Lattice Walks and Primary Decomposition

Persi Diaconis, David Eisenbud, and Bernd Sturmfels *

Introduction

This paper shows how primary decompositions of an ideal can give useful descriptions of components of a graph arising in problems from Combinatorics, Statistics, and Operations Research. We begin this introduction with the general formulation. Then we give the simplest interesting example of our theory, followed by a statistical example similar to that which provided our original motivation. In the body of the paper we study the primary decompositions corresponding to some natural combinatorial problems.

Let $\mathcal{B}$ be a set of vectors in $\mathbf{Z}^n$. Define a graph $G_{\mathcal{B}}$ on whose vertices are the non-negative n-tuples $\mathbf{N}^n$ as follows: $\boldsymbol{u}, \boldsymbol{v} \in \mathbf{N}^n$ are connected by an edge of $G_{\mathcal{B}}$ if and only if $\boldsymbol{u} - \boldsymbol{v}$ is in $\pm\mathcal{B}$. We say $\boldsymbol{u}$ and $\boldsymbol{v}$ in $\mathbf{N}^n$ can be *connected via* $\mathcal{B}$ if they are in the same connected component of $G_{\mathcal{B}}$. We shall consider the problem of characterizing the components of $G_{\mathcal{B}}$.

The simplest sort of characterization we know is by linear functionals. For example, if $n = 2$ and $\mathcal{B} = \{(1, -1)\}$ then two vectors $\boldsymbol{u} = (u_1, u_2)$ and $\boldsymbol{u}' = (u_1', u_2')$ are in the same component of $G_{\mathcal{B}}$ if and only if $u_1 + u_2 = u_1' + u_2'$. However for $\mathcal{B} = \{(2, -2), (3, -3)\}$ there is no such characterization.

To treat such cases, we connect our problem with commutative algebra. For any vector $\boldsymbol{u} = (u_1, \ldots, u_n)$ of positive integers we define a monomial $\boldsymbol{x}^{\boldsymbol{u}} = x_1^{u_1} x_2^{u_2} \ldots x_n^{u_n} \in k[x_1, \ldots, x_n]$. Every vector $\boldsymbol{u} \in \mathbf{Z}^n$ can be written uniquely as $\boldsymbol{u} = \boldsymbol{u}_+ - \boldsymbol{u}_-$ where $\boldsymbol{u}_+, \boldsymbol{u}_-$ are non-negative vectors with disjoint support. For example $(1, -2) = (1, 0) - (0, 2)$. To a vector $\boldsymbol{u} \in \mathbf{Z}^n$ we associate the binomial difference $\boldsymbol{x}^{\boldsymbol{u}_+} - \boldsymbol{x}^{\boldsymbol{u}_-}$. Let k be any field. To the subset $\mathcal{B} \subset \mathbf{Z}^n$ we associate the ideal generated by the corresponding binomials:

$$I_{\mathcal{B}} = \langle \boldsymbol{x}^{\boldsymbol{u}_+} - \boldsymbol{x}^{\boldsymbol{u}_-} : \boldsymbol{u} \in \mathcal{B} \rangle \ \subset \ k[x_1, \ldots, x_n].$$

The following theorem shows that this is a good encoding scheme:

Theorem 1.1. *Two vectors $\boldsymbol{u}, \boldsymbol{v} \in \mathbf{N}^n$ are in the same component of $G_{\mathcal{B}}$ if and only if $\boldsymbol{x}^{\boldsymbol{u}} - \boldsymbol{x}^{\boldsymbol{v}} \in I_{\mathcal{B}}$.*

* The authors are grateful to the NSF for partial support during the preparation of this paper. The third author is also supported by a David and Lucile Packard Fellowship.

Theorem 1.1 has been rediscovered many times. One early reference is [MM]. See also [Stu, §5]. Applications of the graphs $G_{\mathcal{B}}$ to integer programming can be found in [Tho].

As explained further in Section 2, there are various decompositions

$$I_{\mathcal{B}} \quad = \quad J_1 \cap J_2 \cap \ldots \cap J_r,$$

where the J_i correspond to other — and in some ways simpler — combinatorial problems. For example, we might take a primary decomposition. Since $\boldsymbol{u}$ and $\boldsymbol{v}$ are in the same component of $G_{\mathcal{B}}$ if and only if $\boldsymbol{x}^{\boldsymbol{u}} - \boldsymbol{x}^{\boldsymbol{v}} \in J_i,\ 1 \leq i \leq r$, such a decomposition of ideals allows a decomposition of the original problem. The following examples suggest how the theory will go:

Example 1.2.

