A + AE_iA$ whose off-diagonal entries satisfy the local-complementation update formula at the vertex i. In general, the diagonal entries of $A^\sharp$ need not vanish, so the resulting matrix corresponds to a possibly looped graph. Consequently, $W_G \cdot M_i^{LC} = W_{\widetilde{G}}$ holds in the category of looped graphs rather than in the category of simple graphs. The simple graph $G * i$ is recovered by deleting the diagonal of $A^\sharp$. Throughout the sequel, whenever a normal-matrix action produces a symmetric matrix with nonzero diagonal, its zero-diagonal normalization is understood as the associated simple graph.

Proposition 2.14 (Compatibility of diagonal normalization)**.** *Let*

$$A^\sharp = A + AE_iA,$$

be the symmetric matrix obtained in Proposition 2.12, and let

$$\widetilde{A},$$

be the matrix obtained from $A^\sharp$ by replacing its diagonal entries by zero:

$$\widetilde{A}_{jk} = \begin{cases} A^\sharp_{jk}, & \textit{if } j \neq k, \\ 0, & \textit{if } j = k. \end{cases}$$

Then $A^\sharp$ and $\widetilde{A}$ have the same off-diagonal entries. Moreover, the local-complementation update on simple graphs depends only on off-diagonal entries. Hence replacing $A^\sharp$ by $\widetilde{A}$ after the normal-matrix action does not change the simple graph obtained by local complementation, nor any subsequent local-complementation computation performed after zero-diagonal normalization.

Proof. By definition, $A^\sharp$ and $\widetilde{A}$ differ only on the diagonal.

For $j \neq k$, the local-complementation update formula is

$$A(G * v)_{jk} = A(G)_{jk} + A(G)_{jv}A(G)_{kv}.$$

The entries appearing in this formula are

$$A(G)_{jk}, \qquad A(G)_{jv}, \qquad A(G)_{kv}.$$

,

Since $j \neq k$, and since v is fixed, these are off-diagonal entries except in the harmless cases $j = v$ or $k = v$, where the factor $A(G)_{vv}$ is not used because edges incident with v are unchanged under local complementation at v.

Thus the diagonal entries produced in $A^\sharp$ do not affect the off-diagonal adjacency matrix of the simple graph. Therefore replacing $A^\sharp$ by its zero-diagonal normalization $\widetilde{A}$ is compatible with the subsequent local-complementation dynamics on simple graphs. □

2.2.6. Bouchet's equivalence criterion and constructive extraction. Bouchet's isotropic-system theory provides a complete algebraic characterization of local equivalence through the action of normal matrices on isotropic systems.

Theorem 2.15 (Bouchet's isotropic characterization [1])**.** *Let G and H be simple undirected graphs on the same vertex set V. Then G and H are locally equivalent if and only if there exists a normal matrix M such that*

$$W_H = W_G \cdot M.$$

Moreover, the existence of such a matrix can be decided in polynomial time.

The previous theorem is a recognition result. It determines whether two graphs belong to the same local-equivalence class by exhibiting a normal matrix relating their isotropic systems. However, it does not directly provide a sequence of local complementations transforming G into H. Since the ELSP is a search problem, an additional constructive ingredient is required.

Definition 2.16 (Elementary factors)**.** Let G be a simple graph on a vertex set (V).

(a) A *local-complementation factor* at a vertex $v \in V$ is the normal matrix

$$M_v^{LC} = \begin{pmatrix} I_n & 0\, E_v & I_n \end{pmatrix},$$

where (E_v) denotes the diagonal matrix having a single (1) in position (v) and zeros elsewhere.

Its action on isotropic representations satisfies

$$W_{G*v} = W_G \cdot M_v^{LC}.$$

(b) A *pivot factor* associated with an edge $(uv \in E(G))$ is an elementary factor whose graph-theoretic action is the pivot operation $G \longmapsto G \wedge uv$.

The edge (uv) is required to be an edge of the *current graph* at the stage where the factor is applied.

In the present work, pivot factors are used only through their graph-theoretic action in graph-compatible factorizations. An explicit normal-matrix representation of pivot factors is not required for the reduction theorem proved below.

An elementary factor is therefore either a local-complementation factor or a pivot factor. The role of a graph-compatible factorization is to encode a sequence of elementary graph operations transforming one graph into another. In particular, the reconstruction procedure depends only on the graph-theoretic interpretation of the factors and not on an explicit matrix representation of pivot operations.

Remark 2.17 (Role of pivot factors)**.** The reduction theorem established below relies only on the graph-theoretic interpretation of pivot factors. The key property is the classical identity

$$G \wedge uv = G * u * v * u.[1]$$

which allows every pivot factor occurring in a graph-compatible factorization to be replaced by a bounded-length local-complementation word. Consequently, the reconstruction procedure ultimately produces a sequence expressed entirely in terms of local complementations.

Definition 2.18 (Graph-compatible factorization)**.** Let

$$W_H = W_G \cdot M,$$

be a normal-matrix witness of local equivalence.

A factorization

$$M = M_1 M_2 \cdots M_t,$$

is called *graph-compatible* if there exists a sequence of graphs

$$G = G_0, G_1, \ldots, G_t = H,$$

such that, for each i,

- either $M_i = M_v^{LC}$ for some vertex $v \in V(G_{i-1})$, and

$$G_i = G_{i-1} * v,$$

- or M_i is a pivot factor acting on an edge $uv \in E(G_{i-1})$, in which case

$$G_i = G_{i-1} \wedge uv.$$

The Normal-Matrix Factorization Problem. Let G and H be locally equivalent simple graphs on the same vertex set V, where $|V| = n$. By Bouchet's characterization, there exists a normal matrix

$$M \in N(n),$$

such that

$$W_H = W_G \cdot M.$$

The central algebraic problem addressed in this work is the following.

Normal-Matrix Factorization Problem (NMFP). Given a normal matrix $M \in N(n)$ satisfying

$$W_H = W_G \cdot M,$$

determine whether one can compute a factorization

$$M = M_1 M_2 \cdots M_t,$$

where t is bounded by a polynomial in n, and where each factor M_s corresponds to an elementary graph operation performed on the current graph.

More precisely, the factorization must induce a sequence of graphs

$$G = G_0,\ G_1,\ \ldots,\ G_t = H,$$

such that, for every $s \in \{1, \dots, t\}$,

$$W_{G_s} = W_{G_{s-1}} \cdot M_s.$$

Each factor M_s is required to admit a graph-theoretic interpretation: either

$$G_s = G_{s-1} * v,$$

for some vertex $v \in V$, or

$$G_s = G_{s-1} \wedge uv,$$

where uv is an edge of the graph G_{s-1}.

