LEHMAN MATRICES

GÉRARD CORNUÉJOLS, BERTRAND GUENIN, LEVENT TUNÇEL

ABSTRACT. A pair of square $0,1$ matrices A, B such that $AB^T = E + kI$ (where E is the $n \times n$ matrix of all 1s and k is a positive integer) are called *Lehman matrices*. These matrices figure prominently in Lehman's seminal theorem on minimally nonideal matrices. There are two choices of k for which this matrix equation is known to have infinite families of solutions. When $n = k^2 + k + 1$ and $A = B$, we get point-line incidence matrices of finite projective planes, which have been widely studied in the literature. The other case occurs when $k = 1$ and n is arbitrary, but very little is known in this case. This paper studies this class of Lehman matrices and classifies them according to their similarity to circulant matrices.

C & O Research Report: CORR 2006–18

July 27, 2006

Key words and phrases. Lehman matrices, minimally nonideal matrices, 0,1 circulant matrix, finite projective plane.

Gérard Cornuéjols: Tepper School of Business, Carnegie Mellon University, Pittsburgh, PA 15213, USA; and LIF, Faculté des Sciences de Luminy, Université d' Aix-Marseille, France. Supported by NSF grant DMI-0352885 and ONR grant N00014-03-1-0188. gc0v@andrew.cmu.edu

Bertrand Guenin: Department of Combinatorics and Optimization, Faculty of Mathematics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada. Supported by a grant from NSERC. bguenin@math.uwaterloo.ca

Levent Tunçel: Department of Combinatorics and Optimization, Faculty of Mathematics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada. Supported in part by a Discovery Grant from NSERC. ltuncel@math.uwaterloo.ca.

1. INTRODUCTION

Let $M_n(K)$ denote the set of $n \times n$ matrices with elements in K, and let $\mathbb{B}$ denote the set $\{0, 1\}$.

We say that matrices $A, B \in M_n(\mathbb{B})$ form a pair of *Lehman matrices* if there exists a positive integer k such that

$$AB^T = E + kI \tag{1}$$

where E denotes the $n \times n$ matrix of all 1s, and I is the identity matrix. Matrix B is called the *dual* of matrix A. Note that A is the dual of B (indeed $AB^T = E + kI$ implies $BA^T = E + kI$ since $E + kI$ is symmetric). Bridges and Ryser [1] showed that every Lehman matrix is r*-regular* for some integer $r \geq 2$, i.e. it has the same number r of 1s in each row and column, see Section 2. If the dual of A is A itself (i.e. $AA^T = E + kI$) then A is the point-line incidence matrix of a *nondegenerate finite projective plane*, a widely studied topic [7]. Other infinite classes of Lehman matrices occur when $k = 1$ but very little is known in this case. The main purpose of this paper is to initiate a study of these matrices.

We say that A is *thin* when $k = 1$ in equation (1) and *fat* when $k > 1$ (this terminology refers to the volume of the simplex defined by the column vectors of A, see Section 6.2). Nondegenerate finite projective planes with $n \geq 7$ points give rise to fat Lehman matrices. Before presenting examples of thin Lehman matrices, we introduce some notation.

Given indices $t, t' \in [n]$ (where $[n] = \{1, \dots, n\}$), a (t, t')*-interval* is the set of indices visited following the cyclical ordering, starting from t and ending at t'. We denote this interval by $[t, t']$. Its *size* is $t' - t + 1$ when $t' \geq t$ and $t' - t + n + 1$ when $t' < t$. Similarly, we denote the set $\{0, 1, \dots, m\}$ by $[0, m]$. Given $i \in [0, n-1]$, we say that interval $[t + i, t' + i]$ is an i*-shift* of interval $[t, t']$. More generally, the i*-shift* of vector $(v_1, \dots, v_n)$ is the vector $(u_1, \dots, u_n)$ where $u_{j+i} = v_j$ if $j + i \leq n$ and $u_{j+i-n} = v_j$ if $j + i \geq n + 1$. Vector u is a *shift* of vector v if there exists $i \in [0, n-1]$ such that u is an i-shift of v.

1.1. **Examples.** A matrix $X \in M_n(\mathbb{B})$ is *circulant* if for all $i \in [n-1]$, row $1+i$ is an i-shift of row 1. Consider integers r, s, n such that $r, s \geq 2$ and $rs = n+1$. We define matrices $C_r^n, D_s^n \in M_n(\mathbb{B})$ as follows: C_r^n and D_s^n are the circulant matrices with row 1 corresponding to $[r]$ and $\{1, r, 2r, \ldots, (s-1)r\}$ respectively. Note that $C_r^n D_s^{nT} = E + I$. Hence,

Remark 1.1. For all integers r, s, n such that $r, s \geq 2, rs = n+1$, C_r^n and D_s^n form a pair of thin Lehman matrices.

Two matrices X, Y are *isomorphic* if Y can be obtained from X by permuting the columns and the rows of X. If a matrix A is isomorphic to a Lehman matrix, then A is also a Lehman matrix (to see this, perform the same permutations on the dual and observe that (1) still holds).

2-regular Lehman matrices are perfectly understood: They are isomorphic to C_2^n for n odd (they are sometimes called *odd holes*).

Luetolf and Margot [11] enumerated all nonisomorphic Lehman matrices for $n \leq 11$. For example, they found exactly two nonisomorphic Lehman matrices for $n = 8$ (to help visualize 0,1 matrices we do not write down the 0s):

$$C_3^8 = \begin{bmatrix} 1 & 1 & 1 & & & & & \\ & 1 & 1 & 1 & & & & \\ & & 1 & 1 & 1 & & & \\ & & & 1 & 1 & 1 & & \\ & & & & 1 & 1 & 1 & \\ & & & & & 1 & 1 & 1 \\ 1 & & & & & & 1 & 1 \\ 1 & 1 & & & & & & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & & 1 & & 1 & & & \\ & 1 & 1 & 1 & & & & \\ & & 1 & 1 & 1 & & & \\ & 1 & & 1 & & 1 & & \\ & & & & 1 & 1 & 1 & \\ & & & & & 1 & 1 & 1 \\ 1 & & & & & & 1 & 1 \\ 1 & 1 & & & & & & 1 \end{bmatrix}.$$

Note that the second matrix is obtained from C_3^8 by adding a $0, \pm 1$ matrix of rank 1. The main theme of this paper is that this is not a coincidence: thin Lehman matrices are either circulant matrices C_r^n or "similar" to them. We make this more precise below. Define the *level* of a thin r-regular $n \times n$ Lehman matrix A to be the minimum rank of $A' - C_r^n$ over all matrices A' isomorphic to A. For example, the circulant matrices C_r^n have level 0 and the second Lehman matrix with

$n = 8$ above has level 1. To demonstrate that the notion of level is natural in the study of thin Lehman matrices, we appeal to information complexity (also known as Kolmogorov complexity).

1.2. **Results.** A *parameter* is any $\alpha \in [n]$. We say that an $n \times n$ matrix A can be *described with k parameters* $\mathcal{P} = \{p_1, \ldots, p_k\}$ if there exists an algorithm that, given $\mathcal{P}$, constructs a matrix isomorphic to A (note that there is no complexity restriction on the algorithm). We prove the following theorem in Section 3.

Theorem 1.2. *If A is a thin $n \times n$ Lehman matrix of level t, then A can be described with $O(t^4)$ parameters.*

Thus thin Lehman matrices with constant level can be described with a constant number of parameters, whereas one may require $\Omega(n)$ parameters to describe a $0, \pm 1$ matrix of constant rank. This means that thin Lehman matrices with constant level are similar to C_r^n in terms of information complexity.

In Section 4, we give a complete characterization of level one thin Lehman matrices, using only six parameters. This infinite class of Lehman matrices is new.

In Section 5, we prove the existence of thin Lehman matrices of arbitrarily high level and we give some constructions. In Section 6, we briefly discuss fat Lehman matrices and in Section 7 we state open problems and present some concluding remarks.

1.3. **Motivation.** Lehman matrices are key to understanding the *set covering problem* $\min\{c^T x : Mx \geq e_m,\ x \in \mathbb{B}^n\}$, a fundamental problem in combinatorial optimization (here c is a given vector in $\mathbb{R}^n_+$, e_m is the m-vector all of whose components are 1, and M is a given $m \times n$ matrix with entries equal to 0 or 1; x is the vector of unknowns). A basic question is the following: when can the set covering problem be solved by linear programming? This can be done for every objective function c exactly when the *set covering polytope* $P := \{x \in \mathbb{R}^n : \ Mx \geq e_m,\ 0 \leq$

$x \leq e_n\}$ is *integral*, i.e. all its extreme points have only 0,1 components. When this occurs, the matrix M is said to be *ideal*.

If P is an integral polytope, then for all $j \in [n]$ and $\beta \in \mathbb{B}$, so are its faces $P' := P \cap \{x_j = \beta\}$. Let P'' be the restriction of P' to variables distinct from x_j, i.e. $P'' = \{(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n) : (x_1, \ldots, x_n) \in P'\}$. It can readily be checked that P'' is a set covering polytope as well, i.e. $P'' = \{x \in \mathbb{R}^{n-1} : \ M'x \geq e_{m'},\ 0 \leq x \leq e_{n-1}\}$ for some $0,1$ matrix M'. We say that M' is a *minor* of M. Thus if a matrix is ideal then so are all its minors. A $0,1$ matrix is *minimally nonideal* if it is not ideal but all its minors are. Thus if M is minimally nonideal then $P = \{x \in \mathbb{R}^n : \ Mx \geq e_m,\ 0 \leq x \leq e_n\}$ is not an integral polytope but all the polytopes obtained from P by fixing a variable x_j to 0 or to 1 are.

An example of a minimally nonideal matrix is the point-line incidence matrix of a *degenerate finite projective plane* (one line contains $n-1$ points $v_1, \ldots, v_{n-1}$, and the remaining $n-1$ lines contain exactly two points v_j, v_n, for $j = 1, \ldots, n-1$). Define the *core* of a minimally nonideal matrix M to be the submatrix induced by those rows for which the inequalities $M\bar{x} \geq e_m$ hold as equality at a fractional extreme point $\bar{x}$ of P. Lehman [8] gave the following property of minimally nonideal matrices: If M is a minimally nonideal matrix, then either it is the point-line incidence matrix of a degenerate finite projective plane or it has a unique core which is a Lehman matrix. A complete characterization of minimally nonideal matrices or of their cores seems extremely difficult. A step towards a better understanding of these matrices is to study the Lehman equation (1). This is the purpose of this paper.

A $0,1$ matrix M is *Mengerian* if for every nonnegative integral vector c the linear program $\min\{c^T x : \ Mx \geq e_m,\ 0 \leq x \leq e_n\}$ and its dual both have integral solutions. Many classical minimax theorems are associated with an underlying Mengerian matrix [3]. If a matrix is Mengerian then so are all its minors. A $0,1$ matrix is *minimally non-Mengerian* if it is not Mengerian but all its minors are. Clearly, if M is Mengerian then it is ideal. It follows that minimally non-Mengerian matrices are either minimally nonideal or ideal. In [4] it is shown that if a matrix is minimally non-Mengerian and minimally nonideal, then its core must be thin. Hence, thin Lehman matrices are important in understanding minimally non-Mengerian matrices.

Finally, note the analogy between equation (1) and the equation $AB^T = E - I$ that arises in the study of perfect graphs: Lovász [10] showed that minimally imperfect graphs satisfy $AB^T = E - I$ where A (B respectively) is the maximum clique (maximum stable set respectively) versus vertex incidence matrix. Graphs that satisfy this matrix equation are called *partitionable graphs* and they were studied in the 1970s and following decades.

We will drop the subscript or superscript n from C_r^n, D_s^n, e_n etc. when the dimension is clear from the context.

2. Preliminaries

A classical result about the solutions of the Lehman matrix equation (1) was proved by Bridges and Ryser [1].

Theorem 2.1. *Let $A, B \in M_n(\mathbb{B})$ be a Lehman pair. Then, there exist integers $r \geq 2$,$s \geq 2$ such that A is r-regular, B is s-regular and $rs = n + k$. Moreover, A^T, B^T are also a Lehman pair.*

Next, we establish that the notion of *level* of a Lehman matrix is invariant under duality. A matrix is 0-*regular* if the sum of entries in each row and column is equal to 0.

Proposition 2.2. *Let $A, B \in M_n(\mathbb{B})$ be a thin Lehman pair. Then,* $\mathrm{level}(A) = \mathrm{level}(B)$.

Proof. By Theorem 2.1, there exist integers $r \geq 2$,$s \geq 2$ such that A is r-regular, B is s-regular and $rs = n + 1$.

Let $t = \mathrm{level}(A)$. By the definition of level, there exist $n \times n$ permutation matrices P, Q such that $PAQ - C_r$ has rank t.

Claim 1. *$PBQ - D_s$ has rank t.*

Proof. We define

$$\Sigma_A := PAQ - C_r, \quad \Sigma_B := PBQ - D_s.$$

Since C_r and D_s form a thin Lehman pair, we have

$$\begin{aligned} E + I &= (PAQ - \Sigma_A)\,(PBQ - \Sigma_B)^T \\ &= (PAQ)(PBQ)^T - C_r\Sigma_B^T - \Sigma_A(PBQ)^T. \end{aligned}$$

Since $P(E + I)P^T = E + I$ and A, B make a thin Lehman pair, so do PAQ and PBQ. We obtain

$$\Sigma_B C_r^T = -(PBQ)\Sigma_A^T.$$

By Theorem 2.1 C_r^T and D_s^T are a Lehman pair. Multiplying both sides of the above equation from right by D_s and using the fact that Σ_B is 0-regular, we arrive at

$$\Sigma_B = -(PBQ)\Sigma_A^T D_s.$$

PBQ and D_s are nonsingular; therefore, $\operatorname{rank}(\Sigma_B) = \operatorname{rank}(\Sigma_A) = t$ as desired. ◇

The above claim implies that $\operatorname{level}(B) \leq t$. Since the roles of A and B are symmetric in the Lehman equation, if $\operatorname{level}(B) \leq t - 1$, we would arrive at $\operatorname{level}(A) \leq t - 1$, a contradiction. Therefore, $\operatorname{level}(B)$ must equal t. □

Remark 2.3. Suppose $A, B \in M_n(\mathbb{B})$ make a thin Lehman pair. Then using the Lehman equation,

$$A^{-1} = B^T - \frac{1}{r}E. \tag{2}$$

Suppose A, B also satisfy $A = C_r + \Sigma_A$ and $B = D_s + \Sigma_B$, where Σ_A and Σ_B are 0-regular matrices. Using the proof of Proposition 2.2, the identity (2), and the 0-regularity of Σ_A, we deduce

$$\Sigma_B = -B\Sigma_A^T D_s = -A^{-T}\Sigma_A^T D_s = -\left(C_r^{-1}\Sigma_A A^{-1}\right)^T. \tag{3}$$

3. Information complexity

As we hinted in the introduction, thin Lehman matrices can be classified with respect to their relation to the circulant matrices via the notion of level. In particular, we will prove in this section that low level, thin Lehman matrices are very similar to circulant matrices. In this context, two matrices are “similar” or “close” to each other if only “little” extra information is sufficient to describe one in terms of the other. Our approach focuses on the *descriptional complexity* of 0,1 matrices which is in the general domain of well-known notions of *Kolmogorov complexity* and *Shannon information theory*. In such studies one has to decide ahead of time what the communicated data or the computer input “mean.” (How will it be interpreted?) For our purposes, we will require that the input be treated as “positions” in an n-dimensional vector. While both of these areas (Kolmogorov complexity and Shannon information theory) are close to what we need, neither one is exactly suitable. Therefore, we set up our own special model below. For detailed information on Kolmogorov complexity, see [9]; for a comparison of Kolmogorov complexity and Shannon information theory, see [5].