The simplest typical example is provided by the set

$$\mathcal{B} = \{(2,-2),(3,-3)\} \ \subset \ \mathbf{Z}^2.$$

If $\boldsymbol{u}, \boldsymbol{v} \in \mathbf{N}^2$ are connected via $\mathcal{B}$ then clearly $u_1 + u_2 = v_1 + v_2$. We shall see that the converse is true provided that $u_1 + u_2 \geq 3$. When this inequality is not satisfied, the situation is more delicate: Of the vectors $(2,0),(1,1),(0,2)$ with sum 2, only $(0,2)$ and $(2,0)$ are connected. Each of the vectors $(1,0),(0,1)$, and $(0,0)$ is isolated.

These statements are all easy, but we will now derive them using the general method of this paper. We first compute the primary decomposition

$$I_{\mathcal{B}} \quad = \quad \langle x^2 - y^2, x^3 - y^3 \rangle \quad = \quad \langle x - y \rangle \cap \langle x + y, x^3, x^2y, xy^2, y^3 \rangle.$$

From this we see that (u_1, u_2) is connected to (v_1, v_2) via $\mathcal{B}$ if and only if it satisfies two conditions, corresponding to the two ideals on the right side of the equation. The first condition is that $x^{u_1}y^{u_2} - x^{v_1}y^{v_2} \in \langle x - y \rangle$, that is, $x - y$ divides $x^{u_1}y^{u_2} - x^{v_1}y^{v_2}$, or equivalently $u_1 + u_2 = v_1 + v_2$. The second condition is harder to interpret combinatorially. Note that $\langle x + y, x^3, x^2y, xy^2, y^3 \rangle$ contains all monomials of degree ≥ 3. Thus if $u_1 + u_2 = v_1 + v_2 \geq 3$, then $\boldsymbol{u}$ and $\boldsymbol{v}$ are connected via $\mathcal{B}$. Since $x^2 - y^2$ is divisible by $x + y$ it is also in the second ideal, and $(2,0)$ is connected with $(0,2)$. Inspection shows no other difference of monomials is in $I_{\mathcal{B}}$, completing the proof.

Example 1.3 (Poisson regression).

Here is a small example from Statistics. Suppose that a chemical to control insects is sprayed on successive equally infested plots in increasing concentrations 0,1,2,3,4 (in some units). After the spraying the numbers of insects left alive on the plots are 44,25,21,19,11. Roughly: Greater concentration leads to fewer insects.

To extrapolate we need a model. One standard model postulates that the number of insects at concentration i has a Poisson distribution with mean parameter e^{a+bi} where a and b are parameters to be fitted from the data. If $\hat{a}$ and $\hat{b}$ are estimates of a and b, and $\hat{\lambda}_i = e^{\hat{a}+i\hat{b}}$, then a test for goodness of fit of the Poisson model can be based on the chi-square statistic

$$\sum_{i=1}^{5} \frac{(\hat{\lambda}_i - N_i)^2}{\hat{\lambda}_i}.$$

Asymptotic theory predicts an approximate chi-square distribution on 3 degrees of freedom. In this example, $\hat{a} = 3.707$ $\hat{b} = -.3125$, the 5 fitted values are $\hat{\lambda}_i = (40.8, 29.8, 21.8, 16.0, 11.7)$ and the chi-square statistic is 1.7.

Does this value of chi-square show that the data were well fitted? Poorly fitted? Calibrating the chi-square test leads to a combinatorial problem of the type considered above. Let $\mathcal{X}$ be the set of all non-negative 5-tuples $x = (x_0, \ldots, x_4)$ with $S(x) = x_0 + \ldots + x_4 = 120$ and $T(x) = 0x_0 + x_1 + 2x_2 + 3x_3 + 4x_4 = 168$ matching the data above. $\mathcal{X}$ is a finite set, a component of the graph G defined by the linear functionals S and T. We want to know what proportion of the 5-tuples in $\mathcal{X}$ have chi-square greater than 1.7. We do not want to enumerate all 5-tuples to find out (indeed, in realistic problems of this kind there are simply too many to enumerate) and we know no general theory that will solve this problem accurately. Thus we will approximate a solution by choosing examples uniformly from the set, and seeing what proportion of the examples chosen have chi-square greater than 1.7.