Thus the objective is not merely to decompose M as a product of matrices, but to construct a factorization whose successive factors are compatible with the evolving graph structure and collectively realize a transformation path from G to H. The fundamental question is whether such a graph-compatible factorization can be computed in polynomial time.

Remark 2.19 (Normal-matrix factorization as the central open problem)**.** Bouchet's characterization theorem guarantees the existence of a normal matrix

$$M \in N(n),$$

satisfying

$$W_H = W_G \cdot M,$$

whenever G and H are locally equivalent. Thus the recognition problem for local equivalence is already understood.

The additional information required for a constructive recovery of a transformation sequence is encoded in the Normal-Matrix Factorization Problem introduced above. Indeed, once a graph-compatible factorization

$$M = M_1 \cdots M_t,$$

is available, the corresponding sequence of local complementations and pivot operations can be reconstructed directly from the elementary factors.

Consequently, the principal unresolved issue is not the existence of a normal-matrix witness, but the computational complexity of obtaining a graph-compatible factorization. In this sense, the Normal-Matrix Factorization Problem may be viewed as the algebraic bottleneck underlying constructive approaches to local equivalence.

At present, no general polynomial-time algorithm for the Normal-Matrix Factorization Problem is known. Thus, although Bouchet's theory provides a polynomial-time recognition procedure for local equivalence, the complexity status of graph-compatible normal-matrix factorization remains open. Determining whether such factorizations can be computed efficiently is therefore a central problem in the constructive theory of local equivalence.

Proposition 2.20 (Injectivity of the isotropic representation). *Let G and H be simple graphs on the same vertex set. If*

$$W_G = W_H,$$

then

$$G = H.$$

Proof. Write

$$W_G = \mathrm{RowSpace}([I_n \mid A(G)]), \qquad W_H = \mathrm{RowSpace}([I_n \mid A(H)]).$$

Assume that $W_G = W_H$. Then there exists an invertible matrix P such that

$$[I_n \mid A(G)] = P[I_n \mid A(H)].$$

Comparing the left blocks gives

$$P = I_n.$$

Hence

$$A(G) = A(H),$$

and therefore

$$G = H.$$

□

Theorem 2.21 (Reduction from normal-matrix factorization to ELSP recovery). *Let G and H be locally equivalent simple graphs on the same vertex set V. Let*

$$W_H = W_G \cdot M,$$

for some normal-matrix witness M.

Suppose that M admits a graph-compatible factorization

$$M = M_1 M_2 \cdots M_t,$$

where t is bounded by a polynomial in $|V|$, and where each factor M_s corresponds to an elementary graph operation on the current graph, namely either a local complementation or a pivot operation.

Then one can compute in polynomial time a sequence of vertices

$$(v_1, \dots, v_k),$$

such that

$$H = G * v_1 * \cdots * v_k.$$

Proof. Let

$$W_H = W_G \cdot M,$$

and suppose that a graph-compatible factorization

$$M = M_1 M_2 \cdots M_t,$$

is available.

By definition of graph-compatible factorization, there exists a sequence of graphs

$$G = G_0,\ G_1,\ \ldots,\ G_t,$$

such that, for every $s \in \{1, \ldots, t\}$,

$$W_{G_s} = W_{G_{s-1}} \cdot M_s,$$

and each factor M_s corresponds either to a local complementation or to a pivot operation on the current graph G_{s-1}.

Iterating the above identities yields

$$W_{G_t} = W_G \cdot (M_1 M_2 \cdots M_t) = W_G \cdot M = W_H.$$

By Proposition 2.20, the correspondence

$$X \longmapsto W_X,$$

is injective on simple graphs. Consequently,

$$W_{G_t} = W_H,$$

implies

$$G_t = H.$$

We have therefore obtained a transformation path from G to H consisting of local complementations and pivot operations.

By the pivot identity established in Section 2.3,

$$G \wedge uv = G * u * v * u.$$

Replacing each pivot occurring in the transformation path by the corresponding local-complementation word produces a sequence of vertices

$$(v_1, \ldots, v_k),$$

satisfying

$$H = G * v_1 * \cdots * v_k.$$

Let t_v and t_p denote respectively the numbers of local complementations and pivots occurring in the factorization. Then

$$k = t_v + 3t_p \leq 3(t_v + t_p) = 3t.$$

Since t is bounded by a polynomial in $|V|$, the length of the recovered local-complementation sequence is also polynomially bounded. Moreover, the replacement of each pivot by the word

$$*u * v * u,$$

requires only constant time. Hence the reconstruction procedure runs in polynomial time.

Therefore, once a graph-compatible factorization of the normal-matrix witness is available, an explicit local-complementation sequence transforming G into H can be recovered in polynomial time. □

Remark 2.22 (Recognition versus reconstruction)**.** The theorem establishes a bridge between Bouchet's recognition theory and the reconstruction version of the Equivalent Local Sequence Problem. Bouchet's theorem provides a normal-matrix witness certifying local equivalence, whereas a graph-compatible factorization of this witness supplies the additional information required to recover an explicit transformation sequence.

Consequently, within the normal-matrix framework, the reconstruction problem reduces to the Normal-Matrix Factorization Problem. Suppose that a graph-compatible factorization of polynomial length is available, then the corresponding local-complementation sequence can be recovered in polynomial time.

The recovered sequence is generally not unique. Distinct local-complementation words may induce the same transformation on a fixed graph, and different graph-compatible factorizations of the same normal-matrix witness may lead to different reconstruction sequences. Thus the ELSP should be viewed as a search problem rather than a uniqueness problem. This non-uniqueness motivates the stabilizer analysis developed in the next section.

Example 2.23 (Reconstruction from a graph-compatible factorization)**.** The purpose of this example is not to solve the Normal-Matrix Factorization Problem, but rather to illustrate the reconstruction procedure of Theorem 2.21 once a graph-compatible factorization has been obtained.

Let

$$G = P_{13},$$

the undirected Paley graph on the vertex set

$$\mathbb{F}_{13} = \{0, 1, \ldots, 12\}.$$

Suppose that a graph-compatible factorization of a normal-matrix witness

$$W_H = W_G \cdot M,$$

has been obtained in the form

$$M = M_1 M_2 M_3,$$

where

- $M_1 = M_2^{LC}$ is the elementary factor corresponding to local complementation at the vertex 2;
- M_2 is a pivot factor acting on the edge 13 of the current graph;
- $M_3 = M_4^{LC}$ is the elementary factor corresponding to local complementation at the vertex 4.

The reconstruction procedure reads the elementary factors from left to right and applies the corresponding graph operations.