In our approach, we are interested in describing 0,1 matrices or $0, \pm 1$ matrices. Our complexity model allows the usage of parameters in $[n]$. However, we require that any algorithm that is allowed in our model must treat these parameters as “positions” of an n-dimensional vector (or treat a pair of parameters as a position in an $n \times n$ matrix). For instance, to describe a 0,1 vector of length n, we may list the positions where contiguous ones start and end (such a representation would require $\Omega(n)$ parameters in the worst case). However, we do not allow the usage of parameters to encode the 0,1 elements as the digits of a number in $[n]$ (if this were allowed, then $\frac{n}{\log n}$ parameters would suffice to describe any 0,1 vector of length n).

As we explained in the introduction, our classification theory treats isomorphic matrices as equivalent (so does our notion of level of a thin Lehman matrix). Given thin Lehman matrices $A, A' \in M_n(\mathbb{B})$, both r-regular, we are interested in the significant intrinsic combinatorial differences between A and A'. So, classification up to isomorphism also serves us well in the current section.

Let $A, B \in M_n(\mathbb{B})$ be a Lehman pair with A being r-regular and B being s-regular. To describe the 1s in A, rn parameters suffice. Since we allow computation (any algorithm may be used), and A, B satisfy the Lehman equation, each thin Lehman matrix can be described by $\min\{r, s\}n$ parameters. E.g., if $s < r$, we describe B using sn parameters and compute $A = (E + I)B^{-T}$. In contrast, one parameter suffices to describe C_r, namely r. Indeed, if $\mathrm{level}(A) = O(1)$ then $O(1)$ parameters suffice to describe A (see Corollary 3.8).

Given $u \in \mathbb{Z}^n$, $u_+, u_- \in \mathbb{Z}_+^n$ are the positive (negative resp.) parts of u such that $u = u_+ - u_-$ and u_+, u_- have disjoint supports. (Sometimes, we define a vector u by first defining its positive and negative parts u_+ and u_- and then by letting $u := u_+ - u_-$; in this latter definition, the supports of u_+ and u_- need not be disjoint.) We denote the support of a vector u by $\mathrm{supp}(u)$.

We say that $u \in \mathbb{Z}^n$ is (t, C_r)-*compact* if

$$\begin{aligned} \mathrm{supp}(u_+) &\subseteq \text{union of } t \text{ intervals of size } r\text{, and} \\ \mathrm{supp}(u_-) &\subseteq \text{union of } t \text{ intervals of size } r. \end{aligned}$$

We say that $u \in \mathbb{Z}^n$ is (t, D_s)-*compact* if

$$\begin{aligned} \mathrm{supp}(u_+) &\subseteq \text{ union of the supports of } t \text{ columns of } D_s \text{, and} \\ \mathrm{supp}(u_-) &\subseteq \text{ union of the supports of } t \text{ columns of } D_s. \end{aligned}$$

Proposition 3.1. *Let* $\Sigma \in M_n(\{0, \pm 1\})$, *be* 0*-regular with* $\mathrm{rank}(\Sigma) = t$. *If* $C_r + \Sigma$ *is nonnegative then every column and row of* Σ *is* (t, C_r)*-compact.*

Proof. We only prove that every column of Σ is (t, C_r)-compact (our arguments directly apply to the rows of Σ as well). First, we note that for any column x of Σ, x_- is $(1, C_r)$-compact (since $C_r + \Sigma$ is nonnegative). Next, we prove that x_+ is (t, C_r)-compact: Let $\widetilde{\Sigma}$ be the $n \times (n-1)$ matrix obtained from Σ by deleting column x. Since Σ is 0-regular, the system:

$$\widetilde{\Sigma}\alpha = -x, \qquad \alpha \geq 0 \tag{4}$$

has a solution, namely $\alpha := e$. Since $\mathrm{rank}(\widetilde{\Sigma}) \leq t$, there exists an extreme point solution $\bar{\alpha}$ of (4) such that $|\,\mathrm{supp}(\bar{\alpha})| \leq t$. In particular,

$$\mathrm{supp}(x_+) \subseteq \bigcup_{i \in \mathrm{supp}(\bar{\alpha})} \mathrm{supp}\left(\left[\mathrm{col}_i(\widetilde{\Sigma})\right]_-\right).$$

We conclude that x_+, and hence x, is (t, C_r)-compact. □

Corollary 3.2. *Let* $\Sigma \in M_n(\{0, \pm 1\})$, *be* 0*-regular with* $\mathrm{rank}(\Sigma) = t$. *If* $C_r + \Sigma$ *is nonnegative then every* $v \in \mathrm{rowspace}(\Sigma)$ *is* (t^2, C_r)*-compact.*

Proof. Choose a set of rows $\ell_1, \ell_2, \ldots, \ell_t$ of Σ which forms a basis for the row space of Σ. Then $v = \sum_{i=1}^{t} \alpha_i \ell_i^T$, for some coefficients $\alpha_1, \alpha_2, \ldots, \alpha_t$. By Proposition 3.1, each ℓ_i is (t, C_r)-compact; hence, v is (t^2, C_r)-compact as desired. □

For $p \in \mathbb{Z}^n$ and an (i,j)-interval $S \subseteq [n]$, the *transition of* p *over* S is

$$\operatorname{trans}(p,S) := \sum_{k=i-1}^{j} |p(k) - p(k+1)|\,,$$

where the indices are interpreted cyclically in $[n]$.

For $i,j \in [n]$, $\operatorname{dist}(i,j)$ is the size of a smallest interval containing both i and j. Thus, if $j \geq i$, then $\operatorname{dist}(i,j) = \min\{j-i+1, i-j+n+1\}$.

Proposition 3.3. *Let* $r \geq 2$, $s \geq 2$ *be integers and let* $n := rs - 1$. *Also let* $y \in \{0, \pm 1\}^n$ *be* $(1, D_s)$*-compact and* $\ell := C_r^T y$. *Then*

$$\operatorname{trans}(\ell, S) \leq 12, \quad \textit{for every interval } S \textit{ of size } r-1.$$

Proof. Let

$$z_+ := \sum_{i \in y_+} \operatorname{row}_i(C_r) \text{ and } z_- := \sum_{i \in y_-} \operatorname{row}_i(C_r).$$

We say that $i \in [n]$ is *special* if $z_+(i) \geq 2$ or $z_-(i) \geq 2$. Note, $\ell = z_+ - z_-$.

Claim 1. *Let* $i,j \in \operatorname{supp}(\ell_+)$ *be such that* $\operatorname{dist}(i,j) \leq r-1$ *and neither* i *nor* j *is special. Then* i *and* j *lie in the same interval of* $\operatorname{supp}(\ell_+)$.

Proof. Clearly, $i,j \in \operatorname{supp}(z_+)$. Since i,j are not special, $z_+(i) = 1$ and $z_+(j) = 1$. Let S be the smallest interval containing both i and j. Since y is $(1, D_s)$-compact, the rows indexed by y_+ are each shifted by r or $r-1$. Since $\operatorname{dist}(i,j) \leq r-1$, this implies that $S \subseteq \operatorname{supp}(z_+)$. Since $z_-(i) = z_-(j) = 0$ and $\operatorname{dist}(i,j) \leq r-1$, $S \cap \operatorname{supp}(z_-) = \emptyset$. We conclude that $\operatorname{supp}(\ell_+) \supseteq S$ and that the same interval of ℓ_+ contains S.

$\diamond$

Claim 2. *There exist at most two special elements. If a special element* v *appears in* z_+ *then* $z_+(v) = 2$*; if it appears in* z_- *then* $z_-(v) = 2$.

Proof. The claim follows from the matrix equation $C_r^T D_s = E + I$. ◇

Let S be an interval of size $r - 1$. The following includes all potential contributions to $\mathrm{trans}(\ell, S)$:

- at most 4 for each special element (by Claim 2, there are at most two such elements),
- at most 2 for each of ℓ_+, ℓ_- (by Claim 1).

The total is bounded above by 12. □

The next two remarks are useful in estimating the total number of transitions over sums of vectors and unions of intervals.

Remark 3.4. Let $\ell, \ell' \in \mathbb{Z}^n$ and let $S \subseteq [n]$ be an interval. Then

$$\mathrm{trans}(\ell + \ell', S) \leq \mathrm{trans}(\ell, S) + \mathrm{trans}(\ell', S).$$

Remark 3.5. Let $\ell \in \mathbb{Z}^n$ and $S, S' \subseteq [n]$ be intervals. Then

$$\mathrm{trans}(\ell, S \cup S') \leq \mathrm{trans}(\ell, S) + \mathrm{trans}(\ell, S').$$

Proposition 3.6. *Let $y \in \{0, \pm 1\}^n$ be (t, D_s)-compact. Define $\ell := C_r^T y$. If ℓ is (q, C_r)-compact, then*

$$\mathrm{trans}(\ell, [n]) \leq 48tq.$$

Proof.

Claim 1. *For every interval $S \subseteq [n]$ of size $r - 1$, $\mathrm{trans}(\ell, S) \leq 12t$.*

Proof. Since y is (t, D_s)-compact, there exist $\rho_i \in \{0, \pm 1\}^n$ such that each ρ_i is $(1, D_s)$-compact and $\sum_{i=1}^t \rho_i = y$. Let $\ell_i := C_r^T \rho_i$, for all $i \in [t]$. By Proposition 3.6, $\mathrm{trans}(\ell_i, S) \leq 12$. Since $\ell = \sum_{i=1}^t \ell_i$, Remark 3.4 implies the claim. ◇

Since ℓ is (q, C_r)-compact,

$$\begin{aligned} \mathrm{supp}(\ell_+) &\subseteq \text{ union of } q \text{ intervals of size } r, \\ \mathrm{supp}(\ell_-) &\subseteq \text{ union of } q \text{ intervals of size } r. \end{aligned}$$

Therefore,

$$\mathrm{supp}(\ell) \subseteq \text{ union of } 4q \text{ intervals of size } \left\lceil \tfrac{r}{2} \right\rceil \leq r-1.$$

By the claim, every such interval contains at most $12t$ transitions for ℓ. Hence, by Remark 3.5, we have $\mathrm{trans}(\ell, [n]) \leq (4q)(12t)$

as desired. □

Now, we are ready to prove Theorem 1.2.

Proof of Theorem 1.2. Let A be an $n \times n$ thin Lehman matrix of level t. Then (by Theorem 2.1) A is r-regular for some integer $r \geq 2$ and by our definition of level, there exist permutation matrices P, Q such that $\mathrm{rank}(PAQ - C_r) = t$. Let $\Sigma_A := PAQ - C_r$. Denote by B the dual of A (then B is s-regular where $s \geq 2$ is the integer satisfying $rs = n + 1$). Let $\Sigma_B := PBQ - D_s$. We will describe Σ_B with $O(t^4)$ parameters. Since the roles of A and B are symmetric, the same arguments also apply to Σ_A.

By the proof of Proposition 2.2 (or (3)), $\mathrm{rank}(\Sigma_B) = t$. So, there exists a $t \times t$ nonsingular submatrix Γ of Σ_B with row index set J_r, column index set J_c such that after a suitable reordering,

$$\Sigma_B = \begin{bmatrix} \Gamma & M_1 \\ M_2 & M_2\Gamma^{-1}M_1 \end{bmatrix}.$$

We define

$$Y := \begin{bmatrix} \Gamma \\ M_2 \end{bmatrix}, \qquad U^T := [\Gamma \quad M_1].$$

Further let $L := C_r^T Y$, $X := C_r U$. Given L, X, J_r, J_c as the input, the following algorithm computes Σ_B:

- Compute $D_s^T X$, $D_s L$

  (this gives Γ, M_1 and M_2 as follows:

$$D_s^T X = D_s^T C_r U = (E+I)U = U = \begin{bmatrix} \Gamma^T \\ M_1^T \end{bmatrix};$$

  similarly,

$$D_s L = D_s C_r^T Y = (E+I)Y = Y = \begin{bmatrix} \Gamma \\ M_2 \end{bmatrix});$$

- compute $M_2 \Gamma^{-1} M_1$.

We claim that (L, X, J_r, J_c) can be represented by $O(t^4)$ parameters. Clearly, J_r and J_c can be represented by t parameters each. So, it suffices to prove the upper bound for L (since for X we simply transpose the matrix A). By Corollary 3.2, every column ℓ of L is (t^2, C_r)-compact. Since every column y of Y is a column of Σ_B, Proposition 3.1 implies that y is (t, D_s)-compact. Now, Proposition 3.6 implies $\mathrm{trans}(\ell, [n]) \leq 48t^3$. Every transition can be described by one parameter; hence, ℓ can be described by $O(t^3)$, L can be described by $O(t^4)$ parameters. □

Remark 3.7. Theorem 1.2 also applies to partitionable matrices (those satisfying $AB^T = E - I$). We simply redefine the notion of "special" used in the proof of Proposition 3.3.

Corollary 3.8. *Every pair of thin Lehman matrices with fixed level (i.e.* $\mathrm{level}(A) = t = O(1)$*) can be described by* $O(1)$ *parameters.*

The next section gives a complete characterization of all thin Lehman matrices of level one, using only 6 parameters.

4. Complete characterization of level one matrices

Throughout this section $A, B \in M_n(\mathbb{B})$ denote level one matrices and B is the dual of A. Moreover A is r-regular and B is s-regular. A matrix in $M_n(\mathbb{B})$ is identified with the set of pairs in $[n] \times [n]$ corresponding to its nonzero entries.

A $(t, q; t', q')$-*block* is the set of pairs (i, j) where i is in the (t, t')-interval and j is in the (q, q')-interval. A (ρ, σ)-*shift* of a $(t, q; t', q')$- block is the $(t + \rho, q + \sigma; t' + \rho, q' + \sigma)$-block. A *configuration* $\mathcal{C}$ is a 6-tuple $(i, j, n_R, n_C, \rho, \sigma)$ associated with 4 blocks as follows. The *blocks* of $\mathcal{C}$ are denoted $B_{11}, B_{12}, B_{21}, B_{22}$ where B_{11} is the $(i, j; i + n_R - 1, j + n_C - 1)$-block, B_{21} is a $(\rho, 0)$-shift of B_{11}, B_{12} is a $(0, \sigma)$-shift of B_{11} and B_{22} is a (ρ, σ)-shift of B_{11}. The matrix $\Sigma(\mathcal{C})$ is defined as $-B_{11} - B_{22} + B_{21} + B_{12}$.