To make these choices, we might run a random walk starting at the original data vector $x^* = (44, 25, 21, 19, 11)$. As a first approximation, it might seem reasonable to take, for basic moves in the walk, any set of elements that span the sublattice of $\mathbf{Z}^n$ defined by the vanishing of the functionals S and T. For example, we might take

$$\mathcal{B} = \{(1, -1, -1, 1, 0), (1, -1, 0, -1, 1), (0, 1, -1, -1, 1)\}.$$

At each step of our walk we randomly choose $\pm$ one of the vectors in $\mathcal{B}$ and then add it to the current vector in $\mathcal{X}$. If the entries of the result is positive, we step to the sum, which is again a vector in $\mathcal{X}$. Otherwise we discard it. Thus, the walk might go

$$(44, 25, 21, 19, 11) \to (45, 24, 20, 20, 11) \to (45, 23, 21, 21, 10) \to \ldots\ .$$

This walk generates a symmetric process which leads to the uniform distribution on the component of $G_{\mathcal{B}}$ containing x^*.

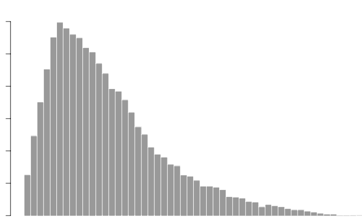
Although it turns out in this example that that the observed chi-square distribution for this walk is rather close to the true diestribution.Unfortunately, not every pair of vectors in $\mathcal{X}$ can be connected by steps in $\mathcal{B}$, so the set of 5-tuples over which we are averaging is not quite the same as the set we want! For example, the vector $(36, 0, 84, 0, 0)$ cannot be connected to x^* by steps in $\mathcal{B}$ keeping all entries positive. The primary decomposition exhibited below shows that two non-negative integer vectors $(i_1, j_1, h_1, l_1, m_1)$ and $(i_2, j_2, h_2, l_2, m_2)$ in $\mathcal{X}$ are connected via $\mathcal{B}$ if and only if

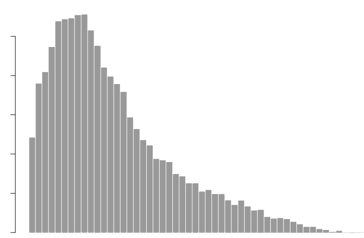
$$\begin{aligned} i_r + j_r + h_r &\geq 1 \text{ and} \\ i_r + j_r + l_r &\geq 1 \text{ and} \\ j_r + l_r + m_r &\geq 1 \text{ and} \\ h_r + l_r + n_r &\geq 1. \end{aligned} \tag{1.1}$$

The set $\mathcal{B}$ can be enlarged to

$$\mathcal{B}' = \mathcal{B} \cup \{(1, -2, 1, 0, 0), (0, 1, -1, 1, 0), (0, 0, 1, -2, 1)\},$$

and we shall see that this enlargement is sufficient. However, the distribution observed for chi-square coming from a random walk based on $\mathcal{B}$ is close to one based on $\mathcal{B}'$. In particular, using $\mathcal{B}$, the proportion of samples with chi-squared < 1.7 is .0031, whereas using $\mathcal{B}'$ the proportion is .0046. See the histograms below, each of which is based on a walk of $90,000$ steps, an initial $10,000$ having been discarded.





Walk with 3 moves   Walk with 6 moves

To understand the situation we turn to primary decomposition. We work in the polynomial ring $k[x_1, x_2, x_3, x_4, x_5]$. The set $\mathcal{B}$ is encoded by the binomial ideal $I_{\mathcal{B}} = \langle x_2x_3 - x_1x_4, x_2x_4 - x_1x_5, x_3x_4 - x_2x_5 \rangle$. Two 5-tuples are connected via $\mathcal{B}$ if and only if $I_{\mathcal{B}}$ contains

$$x_1^{i_1} x_2^{j_1} x_3^{k_1} x_4^{l_1} x_5^{m_1} - x_1^{i_2} x_2^{j_2} x_3^{k_2} x_4^{l_2} x_5^{m_2} \tag{1.2}$$