Set

$$G_0 = G = P_{13}.$$

Step 1. The first factor is $M_1 = M_2^{LC}$. Applying local complementation at vertex 2 gives

$$G_1 = G_0 * 2.$$

Step 2. The second factor is the pivot factor M_2. Since the edge 13 is assumed to be present in the current graph G_1, the corresponding operation is a pivot on this edge:

$$G_2 = G_1 \wedge 13.$$

Step 3. The final factor is $M_3 = M_4^{LC}$. Applying local complementation at vertex 4 yields

$$G_3 = G_2 * 4.$$

Since $G_3 = H$, we obtain

$$H = ((G * 2) \wedge 13) * 4.$$

Consequently, the graph-compatible factorization determines the transformation sequence

$$G \longrightarrow G * 2 \longrightarrow (G * 2) \wedge 13 \longrightarrow ((G * 2) \wedge 13) * 4.$$

To express the transformation entirely in terms of local complementations, we use the classical pivot identity

$$G \wedge uv = G * u * v * u,$$

(see Bouchet [1]). Applying this identity to the pivot on the edge 13, we obtain

$$(G * 2) \wedge 13 = (G * 2) * 1 * 3 * 1.$$

Substituting this expression into the previous sequence gives

$$H = G * 2 * 1 * 3 * 1 * 4.$$

Hence the graph-compatible factorization

$$M = M_1 M_2 M_3,$$

is converted into the explicit local-complementation sequence

$$(2, 1, 3, 1, 4).$$

Equivalently,

$$W_H = W_G \cdot M_1 M_2 M_3.$$

This example illustrates the reconstruction stage of Theorem 2.21. Once a graph-compatible factorization is available, each elementary factor is translated into a graph operation, and every pivot factor is replaced by the equivalent local-complementation word. The resulting sequence is therefore expressed entirely in terms of local complementations.

Remark 2.24. This example contains both a local-complementation factor and a pivot factor. In general, a graph-compatible factorization of a normal-matrix witness may contain both local-complementation factors and pivot factors. The reconstruction procedure processes the elementary factors in order. Whenever a pivot factor corresponding to an edge uv of the current graph appears, it is replaced by the standard local-complementation word

$$G \wedge uv = G * u * v * u.$$

Thus every graph-compatible factorization gives rise to a transformation sequence expressed entirely in terms of local complementations.

2.2.7. Complexity. *Complexity of Bouchet's recognition procedure.* Bouchet's algorithm [1] reduces the recognition of local equivalence to a sequence of linear-algebraic transformations on matrices over $\mathbb{F}_2$. The principal computational tasks consist of Gaussian elimination, rank computations, and elementary row operations on matrices of size $n \times n$.

Using standard implementations of Gaussian elimination [4], these operations require $O(n^3)$ time. Since the recognition procedure performs only a polynomial number of such linear-algebraic operations, the overall running time remains polynomial in n.

Length of the recovered local-complementation sequence. Let

$$M = M_1 M_2 \cdots M_t,$$

be a graph-compatible factorization of a normal-matrix witness of local equivalence between G and H, where each factor M_s corresponds either to a local complementation or to a pivot operation on the current graph. Assume that t is bounded by a polynomial in n.

The sequence of elementary factors determines a corresponding sequence of graph operations transforming G into H. Moreover, each pivot operation on an edge uv can be replaced by the standard local-complementation word

$$G \wedge uv = G * u * v * u,$$

which has constant length three.

Let t_v and t_p denote respectively the numbers of local complementations and pivots appearing in the factorization. The length k of the resulting local-complementation sequence satisfies

$$k = t_v + 3t_p \leq 3(t_v + t_p) = 3t.$$

Consequently, if t is polynomially bounded, then the recovered local-complementation sequence is also polynomially bounded.

It is important to emphasize that the essential requirement is not merely the existence of a factorization of the normal matrix M, but the existence of a graph-compatible factorization in which each factor admits a valid interpretation as an elementary graph operation at the stage where it is applied.

Overall complexity of the reconstruction procedure. Suppose that a graph-compatible factorization

$$M = M_1 \cdots M_t,$$

of a normal-matrix witness

$$W_H = W_G \cdot M,$$

is available and that t is polynomially bounded in n.

The reconstruction procedure processes the elementary factors in order. Each local complementation factor contributes one vertex to the output sequence, while each pivot factor is replaced by the equivalent local-complementation word

$$*u * v * u.$$

This replacement introduces only constant overhead.

Therefore the recovery of an explicit local-complementation sequence from a graph-compatible factorization can be carried out in polynomial time. In particular, once a solution to the Normal-Matrix Factorization Problem is available, the corresponding transformation sequence between two locally equivalent graphs can be recovered efficiently.

This shows that, within the normal-matrix framework, the constructive component of the Equivalent Local Sequence Problem reduces to the Normal-Matrix Factorization Problem.

2.3. Pivot operations and reduction to pure local complementations

In the constructive procedure, the isotropic recognition algorithm may produce pivot operations. To obtain a solution to ELSP entirely in terms of local complementations, we now give an algebraic treatment of pivots and show that each pivot can be replaced by a bounded-length LC sequence.

Remark on the pivot identity. The identity

$$G \wedge uv = G * u * v * u,$$

is classical. The calculation below verifies it directly on the adjacency matrix.

Block decomposition of the adjacency matrix. Let G be a simple undirected graph on vertex set V, with adjacency matrix $A(G)$ over $\mathbb{F}_2$.

Let $u, v \in V$ be distinct adjacent vertices, so $A_{uv} = A_{vu} = 1$. Reorder vertices so that the first two are u, v, and let

$$R := V \setminus \{u, v\}.$$

With respect to the decomposition $V = \{u, v\} \cup R$, write

$$A(G) = \begin{pmatrix} 0 & 1 & \alpha^\top \\ 1 & 0 & \beta^\top \\ \alpha & \beta & B \end{pmatrix},$$

where

- $\alpha \in \mathbb{F}_2^{|R|}$ with entries $\alpha_x = A_{ux}$,
- $\beta \in \mathbb{F}_2^{|R|}$ with entries $\beta_x = A_{vx}$,
- B is the adjacency matrix of the induced subgraph $G[R]$.

Because G is simple and undirected, B is symmetric with zero diagonal.

Definition of Pivot on uv. Since

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

is invertible over $\mathbb{F}_2$, the principal pivot transform on $\{u, v\}$ is defined [12]. The resulting adjacency matrix is

$$A(G \wedge uv) = \begin{pmatrix} 0 & 1 & \beta^\top \\ 1 & 0 & \alpha^\top \\ \beta & \alpha & B + \alpha\beta^\top + \beta\alpha^\top \end{pmatrix}.$$

Interpretation. Pivot on uv:

(a) swaps the neighborhoods of u and v outside $\{u, v\}$,

(b) toggles adjacency between $x, y \in R$ precisely when

$$\alpha_x\beta_y + \beta_x\alpha_y = 1.$$

Local Complementation Formula in Coordinates. For any vertex w, local complementation at w changes adjacency according to

$$A(G * w)_{xy} = A(G)_{xy} + A(G)_{xw}A(G)_{yw} \qquad (x \neq y).$$

Step-by-step computation of $G * u * v * u$. We start from

$$A(G) = \begin{pmatrix} 0 & 1 & \alpha^\top \\ 1 & 0 & \beta^\top \\ \alpha & \beta & B \end{pmatrix}.$$

After applying local complementation at u, the vector α remains unchanged, while the neighborhood vector of v outside $\{u, v\}$ becomes $\beta + \alpha$. The $R \times R$ block becomes

$$B + \alpha\alpha^\top.$$

Thus

$$A(G * u) = \begin{pmatrix} 0 & 1 & \alpha^\top \\ 1 & 0 & (\beta+\alpha)^\top \\ \alpha & \beta+\alpha & B + \alpha\alpha^\top \end{pmatrix},$$

up to the zero-diagonal convention.