Theorem 4.1. *A matrix A is a level one (Lehman) matrix if and only if A is isomorphic to $C_r + \Sigma(\mathcal{C})$ where $\mathcal{C}$ is the configuration $(1, 1 + n_R, n_R, r - n_R, tr, tr - 1)$ where $n_R \in [r - 1]$ and $t \in [s - 1]$.*

We call any configuration of the form given in Theorem 4.1 a *basic* configuration. Consider, for instance, the basic configuration with $n = 14, r = 5, n_R = 2, t = 1$ and $\mathcal{C} = (1, 3, 2, 3, 5, 4)$.

$$C_r + \Sigma(\mathcal{C}) = \begin{bmatrix}
1 & 1 & & & & & 1 & 1 & 1 & & & & & \\
& 1 & & & & 1 & 1 & 1 & 1 & & & & & \\
& & 1 & 1 & 1 & 1 & 1 & & & & & & & \\
& & & 1 & 1 & 1 & 1 & 1 & & & & & & \\
& & & & 1 & 1 & 1 & 1 & 1 & & & & & \\
& & 1 & 1 & 1 & 1 & & & & 1 & & & & \\
& & 1 & 1 & 1 & & & & & 1 & 1 & & & \\
& & & & & & & 1 & 1 & 1 & 1 & 1 & & \\
& & & & & & & & 1 & 1 & 1 & 1 & 1 & \\
& & & & & & & & & 1 & 1 & 1 & 1 & 1 \\
1 & & & & & & & & & & 1 & 1 & 1 & 1 \\
1 & 1 & & & & & & & & & & 1 & 1 & 1 \\
1 & 1 & 1 & & & & & & & & & & 1 & 1 \\
1 & 1 & 1 & 1 & & & & & & & & & & 1
\end{bmatrix}$$

Next we describe briefly the major steps of the proof of Theorem 4.1. The “if” part is easy to check using the dual B defined in Remark 4.3 below. The proof of the “only if” part consists of the following steps. Since A has level one it can be written as $C_r + x\ell^T$ where $x, \ell \in \{0, \pm 1\}^n$. We first show in Section 4.2 that x, ℓ have a simple structure, i.e. only a small number of parameters are needed to describe them. This result is refined in Section 4.3 where we show that x, ℓ define a special type of configuration. In Section 4.4 it is proved that there exists a bijection between the configurations for A and those for B (after isomorphism). The proof is completed after a brief case analysis in Section 4.5.

4.1. **Preliminaries.** In this section, the support of a 0,1 vector u will also be denoted by u, i.e. we use the same notation for a 0,1 vector and its support.

We say that (P, Q) define the *standard* (D_s, C_s)*-isomorphism* if P, Q are permutation matrices (of order n) such that for all indices i, $P(i, (i-1)r+1) = 1$ and $Q(i, is) = 1$.

Remark 4.2. $PD_sQ = C_s$.

Proof. By definition of D_s, $\text{row}_i(D_s) = \{i-1+tr : t \in [s]\}$. Since $Q(i, is) = 1$ and $rs = n+1$, it follows that $Q(ri, i) = 1$ for all indices i. Now $(PD_sQ)_{ij} = \text{row}_i(P) D_s \, \text{col}_j(Q) = D_s((i-1)r+1, rj)$ which is equal to 1 if and only if $rj = (i-1)r+1-1+tr$ for some $t \in [s]$. We can rewrite this last condition as $rj = r(i+t)$ where $t \in [0, s-1]$. Thus $j = i+t$ where $t \in [0, s-1]$, i.e. $j \in \text{row}_i(C_s)$. □

We say that a permutation matrix P defines a *simple* isomorphism if there exists $\delta \in [0, n-1]$ such that $P(i, i+\delta) = 1$ for all indices i. Observe that $PC_rP^T = C_r$. Let P, Q be the permutation matrices such that for all indices i, $P(i, n-i) = 1$ and $Q(i, n-i+r-1) = 1$. Then given $X \in M_n(\{0, \pm 1\})$, PXQ is called the *reverse* of X. Note that the reverse of C_r is C_r. Given a vector $x \in \{0, \pm 1\}^n$ the *reverse* of x is Px. We say that Q defines the *standard* (C_r^T, C_r)*-isomorphism* if $Q(i, i+r-1) = 1$ for all indices i. Note that $C_r^T Q = C_r$ and that the isomorphism maps column j to column $j+r-1$.

For the remainder of this section when we talk about A, B, we mean isomorphic copies PAQ, PBQ such that $\text{level}(A) = \text{rank}(PAQ - C_r)$ (and by Proposition 2.2, $\text{level}(A) = \text{level}(B) = \text{rank}(PBQ - D_s)$).

Remark 4.3. There are vectors $x, \ell, y, u \in \{0, \pm 1\}^n$ and $\Phi = \pm 1$ such that $A = C_r + x\ell^T$, $B = D_s + \Phi y u^T$ and $\ell = C_r^T y$, $x = C_r u$, $\Phi = -\frac{1}{1+x^T y}$. Moreover, $x^T e = \ell^T e = y^T e = u^T e = 0$.

Proof. Since A has level one, there exist vectors x, ℓ such that $A = C_r + x\ell^T$. Since A is r-regular $x^T e = \ell^T e = 0$. Define $y := C_r^{-T}\ell$ and $u := C_r^{-1}x$. By (2) we have $y = (D_s - \frac{1}{r}E)\ell = D_s\ell$ and $u = (D_s^T - \frac{1}{r}E)x = D_s^T x$. Moreover, $y^T e = \ell^T D_s^T e = \ell^T s e = 0$ and similarly we can show $u^T e = 0$. We have,

$$A = C_r + x\ell^T = (I + x\ell^T C_r^{-1})C_r = (I + xy^T)C_r.$$

Using Remark 6.2(1) and the above equation, we conclude that $\pm 1 = \det(I + xy^T) = 1 + x^T y$. Therefore, $x^T y \in \{0, -2\}$ and $\Phi = -\frac{1}{1+x^T y}$ is well-defined and is ± 1. Then it can be checked that $B = (I + \Phi y x^T)D_s$ (multiply AB^T and use the fact that $x^T e = y^T e = 0$). Thus

$$B = D_s + \Phi y x^T D_s = D_s + \Phi y u^T.$$

Since A is a $0,1$ matrix, we have $x\ell^T \in M_n(\{0, \pm 1\})$. Thus, we can choose $x, \ell \in \{0, \pm 1\}^n$. Since B is a $0,1$ matrix and $\Phi = \pm 1$, we must have $yu^T \in M_n(\{0, \pm 1\})$. We established above that $y = D_s\ell$ and $u = D_s^T x$. Since we have $x, \ell \in \{0, \pm 1\}^n$, y and u are integral vectors. Therefore, $y, u \in \{0, \pm 1\}^n$ as desired. □

Let (P, Q) define the standard (D_s, C_s)-isomorphism. Since $B = D_s + \Phi y u^T$ it implies that $PBQ = P(D_s + \Phi y u^T)Q = PD_sQ + P\Phi y u^T Q = C_s + (\Phi P y)(Q^T u)^T$. Define $\tilde{y} := \Phi P u$ and $\tilde{u} = Q^T u$ then $PBQ = C_s + \tilde{y}\tilde{u}^T$. Hence all results about x, ℓ and A apply to $\tilde{y}, \tilde{u}$ and PBQ. The notation $\ell, x, y, u, \Phi, \tilde{y}$ and $\tilde{u}$ will be used throughout the remainder of this section.

Remark 4.4. Suppose that ℓ_+ is a (j, j')-interval and that ℓ_- is a σ-shift of ℓ_+. Suppose that x_- is an (i, i')-interval and that x_+ is a ρ-shift of x_-. Then we can define two distinct configurations $\mathcal{C}, \mathcal{C}'$ from x and ℓ such that $x\ell^T = \Sigma(\mathcal{C}) = \Sigma(\mathcal{C}')$ where: $\mathcal{C} = (i, j, i' - i + 1, j' - j + 1, \rho, \sigma)$

with blocks $B_{11} = x_-\ell_+^T, B_{12} = x_-\ell_-^T, B_{21} = x_+\ell_+^T, B_{22} = x_+\ell_-^T$; and $\mathcal{C}' = (i+\rho, j+\sigma, i'-i+1, j'-j+1, n-\rho, n-\sigma)$ with blocks $B'_{11} = x_+\ell_-^T, B'_{12} = x_+\ell_+^T, B'_{21} = x_-\ell_-, B'_{22} = x_-\ell_+$.

Observe that $\mathcal{C}$ and $\mathcal{C}'$ are determined from x, ℓ and the choice of B_{11}. Thus, we will say that $\mathcal{C}$ is the (x,ℓ)-configuration with $B_{11} = x_-\ell_+$ and that $\mathcal{C}'$ is the (x,ℓ)-configuration with $B_{11} = x_+\ell_-$.

4.2. r**-structures.** We use the notion of vector shift given in the introduction. A vector in $\{0,\pm 1\}^n$ is a *type I, r-structure* if it is a shift of a vector v whose positive and negative parts are the intervals $v_+ = [1,q]$, $v_- = [1+tr, q+tr]$ where $q \in [r-1], t \in [s-1]$. A vector $v \in \{0,\pm1\}^n$ is a *Type II, r-structure* if v or $-v$ is a shift of a vector v' where $v'_+ = [1,q] \cup \{r\}$, $v'_- = [tr, q+tr]$ and $q \in [r-2], t \in [s-1]$. A vector in $\{0,\pm1\}^n$ is a *Type III, r-structure* if it is a shift of a vector v where $v_+ = [1,q] \cup \{r\}$, $v_- = [tr, q+tr-1] \cup \{q+(t-1)r\}$, where $q \in [r-2]$ and $t \in [s-1]$. The *order* of an r-structure v is given by the parameter t. If there exists an index δ such that δ and $\delta + r - 1$ are both indices of y_+ (resp. y_-) then $\{\delta, \delta+r-1\}$ form a *special pair* of y_+ (resp. y_-) and y_+ (resp. y_-) is *special*.

Lemma 4.5. *ℓ or its reverse is an r-structure of order $|y_+|$. Moreover, it is of type I if and only if neither y_+ nor y_- are special; it is of type II if and only if exactly one of y_+, y_- is special; it is of type III if both y_+ and y_- are special.*

Proof. Since A does not have level 0, x_-, x_+, ℓ_-, ℓ_+ are all non-empty.

Claim 1.

(1) *ℓ_+ (resp. ℓ_-) is contained in an interval of cardinality r.*
(2) *ℓ_+ (resp. ℓ_-) is not an interval of cardinality r.*

Proof. $A = C_r + x\ell^T \geq 0$. In particular, $C_r - x_-\ell_+^T \geq 0$, thus $\ell_+^T \subseteq \mathrm{row}_\alpha(C_r)$ for all $\alpha \in x_-$. This implies (1). Furthermore if ℓ_+ is an interval of size r, then x_- contains a unique element

α. Since $e^T x = 0$, x_+ contains a unique element β. As $C_r - x_+ \ell_-^T \geq 0$, and $\ell^T e = 0$, ℓ_- is an interval of size r. Then A is obtained from C_r by permuting the rows α, β, contradicting the fact that A has level 1. $\diamond$

Claim 2.

(1) *If* $\Phi = +1$ *then* $y_+ \subseteq \mathrm{col}_\delta(D_s)$, $\forall \delta \in u_-$. *If* $\Phi = -1$ *then* $y_+ \subseteq \mathrm{col}_\delta(D_s)$, $\forall \delta \in u_+$.

(2) *Consider* δ *such that* $y_+ \subseteq \mathrm{col}_\delta(D_s)$. *Then* $\forall i, j \in y_+$, $i \neq j$, $\mathrm{row}_i(C_r) \cap \mathrm{row}_j(C_r) \subseteq \{\delta\}$. *Moreover, "*$\subseteq$*" holds with "=" if and only if* $\{i, j\}$ *is a special pair of* y_+.

Proof. $D_s + \Phi y u^T \geq 0$. Suppose $\Phi = 1$ as the case $\Phi = -1$ is similar. Then $D_s - \Phi y_+ u_-^T \geq 0$ which implies (1). Consider δ such that $y_+ \subseteq \mathrm{col}_\delta(D_s)$. We have $E + I = C_r^T D_s$ thus $e + e_\delta = C_r^T \mathrm{col}_\delta(D_s) \geq C_r^T y_+ = \sum_{i \in y_+} \mathrm{row}_i(C_r)$. Moreover, if $\delta \in \mathrm{row}_i(C_r) \cap \mathrm{row}_j(C_r)$ then i, j must be a special pair. This implies (2). $\diamond$

We define,

$$P := \sum_{i \in y_+} \mathrm{row}_i(C_r) \qquad \text{and} \qquad N := \sum_{i \in y_-} \mathrm{row}_i(C_r).$$

Then $\ell^T = y^T C_r = P - N$. Let $\mathcal{P}$ denote the support of P and let $\mathcal{N}$ denote the support of N. We will show that $\mathcal{P}$ and $\mathcal{N}$ are both intervals. Partition $\mathcal{P}$ into maximal intervals $P_1, \ldots, P_\alpha$ and partition $\mathcal{N}$ into maximal intervals $N_1, \ldots, N_\beta$.

We say that sets $S, T \subseteq [n]$ *cross* if $S \setminus T$ and $T \setminus S$ are both non-empty.

Claim 3. P_i, N_j *cross for every pair* $i \in [\alpha], j \in [\beta]$.

Proof. Suppose P_i, N_j do not cross. We consider the case where $P_i \supseteq N_j$ as the case $P_i \subseteq N_j$ can be proved in the same way. For some indices a, b, c, d, $P_i = [a, b]$ and $N_j = [c, d]$. Since $\mathrm{row}_a(C_r) = [a, a + r - 1]$, $a \in y_+$. Since $\mathrm{row}_c(C_r) = [c, c + r - 1]$, $c \in y_-$. As $y_+ \cap y_- = \emptyset$, $a \neq c$. We omit the proof that $b \neq d$ as it is similar. Consider indices $a' = c - 1$ and $b' = d + 1$.