The primary decomposition of $I_{\mathcal{B}}$ is found to be

$$I_{\mathcal{B}} = I \cap \langle x_1, x_2, x_3 \rangle \cap \langle x_1, x_2, x_4 \rangle \cap \langle x_2, x_4, x_5 \rangle \cap \langle x_3, x_4, x_5 \rangle \tag{1.3}$$

where I is the prime ideal generated by the 2×2-minors of the matrix as is

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_3 & x_4 & x_5 \end{pmatrix}.$$

Note that (1.2) is in $I_{\mathcal{B}}$ if and only if it is in each ideal on the right of (1.3). It is in I if and only if $i_1 + j_1 + h_1 + l_1 + m_1 = i_2 + j_2 + k_2 + l_2 + m_2$ and $j_1 + 2k_1 + 3l_1 + 4m_1 = j_2 + 2k_2 + 3l_2 + 4m_2$. The remaining ideals on the right side of (1.3) are generated by monomials. A polynomial is in a monomial ideal J if and only if each term in J. This gives the remaining characterizing relations claimed in (1.1).

The ideal I encodes a lattice walk that connects all of $\mathcal{X}$. The reader may wonder why we didn't simply begin with the set $\mathcal{B}'$, corresponding to the six generators of I, in constructing the random walk above. In larger problems, it is computationally quite taxing to find connecting sets of moves. It is natural to take a smaller set of moves such as a lattice basis and "hope for the best"; indeed, this approach is taken in several published studies. The goal of the theory initiated in this paper is to understand the nature of such approximations.

The rest of this paper is laid out as follows. In Section two we set up the algebraic technique which comes from the work on binomial ideals [ES]. Section three treats contingency tables; $a \times b$ arrays of non-negative integers with given row and column sums. Section 4 describes a different basis $\mathcal{B}$ for the problem of contingency tables, the "adjacent minors". In the final section we discuss a systematic way of making a relatively small choice of basis for any lattice walk problem: we call these circuit walks.

2. Lattice ideals

With notation as above let $\mathcal{B}$ be a set of vectors in $\mathbf{Z}^n$. Let $\mathcal{L}$ be the subgroup of $\mathbf{Z}^n$ generated by $\mathcal{B}$. Call $\boldsymbol{u}, \boldsymbol{v} \in \mathbf{N}^n$ *equivalent* if $\boldsymbol{u} - \boldsymbol{v} \in \mathcal{L}$. In Example 1.2 $\mathcal{L}$ is the set $(u_1, u_2) \in \mathbf{Z}^2$ with $u_1 + u_2 = 0$ and $(u_1, u_2), (v_1, v_2) \in \mathbf{N}^2$ are equivalent if and only if $u_1 + u_2 = v_1 + v_2$. In Example 1.3 the equivalence classes generated by $\mathcal{L}$ are the set of all $\boldsymbol{u} \in \mathbf{N}$ with $u_1 + u_2 + u_3 + u_4 + u_5$, $0 \cdot u_1 + 1u_2 + 2u_3 + 3u_4 + 4u_5$ having fixed values. In applied problems the equivalence classes are often the basic objects of interest. One wants to construct a set of edges (that is a choice of $\mathcal{B}$) that connects elements within an equivalence class by a path along which all components stay non-negative. In [DS] it is shown how to find a finite set $\mathcal{B}$ by finding a Gröbner basis for

$I_{\mathcal{L}}$. The division algorithm gives an effective algorithm for finding a connecting path.

If $\boldsymbol{u}$ and $\boldsymbol{v}$ lie in the same connected component of $G_{\mathcal{B}}$ they are equivalent but not conversely. It can be shown that two vectors $\boldsymbol{u}, \boldsymbol{v} \in \mathbf{N}^n$ are equivalent if and only if $\boldsymbol{u}+\boldsymbol{w}$ can be connected to $\boldsymbol{v}+\boldsymbol{w}$ by move in $\mathcal{B}$ for some (sufficiently large) $\boldsymbol{w} \in \mathbf{N}^n$. It is an interesting problem to give useful bounds on $\boldsymbol{w}$. Theorem 1.1 gives the following condition for equivalence.

Corollary 2.1. *Let $\mathcal{B} \subseteq \mathbf{Z}^n$ generate $\mathcal{L} = \mathbf{Z}\mathcal{B}$. Every pair of $\mathcal{L}$ equivalent vectors is connected via $\mathcal{B}$ if and only if $I_{\mathcal{L}} = I_{\mathcal{B}}$.*

The ideals considered here are all generated by binomials $\boldsymbol{x}^{\boldsymbol{u}_+} - \boldsymbol{x}^{\boldsymbol{u}_-}$. We shall need a few results from the recently developed theory of binomial ideals [ES], and we briefly review now. General references for commutative algebra with emphasis on computational aspects are [CLO], [Stu]. Thorough treatments of primary decomposition can be found in [AM], [ES].