Now apply local complementation at v. At this stage, the neighborhood vector of v outside $\{u, v\}$ is $\beta + \alpha$. Hence the $R \times R$ block becomes

$$B + \alpha\alpha^\top + (\beta+\alpha)(\beta+\alpha)^\top.$$

Moreover, since u is adjacent to v, the neighborhood vector of u outside $\{u, v\}$ becomes

$$\alpha + (\beta + \alpha) = \beta.$$

Finally apply local complementation at u. At this stage, the neighborhood vector of u outside $\{u, v\}$ is β. Hence the $R \times R$ block becomes

$$\begin{aligned} B^{(3)} &= B + \alpha\alpha^\top + (\beta+\alpha)(\beta+\alpha)^\top + \beta\beta^\top \\ &= B + \alpha\beta^\top + \beta\alpha^\top. \end{aligned}$$

The neighborhood vector of v outside $\{u, v\}$ becomes

$$(\beta + \alpha) + \beta = \alpha.$$

Therefore

$$A(G * u * v * u) = \begin{pmatrix} 0 & 1 & \beta^\top \\ 1 & 0 & \alpha^\top \\ \beta & \alpha & B + \alpha\beta^\top + \beta\alpha^\top \end{pmatrix},$$

after resetting diagonal entries to zero. This is exactly the adjacency matrix of $G \wedge uv$. Hence

$$G \wedge uv = G * u * v * u.$$

Lemma 2.25 (Neighborhood swap under the word $*u*v*u$)**.** *Let G be a simple undirected graph on vertex set V and let $u, v \in V$ be adjacent. Define*

$$G' := G * u * v * u.$$

Then for every vertex $x \in V \setminus \{u, v\}$,

$$A(G')_{ux} = A(G)_{vx} \qquad \textit{and} \qquad A(G')_{vx} = A(G)_{ux}.$$

Equivalently,

$$N_{G'}u \setminus \{v\} = N_G v \setminus \{u\}, \qquad N_{G'}(v) \setminus \{u\} = N_G u \setminus \{v\}.$$

Proof. Write a_{ij} for the entries of $A(G)$, and let $a_{ij}^{(1)}$, $a_{ij}^{(2)}$, $a_{ij}^{(3)}$ denote the entries after the successive operations $*u$, then $*v$, then $*u$.

Fix $x \in V \setminus \{u, v\}$ and set

$$\alpha := a_{ux}, \qquad \beta := a_{vx}.$$

Since uv is an edge,

$$a_{uv} = 1.$$

Step 1: Apply $*u$. Edges incident to u are unchanged, so

$$a_{ux}^{(1)} = \alpha, \qquad a_{uv}^{(1)} = 1.$$

Also

$$a_{vx}^{(1)} = a_{vx} + a_{vu}a_{xu} = \beta + 1 \cdot \alpha = \beta + \alpha.$$

Step 2: Apply $*v$. Edges incident to v are unchanged, hence

$$a_{vx}^{(2)} = \beta + \alpha, \qquad a_{uv}^{(2)} = 1.$$

Now

$$a_{ux}^{(2)} = a_{ux}^{(1)} + a_{uv}^{(1)}a_{xv}^{(1)} = \alpha + 1 \cdot (\beta + \alpha) = \beta.$$

Step 3: Apply $*u$ again. Edges incident to u are unchanged, so

$$a_{ux}^{(3)} = \beta.$$

Finally,

$$a_{vx}^{(3)} = a_{vx}^{(2)} + a_{vu}^{(2)}a_{xu}^{(2)} = (\beta + \alpha) + 1 \cdot \beta = \alpha.$$

Therefore

$$A(G')_{ux} = a_{ux}^{(3)} = \beta = A(G)_{vx}, \qquad A(G')_{vx} = a_{vx}^{(3)} = \alpha = A(G)_{ux}.$$

This proves the claim. □

2.4. Specialization to undirected paley graphs

Paley graphs provide a natural setting for studying local complementation because their adjacency matrices exhibit strong algebraic symmetry. In particular, they are Cayley graphs over the additive group of $\mathbb{F}_p$ and their adjacency matrices are circulant. This structure gives translation invariance and uniform local neighborhoods.

For ELSP, such symmetry offers a controlled setting in which the interaction between local operations and global structure can be analyzed explicitly. We now specialize the general framework to undirected Paley graphs.

2.4.1. Algebraic definition. Let p be a prime such that

$$p \equiv 1 \pmod 4.$$

Let $\mathbb{F}_p$ denote the finite field with p elements, and let

$$Q = \{x^2 : x \in \mathbb{F}_p^\times\} \subset \mathbb{F}_p^\times,$$

be the set of nonzero quadratic residues.

Define

$$A_{xy} = \begin{cases} 1, & x \neq y \text{ and } y - x \in Q, \\ 0, & \text{otherwise.} \end{cases}$$

Definition 2.26. The undirected Paley graph P_p is the simple graph on vertex set $\mathbb{F}_p$ with adjacency matrix $A = (A_{xy})$ defined above.

Symmetry condition. Because $p \equiv 1 \pmod 4$, one has $-1 \in Q$, so

$$y - x \in Q \iff x - y \in Q.$$

Hence the adjacency matrix is symmetric.

2.4.2. Cayley Structure and Translation Invariance. The Paley graph is the Cayley graph

$$P_p = \mathrm{Cay}(\mathbb{F}_p, Q).$$

Therefore:

- for every $a \in \mathbb{F}_p$, the translation $T_a(x) = x + a$ is an automorphism;
- the adjacency matrix is circulant:

$$A_{xy} = f(y - x),$$

  for a fixed function f;
- all vertices have the same local structure.

In particular, P_p is vertex-transitive.

2.4.3. Strong regularity and intersection numbers. Paley graphs are strongly regular [2].

Proposition 2.27. *P_p is strongly regular with parameters*

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

Consequences.

- Every vertex has degree $\frac{p-1}{2}$.
- Any two adjacent vertices share exactly $\frac{p-5}{4}$ neighbors.
- Any two nonadjacent vertices share exactly $\frac{p-1}{4}$ neighbors.