Then $\{a', b'\} \in \ell_+$. By Claim 1, a', b' are contained in an interval S of size at most r. Since N_j is a union of rows of C_r, $|N_j| \geq r$. Hence we may assume $S = [b', a']$. Since $\ell_- \neq \emptyset$, there exists $N_{j'}$ where $j \neq j' \in [\beta]$. But $N_{j'} \subseteq S \setminus \{a', b'\}$. A contradiction as $|N_{j'}| \geq r$. $\diamond$

Claim 4. *$\mathcal{P}$ and $\mathcal{N}$ are both intervals.*

Proof. Suppose for a contradiction $\mathcal{P}$ or $\mathcal{N}$ is not an interval. If $\mathcal{N}$ is not an interval, relabel ℓ by $-\ell$ and x by $-x$ (as $A = C_r + x\ell^T = C_r + (-x)(-\ell)^T$). Then $\mathcal{P}$ becomes $\mathcal{N}$ and vice-versa. Thus, we may assume there exist P_{i_1}, P_{i_2} where $i_1, i_2 \in [\alpha]$ and $i_1 \neq i_2$. Since $|P_{i_1}| \geq r$, Claim 1 implies that there exists $j_1 \in [\beta]$ such that $P_{i_1} \cap N_{j_1} \neq \emptyset$. Similarly, there exists $j_2 \in [\beta]$ such that $P_{i_2} \cap N_{j_2} \neq \emptyset$. Note that N_{j_1}, N_{j_2} need not be distinct. There exist indices $a_1, b_1, a_2, b_2, c_1, d_1, c_2, d_2$ such that $P_{i_1} = [a_1, b_1], P_{i_2} = [a_2, b_2], N_{j_1} = [c_1, d_1], N_{j_2} = [c_2, d_2]$. Since P_{i_1}, N_{j_1} cross (by Claim 3) exactly one of c_1, d_1 is in P_{i_1}. We may assume $c_1 \in P_{i_1}$ for otherwise we consider the reverse of A instead of A, this exchanges the roles of c_1 and d_1. Since P_{i_2}, N_{i_2} cross, exactly one of c_2, d_2 is in P_{i_2}. Thus there are two cases: (1) $c_2 \in P_{i_2}$ and (2) $d_2 \in P_{i_2}$.

Consider case (1). Note $N_{j_1} \neq N_{j_2}$. Then $c_1 - 1,\ c_2 - 1 \in \ell_+$. Claim 1 implies that $c_1 - 1, c_2 - 1$ are contained in an interval S of cardinality r. But S must contain strictly one of N_{j_1} or N_{j_2}. A contradiction as $|N_{j_1}|, |N_{j_2}| \geq r$.

Consider case (2). Note $c_1 - 1,\ d_2 + 1 \in \ell_+$. Claim 1 implies $c_1 - 1,\ d_2 + 1$ are contained in an interval S of cardinality r. Similarly, $b_1 + 1,\ a_2 - 1 \in \ell_-$ implies $b_1 + 1,\ d_2 - 1$ are in an interval S' of cardinality r. Then $S \cup S' \cup (N_{j_1} \setminus \{b_1 + 1\}) \cup (N_{j_2} \setminus \{a_2 - 1\}) \supseteq [n]$. Hence, $2r + |N_{j_1}| + |N_{j_2}| - 2 \geq n = rs - 1$, i.e. $|\mathcal{N}| \geq |N_{j_1}| + |N_{j_2}| \geq (s-2)r + 1$. It follows that $|y_-| \geq s - 1$. If $|y_+| = |y_-| = s$ then it can be readily checked that B is obtained from D_s by permuting two columns, a contradiction as this implies B (hence A) has level zero. Thus $|y_+| = |y_-| = s - 1$. Claim 2(1) implies that there exists an index δ such that $y_+ \subseteq \mathrm{col}_\delta(D_s)$.

Let i be the unique element in $\mathrm{col}_\delta(D_s) \setminus y_+$. Then $P = e + e_\delta - \mathrm{row}_i(C_r)$. Since P decomposes into at least two intervals P_{i_1}, P_{i_2}, we must have $\delta \in \mathrm{row}_i(C_r)$ with $i < \delta < i + r - 1$, i.e. one of the intervals P_{i_1}, P_{i_2} is $\{\delta\}$. But this contradicts $|P_{i_j}| \geq r$ for all $j \in [\alpha]$. It follows that $\mathcal{P}$ is an interval. Similarly $\mathcal{N}$ is an interval. ◇

By Claim 4, there are indices a, b, c, d such that $\mathcal{P} = [a, b]$ and $\mathcal{N} = [c, d]$. Since $|\mathcal{P}| \geq r$, Claim 1 implies that $\mathcal{P} \cap \mathcal{N} = \emptyset$. Since by Claim 3, $\mathcal{P}$ and $\mathcal{N}$ cross, exactly one of c, d is in $\mathcal{P}$. If $d \in \mathcal{P}$ then consider the reverse of A instead of A. This will exchange the roles of c and d, proving the result for the reverse of ℓ. As the statement is symmetric with respect to ℓ and its reverse, this is acceptable. Thus, we may assume $c \in \mathcal{P}$ and $d \notin \mathcal{P}$. Let $t := |y_+| = |y_-|$. Label elements in y_+ by $\{i_1, \ldots, i_t\}$ and elements in y_- by $\{j_1, \ldots, j_t\}$. We may assume that, starting from a and ending at b, we visit rows $i_1, \ldots, i_t$ of C_r when following the cyclic ordering. Similarly, starting from c and ending at d, we visit rows $j_1, \ldots, j_t$ of C_r when following the cyclic ordering.

Claim 5.

(1) *if* y_+ *is special then* $\mathrm{row}_{i_1}(C_r) \cap \mathrm{row}_{i_2}(C_r) = \{a + r - 1\}$,

(2) *if* y_- *is special then* $\mathrm{row}_{j_{t-1}}(C_r) \cap \mathrm{row}_{j_t}(C_r) = \{d - r + 1\}$.

Proof. Suppose y_+ is special. Claim 2(2) implies that for some $p \in [t-1]$, $\mathrm{row}_{i_p}(C_r) \cap \mathrm{row}_{i_{p+1}}(C_r) \neq \emptyset$. The unique element common to these rows is $a + rp - 1$. Since $P(a + rp - 1) = 2$, $a + rp - 1 \in \ell_+$. Since $a \in \ell_+$, Claim 1 implies that $\{a, a + rp - 1\}$ is contained in an interval S of size r. Thus S does not contain $\mathrm{row}_{i_{p+1}}(C_r)$. It follows that $a \in \mathrm{row}_{i_p}(C_r)$, i.e. $p = 1$. Then clearly $\mathrm{row}_{i_1}(C_r) \cap \mathrm{row}_{i_2}(C_r) = \{a + r - 1\}$. This proves (1). The proof for (2) can be obtained by considering the reverse of A. ◇

Since r-structures are invariant under shifting we may assume $a = 1$. Let $q := c - 1$, then $[1, q] \subseteq \ell_+$ and $[b + 1, d] \subseteq \ell_-$.

In the remainder of the proof we consider cases depending on whether y_+ and y_- are special.

Case 1. *Neither y_+ nor y_- are special.*

Then $\ell_+ = [1, q]$ and $\ell_- = [b+1, d]$. Since rows $i_1, \dots, i_t$ of C_r are disjoint, $b + 1 = 1 + tr$ and $d = q + tr$. Hence, $\ell_- = [1 + tr, q + tr]$ and ℓ is a type I, r-structure.

Case 2. *Both y_+, y_- are special.*

By Claim 5, $\mathrm{row}_{i_1}(C_r) \cap \mathrm{row}_{i_2}(C_r) = \{r\}$, and $\mathrm{row}_{j_{t-1}}(C_r) \cap \mathrm{row}_{j_t}(C_r) = \{d - r + 1\}$. Then $\ell_+ = [1, q] \cup \{r\}$, $\ell_- = [b + 1, d] \cup \{d - r + 1\}$. Note $q \in [r - 1]$. But $q \neq r - 1$ because of Claim 1. Since rows i_1, i_2 of C_r intersect exactly in one position and since all other pairs of rows among $i_1, \dots, i_t$ are disjoint, $b + 1 = 1 + (tr - 1) = tr$ and $d = q + (tr - 1)$. Thus $\ell_- = [tr, q + tr - 1] \cup \{q + (tr - 1) - r + 1\}$ where $q + (tr - 1) - r + 1 = q + (t - 1)r$. Hence ℓ is a type III, r-structure.

Case 3. *y_+ is special and y_- is not special.*

By Claim 5, $\mathrm{row}_{i_1}(C_r) \cap \mathrm{row}_{i_2}(C_r) = \{r\}$. Then $\ell_+ = [1, q] \cup \{r\}$, and $\ell_- = [b + 1, d]$. By the same argument as in Case 2, $b + 1 = tr$. Then $d = q + tr$ (as we must have $|\ell_+| = |\ell_-|$). Thus $\ell_- = [tr, q + tr]$. Hence ℓ is an type II, r-structure.

Case 4. *y_+ is not special and y_- is special.*

We want to show ℓ is a type II, r-structure. Since if ℓ is a type II, r-structure, so is $-\ell$, we redefine ℓ by $-\ell$ and x by $-x$. This exchanges the roles of $\mathcal{P}$ and $\mathcal{N}$. But now $d \in \mathcal{P}$ and $c \notin \mathcal{P}$, so we consider the reverse of A instead of A. As we exchanged y for $-y$ we are in Case 3. $\square$

4.3. **Block configuration.** The goal of this section is to prove:

Lemma 4.6. *Let A be a level one matrix. Then $A = C_r + \Sigma(\mathcal{C})$ where $\mathcal{C}$ is a configuration $(i, j, n_R, n_C, tr, t'r - \delta)$. where $t, t' \in [s-1]$ and $\delta \in \{0, 1\}$.*

Given $S \subseteq [n] \times [n]$ we define $\mathrm{val}(S)$ to be $|S \cap D_s|$.

Remark 4.7. $x^T y = -\,\mathrm{val}(x_- \ell_+^T) - \mathrm{val}(x_+ \ell_-^T) + \mathrm{val}(x_+ \ell_+^T) + \mathrm{val}(x_- \ell_-^T) \in \{0, -2\}$.

Proof. Since $\ell = C_r^T y$,

$$x^T y = x^T C_r^{-T} \ell = x^T (D_s - \frac{1}{r} E)\ell = x^T D_s \ell$$

$$= -\, x_-^T D_s \ell_+ - x_+^T D_s \ell_-^T + x_+^T D_s \ell_+ + x_-^T D_s \ell_-$$

$$= -\,\mathrm{val}(x_- \ell_+^T) - \mathrm{val}(x_+ \ell_-^T) + \mathrm{val}(x_+ \ell_+^T) + \mathrm{val}(x_- \ell_-^T).$$

Remark 4.3 states that $\Phi = -\frac{1}{1+x^T y} = \pm 1$. Thus $x^T y \in \{0, -2\}$ and the result holds. □

Let $S, S' \subseteq [n] \times [n]$. We say that S' is a *horizontal translation* of S if S' is a $(0, tr)$-shift of S where $t \in [s-1]$ and $\forall (i, j) \in S$ the numbers $j, i, i + r - 1, j + tr$ do not appear in that cyclical order (note these numbers need not be all distinct). We say that S' is a *vertical translation* of S if S' is a $(tr, 0)$-shift of S where $t \in [s-1]$ and $\forall (i, j) \in S$ the numbers $i, j - r + 1, j, i + tr$ do not appear in that cyclical order.

Remark 4.8. If S' is a horizontal (resp. vertical) translation of S then $\mathrm{val}(S') = \mathrm{val}(S)$.

Proof. Let S' be a horizontal translation of S. Then S is a $(0, tr)$-shift of S. Then $(i, j) \in S$ if and only if $(i, j + tr) \in S'$. Moreover, $(i, j) \in D_s$ if and only if $(i, j + tr) \in D_s$ since $\mathrm{row}_i(D_s) = \{i, i + r - 1, \ldots, i + (s-1)r - 1\}$. The case for vertical translations is similar. □

Remark 4.9. Let S, S' be intervals. Then S' is a tr-shift of S for some $t \in [s-1]$ if and only if S is a $(t'r - 1)$-shift of S' where $t' = s - t \in [s-1]$.

Proof. S' is a tr-shift of S if and only if S is an $(n-tr)$-shift of S' and $n - tr = rs - 1 - tr = t'r - 1$. $\square$

Given $S \subseteq [n] \times [n]$ and $(i,j) \in [n] \times [n]$ we abbreviate $S \setminus \{(i,j)\}$ by $S \setminus (i,j)$.

Lemma 4.10. *ℓ is not a type II, r-structure.*

Proof. Suppose for a contradiction, ℓ is a type II, r-structure. By considering either x or ℓ or $-x, -\ell$ and A or its reverse we may assume (after a simple isomorphism) that $\ell_+ = [1,q] \cup \{r\}$, that $\ell_- = [tr, q+tr]$, and that $q \in [r-2], t \in [s-1]$. Since the smallest interval containing ℓ_+ has cardinality r, $|x_-| = |x_+| = 1$ and $x_- = \{1\}$. Applying Lemma 4.5 to A^T, it follows that x or its reverse is a type I, r-structure. Let χ be the unique element in x_+. Remark 4.9 implies that $\chi = 1 + t'r - \delta$ where $t' \in [s-1]$ and $\delta \in \{0,1\}$ ($\delta = 1$ corresponds to the case where x is a Type I, r-structure; $\delta = 0$ corresponds to the case where the reverse of x is).

Claim. $t = t'$ *and* $\delta = 1$.

Proof. $\mathrm{row}_\chi(C_r) = [1 + t'r - \delta, (t'+1)r - \delta]$. Since $C_r - x_+\ell_-^T \geq 0$, $\ell_-^T \subseteq \mathrm{row}_\chi(C_r)$. Thus, (1) $tr \geq 1 + t'r - \delta$ and (2) $q + tr \leq (t'+1)r - \delta$. We write (2) as $t \leq t' + 1 - \frac{1}{r}(\delta + q)$. Hence $t \leq t'$. We write (1) as $t \geq t' + \frac{1}{r}(1-\delta)$. As $t \leq t'$ this implies $t = t'$ and $\delta = 1$. $\diamond$

The claim implies that $\chi = tr$. Remark 4.9 implies that $x_-\ell_-^T$ is a $((s-t)r, 0)$-shift of $x_+\ell_-^T$. It follows that $x_-\ell_-^T$ is a vertical translation of $x_+^T\ell_-^T$. Hence by Remark 4.7 $\mathrm{val}(x_+\ell_-^T) = \mathrm{val}(x_-\ell_-^T)$. Similarly $x_-\ell_+^T \setminus (1,1)$ is a vertical translation of $x_+\ell_+^T \setminus (tr, 1)$. Hence $\mathrm{val}(x_-\ell_+^T \setminus (1,1)) = \mathrm{val}(x_+\ell_+^T \setminus (tr,1))$. Moreover, $(1,1) \in D_s$ and $(tr,1) \notin D_s$. Thus $\mathrm{val}(x_+\ell_+^T) = \mathrm{val}(x_-\ell_+^T) - 1$. It follows that $-\mathrm{val}(x_-\ell_+^T) - \mathrm{val}(x_+\ell_-^T) + \mathrm{val}(x_+\ell_+^T) + \mathrm{val}(x_-\ell_-^T) = -1$, a contradiction to Remark 4.7. $\square$

A *simple*-$C4$ is the matrix $\Sigma(\mathcal{C})$ where $\mathcal{C}$ is the configuration $(1,1,1,1,tr,(t+1)r-1)$. A *twin*-$C4$ is the matrix $x\ell^T$ where $\ell_+ = \{1\} \cup \{r\}$, $\ell_- = \{tr\} \cup \{(t-1)r+1\}$ and $x_- = \{1\}$, $x_+ = \{(t-1)r+1\}$ where $t \in [2, s-1]$. The *order* of the twin-$C4$ is given by t.