A *binomial* in $k[x_1, \ldots, x_n]$ is a polynomial with at most two terms. A *binomial ideal* is an ideal generated by binomials. Thus, monomial ideals are also binomial ideals. The following theorem is proved in [ES].

Theorem 2.2. *Every binomial ideal has a binomial primary decomposition.*

In [ES, §9] there is an explicit algorithm which expresses a given binomial ideal as an intersection of primary binomial ideals. A primary decomposition algorithm for general polynomial ideals is given in [BW §8]. Specializing to the situation of the paper we get

$$I_{\mathcal{B}} = J_1 \cap J_2 \cap \ldots \cap J_r$$

where each J_i is primary and generated by binomials $\alpha \boldsymbol{x}^{\boldsymbol{u}} - \beta \boldsymbol{x}^{\boldsymbol{v}}$.

Let $\mathcal{L}$ be a lattice in $\mathbf{Z}^n$. Call $\mathcal{L}$ *saturated* if for each $r \in \mathbf{Z}, \boldsymbol{u} \in \mathbf{Z}^n, r \cdot \boldsymbol{u} \in \mathcal{L}$ implies $\boldsymbol{u} \in \mathcal{L}$. Equivalently, $\mathcal{L}$ is saturated if and only if the quotient group $\mathbf{Z}^n/\mathcal{L}$ is free abelian. All of the lattices that appear in the examples of this paper are saturated. In [ES] it is proved that the binomial ideal $I_{\mathcal{L}}$ is prime if and only if $\mathcal{L}$ is saturated.

If $\mathcal{L} = \mathbf{Z}\mathcal{B}$ is saturated then [ES] show that the prime $I_{\mathcal{L}}$ appears among the J_i. Otherwise, $I_{\mathcal{L}}$ equals the intersection of some of the J_i. All other J_i's must contain monomials by [ES §2].

Theorem 1.1 shows that $\boldsymbol{u}$ and $\boldsymbol{v}$ are connected via $\mathcal{B}$ if and only if $\boldsymbol{x}^{\boldsymbol{u}} - \boldsymbol{x}^{\boldsymbol{v}}$ lies in J_i for all i. If J_i is a monomial ideal, the corresponding combinatorial condition is easy: suppose

$$J_i \quad = \quad \langle \boldsymbol{x}^{\boldsymbol{a}}, \boldsymbol{x}^{\boldsymbol{b}}, \ldots, \boldsymbol{x}^{\boldsymbol{c}} \rangle.$$

then $\boldsymbol{x}^{\boldsymbol{u}} - \boldsymbol{x}^{\boldsymbol{v}} \in J_i$ if and only if $\boldsymbol{x}^{\boldsymbol{u}}, \boldsymbol{x}^{\boldsymbol{v}} \in J_i$. Further, $\boldsymbol{x}^{\boldsymbol{u}} \in J_i$ if and only if $\boldsymbol{u} \geq \boldsymbol{a}$ or $\boldsymbol{u} \geq \boldsymbol{b}$ or ... or $\boldsymbol{u} \geq \boldsymbol{c}$. Even if the J_i's are not monomial ideals, artful choices may allow neat necessary and sufficient conditions or neat necessary conditions. Examples appear in Section 3 and 4 below. It is often convenient to combine the J_i in groups, so that the intersection of each group is generated by monomials $\boldsymbol{x}^{\boldsymbol{w}}$ and pure binomials $\boldsymbol{x}^{\boldsymbol{u}} - \boldsymbol{x}^{\boldsymbol{v}}$. Such a regrouping facilitates the combinatorial translation of containment in J_i. See [ES, Cor. 8.2] for further details.