2.4.4. Explicit effect of local complementation on P_p. Fix a vertex $u \in \mathbb{F}_p$. Its neighborhood is

$$Nu = \{u + q : q \in Q\}.$$

Local complementation at u toggles adjacency among all pairs of vertices in Nu. Thus, for $x, y \in \mathbb{F}_p \setminus \{u\}$,

$$A(P_p * u)_{xy} = A(P_p)_{xy} + \mathbf{1}_{\{x,y \in Nu\}}.$$

Equivalently, edges between two quadratic shifts of u are complemented, while all other adjacencies remain unchanged.

Important observation. Since $|Nu| = \frac{p-1}{2}$, local complementation modifies

$$\binom{(p-1)/2}{2}$$

edges, so the transformation is highly nontrivial for large p.

2.4.5. Noncommutativity of Local Complementations. In the directed Paley case, local complementations commute, yielding an abelian action. In contrast, the undirected Paley graph generally exhibits noncommutative local-complementation dynamics. The next proposition establishes this phenomenon by exhibiting an explicit edge whose final adjacency depends on the order in which two adjacent local complementations are applied.

Proposition 2.28 (Noncommutativity of local complementations in the undirected Paley case)**.** *Let $(p \equiv 1 \pmod 4)$ be prime, and let P_p be the undirected Paley graph on $(\mathbb{F}_p)$. If $(u, v \in \mathbb{F}_p)$ are adjacent, then $P_p * u * v \neq P_p * v * u$.*

Proof. Let (A) be the adjacency matrix of P_p. Since$u$ and(v) are adjacent, we have $A_{uv} = A_{vu} = 1$. Moreover, P_p has degree $((p-1)/2)$. Since $(p \geq 5)$, this degree is at least (2). Hence, there exists a vertex $x \in N_{P_p} u \setminus v$. Set $\alpha = A_{ux}, \qquad \beta = A_{vx}$. By the choice of (x), we have $(\alpha = 1)$.

We compare the final adjacency of the edge (ux) after the two words $(*u * v)$ and $(*v * u)$.

First consider $P_p * u * v$. Local complementation at u does not change edges incident with u, but it changes the edge (vx) as follows:

$$\begin{aligned} A^{(1)}_{vx} &= A_{vx} + A_{vu} A_{ux} \\ &= \beta + 1 \cdot \alpha \\ &= \beta + \alpha. \end{aligned}$$

Now applying local complementation at (v), the edge (ux) becomes

$$\begin{aligned} A^{(2)}_{ux} &= A_{ux} + A_{uv} A^{(1)}_{vx} \\ &= \alpha + 1 \cdot (\beta + \alpha) \\ &= \beta. \end{aligned}$$

Thus, in $P_p * u * v$, the final adjacency of (ux) is (β).

Conversely, consider $P_p * v * u$. After applying local complementation at (v), the edge (ux) becomes

$$\begin{aligned}\widetilde{A}^{(1)}_{ux} &= A_{ux} + A_{uv}A_{vx}\\ &= \alpha + \beta.\end{aligned}$$

The subsequent local complementation at u does not change edges incident with u. Hence, in $P_p * v * u$, the final adjacency of (ux) is

$$\widetilde{A}^{(2)}_{ux} = \alpha + \beta.$$

Since $(\alpha = 1)$, we have $\beta \neq \alpha + \beta$, over

$$\mathbb{F}_2.$$

Therefore the edge (ux) has different final adjacency in $P_p * u * v$ and $P_p * v * u$. Hence $P_p * u * v \neq P_p * v * u$. □

Thus, the LC action is non-abelian.

2.4.6. Constructive ELSP in the Paley Case. We emphasize that Bouchet's original recognition algorithm guarantees the existence of such a normal matrix M, but does not explicitly provide a factorization into elementary factors. The following theorem isolates the additional constructive hypothesis required to recover an explicit sequence of graph operations.

Theorem 2.29. *Let H be a simple graph on $\mathbb{F}_p$ locally equivalent to the undirected Paley graph P_p.*

Suppose that a graph-compatible factorization of a normal-matrix witness

$$W_H = W_{P_p} \cdot M,$$

is available and has length polynomial in p.

Then one can compute in polynomial time an explicit sequence of vertices

$$(v_1, \ldots, v_k),$$

such that

$$H = P_p * v_1 * \cdots * v_k.$$

Proof. Since H is locally equivalent to P_p, Bouchet's theorem guarantees the existence of a normal matrix

$$M \in N(p),$$

satisfying

$$W_H = W_{P_p} \cdot M.$$

Assume that a graph-compatible factorization

$$M = M_1 M_2 \cdots M_t,$$

is available, where t is polynomially bounded in p and each factor corresponds either to a local complementation or to a pivot operation on the current graph.

Applying Theorem 2.21 to the pair (P_p, H), the factorization determines a transformation path

$$P_p = G_0,\ G_1,\ \dots,\ G_t = H.$$

Each local-complementation factor contributes one vertex to the recovered sequence. Whenever a pivot operation occurs, it is replaced by the equivalent local-complementation word

$$G \wedge uv = G * u * v * u.$$

Consequently, the transformation path can be rewritten entirely in terms of local complementations, yielding a sequence of vertices

$$(v_1, \dots, v_k),$$

such that

$$H = P_p * v_1 * \cdots * v_k.$$

Since the factorization has polynomial length and each pivot replacement introduces only constant overhead, the reconstruction procedure runs in polynomial time. □

2.4.7. Structural implications for orbit and stabilizer. Define

$$\mathrm{Orb} P_p = \{P_p * \sigma : \sigma \in \Gamma\},$$

where Γ is the LC-generated group, and

$$\mathrm{Stab} P_p = \{\sigma \in \Gamma : P_p * \sigma = P_p\}.$$

Although P_p has a large automorphism group induced by translations of $\mathbb{F}_p$, this does not automatically yield nontrivial stabilizing words in the LC-generated group. Determining the stabilizer therefore reduces to solving the algebraic equations derived below.

3. Stabilizer of the undirected paley graph under local complementation

Having developed the normal-matrix formalism for describing local equivalence, we now investigate the corresponding stabilizer structures.

Let

$$V^* := \bigcup_{k \geq 0} V^k,$$

denote the set of all finite words over the vertex set V.

For a word

$$\sigma = (v_1, \dots, v_k) \in V^*,$$

we define

$$G * \sigma := G * v_1 * \cdots * v_k.$$

Definition 3.1 (LC-stabilizer of a graph)**.** Let G be a simple undirected graph on V. The *LC-stabilizer* of G is defined by

$$\mathrm{Stab}_{LC}(G) := \{\sigma \in V^* : \ G * \sigma = G\}.$$

Every word $\sigma = (v_1, \ldots, v_k) \in V^*$ determines an element

$$\tau_\sigma := \tau_{v_k} \circ \cdots \circ \tau_{v_1} \in \Gamma_{LC}.$$

Different words may induce the same element of Γ_{LC}.