Remark 4.11. Suppose $A = C_r + \Gamma$ where Γ is a twin-$C4$ of order 2, or a simple-$C4$. Then A is isomorphic to $C_r + \Sigma(\mathcal{C})$ where $\mathcal{C}$ is a basic configuration.

Proof. By permuting columns r and $r+1$ of a twin-$C4$ of order 2 we obtain a simple-$C4$. By permuting rows 1 and $tr+1$ of a simple twin-$C4$ we obtain $\Sigma(\mathcal{C})$ where $\mathcal{C} = (1,2,1,r-1,tr,tr-1)$. □

Lemma 4.12. *Suppose ℓ is a type III, r-structure. Then after a simple isomorphism (x,ℓ) defines a twin-$C4$ of order $|y_+| \geq 2$.*

Proof. ¿From the hypothesis we may assume $\ell_+ = [1,q] \cup \{r\}$, and $\ell_- = [tr, q+tr-1] \cup \{q+(t-1)r\}$. Proceeding as in the proof of Lemma 4.10 we show that $x_- = \{1\}$ and x_+ consists of a single element χ where $\chi = 1 + t'r - \delta$ where $t' \in [s-1]$ and $\delta \in \{0,1\}$.

Claim. *$t' = t-1, \delta = 0$, and $q = 1$.*

Proof. Since $C_r - x_+\ell_-^T \geq 0$, $\ell_-^T \subseteq \text{row}_\chi(C_r) = [1+t'r-\delta, (t'+1)r-\delta]$ and the following relation must hold: $q + (t-1)r \geq 1 + t'r - \delta$ and $q + tr - 1 \leq (t'+1)r - \delta$. We can rewrite these relations as: $t - 1 \geq t' - \frac{1}{r}(q+\delta-1)$ and $t-1 \leq t' - \frac{1}{r}(q+\delta-1)$. It follows that $t - 1 = t' - \frac{1}{r}(q+\delta-1)$. Since t an integer, $q+\delta-1$ is a multiple of r. But $1 \leq q \leq r-2$ and $0 \leq \delta \leq 1$. It follows that $q+\delta-1 = 0$ hence $q = 1$ and $\delta = 0$. Then $t' = t-1$. ◇

The result follows immediately from the claim. □

Consider a $(t,q;t',q')$-block D. We use the following notation: $^\ulcorner D = (t,q)$, $D^\urcorner = (t,q')$, $_\llcorner D = (t',q)$ and $D_\lrcorner = (t',q')$. We say that $^\ulcorner D, D^\urcorner, {}_\llcorner D$ and $D_\lrcorner$ are the *corners* of D.

Lemma 4.13. *If $A^T = C_r + \Sigma(\mathcal{C})$ where $\mathcal{C}$ is a basic configuration, then A is isomorphic to $C_r + \Sigma(\mathcal{C}')$ where $\mathcal{C}'$ is a basic configuration.*

Proof. Suppose $A^T = C_r + \Sigma(\mathcal{C})$ where $\mathcal{C} = (1, 1 + n_R, n_R, r - n_R, tr, tr - 1)$ where $n_R \in [r-1]$ and $t \in [s-1]$. Let $B_{11}, B_{12}, B_{21}, B_{22}$ be blocks of $\mathcal{C}$. Then the support of $\Sigma(\mathcal{C})^T$ can be partitioned into blocks $B_{11}^T, B_{12}^T, B_{21}^T, B_{22}^T$. Define $B'_{11} = B_{22}^T$, $B'_{12} = B_{12}^T$, $B'_{21} = B_{21}^T$ and $B'_{22} = B_{11}^T$. B_{22} is a $(0, tr-1)$-shift of B_{21} in $\Sigma(\mathcal{C})$. Remark 4.9 implies that B_{21} is a $(0, (s-t)r)$-shift of B_{22} in $\Sigma(\mathcal{C})$. Thus $B_{21}^T = B'_{21}$ is an $((s-t)r, 0)$-shift of $B_{22}^T = B'_{11}$ in $\Sigma(\mathcal{C})^T$. B_{22} is a $(tr, 0)$-shift of B_{12}. Remark 4.9 implies that B_{12} is a $((s-t)r - 1, 0)$-shift of B_{22} in $\Sigma(\mathcal{C})$. Thus $B_{12}^T = B'_{12}$ is a $(0, (s-t)r - 1)$-shift of $B_{22}^T = B'_{11}$ in $\Sigma(\mathcal{C})^T$. Block $B'_{11} = B_{22}^T$ has $r - n_R$ rows and n_R columns. Let Q define the standard (C_r^T, C_r)-isomorphism and let P define the simple isomorphism mapping row $n_R + tr$ to row 1. Then $PAQP^T = C_r + P\Sigma(\mathcal{C})^T QP^T = C_r + \Sigma(\mathcal{C}')$ where $\mathcal{C}' = (1, 1 + (r - n_R), r - n_R, n_R, (s-t)r, (s-t)r - 1)$ as $B'_{11} = (1, (1 + tr) + (r-1) - (n_R + tr - 1))$ where $r - 1$ arises from Q and $-(n_R - tr - 1)$ arises from P. Observe that $\mathcal{C}'$ is basic. □

Proof of Lemma 4.6. Lemma 4.5 implies that ℓ or its reverse is an r-structure. Let Q be the permutation matrix which defines the standard (C_r^T, C_r)-isomorphism. Theorem 2.1 implies that A^T is a Lehman matrix. We have $A^T = C_r^T + \ell x^T$ thus $A^T Q = C_r^T Q + \ell x^T Q = C_r + \ell(Q^T x)^T$. Note that $Q^T x$ is an $(r-1)$-shift of x. Lemma 4.5 implies that x or the reverse of x is an r-structure. Lemma 4.10 implies that none of ℓ, x, or the reverse of ℓ or x are type II, r-structures.

Suppose ℓ or its reverse is a type I, r-structure. Consider the case where x is a type I, r-structure. Then x_- is a tr-shift of x_+. Let $\mathcal{C}$ be the configuration defined by (x, ℓ) with $B_{11} = x_+ \ell_-^T$ (see Remark 4.4). Remark 4.9 implies that ℓ_+ is a $(t'r - \delta)$-shift of ℓ_- where $t' \in [s-1]$ and $\delta \in \{0, 1\}$. Then $\mathcal{C}$ is as required in the statement of Lemma 4.6. Consider the case where the reverse of x is a type I, r-structure. Then x_+ is a tr-shift of x_-. Let $\mathcal{C}$ be the configuration defined by (x, ℓ) with $B_{11} = x_- \ell_+^T$. Remark 4.9 implies that ℓ_- is a $(t'r - \delta)$-shift of ℓ_+ where $t' \in [s-1]$ and $\delta \in \{0, 1\}$. Then $\mathcal{C}$ is as required in Lemma 4.6.

Thus one of the following holds: (1) neither ℓ nor its reverse is a type I, r-structure, (2) neither x nor its reverse is a type I, r-structure. We will show that if (1) holds then $A = C_r + \Sigma(\mathcal{C})$ where $\mathcal{C}$ is a basic configuration. If (2) holds, then, using the same argument (applied to A^T instead of A, x instead of ℓ, and ℓ instead of x) we also obtain that $A^T = C_r + \Sigma(\mathcal{C}')$ where $\mathcal{C}'$ is basic. But then Lemma 4.13 implies that $A = C_r + \Sigma(\mathcal{C})$ where $\mathcal{C}$ is basic. Thus Theorem 4.1 holds for A and so does the weaker Lemma 4.6.

Hence it suffices to consider that (1) holds. Thus ℓ or its reverse is a type III, r-structure. We can assume we are in the former case, for if we are in the latter one, it suffices to consider $-\ell$ and $-x$ instead of ℓ and x. Lemma 4.12 implies that (x, ℓ) defines a twin-$C4$ of order $|y_+|$. Let (P, Q) define the standard (D_s, C_s)-isomorphism. Remarks 4.2 and 4.3 imply that $PBQ = C_s + \tilde{y}\tilde{u}^T$.

Claim. *$\tilde{y}_+$ is not an interval of cardinality $\leq s - 1$.*

Proof. Lemma 4.5 implies that y_+ is special, i.e. there exists an index δ such that $\delta, \delta + r - 1 \in y_+$. We have $\tilde{y} = \Phi P y$ where $P(i, (i-1)r + 1) = 1$ for all indices i or equivalently $P(si, i) = 1$ for all indices i. As $\delta, \delta + r - 1 \in y_+$, Py contains elements, $s\delta, s\delta + sr - s = s\delta - s + 1$. Thus the smallest interval containing $\tilde{y}_+$ has cardinality at least s. $\diamond$

Lemma 4.5 applied to PBQ and its transpose implies that $\tilde{y}, \tilde{u}$ are s-structures or their reverse (note the reverse of a type III s-structure is equal to the inverse of a type III s-structure). Lemma 4.10 implies that $\tilde{y}$ is not of type II. Because of the claim, $\tilde{y}$ is not of type I either. Hence $\tilde{y}$ is of type III and Lemma 4.12 implies that $(\tilde{u}, \tilde{y})$ define a twin-$C4$ of $(PBQ)^T$. In particular $|\tilde{y}_+| = |y_+| = 2$. Hence (x, ℓ) is a twin-$C4$ of order 2. Then Remark 4.11 completes the proof. $\square$

4.4. **Block configurations in the dual.** The goal of this section is to prove the following result.

Lemma 4.14. *Suppose $A = C_r + \Sigma(\mathcal{C})$ where $\mathcal{C}$ is a configuration $(i, j, n_R, n_C, tr, t'r - \delta)$ where $t, t' \in [s-1]$ and $\delta \in \{0, 1\}$. Let (P, Q) define the standard (D_s, C_s)-isomorphism. Then $PBQ = C_s + \Sigma(\mathcal{C}')$ where $\mathcal{C}'$ has the following parameters:*

(1) *If $\Phi = +1$ and $\delta = 0$ then $\mathcal{C}' = (\tilde{\jmath}, \tilde{\imath}, t', t, n_C s, n_R s)$,*

(2) *If $\Phi = -1$ and $\delta = 0$ then $\mathcal{C}' = (\tilde{\jmath}, \tilde{\imath} + n_R s, t', t, n_C s, (r - n_R)s - 1)$,*

(3) *If $\Phi = +1$ and $\delta = 1$ then $\mathcal{C}' = (\tilde{\jmath} - (s - t'), \tilde{\imath} + n_R s, s - t', t, n_C s, (r - n_R)s - 1)$,*

(4) *If $\Phi = -1$ and $\delta = 1$ then $\mathcal{C}' = (\tilde{\jmath} - (s - t'), \tilde{\imath}, s - t', t, n_C s, n_R s)$,*

where $\tilde{\imath} = (i-1)s + 1$ and $\tilde{\jmath} = (j-1)s + 1$.

We will need a number of preliminary results.

Lemma 4.15. *Suppose (P, Q) defines the standard (D_s, C_s)-isomorphism. Let v be an (a, b)-interval and $|v| \le r - 1$. Let $\tilde{a} = (a-1)s + 1$ and let $\tilde{b} = bs$. Then*

(1) *$PD_s v$ is an $(\tilde{a}, \tilde{b})$-interval,*

(2) *$Q^T D_s^T v$ is an $(\tilde{a}, \tilde{b})$-interval.*

Proof. Consider part (1). Note $PD_s Q = C_s$, thus $PD_s = C_s Q^T$ which implies that $PD_s v = C_s Q^T v$. Since $Q(i, si) = 1$, $\mathrm{col}_i(C_s Q^T) = \mathrm{col}_{si}(C_s)$. Thus $C_s Q^T v = \sum_{i \in v} \mathrm{col}_{si}(C_s)$. Note $\mathrm{col}_{si}(C_s) = [(i-1)s + 1, is]$. Thus for any index i, $\mathrm{col}_{si}(C_s) \cap \mathrm{col}_{s(i+1)}(C_s) = \emptyset$ and $\mathrm{col}_{si}(C_s) \cup \mathrm{col}_{s(i+1)}(C_s)$ forms an interval. It follows that $C_s Q^T v$ is the required interval.

Consider part (2). Note $Q^T D_s^T P^T = C_s^T$, thus $Q^T D_s^T = C_s^T P$ which implies that $Q^T D_s^T v = C_s^T P v$. Since $P(i, (i-1)r+1) = 1$ we have that $P(is, i-1+s) = 1$ and $P((i-1)s+1, i) = 1$ for all indices i. Hence $\mathrm{row}_i(C_s^T P) = \mathrm{row}_{(i-1)s+1}(C_s) = [(i-1)+1, is]$ and $Q^T D_s^T v = C_s^T P v = \sum_{i \in v} \mathrm{row}_{(i-1)s+1}(C_s)$. Proceed now as in part (1). □

Lemma 4.16. *Let $t, \Delta \in [s-1]$ and $a \in [n]$ and let $\delta \in \{0, 1\}$. Suppose ℓ_+ is an $(a, a + \Delta - 1)$-interval and ℓ_- is a $(tr - \delta)$-shift of ℓ_+. Define y by $\ell = C_r^T y$ and let $\tilde{a} = (a-1)s + 1$.*

(1) *If* $\delta = 0$ *then* $(Py)_+ = [\tilde{a}, \tilde{a} + t - 1]$ *and* $(Py)_-$ *is a* Δs*-shift of* $(Py)_+$.

(2) *If* $\delta = 1$ *then* $(Py)_- = [\tilde{a} - (s + t), \tilde{a} - 1]$ *and* $(Py)_+$ *is a* Δs*-shift of* $(Py)_-$.

(3) *Statement (1) remains true if we replace* ℓ *by* x', y *by* u' *and* Py *by* $Q^T u'$ *where* $x' = C_r u'$.

Proof. Consider part (1). We have $\ell = C_r^T y$. Thus $y = C_r^{-T}\ell = (D_s - \frac{1}{r}E)\ell = D_s\ell$ where the last equality follows from the fact that ℓ is 0-regular. Define $\mathcal{P} = PD_s\ell_+$ and $\mathcal{N} = PD_s\ell_-$. Since $\ell = \ell_+ - \ell_-$ it follows that $Py = PD_s\ell_+ - PD_s\ell_- = \mathcal{P} - \mathcal{N}$. Applying Lemma 4.15(1) we obtain that $\mathcal{P} = [\tilde{a}, \tilde{b}]$ where $\tilde{a} = (a-1)s+1$ and $\tilde{b} = (a+\Delta-1)s = \tilde{a} + \Delta s - 1$. Applying Lemma 4.15(1) we also obtain that $\mathcal{N} = [\tilde{a}', \tilde{b}']$ where $\tilde{a}' = (a + tr - 1)s + 1 = \tilde{a} + trs = \tilde{a} + t$ and $\tilde{b}' = (a + \Delta - 1 + tr)s = \tilde{b} + t = (\tilde{a} + \Delta s - 1) + t$. Hence, $\mathcal{N}$ is a t-shift of $\mathcal{P}$. Since $t < s$, $\emptyset \neq \mathcal{P} \cap \mathcal{N} = [\tilde{a} + t, \tilde{b}]$. It follows that $(Py)_+ = \mathcal{P} - \mathcal{N} = [\tilde{a}, \tilde{a} + t - 1]$ and $(Py)_- = \mathcal{N} - \mathcal{P} = [\tilde{b} + 1, \tilde{b} + t] = [\tilde{a} + \Delta s, \tilde{a} + \Delta s + t - 1]$. Hence (1) holds.