3. Corner minors

The prototype of the problems considered here is that of generating random "contingency tables" — tables of nonnegative integers of given size with fixed row and column sums. The statisticians J. Darroch and G. Glonek (see [GL]) introduced a random walk technique: Start at a given table and take steps that do not change the nonnegativity or the row and column sums. For example, consider the following procedure: at each step, a position l in the first row and m in the first column are chosen randomly. The current table is changed to a new table by altering the four entries in positions $(1,1)$, $(l,1)$, $(1,m)$, (l,m) by adding or subtracting 1 following either the pattern of signs $\begin{pmatrix} + & - \\ - & + \end{pmatrix}$ or $\begin{pmatrix} - & + \\ + & - \end{pmatrix}$, the choice being random as well. For instance, for $a = b = 3$ this basis is

$$\mathcal{B}_{cor} = \left\{ \begin{pmatrix} +1 & -1 & 0 \\ -1 & +1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} +1 & 0 & -1 \\ -1 & 0 & +1 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} +1 & -1 & 0 \\ 0 & 0 & 0 \\ -1 & +1 & 0 \end{pmatrix}, \begin{pmatrix} +1 & 0 & -1 \\ 0 & 0 & 0 \\ -1 & 0 & +1 \end{pmatrix} \right\}.$$

A change is suppressed if it would lead to a table with negative entries. This process defines a symmetric random walk with a uniform stationary distribution on the set of tables connected to the starting table by the given moves. It turns out, however, that these moves may not connect all the non-negative tables with the given row and column sums. Glonek showed that they do suffice to connect these tables when the row and column sums are all ≥ 2. In this section we derive a strengthening of Glonek's result by describing the primary decomposition of the ideal corresponding to the set of chosen moves.

More formally, we are concerned with the lattice $\mathbf{Z}^{a \times b}$ of $a \times b$-integer matrices and $\mathcal{L}$ is the sublattice of matrices with zero row sums and zero column sums. We begin by considering a random walk with a larger set $\mathcal{B}_{all}$ of possible moves: Again, the walk is over all non-negative integer $a \times b$-matrices with fixed row and column sums. To describe a move in $\mathcal{B}_{all}$ we select the positions in a 2×2-submatrix and alter them by adding

$$\begin{pmatrix} +1 & -1 \\ -1 & +1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} -1 & +1 \\ +1 & -1 \end{pmatrix}. \tag{3.1}$$

The following result appears in [GL] but was probably known before.

Lemma 3.1. *The moves (3.1) are necessary and sufficient to connect any pair of non-negative integer $a \times b$-matrices with the same row and column sums.*

Proof. It is known (see e.g. [Stu, Prop. 5.4]) that $I_{\mathcal{L}}$ is a prime ideal which is minimally generated by the 2×2-minors of an $a \times b$-matrix of indeterminates:

$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1b} \\ x_{21} & x_{22} & \cdots & x_{2b} \\ \vdots & \vdots & \ddots & \vdots \\ x_{a1} & x_{a2} & \cdots & x_{ab} \end{pmatrix} \tag{3.2}$$

Lemma 3.1 now follows from Corollary 2.1. ∎

The number of moves (3.1) is $\binom{a}{2}\binom{b}{2}$, which is much larger than $rank(\mathcal{L}) = (a-1)(b-1)$, the size of the collection of moves $\mathcal{B}_{cor}$ described at the beginning of this section — quartic rather than quadratic in the size of the tables. It turns out that though the moves $\mathcal{B}_{cor}$ do not connect all possible tables with the given row and column sums, they come rather close. The following primary decomposition result allows an analysis of the situation.

Theorem 3.2. *Let $I_{\mathcal{L}}$ be the prime ideal generated by all 2×2-minors of (3.2), where $a, b \geq 2$. Let $R := \langle x_{11}, \ldots, x_{1b} \rangle$ and $C := \langle x_{11}, \ldots, x_{a1} \rangle$. The ideal of "corner minors" $I_{\mathcal{B}_{cor}} := \langle\, x_{11}x_{ij} - x_{1j}x_{i1} \;:\; 2 \leq i \leq a,\, 2 \leq j \leq b \,\rangle$ has the primary decomposition*

$$I_{\mathcal{B}_{cor}} \quad = \quad I_{\mathcal{L}} \cap R \cap C \cap (I_{\mathcal{B}_{cor}} + R^2 + C^2). \tag{3.3}$$

If $a, b > 2$ then this primary decomposition is minimal, whereas if $b = 2$ the last two terms can be dropped, and similarly if $a = 2$.

From (3.3) we can read off the connectivity properties of the basis $\mathcal{B}_{cor}$.

Corollary 3.3. *Two non-negative integer $a \times b$-matrices U, V are connected via $\mathcal{B}_{cor}$ if*
(a) U and V have the same row and column sums, and
(b) U, V have positive first row sum,
(c) U, V have positive first column sum,
(d) U, V have either row sum ≥ 2 or column sum ≥ 2.