We now give an algebraic description of the stabilizer of the undirected Paley graph P_p under the action generated by local complementations.

Bouchet's isotropic-system formalism associates a normal matrix with every finite sequence of local complementations. Consequently, stabilizing local-complementation words give rise to normal matrices that fix the associated isotropic system. This observation reduces the study of local-complementation stabilizers to an algebraic problem involving normal matrices over $\mathbb{F}_2$.

3.1. The local-complementation action and the stabilizer

Let V be a vertex set of size n and let $\mathcal{G}(V)$ be the set of simple undirected graphs on V.

For $v \in V$, denote by τ_v the local complementation map

$$\tau_v : \mathcal{G}(V) \to \mathcal{G}(V), \qquad \tau_v(G) = G * v.$$

Let Γ_{LC} be the subgroup of the permutation group of $\mathcal{G}(V)$ generated by all τ_v:

$$\Gamma_{LC} := \langle \tau_v : v \in V \rangle.$$

For a graph G on V, define

$$\mathrm{Orb}(G) := \{\gamma(G) : \gamma \in \Gamma_{LC}\}, \qquad \mathrm{Stab}(G) := \{\gamma \in \Gamma_{LC} : \gamma(G) = G\}.$$

The group $\mathrm{Stab}(G)$ consists of all local-complementation transformations that fix G. It should be distinguished from the word stabilizer $\mathrm{Stab}_{LC}(G)$, whose elements are finite local-complementation words returning G to itself. In this paper we take $G = P_p$, where $p \equiv 1 \pmod 4$ is prime and $V = \mathbb{F}_p$.

3.2. Normal-matrix interpretation of stabilizers

We now apply the isotropic-system formalism developed in Section 2 to the study of stabilizers. Recall that every local-complementation word determines a product of elementary normal matrices acting on the isotropic system W_G.

Proposition 3.2 (From LC words to normal matrices)**.** *For every word*

$$\sigma = (v_1, \ldots, v_k) \in V^*,$$

define

$$\Phi(\sigma) := M^{LC}_{v_1} \cdots M^{LC}_{v_k}.$$

Then, for every graph G,

$$W_{G*\sigma} = W_G \cdot \Phi(\sigma).$$

In particular, if

$$\sigma \in \mathrm{Stab}_{LC}(G),$$

then

$$\Phi(\sigma) \in \mathrm{Fix}_N(W_G).$$

Proof. We proceed by induction on the length of the word σ.

For the empty word ε, one has

$$G * \varepsilon = G \qquad \text{and} \qquad \Phi(\varepsilon) = I.$$

Hence

$$W_{G*\varepsilon} = W_G = W_G \cdot I = W_G \cdot \Phi(\varepsilon).$$

Assume now that

$$\sigma = (v_1, \ldots, v_k),$$

with $k \geq 1$, and write

$$\sigma' = (v_1, \ldots, v_{k-1}).$$

By the induction hypothesis,

$$W_{G*\sigma'} = W_G \cdot \Phi(\sigma').$$

By Proposition 2.12 and the zero-diagonal normalization convention of Remark 2.13, the local complementation at v_k is represented by the elementary normal matrix $M^{LC}_{v_k}$. Therefore

$$W_{G*\sigma} = W_{(G*\sigma')*v_k} = W_{G*\sigma'} \cdot M^{LC}_{v_k}.$$

Using the induction hypothesis, we obtain

$$W_{G*\sigma} = W_G \cdot \Phi(\sigma') M^{LC}_{v_k}.$$

Since

$$\Phi(\sigma) = \Phi(\sigma') M^{LC}_{v_k},$$

it follows that

$$W_{G*\sigma} = W_G \cdot \Phi(\sigma).$$

Finally, assume that

$$\sigma \in \mathrm{Stab}_{LC}(G).$$

Then

$$G * \sigma = G.$$

Therefore
$$W_G = W_{G*\sigma} = W_G \cdot \Phi(\sigma).$$
Hence
$$\Phi(\sigma) \in \mathrm{Fix}_N(W_G).$$
□

Proposition 3.3 (Functoriality of the map Φ)**.** *Let V^* be the free monoid of finite words on the vertex set V. Define*
$$\Phi : V^* \longrightarrow N(n),$$
by
$$\Phi(\varepsilon) = I_{2n},$$
for the empty word ε, and by
$$\Phi(v_1, \dots, v_k) = M_{v_1}^{LC} \cdots M_{v_k}^{LC},$$
for every nonempty word $(v_1, \dots, v_k)$.

Then Φ is a monoid homomorphism. In particular, for any words $\sigma, \tau \in V^*$, one has
$$\Phi(\sigma\tau) = \Phi(\sigma)\Phi(\tau).$$

Proof. Let
$$\sigma = (v_1, \dots, v_k), \qquad \tau = (u_1, \dots, u_m).$$
Then
$$\sigma\tau = (v_1, \dots, v_k, u_1, \dots, u_m).$$
By definition,
$$\Phi(\sigma\tau) = M_{v_1}^{LC} \cdots M_{v_k}^{LC} M_{u_1}^{LC} \cdots M_{u_m}^{LC}.$$
Grouping the factors gives
$$\Phi(\sigma\tau) = \left(M_{v_1}^{LC} \cdots M_{v_k}^{LC}\right) \left(M_{u_1}^{LC} \cdots M_{u_m}^{LC}\right) = \Phi(\sigma)\Phi(\tau).$$

The same identity is immediate if one of the two words is empty, since $\Phi(\varepsilon) = I_{2n}$. Therefore Φ is a monoid homomorphism. □

Remark 3.4 (On the converse)**.** Proposition 3.2 yields the inclusion
$$\Phi\left(\mathrm{Stab}_{LC}(G)\right) \subseteq \mathrm{Fix}_N(W_G).$$

In general, the converse inclusion is not known. Thus $\mathrm{Fix}_N(W_G)$ should be viewed as an algebraic enlargement of the local-complementation stabilizer rather than an equivalent description of it.