Consider case (2). We define $\mathcal{P}$ and $\mathcal{N}$ in the same manner as in case (1). Applying Lemma 4.15(1) to $\mathcal{P}$ we obtain that (as in case (1)) $\mathcal{P} = [\tilde{a}, \tilde{b}]$ where $\tilde{b} = \tilde{a} + \Delta s - 1$. Applying Lemma 4.15(1) to $\mathcal{N}$ we obtain that $\mathcal{N} = [\tilde{a}', \tilde{b}']$ where $\tilde{a}' = (a + tr - 1 - 1)s + 1 = \tilde{a} + t - s$ and $\tilde{b}' = (a + \Delta - 1 + tr - 1)s = \tilde{a} + \Delta s - 1 - (s - t) = \tilde{b} - (s - t)$. Thus $\mathcal{N}$ is a $(t - s)$-shift of $\mathcal{P}$. As $t \leq s$, $\mathcal{P} \cap \mathcal{N} = [\tilde{a}, \tilde{b} - (s - t)]$. It follows that $(Py)_- = \mathcal{N} \setminus \mathcal{P} = [\tilde{a} - (s - t), \tilde{a} - 1]$ and $(Py)_+ = \mathcal{P} \setminus \mathcal{N} = [\tilde{a} - (s - t), \tilde{a} - 1]$ and $(Py)_+ = \mathcal{P} \setminus \mathcal{N} = [\tilde{b} - (s - t) + 1, \tilde{b}] = [\tilde{a} + \Delta s - (s - t), \tilde{a} + \Delta s - 1]$. This proves (2).

Consider case (3). We have $x' = C_r u'$, thus $u' = C_r^{-1}x' = (D_s^T - \frac{1}{r}E)x' = D_s^T x'$. Define $\mathcal{P} = Q^T D_s^T x'_+$ and $\mathcal{N} = Q^T D_s^T x'_-$. Since $x' = x'_+ - x'_-$ it follows that $Q^T u' = Q^T D_s^T x'_+ - Q^T D_s^T x'_- = \mathcal{P} - \mathcal{N}$. Using Lemma 4.15(2) we obtain that $\mathcal{P}, \mathcal{N}$ are the same intervals that as in part (1). The proof now proceeds in the same way. □

We are now ready for the main result of this section.

Proof of Lemma 4.14. We have $\mathcal{C} = (i, j, n_R, n_C, tr, t'r - \delta)$ and $\Sigma(\mathcal{C}) = x\ell^T$ for some $x, \ell \in \{0, \pm 1\}^n$. We can choose x, ℓ such that $x_- = [i, i + n_R - 1]$, x_+ is a tr-shift of x_-; $\ell_+ = [j, j + n_C - 1]$, ℓ_- is a $(t'r - \delta)$-shift of ℓ_+. Recall that $\Sigma(\mathcal{C}') = \tilde{y}\tilde{u}^T$ where $\tilde{y} = \Phi P y$ and $\tilde{u} = Q^T u$. Let $x' = -x$ and $u' = -u$. Since $x = C_r u$, $x' = C_r u'$. Lemma 4.16(3) implies that $(Q^T u')_+ = \tilde{u}_- = [\tilde{\imath}, \tilde{\imath} + t - 1]$ and $(Q^T u')_- = \tilde{u}_+$ is a $n_R s$-shift of u_- where $\tilde{\imath} = (i-1)s + 1$.

Consider part (1), i.e $\Phi = 1, \delta = 0$. Then the relation $\tilde{y} = Py$ and Lemma 4.16(1) imply that $\tilde{y}_+ = (Py)_+ = [\tilde{\jmath}, \tilde{\jmath} + t' - 1]$ and $\tilde{y}_- = (Py)_-$ is a $n_C s$-shift of $\tilde{y}_+$, where $\tilde{\jmath} = (j-1)s + 1$. Let $\mathcal{C}'$ be the configuration defined by $(\tilde{y}, \tilde{u})$ with $B'_{11} = \tilde{y}_+ \tilde{u}_-^T$ (see Remark 4.4). The first two parameters of $\mathcal{C}'$ are given by the corner $\ulcorner B'_{11} = (\tilde{\jmath}, \tilde{\imath})$ and each of the blocks have t' rows and t columns.

Consider part (2), i.e. $\Phi = -1$ and $\delta = 0$. Then $\tilde{y} = -Py$ and Lemma 4.16(1) implies that $\tilde{y}_- = (Py)_- = [\tilde{\jmath}, \tilde{\jmath} + t' - 1]$ and $\tilde{y}_+ = (Py)_-$ is an $n_C s$-shift of $\tilde{y}_-$ (and $\tilde{\jmath}$ is as above). Let $\mathcal{C}'$ be the configuration defined by $(\tilde{y}, \tilde{u})$ with $B'_{11} = \tilde{y}_- \tilde{u}_+^T$. The first two parameters of $\mathcal{C}'$ are given by the corner $\ulcorner B'_{11} = (\tilde{\jmath}, \tilde{\imath} + n_R s)$ and each of the blocks have t' rows and t columns. Since $\tilde{u}_+$ is an $n_R s$-shift of $\tilde{u}_-$, Remark 4.9 implies that $\tilde{u}_-$ is an $((r - n_R)s - 1)$-shift of $\tilde{u}_+$.

Consider part (3), i.e. $\Phi = 1$ and $\delta = 1$. Then $\tilde{y} = Py$ and Lemma 4.16(2) implies that $\tilde{y}_- = (Py)_- = [\tilde{\jmath} - (s - t'), \tilde{\jmath} - 1]$ and $\tilde{y}_+ = (Py)_+$ is an $n_C s$-shift of $\tilde{y}_-$. Let $\mathcal{C}'$ be the configuration defined by $(\tilde{y}, \tilde{u})$ with $B'_{11} = \tilde{y}_- \tilde{u}_+^T$. Note that $\ulcorner B'_{11} = (\tilde{\jmath} - (s - t'), \tilde{\imath} + n_R s)$ and that the blocks have $s - t'$ rows and t columns. Since $\tilde{u}_+$ is an $n_R s$-shift of $\tilde{u}_-$, Remark 4.9 implies that $\tilde{u}_-$ is an $((r - n_R)s - 1)$-shift of $\tilde{u}_+$.

Consider part (4), i.e. $\Phi = -1$ and $\delta = 1$. Then $\tilde{y} = -Py$ and Lemma 4.16(2) implies that $\tilde{y}_+ = (Py)_- = [\tilde{\jmath} - (s - t'), \tilde{\jmath} - 1]$ and $\tilde{y}_- = (Py)_+$ is an $n_C s$-shift of $\tilde{y}_+$. Let $\mathcal{C}'$ be the configuration defined by $(\tilde{y}, \tilde{u})$ with $B'_{11} = \tilde{y}_+ \tilde{u}_-^T$. Note that $\ulcorner B_{11} = (\tilde{\jmath} - (s - t'), \tilde{\imath})$ and the blocks have $s - t'$ rows and t columns. $\square$

4.5. **Case analysis.** Lemma 4.6 implies (after possibly a simple isomorphism) that $A = C_r + \Sigma(\mathcal{C})$ where $\mathcal{C}$ is a configuration $(1, b, n_R, n_C, tr, t'r - \delta)$ where b is an index, $n_R, n_C \in [r - 1], t, t' \in [s-1]$ and $\delta \in \{0, 1\}$. Let $B_{11}, B_{12}, B_{21}, B_{22}$ denote the blocks of $\mathcal{C}$. The variables b, n_R, n_C, t, t' and δ are used throughout the remainder of this section.

Lemma 4.17. *We may assume* $t = t'$.

Proof. Note $\ulcorner B_{22} = (1+tr, b+t'r-\delta)$. Thus $b+t'r-\delta \in \mathrm{row}_{1+tr}(C_r)$ i.e. there exists $q \in [0, r-1]$ such that $b + t'r - \delta = 1 + tr + q$, i.e $r(t' - t) = q - b + \delta + 1$. As $b \leq r$, $q - b + \delta + 1 > -r$; hence $t' - t \geq 0$. Suppose $t' - t \geq 1$. Then $q - b + \delta + 1$ is a multiple of r, but as $q \leq r - 1, b \geq 1$ and $\delta \leq 1$ we must have $q = r - 1, b = \delta = 1$. As $\ulcorner B_{11} = (1, b) = (1, 1), n_R = 1$ and as $\ulcorner B_{22} = (1 + tr, (t+1)r), n_C = 1$. Thus $\mathcal{C} = (1, 1, 1, 1, tr, (t+1)r - 1)$, i.e. it is a simple-$C4$. We are then done by Remark 4.11. $\square$

Thus throughout the remainder of the section $t = t'$.

Lemma 4.18. *If* $\delta = 0$ *then* $\mathrm{val}(B_{11}) = \mathrm{val}(B_{22})$ *and* $\mathrm{val}(B_{11}) \neq 1$.

Proof. Since $B_{11} \subseteq C_r, B_{11} \cap D_s \subseteq \{B_{11}^{\urcorner}, \llcorner B_{11}\}$. Similarly, $B_{22} \cap D_s \subseteq \{B_{22}^{\urcorner}, \llcorner B_{22}\}$. Since $t = t'$ and $\delta = \emptyset, B_{11}^{\urcorner} \cap D_s \neq \emptyset$ if and only if $B_{22}^{\urcorner} \cap D_s \neq \emptyset$ and $\llcorner B_{11} \cap D_s \neq \emptyset$ if and only if $\llcorner B_{22} \neq \emptyset$. It follows that $\mathrm{val}(B_{11}) = \mathrm{val}(B_{22})$. Suppose $\mathrm{val}(B_{11}) = \mathrm{val}(B_{22}) = 1$. Assume $B_{11}^{\urcorner} \in D_s$ as the case $\llcorner B_{11} \in D_s$ can be dealt with similarly. Then $B_{22}^{\urcorner} \in D_s$. Since $\delta = 0$, B_{12} is a horizontal translation of B_{11}, hence Remark 4.8 implies that $\mathrm{val}(B_{11}) = \mathrm{val}(B_{12})$. $B_{22} \setminus B_{22}^{\urcorner}$ is a horizontal translation of $B_{21} \setminus B_{21}^{\urcorner}$, hence Remark 4.8 implies that $\mathrm{val}(B_{21} \setminus B_{21}^{\urcorner}) = \mathrm{val}(B_{22} \setminus B_{22}^{\urcorner})$. Moreover, $B_{21}^{\urcorner} \notin D_s$ and $B_{22}^{\urcorner} \in D_s$. It follows that $\mathrm{val}(B_{21}) - \mathrm{val}(B_{22}) = -1$. Hence $-\mathrm{val}(B_{11}) + \mathrm{val}(B_{12}) + \mathrm{val}(B_{21}) - \mathrm{val}(B_{22}) = -1$, contradicting Remark 4.7. $\square$

Lemma 4.19. *Let (P,Q) define the standard (C_s,D_s)-isomorphism. (1) Suppose $A = C_r + \Sigma(\mathcal{C})$ where $\mathcal{C}$ is basic, then $PBQ = C_s + \Sigma(\mathcal{C}')$ where $\mathcal{C}'$ is basic. (2) Suppose $PBQ = C_s + \Sigma(\mathcal{C}')$ where $\mathcal{C}'$ is basic then $A = C_r + \Sigma(\mathcal{C})$ where $\mathcal{C}$ is basic.*

Proof. Since we can interchange the roles of A and PBQ it suffices to prove (1). $B_{21} \setminus B_{21}^{\urcorner}$ is a vertical translation of $B_{11} \setminus B_{11}^{\urcorner}$. Remark 4.8 implies that $\mathrm{val}(B_{11} \setminus B_{11}^{\urcorner}) = \mathrm{val}(B_{21} \setminus B_{21}^{\urcorner})$. Moreover, $B_{11}^{\urcorner} \in D_s$; but $B_{21}^{\urcorner} \notin D_s$. Thus, $\mathrm{val}(B_{11}) = \mathrm{val}(B_{21}) + 1$. Similarly, we prove that $\mathrm{val}(B_{22}) = \mathrm{val}(B_{12}) + 1$. Hence $-\mathrm{val}(B_{11}) + \mathrm{val}(B_{12}) + \mathrm{val}(B_{21}) - \mathrm{val}(B_{22}) = -2$. Remark 4.7 implies that $x^T y = -2$ hence (Remark 4.3) $\Phi = +1$. Thus, we are in case (3) of Lemma 4.14 with $i = 1$ and $j = 1 + n_R$. Then $\tilde{\imath} = 1$ and $\tilde{\jmath} = n_R s + 1$. Thus $\mathcal{C}' = (n_R s + 1 - (s-t), n_R s + 1, s-t, t, (r-n_R)s, (r-n_R)s - 1)$. After a simple isomorphism, mapping row $n_R s + 1 - (s-t)$ to 1, we have $\mathcal{C}' = (1, (s-t)+1, s-t, t, (r-n_R)s, (r-n_R)s-1)$. Define $n'_R = s-t$ and $q = r - n_R$, then $\mathcal{C}' = (1, 1+n'_R, n'_R, s-n'_R, qs, qs-1)$ which is basic. □

We can now prove the main theorem of this section.

Proof of Theorem 4.1: The "if" part of the statement follows from Lemma 4.19. Let $\mathcal{C}'$ be the configuration obtained from $\mathcal{C} = (i, j, n_R, n_C, tr, t'r - \delta)$ in Lemma 4.14 where $i = 1$ (we will consider each of the 4 cases of the lemma separately). Note, $\tilde{\imath} = 1$. Denote by $B_{11}, B_{12}, B_{21}, B_{22}$ the blocks corresponding to $\mathcal{C}$.

Case 1. $\Phi = 1$ *and* $\delta = 0$.

Then $\mathcal{C}' = (\tilde{\jmath}, 1, t, t, n_C s, n_R s)$. By applying Lemma 4.17 to PBQ instead of A we obtain that $n_C = n_R$. Suppose $\mathrm{val}(B_{11}) = \mathrm{val}(B_{22}) = 0$. Then B_{12} is a horizontal translation of B_{11} and B_{22} is a horizontal translation of B_{21}. Remark 4.8 implies that $\mathrm{val}(B_{11}) = \mathrm{val}(B_{12})$ and $\mathrm{val}(B_{21}) = \mathrm{val}(B_{22})$. Then $-\mathrm{val}(B_{11}) + \mathrm{val}(B_{12}) + \mathrm{val}(B_{21}) - \mathrm{val}(B_{22}) = 0$. Remark 4.7 implies that $x^T y = 0$. Remark 4.3 implies that $\Phi = -1$, a contradiction. Lemma 4.18 implies $\mathrm{val}(B_{11}) =$

$\mathrm{val}(B_{22}) \neq 1$. Hence $\mathrm{val}(B_{11}) = \mathrm{val}(B_{22}) \geq 2$. Thus $\mathrm{val}(B_{11}) = 2$ and $\{{}_\llcorner B_{11}, B_{11}^\urcorner\} \subseteq D_s$. It follows that $n_C = n_R = \frac{r+1}{2}$ and that r is odd. Since $i = 1$ we must have $j = r - n_C + 1 = \frac{r+1}{2}$. It follows that $\tilde{\jmath} = (\frac{r-1}{2})s + 1 = \frac{1}{2}(n + 1 - s) + 1$. We must have $(\tilde{\imath}, \tilde{\jmath}) \in C_s$ thus $\tilde{\jmath} \in \mathrm{col}_1(C_s) = \{n - s + 2, \ldots, n\} \cup \{1\}$, i.e. $\frac{1}{2}(n + 1 - s) + 1 \geq n - s + 2$, which implies $1 \geq n - s + 2$, a contradiction.

Case 2. $\Phi = -1$ *and* $\delta = 0$.

Then $\mathcal{C}' = (\tilde{\jmath}, 1 + n_R s, t, t, n_C s, (r - n_R)s - 1)$. By applying Lemma 4.17 to PBQ instead of A we obtain that $n_C = r - n_R$. It follows that exactly one of ${}_\llcorner B_{11}, B_{11}^\urcorner$ is in D_s, i.e. that $\mathrm{val}(B_{11}) = 1$. But this contradicts Lemma 4.18.

Case 3. $\Phi = 1$ *and* $\delta = 1$.

Then $\mathcal{C}' = (\tilde{\jmath} - (s - t), 1 + n_R s, s - t, t, n_C s, (r - n_R)s - 1)$. By applying Lemma 4.17 to PBQ instead of A we obtain that $n_C = r - n_R$. Then exactly one of ${}_\llcorner B_{11}, B_{11}^\urcorner$ is in D_s. By Lemma 4.18 exactly one of ${}_\llcorner B_{22}, B_{22}^\urcorner$ is in D_s. Moreover, since $\delta = 1$, we must have $B_{11}^\urcorner \in D_s$ and ${}_\llcorner B_{22} \in D_s$. Since $i = 1$, $j = r - n_C + 1 = r - (r - n_R) + 1 = n_R + 1$. Thus $\mathcal{C} = (1, n_R + 1, n_R, r - n_R, tr, tr - 1)$, i.e. it is a basic configuration.

Case 4. $\Phi = -1$ *and* $\delta = 1$.

Then $\mathcal{C}' = (\tilde{\jmath} - (s - t), 1, s - t, t, n_C s, n_R s)$. By applying Lemma 4.17 to PBQ instead of A we obtain that $n_C = n_R$. Since for $\mathcal{C}'$ the last parameter is $n_R s$ and not $n_R s - 1$, $\mathcal{C}'$ is of the same form of $\mathcal{C}$ as in either case 1 or case 2 (the two cases with $\delta = 0$). But we excluded these cases already. $\square$

5. Higher level matrices

In this section, we address the following questions:

- Are there simple composition techniques for constructing high level thin Lehman matrices from low level thin Lehman matrices?
- Are there thin Lehman matrices of arbitrarily high level?

5.1. **Compositions.** We describe ways of composing Lehman matrices to obtain more complicated, potentially higher level, Lehman matrices.

Proposition 5.1. *Let* $A, B \in M_n(\mathbb{B})$*,* $\Sigma_A, \Sigma_{A'}, \Sigma_B, \Sigma_{B'} \in M_n(\{0, \pm 1\})$ *such that* $(A, B), (A + \Sigma_A, B + \Sigma_B), (A + \Sigma_{A'}, B + \Sigma_{B'})$ *are all Lehman pairs and* $A + \Sigma_A + \Sigma_{A'}, B + \Sigma_B + \Sigma_{B'} \in M_n(\mathbb{B})$*. Then* $(A + \Sigma_A + \Sigma_{A'}, B + \Sigma_B + \Sigma_{B'})$ *is a Lehman pair iff*

$$\Sigma_A \Sigma_{B'}^T + \Sigma_{A'} \Sigma_B^T = 0.$$

Proof. Since $(A, B), (A + \Sigma_A, B + \Sigma_B), (A + \Sigma_{A'}, B + \Sigma_{B'})$ are all Lehman pairs, we have

$$A\Sigma_B^T + \Sigma_A (B + \Sigma_B)^T = 0 \text{ and } A\Sigma_{B'}^T + \Sigma_{A'}(B + \Sigma_{B'})^T = 0.$$

Using these two matrix equations and the fact that $AB^T = E + I$, we find that

$$(A + \Sigma_A + \Sigma_{A'})(B + \Sigma_B + \Sigma_{B'})^T = (E + I) + \Sigma_A \Sigma_{B'}^T + \Sigma_{A'} \Sigma_B^T.$$

Therefore, $(A + \Sigma_A + \Sigma_{A'}, B + \Sigma_B + \Sigma_{B'})$ is a Lehman pair iff $\Sigma_A \Sigma_{B'}^T + \Sigma_{A'} \Sigma_B^T = 0$, as desired. □

Corollary 5.2. *Let* $A, B \in M_n(\mathbb{B})$*,* $\Sigma_A, \Sigma_{A'}, \Sigma_B, \Sigma_{B'} \in M_n(\{0, \pm 1\})$ *such that* $(A, B), (A + \Sigma_A, B + \Sigma_B), (A + \Sigma_{A'}, B + \Sigma_{B'})$ *are all Lehman pairs and* $\text{supp}(\Sigma_A) \bigcap \text{supp}(\Sigma_{A'}) = \emptyset$*,* $\text{supp}(\Sigma_B) \bigcap \text{supp}(\Sigma_{B'}) = \emptyset$*. Then* $(A + \Sigma_A + \Sigma_{A'}, B + \Sigma_B + \Sigma_{B'})$ *is a Lehman pair iff*

$$\Sigma_A \Sigma_{B'}^T + \Sigma_{A'} \Sigma_B^T = 0.$$

Proof. Since, Σ_A and $\Sigma_{A'}$ have disjoint support, $(A+\Sigma_A+\Sigma_{A'}) \in M_n(\mathbb{B})$ follows. Similarly, Σ_B and $\Sigma_{B'}$ have disjoint support implies $(B+\Sigma_B+\Sigma_{B'}) \in M_n(\mathbb{B})$. Now, we can apply Proposition 5.1. □

5.2. **Long cycles.** In some sense, the simplest level-1 update is the one given by a configuration in which all blocks are 1×1. (See *simple-*$C4$ in Section 4.) There is a nice generalization of this simple combinatorial structure to an arbitrary level. We call the general structure 2δ*-cycle*, for $\delta \in \{2, 3, \dots, s-1\}$. We define the underlying update by describing the primal perturbation Σ_A and the dual perturbation Σ_B.

The nonzero entries of Σ_A are given as follows:

$$(\Sigma_A)_{11} := -1; \quad (\Sigma_A)_{(\delta-1)r+1,1} := 1;$$

$$(\Sigma_A)_{kr+1,(k+1)r} := -1, \quad (\Sigma_A)_{(k-1)r+1,(k+1)r} := 1 \; \forall k \in \{1, 2, \dots, \delta-1\}.$$

All nonzero entries of Σ_B are in the following 2-by-2 block structure:

	ℓr	$\ell r+1$
kr	-1	$+1$
$kr+1$	$+1$	-1

for all $1 \leq \ell < k \leq \delta$ such that $(\ell + k)$ is odd.

We denote the above matrices by $\Sigma_A(\delta)$ and $\Sigma_B(\delta)$.

Proposition 5.3. *Let $r \geq 2$, $s \geq 2$ be arbitrary integers and let $n := rs - 1$. Then for every $\delta \in \{2, 3, \dots, s-1\}$, $A := C_r + \Sigma_A(\delta)$ and $B := D_s + \Sigma_B(\delta)$ make a thin Lehman pair.*

Proof. It is easy to verify that $A, B \in M_n(\mathbb{B})$. To verify that $AB^T = E + I$, it suffices to check the matrix equation

$$C_r \left[\Sigma_B(\delta)\right]^T + \Sigma_A(\delta) D_s^T + \Sigma_A(\delta) \left[\Sigma_B(\delta)\right]^T = 0.$$

It is easily seen that (restricted to their nonzero rows and columns),

$$C_r\,[\Sigma_B(\delta)]^T = \begin{array}{r|rrrrrrcrr|} & 2r & 2r+1 & 3r & 3r+1 & 4r & 4r+1 & \cdots & \delta r & \delta r+1 \\ \hline 1 & -1 & 1 & 0 & 0 & -1 & 1 & \cdots & 0 & 0 \\ r+1 & 1 & -1 & -1 & 1 & 1 & -1 & \cdots & -1 & 1 \\ 2r+1 & 0 & 0 & 1 & -1 & -1 & 1 & \cdots & 1 & -1 \\ 3r+1 & 0 & 0 & 0 & 0 & 1 & -1 & \cdots & -1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (\delta-1)r+1 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 1 & -1 \end{array}$$

$$\Sigma_A(\delta)D_s^T = \begin{array}{r|rrrrrrcrr|} & 2r & 2r+1 & 3r & 3r+1 & 4r & 4r+1 & \cdots & \delta r & \delta r+1 \\ \hline 1 & 1 & -1 & 1 & -1 & 1 & -1 & \cdots & 1 & -1 \\ r+1 & -1 & 1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 2r+1 & 0 & 0 & -1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 3r+1 & 0 & 0 & 0 & 0 & -1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (\delta-1)r+1 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & -1 & 1 \end{array}$$

$$\Sigma_A(\delta)\,[\Sigma_B(\delta)]^T = \begin{array}{r|rrrrrrcrr|} & 3r & 3r+1 & 4r & 4r+1 & 5r & 5r+1 & \cdots & \delta r & \delta r+1 \\ \hline 1 & -1 & 1 & 0 & 0 & -1 & 1 & \cdots & -1 & 1 \\ r+1 & 1 & -1 & -1 & 1 & 1 & -1 & \cdots & 1 & -1 \\ 2r+1 & 0 & 0 & 1 & -1 & -1 & 1 & \cdots & -1 & 1 \\ 3r+1 & 0 & 0 & 0 & 0 & 1 & -1 & \cdots & 1 & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (\delta-1)r+1 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \end{array}$$

where we illustrated the last two columns and the last rows of the matrices for δ odd. Therefore, $AB^T = E + I$ and (A, B) is a thin Lehman pair. □

What is the level of the thin Lehman matrix $C_r + \Sigma_A(\delta)$ defined above? A likely answer is $\delta - 1$ but we could not prove it. It is easy to see that the level of $C_r + \Sigma_A(\delta)$ is at most $\delta - 1$: Indeed $\Sigma_A(\delta)$ has δ nonzero rows (and columns). When restricted to its support, this matrix is the node-arc incidence matrix of a circuit on δ nodes. Therefore, $\mathrm{rank}(\Sigma_A(\delta)) = \delta - 1$. Hence, the level of A is at most $(\delta - 1)$. Note that the highest possible level of $C_r + \Sigma_A(\delta)$ is $\max\{r, s\} - 2$.

Proving lower bounds is much harder. In the next section, we give a lower bounding technique. Note however that the resulting lower bounds are typically not tight.

5.3. **Lower bounding the level of thin Lehman matrices.** Let $A \in M_n(\mathbb{B})$ be r-regular for some $r \geq 2$. We define the simple undirected graph $G_A := (V(G_A), E(G_A))$ by

- $V(G_A) := \{i : i \text{ is a row of } A\}$,
- $ij \in E(G_A)$ iff $|\mathrm{row}_i(A) \cap \mathrm{row}_j(A)| = r - 1$.

Then, the maximum degree of any node in G_A is at most 2. Thus, G_A can be partitioned into vertex-disjoint paths called *segments*. We denote by $\mathrm{segment}(A)$ the number of segments of G_A. This parameter is invariant under the isomorphisms of A.

Remark 5.4. Let A be as above and let P and Q be $n \times n$ permutation matrices. Then

$$\mathrm{segment}(A) = \mathrm{segment}(PAQ).$$

Lemma 5.5. *Let A, P, and Q be as above. Define $\Sigma := PAQ - C_r$, $t := \mathrm{rank}(\Sigma)$. Then Σ has at most $2tr$ non-zero rows.*

Proof. Suppose for a contradiction that Σ has more than $2tr$ non-zero rows. Let S be a minimal set of columns of Σ such that the union of their supports covers all non-zero rows of Σ.

Claim 1. $|S| \geq t + 1$.

Proof. By definition, the number of "-1"s as well as the number of "$+1$"s in each column of Σ is at most r. So,

$$|\mathrm{supp}\,[\mathrm{col}_j(\Sigma)]| \leq 2r, \text{ for all } j.$$

Thus, $|S| \geq t + 1$ as desired. ◇

Claim 2. $\mathrm{col}_j(\Sigma)$ *for $j \in S$ are linearly independent.*

Proof. For every column $j \in S$, the minimality of S implies that there exists a row $i(j)$ that is covered by column j only. Consider the submatrix of Σ indexed by the column-row pairs $(j, i(j))$. This submatrix is the $|S| \times |S|$ identity matrix. ◇

We have $\operatorname{rank}(\Sigma) \geq |S| \geq t+1$ (where the first inequality uses Claim 2 and the second uses Claim 1), a contradiction. $\square$

Lemma 5.6. *Let $\Sigma \in M_n(\{0, \pm 1\})$ be 0-regular with q non-zero rows. Then $C_r + \Sigma$ has at most $2q$ segments.*

Proof. Note that G_{C_r} is the n-circuit. The next elementary observation is all we need.