Proposition 3.5 (Stabilizer equation)**.** *Let G be a simple undirected graph on n vertices, with adjacency matrix $A \in \mathbb{F}_2^{n\times n}$, and let*

$$M = \begin{pmatrix} Z & T \\ X & Y \end{pmatrix} \in \mathcal{N}(n),$$

where X, Y, Z, T are diagonal matrices over $\mathbb{F}_2$, and $\mathcal{N}(n)$ denotes the group of normal matrices of size $2n$. Assume that

$$YZ + XT = I_n.$$

Assume that $Z + AX$ is invertible. Then the following are equivalent:
(a) *$M \in \mathrm{Fix}_N(W_G)$, that is,*

$$W_G \cdot M = W_G;$$

(b)

$$(Z + AX)A = T + AY. \tag{1}$$

Proof. By definition,

$$W_G = \mathrm{RowSpace}([\, I_n \mid A\,]).$$

Multiplying on the right by M, we obtain

$$[\, I_n \mid A\,] \begin{pmatrix} Z & T \\ X & Y \end{pmatrix} = [\, Z + AX \mid T + AY\,].$$

Since $Z + AX$ is invertible, left multiplication by $(Z + AX)^{-1}$ preserves row space, and hence

$$W_G \cdot M = \mathrm{RowSpace}\left([\, I_n \mid (Z + AX)^{-1}(T + AY)\,]\right).$$

Therefore

$$W_G \cdot M = W_G,$$

if and only if

$$\mathrm{RowSpace}\left([\, I_n \mid (Z + AX)^{-1}(T + AY)\,]\right) = \mathrm{RowSpace}([\, I_n \mid A\,]).$$

Now the representation

$$W_X = \mathrm{RowSpace}([\, I_n \mid A(X)\,]),$$

is canonical: if

$$\mathrm{RowSpace}([\, I_n \mid B\,]) = \mathrm{RowSpace}([\, I_n \mid C\,]),$$

then necessarily $B = C$. Indeed, there exists an invertible matrix P such that

$$[\, I_n \mid B\,] = P[\, I_n \mid C\,] = [\, P \mid PC\,],$$

and comparison of the left blocks gives $P = I_n$, hence $B = C$.

Applying this with

$$B = (Z + AX)^{-1}(T + AY), \qquad C = A,$$

we conclude that

$$W_G \cdot M = W_G,$$

if and only if

$$(Z + AX)^{-1}(T + AY) = A.$$

Multiplying on the left by $Z + AX$ gives

$$T + AY = (Z + AX)A,$$

which is exactly (1).

Conversely, (2) immediately implies (1). $\square$

Interpretation. The stabilizer equations reduce the stabilizer problem to solving a system in the diagonal unknowns X, Y, Z, T for a fixed adjacency matrix A.

Corollary 3.6 (Algebraic constraints on stabilizing words)**.** *Let P_p be an undirected Paley graph with adjacency matrix A.*

For every stabilizing local-complementation word

$$\sigma \in \mathrm{Stab}_{LC}(P_p),$$

the associated normal matrix

$$\Phi(\sigma) = \begin{pmatrix} Z & T \\ X & Y \end{pmatrix},$$

satisfies the stabilizer equation

$$(Z + AX)A = T + AY.$$

Proof. By Proposition 3.2, every stabilizing local-complementation word $\sigma \in \mathrm{Stab}_{LC}(P_p)$ satisfies

$$\Phi(\sigma) \in \mathrm{Fix}_N(W_{P_p}).$$

Applying Proposition 3.5 to $G = P_p$ gives

$$(Z + AX)A = T + AY.$$

$\square$

We now exploit the translation-invariant structure of the Paley adjacency matrix to specialize these constraints further.

3.3. Specialization to P_p: translation invariance and structured constraints

We now take $G = P_p$ with vertex set $V = \mathbb{F}_p$ and adjacency matrix

$$A_{xy} = f(y - x), \qquad f(t) = \mathbf{1}_Q(t), \qquad f(0) = 0,$$

where Q is the set of nonzero quadratic residues.

A key feature of A is translation invariance: for each $a \in \mathbb{F}_p$, let P_a be the permutation matrix corresponding to $x \mapsto x + a$. Then

$$P_a^{-1} A P_a = A.$$

Thus A is circulant, and the stabilizer equations inherit this symmetry.

Proposition 3.7 (Translation covariance of stabilizer equations)**.** *Let $A = AP_p$ and let*

$$M = \begin{pmatrix} Z & T \\ X & Y \end{pmatrix} \in \mathcal{N}(p),$$

satisfy the corrected stabilizer equations. For any $a \in \mathbb{F}_p$, define

$$X^{(a)} := P_a^{-1} X P_a, \qquad Y^{(a)} := P_a^{-1} Y P_a, \qquad Z^{(a)} := P_a^{-1} Z P_a, \qquad T^{(a)} := P_a^{-1} T P_a,$$

and

$$M^{(a)} := \begin{pmatrix} Z^{(a)} & T^{(a)} \\ X^{(a)} & Y^{(a)} \end{pmatrix}.$$

Then $M^{(a)} \in \mathcal{N}(p)$ and satisfies the same stabilizer equations for A.

Proof. Conjugation by P_a preserves diagonal matrices, so the blocks of $M^{(a)}$ remain diagonal. Moreover,

$$Y^{(a)} Z^{(a)} + X^{(a)} T^{(a)} = P_a^{-1} (YZ + XT) P_a = I,$$

so $M^{(a)}$ is normal. Using $P_a^{-1} A P_a = A$, we also obtain

$$\begin{aligned} (Z^{(a)} + AX^{(a)})A &= P_a^{-1} (Z + AX) A P_a \\ &= P_a^{-1} (T + AY) P_a \\ &= T^{(a)} + AY^{(a)}. \end{aligned}$$

which is exactly the corrected stabilizer equation. □

Problem 3.8. *Determine the image*

$$\operatorname{Im}(\Phi) \subseteq Fix_N(W_G),$$

and characterize the kernel

$$\ker(\Phi).$$

A solution would clarify the relationship between the algebraic stabilizer $Fix_N(W_G)$ and the combinatorial stabilizer $Stab_{LC}(G)$.

Remark 3.9. A characterization of the image of Φ would provide information on which normal matrices admit graph-compatible factorizations. Thus the study of $\mathrm{Im}(\Phi)$ appears closely related to the Normal-Matrix Factorization Problem and may offer a route toward a constructive theory of local equivalence.

3.4. Computational verification for P_5

The stabilizer equations derived in Proposition 3.5 reduce the normal-matrix stabilizer problem to a finite algebraic system over $\mathbb{F}_2$ involving diagonal matrices

$$X, Y, Z, T.$$

To investigate this system computationally, we implemented an exhaustive enumeration procedure in Python. The adjacency matrix A of the Paley graph P_5 was generated from the quadratic-residue construction, and all matrix operations were performed over $\mathbb{F}_2$.

For each vertex, the normality condition

$$yz + xt = 1,$$

admits exactly six quadruples

$$(x, y, z, t) \in \mathbb{F}_2^4.$$

Consequently, for $p = 5$, the total number of admissible assignments is

$$6^5 = 7776.$$

The computation proceeds as follows.

(a) Generate all admissible quadruples $(x, y, z, t) \in \mathbb{F}_2^4$, satisfying $yz + xt = 1$.