Claim 1. *Let $A \in M_n(\mathbb{B})$ be r-regular. Also let $\ell \in \{0, \pm 1\}^n$ be 0-regular. Let e_i denote the ith unit vector. Then the only edges in G_A possibly not in $G_{A+e_i\ell^T}$ are incident to vertex i.*

We apply the above claim repeatedly, starting with G_{C_r}. There are at most $2q$ edges of G_{C_r} that are not in $G_{C_r+\Sigma}$. Since the edges of $G_{C_r+\Sigma}$ that are not in G_{C_r} can only decrease the total number of segments, $G_{C_r+\Sigma}$ has at most $2q$ segments. $\square$

Proposition 5.7. *Let $A \in M_n(\mathbb{B})$ be a thin Lehman matrix that is r-regular. Then*

$$\operatorname{level}(A) \geq \frac{\operatorname{segment}(A)}{4r}.$$

Proof. Let $t := \operatorname{level}(A)$. Then, there exist $n \times n$ permutation matrices P, Q such that $\Sigma := PAQ - C_r \in M_n(\{0, \pm 1\})$ is 0-regular and has rank t. Now, Lemma 5.5 implies that Σ has at most $2tr$ non-zero rows. Lemma 5.6 implies that

$$\operatorname{segment}(PAQ) \leq 4tr.$$

Using Remark 5.4 we conclude $t \geq \operatorname{segment}(A)/(4r)$. $\square$

Theorem 5.8. *There exist thin Lehman matrices of arbitrarily high level.*

Proof. We let $r := 3$ and for large integers s, set $n := rs - 1$. We define A from C_r by applying the configurations

$$(1, 2, 1, 1, 3, 3), (6, 7, 1, 1, 3, 3), (11, 12, 1, 1, 3, 3), (16, 17, 1, 1, 3, 3), \cdots$$

It is easy to verify that A is a Lehman matrix. Indeed the dual of A is defined from D_s by applying the configurations

$$(2,3,1,1,1,1),(7,8,1,1,1,1),(12,13,1,1,1,1),(17,18,1,1,1,1),\cdots$$

as can be checked by multiplying these two matrices. Consider those integers n satisfying the above condition and $n=5k$, for some integer $k\geq 4$. Then $\mathrm{segment}(A)\geq 2k$. Using Proposition 5.7, we conclude that

$$\mathrm{level}(A)\geq \frac{n}{30}.$$

Therefore, $\mathrm{level}(A)=\Omega(n)$ for this construction. □

Remark 5.9. Consider the long cycle construction. Let A be as defined in Proposition 5.3. It is easy to check that a 2δ-cycle creates δ segments, the largest value δ can take is $s-1$. Thus, Proposition 5.7 implies

$$\mathrm{level}(A)\geq \frac{s-1}{4r},$$

for the largest value of δ. If $r=3$, then $3s=n+1$ and the long cycle construction also yields a proof of Theorem 5.8:

$$\mathrm{level}(A)\geq \frac{n-2}{36}.$$

6. Fat matrices

6.1. **Examples.**

$$(5)\qquad F_7=\begin{bmatrix}1&1&&1&&&\\&1&1&&1&&\\&&1&1&&1&\\&&&1&1&&1\\1&&&&1&1&\\&1&&&&1&1\\1&&1&&&&1\end{bmatrix}\qquad P_{10}=\begin{bmatrix}&&&1&&&&&1&1\\&&&1&&&1&1&&\\&&&1&1&1&&&&\\1&1&1&&&&&&&\\&&1&&&&&1&1&\\&&1&&&&1&&&1\\&1&&&&1&&&1&\\&1&&&1&&&&&1\\1&&&&1&&1&&&\\1&&&&&1&&1&&\end{bmatrix}$$

Matrices F_7 and P_{10} are fat Lehman matrices. Matrix F_7 is the point-line incidence matrix of the Fano plane. F_7 is self-dual, thus $k = 2$ in (1). Matrix P_{10} is the matrix whose columns correspond to the edges of K_5 and whose rows are the incidence vectors of the triangles of K_5. Equivalently, P_{10} can be viewed as the vertex-vertex incidence matrix of the Petersen graph (hence the notation). $P_{10}, P_{10} + I$ form a Lehman pair, thus $k = 2$ in (1).

6.2. **Determinant.**

Remark 6.1. In this section E_n denotes the $n \times n$ matrix of 1s. For $n \geq 2$ and $k \geq 1$, the matrix $E_n + kI_n$ has two distinct eigenvalues, namely k with multiplicity $n - 1$, and $n + k$ with multiplicity 1. In particular,

$$\det(E_n + kI_n) = k^{n-1}(n + k).$$

Proof. Since $(E_n+kI_n)-kI_n = E_n$ and there are $n-1$ linearly independent vectors in $Null\{e_n\}$, the multiplicity of k is at least $n - 1$. Vector e_n is the eigenvector for the eigenvalue $n + k$. Since the total multiplicity is at most n, the result about eigenvalues follows. Finally, the determinant is the product of the eigenvalues. □

As an example, consider F_7 in (5). Then $n = 7$ and since F_7 is self-dual, $k = 2$. Hence $\det(E_7 + 2I_7) = 9 \times 2^6$ and $\det(F_7) = 3 \times 2^3$.

Remark 6.2. Let A be an r-regular Lehman matrix.

(i) If A is thin, then $|\det(A)| = r$,

(ii) If A is self-dual, then $|\det(A)| = (r - 1)^{\frac{r(r-1)}{2}} r$.

Proof. (i) By Theorem 2.1, the dual of A is an s-regular matrix B such that $rs = n + 1$. Remark 6.1 implies that $\det(E_n + I_n) = n + 1 = rs$. Thus $\det(A)\det(B) = \det(E_n + I_n) = rs$.

Since A is an r-regular nonsingular integral matrix, it follows that its determinant is a nonzero integer multiple of r. Thus $|\det(A)| \geq r$ and similarly $|\det(B)| \geq s$, and the result follows.

(ii) Since A is self-dual, $k = r - 1$. By Theorem 2.1, $r^2 = n + r - 1$. Remark 6.1 implies that $\det(A)^2 = \det(E_n + (r-1)I_n) = (r-1)^{r(r-1)}r^2$. The result follows. □

Recall that $|\det(A)|$ equals the volume of the parallelopiped defined by the columns of A (viewed as vectors of $\mathbb{R}^n$). This justifies our terminology of *thin* Lehman matrix (the parallelopiped formed by its columns has the smallest possible volume among all nonsingular r-regular matrices in $M_n(\mathbb{B})$). By contrast, *fat* Lehman matrices give rise to parallelopipeds with larger volumes, the extreme case being that of nondegenerate finite projective planes.

6.3. **Lehman matrices from projective planes.** A *projective plane* consists of points and lines such that any two distinct points belong to exactly one line, and any two distinct lines intersect in exactly one point. A projective plane is *degenerate* if at least three of any four points belong to the same line. It can be shown that all the lines of a nondegenerate finite projective plane have the same number of points. Therefore, point-line incidence matrices $A \in M_n(\mathbb{B})$ of nondegenerate finite projective planes are exactly the solutions of the equation $AA^T = E + kI$, i.e. they are the self-dual Lehman matrices. We review known results about these matrices. First note that Theorem 2.1 implies that $n = k^2 + k + 1$. The integer k is called the *order* of the projective plane.

Not all orders k are possible, as proved by Bruck and Ryser [2] in the following theorem.

Theorem 6.3. *If $k = 1, 2$ (mod 4) and $y^2 + z^2 = k$ has no solution in integers, then there is no projective plane of order k.*

For example, this implies that there are no projective planes of orders 6 and 14. What is the idea of the proof of the Bruck-Ryser theorem? Observe that $E + kI$ is a positive definite matrix. Therefore it always has a decomposition $AA^T = E + kI$. Bruck and Ryser [2] address the question of whether there exists such a decomposition where A has *rational* entries. (When

$n = 1$, this question reduces to: When does there exist a rational number a such that $a^2 = 1+k$?) By clever arguments, Bruck and Ryser massage the quadratic form $x^T AA^T x = x^T(E + kI)x$ (which has nonzero rational solutions) until they eventually reduce it to $y^2 + z^2 = k$ in integers.

Does this line of proof carry over to the general Lehman equation $AB^T = E + kI$, i.e. can we use the fact that A and B have rational entries to exclude certain values of k? Unfortunately not: For any nonsingular rational matrix A, we can set $B^T = A^{-1}(E + kI)$ which is also rational. In order to prove the nonexistence of Lehman matrices for certain values of k, one needs combinatorial arguments using the fact that A, B are 0,1 matrices.

The following table gives the number of projective planes for small orders k.

k	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Number	1	1	1	1	0	1	1	4	0	≥ 1	?	≥ 1	0	?	≥ 22

Next we describe an infinite family of projective planes denoted by PG$(2, k)$. Let V be a 3-dimensional vector space over a finite field with k elements. The points of PG$(2, k)$ are the 1-dimensional subspaces of V and its lines are the 2-dimensional subspaces of V. Then PG$(2, k)$ is a projective plane of order k. For example, when $k = 2$ we get the Fano plane F_7.

This construction implies that a projective plane of order k exists whenever k is a prime power, since there always exists a finite field with k elements in this case. Interestingly, all known examples of finite projective planes have an order which is a prime power.

6.4. **Nearly self-dual Lehman matrices.** We call *nearly self-dual* a Lehman matrix A with the following properties:

(i) $A = A^T$ and

(ii) the dual of A is $A + I$.

Theorem 6.4. *Let A be a nearly self-dual Lehman matrix which is r-regular. Then $r = 2, 3, 7$ or 57.*

Proof. Since $A+I$ is a 0,1 matrix, the entries in the diagonal of A are all equal to 0. Since $A = A^T$, the matrix A is the vertex-vertex incidence matrix of a graph G. Since A is r-regular, G is r-regular.

Claim 1. *The graph G has girth at least 5.*

Proof. Suppose otherwise. Then G contains a triangle with vertices i, j, k or a 4-cycle with vertices i, k, j, l in that order. In both cases, the scalar product $\langle \mathrm{row}_i(A), \mathrm{row}_j(A+I)\rangle \geq 2$. But this contradicts Lehman's equation, which implies $\langle \mathrm{row}_i(A), \mathrm{row}_j(A+I)\rangle = 1$ for $i \neq j$. ◇

An (r, g)-*cage* is a graph that (i) is r-regular, (ii) has girth at least g, and has the smallest possible number of vertices among all graphs satisfying (i) and (ii).

Claim 2. *The graph G is an $(r, 5)$-cage with $1 + r^2$ vertices.*

Proof. Consider any r-regular graph H with girth at least 5, and let v be a vertex of H. Vertex v has r neighbors $v_1, \dots, v_r$ and each of these vertices v_i has $r-1$ neighbors distinct from v. Furthermore, all these vertices are distinct since H contains no 4-cycle. Therefore, H has at least $1 + r + r(r-1) = 1 + r^2$ vertices.

Since A, A_I is a Lehman pair, it follows from Theorem 2.1 (ii) that $r(r+1) = n + (r-1)$, i.e. the graph G has $n = 1 + r^2$ vertices. Thus G is an $(r, 5)$-cage. ◇

A theorem of Hoffman and Singleton [6] states that, for any $(r, 5)$-cage, $n \geq 1 + r^2$ and equality holds if and only if $r \in \{2, 3, 7, 57\}$. □

Hoffman and Singleton [6] show that there is a unique solution (up to isomorphism) for each of the cases $r = 2, 3, 7$. The existence of a solution for the case $r = 57$ is unknown.

The case $r = 2$ (i.e. $n = 5$) is the circulant C_2^5.

The case $r = 3$ (i.e. $n = 10$) is the Petersen matrix P_{10} mentioned earlier.

The case $r = 7$ (i.e. $n = 50$) was constructed by Hoffman and Singleton [6].

6.5. **Fat Lehman matrices and minimally nonideal matrices.** The point-line matrices of degenerate finite projective planes are minimally nonideal. The cores of most other known minimally nonideal matrices are thin Lehman matrices. We know only three exceptions: F_7, P_{10} and its dual. These three fat Lehman matrices play a central role in Seymour's conjecture about ideal binary matrices [13]. A 0,1 matrix is *binary* if the sum modulo 2 of any three of its rows is greater than or equal to at least one row of the matrix. Seymour's conjecture states that there are only three minimally nonideal binary matrices (F_7, $\mathcal{O}_{K_5}$ whose columns are indexed by the edges of K_5 and whose rows are the characteristic vectors of the odd cycles of K_5, and its blocker): Their cores are F_7, P_{10} and its dual respectively.

7. Open problems and concluding remarks

The Lehman matrix equation (1) occurs prominently in the study of minimally nonideal matrices. Bridges and Ryser [1] give basic properties of its solutions (Theorem 2.1). Two infinite families of solutions are known: thin Lehman matrices and finite projective planes. In this paper, we classify thin Lehman matrices according to their similarity to the circulant matrices C_r^n: Level t matrices are isomorphic to C_r^n plus a rank t matrix. We were able to describe explicitly all level 1 matrices and we showed that level t matrices can be described by a number of parameters that only depends on t (independent of n and r). We also gathered results from the literature that are relevant to our understanding of fat Lehman matrices. There remain many open problems.

Question 1: Are there other infinite families of Lehman matrices beside thin matrices and projective planes?

Question 2: Can Theorem 1.2 be strengthened as follows: If A is a thin Lehman matrix of level t, then A can be described with $O(t)$ parameters?

In particular, can every thin $n \times n$ matrix be described with only $O(n)$ parameters?

Question 3: Do all thin Lehman matrices have level at most $\frac{n}{\min(r,s)}$?

Question 4: Is there a decomposition theorem stating that a thin Lehman matrix either is in a well-described family (such as matrices with low level or long cycles) or has a decomposition (such as presented in Section 5)?

Question 5: Is a thin Lehman matrix always the core of some minimally nonideal matrix?

Question 6: Is F_7 the only nondegenerate finite projective plane whose point-line matrix is the core of a minimally nonideal matrix? Beth Novick [12] answered this question positively when "the core of" is removed from the statement.

REFERENCES

[1] W.R. Bridges and H.J. Ryser, Combinatorial designs and related systems, *J. Algebra 13* (1969) 432–446.

[2] R.H. Bruck and H.J. Ryser, The nonexistence of certain projective planes, *Canadian Journal of Mathematics 1* (1949) 88–93.

[3] G. Cornuéjols, *Combinatorial Optimization, Packing and Covering*, CBMS-NSF Regional conference series in applied mathematics, SIAM, 2001.

[4] G. Cornuéjols, B. Guenin, and F. Margot, The Packing Property, *Math. Prog., Ser. A* 89 (2000) 113–126.

[5] P.D. Grünwald and P.M.B. Vitanyi, Kolmogorov Complexity and Information Theory, *Journal of Logic, Languages and Information* 12 (2003) 497–529.

[6] A.J. Hoffman and R.R. Singleton, On Moore Graphs with Diameters 2 and 3, *IBM Journal Res. Dev. 4* (1960) 497–504.

[7] D. Hughes and F. Piper, *Projective Planes*, Springer-Verlag, New York, 1973.

[8] A. Lehman, On the Width-Length Inequality and Degenerate Projective Planes, in *Polyhedral Combinatorics* (W. Cook and P.D. Seymour eds.), *DIMACS Series in Discrete Mathematics and Theoretical Computer Science 1*, American Mathematical Society, Providence, RI (1990) 101–105.

[9] M. Li and P.M.B. Vitanyi, *An Introduction to Kolmogorov Complexity and its Applications*, Springer-Verlag NY, USA, 1997.

[10] L. Lovász, A Characterization of perfect graphs, *Journal of Combinatorial Theory B* 13 (1972) 95–98.

[11] C. Luetolf and F. Margot, A Catalog of Minimally Nonideal Matrices, *Math. Methods of Oper. Res.* 47 (1998) 221–241.

[12] B. Novick, *Ideal 0,1 Matrices*, PhD dissertation, Carnegie Mellon University, Pittsburgh, PA (1990).

[13] P.D. Seymour, The Matroids with the Max-Flow Min-Cut Property, *Journal of Combinatorial Theory B* 23 (1977) 189-222.