(b) Assign one admissible quadruple to each of the five vertices of P_5.

(c) Construct the corresponding diagonal matrices

$$X, Y, Z, T.$$

(d) Compute

$$Z + AX.$$

(e) Discard all configurations for which

$$Z + AX,$$

is singular.

(f) For the remaining configurations, test the stabilizer equation

$$(Z + AX)A = T + AY.$$

(g) Record all normal matrices satisfying the equation.

No search-space reduction or heuristic pruning was used. The reported result is therefore obtained by complete enumeration of all admissible configurations. The implementation was written in Python, and the computation completed in negligible time on a standard desktop computer.

The exhaustive computation yields

$$Fix_N(W_{P_5}) = \{I_{10}\}.$$

Hence the identity matrix is the unique normal matrix satisfying the stabilizer equations for P_5.

For larger primes, a direct exhaustive search rapidly becomes impractical. Indeed,

$$6^{13} = 13060694016,$$

already exceeds 10^{10} admissible configurations. Consequently, the present work makes no exhaustive computational claim for $p \geq 13$. Treating larger Paley graphs requires additional techniques, such as algebraic reductions, SAT-based methods, Gröbner-basis approaches, or structural exploitation of the circulant symmetry of Paley adjacency matrices.

The computation for P_5 nevertheless provides a first indication of a possible rigidity phenomenon and motivates the following conjecture.

Conjecture 3.10 (Rigidity of the normal-matrix stabilizer)**.** *Let $p \equiv 1 \pmod 4$ be a prime, and let P_p be the undirected Paley graph with adjacency matrix A. Then*

$$Fix_N(W_{P_p}) = \{I_{2p}\}.$$

Equivalently, if

$$M = \begin{pmatrix} Z & T \\ X & Y \end{pmatrix} \in N(p),$$

satisfies

$$W_{P_p} \cdot M = W_{P_p},$$

or, equivalently,

$$(Z + AX)A = T + AY,$$

then

$$M = I_{2p}.$$

The exhaustive verification for P_5 gives

$$Fix_N(W_{P_5}) = \{I_{10}\},$$

providing initial evidence for the conjecture. A proof would establish a rigidity property for the isotropic representation of undirected Paley graphs and would clarify the structure of their normal-matrix stabilizers.

4. Conclusion and perspectives

We studied the Equivalent Local Sequence Problem (ELSP) for simple undirected graphs within Bouchet's isotropic-system framework. Our approach identifies the additional algebraic information required to pass from the recognition of local equivalence to the explicit recovery of transformation sequences.

More precisely, we introduced the Normal-Matrix Factorization Problem (NMFP), which asks whether a normal-matrix witness of local equivalence can be decomposed into a graph-compatible sequence of elementary transformations. We showed that, once such a factorization is available, an explicit local-complementation sequence can be recovered in polynomial time. This establishes a reduction from the constructive component of the Equivalent Local Sequence Problem to the Normal-Matrix Factorization Problem and clarifies the relationship between Bouchet's algebraic characterization of local equivalence and its constructive realization.

The normal-matrix formalism developed in this work also provides a convenient framework for investigating structural aspects of local-complementation dynamics. In the particular setting of undirected Paley graphs, the stabilizer problem can be reduced to a system of algebraic equations over $\mathbb{F}_2$, yielding an explicit characterization of stabilizing normal matrices.

Computational experiments for small primes suggest that the normal-matrix stabilizer is trivial in the cases considered, indicating a possible rigidity phenomenon in the isotropic representation of Paley graphs. These observations motivate a broader investigation of the relationship between algebraic symmetry and local-complementation dynamics.

Future directions. The principal open problem emerging from this work is to determine the computational complexity of the Normal-Matrix Factorization Problem. While Bouchet's theory provides a polynomial-time recognition procedure for local equivalence, the complexity of constructing a graph-compatible factorization of a normal-matrix witness remains unknown. A solution to this problem would immediately yield a constructive polynomial-time recovery procedure for local-complementation sequences.

A second direction is to extend the computational study of normal-matrix stabilizers and orbit structures for larger Paley graphs in order to gather further evidence for Conjecture 3.10. It would also be interesting to exploit the circulant structure of Paley adjacency matrices and their Fourier diagonalization in order to derive theoretical constraints on stabilizer solutions.

More generally, understanding how algebraic symmetry interacts with local graph transformations may provide new insights into the geometry of local-complementation orbits, isotropic representations, and the structure of normal-matrix actions on graph classes possessing strong algebraic regularity.

From a broader perspective, the results of this paper suggest that the Normal-Matrix Factorization Problem constitutes the algebraic bottleneck underlying constructive approaches to local equivalence. Determining whether every normal-matrix witness arising from Bouchet's characterization admits an efficiently computable graph-compatible factorization remains an important open question. Resolving this problem would clarify the precise boundary between the existential recognition theory of local equivalence and its constructive realization.

References

[1] A. Bouchet. An efficient algorithm to recognize locally equivalent graphs. *Combinatorica*, 11(4):315–329, 1991. https://doi.org/10.1007/BF01275668.

[2] A. E. Brouwer and W. H. Haemers. *Spectra of Graphs*. Universitext. Springer, New York, 2012. https://doi.org/10.1007/978-1-4614-1939-6.

[3] D. S. Dummit and R. M. Foote. *Abstract Algebra*. Wiley, 3rd edition, 2004.

[4] G. H. Golub and C. F. Van Loan. *Matrix Computations*. Johns Hopkins University Press, 4th edition, 2013.

[5] M. Hein, J. Eisert, and H. J. Briegel. Multiparty entanglement in graph states. *Physical Review A*, 69(6):062311, 2004. https://doi.org/10.1103/PhysRevA.69.062311.

[6] S.-i. Oum. Rank-width and vertex-minors. *Journal of Combinatorial Theory, Series B*, 95(1):79–100, 2005. https://doi.org/10.1016/j.jctb.2005.03.003.

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

[8] 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.

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

[10] Z. Oumazouz and D. Karim. A new symmetric key cryptographic algorithm using paley graphs and ascii values. In *E3S Web of Conferences*, volume 297, page 01046. EDP Sciences, 2021. https://doi.org/10.1051/e3sconf/202129701046.

[11] Z. Oumazouz and D. Karim. The analysis and implementation of the symmetric key cryptographic algorithm based on the algebraic paley graphs. *International Journal of Mathematics and Computer Science*, 17(4):1563–1567, 2022.

[12] A. W. Tucker. A combinatorial equivalence of matrices. In *Combinatorial Mathematics and its Applications*, pages 129–140. University of North Carolina Press, 1971.

Zhour Oumazouz
Faculty of Sciences and Techniques Mohammedia
Hassan II University, Mohammedia, Morocco
E-mail oumazouzzhour@gmail.com