Proof. The primary decomposition (3.3) implies

$$I_{\mathcal{B}_{cor}} \quad \supseteq \quad I_{\mathcal{L}} \cap R \cap C \cap (R^2 + C^2).$$

This inclusion of ideals is equivalent to the assertion of Corollary 3.3. ■

Proof of Theorem 3.2. We will deal only with the case $a, b > 2$, leaving the (easy) remaining cases to the reader.

The left side of (3.3) is clearly contained in the right side of (3.3). Order the variables row-wise $x_{11} < x_{12} < \ldots < x_{1b} < x_{21} < \ldots < x_{ab}$ and let $<$ denote the resulting reverse lexicographic term order. We shall prove the equality

$$in_<(I_{\mathcal{L}}) \cap in_<(R) \cap in_<(C) \cap in_<(I_{\mathcal{B}_{cor}} + R^2 + C^2) \quad = \quad in_<(I_{\mathcal{B}_{cor}}) \qquad (3.4)$$

This implies (3.3) because the left side of (3.4) contains the initial ideal of the right side of (3.3); hence both sides of (3.3) have the same initial ideal and are thus equal.

In order to evaluate the constituents in (3.4) we introduce the ideals

$$\begin{array}{lll} R' := \langle x_{12}, x_{13} \ldots, x_{1b} \rangle & \text{and} \qquad C' := \langle x_{21}, x_{31} \ldots, x_{a1} \rangle & \text{and} \\ I_{s,t} := \langle \; x_{ij} x_{kl} \mid s \leq i < k, \; j > l \geq t \; \rangle & \text{for } 1 \leq s \leq a \text{ and } 1 \leq t \leq b. & \end{array}$$

Since the 2×2-minors are a Gröbner basis (see e.g. [Stu, Prop. 5.4]), we have

$$in_<(I_{\mathcal{L}}) \quad = \quad I_{1,1}. \qquad (3.5)$$

Note that $in_<(R) = R$ and $in_<(C) = C$. We next derive the identity

$$in_<(I_{\mathcal{B}_{cor}} + R^2 + C^2) \quad = \quad (R + C)^2. \qquad (3.6)$$

It is evident that $R'C' \subseteq in_<(I_{\mathcal{B}_{cor}})$ and it follows that $(R+C)^2 \subseteq in_<(I_{\mathcal{B}_{cor}} + R^2 + C^2)$. For the reverse inclusion it suffices to show that the minimal generators of $I_{\mathcal{B}_{cor}} + R^2 + C^2$ are a Gröbner basis. Using Buchberger's first criterion [BW, Theorem 5.68], this reduces to a few easily checked cases, such as

$$\text{s-pol}\big(x_{k1} x_{1j} - x_{11} x_{kj} \, , \, x_{k1} x_{1l} - x_{11} x_{kl} \big) \;\; = \;\; x_{11} x_{1j} x_{kl} - x_{11} x_{1l} x_{kj} \in R^2 \quad (3.7)$$

For the definition of *s-pol(ynomial)* see [BW, pp. 211] or [CLO, pp. 82]. Having thus verified (3.6), we now claim the following more complicated identity:

$$\begin{aligned} in_<(I_{\mathcal{B}_{cor}}) \;\; = \;\; & R'C' \; + \; x_{11}^2 I_{2,2} \; + \; \sum_{t \geq 2} x_{11} x_{1t} I_{2,t} \; + \; \sum_{s \geq 2} x_{11} x_{s1} I_{s,2} \\ & + \; x_{11} \cdot \langle \; x_{ij} x_{kl} \mid i < k \text{ and } j > l \text{ and } (i = 1 \text{ or } l = 1) \rangle. \end{aligned} \qquad (3.8)$$

Here each summand is a product of ideals. We abbreviate the last summand by M. We first show that $in_<(I_{\mathcal{B}_{cor}})$ contains the right side of (3.8). To see that $in_<(I_{\mathcal{B}_{cor}})$ contains M, it suffices (by symmetry) to check that it contains $x_{11}x_{1j}x_{kl}$ for $1 < k, j > l$. This is clear from (3.7). Next let $s \leq i < k$, $j \geq l \geq 2$ and consider the following $\mathcal{B}_{cor}$-walk:

$$\begin{aligned} x_{11}x_{s1}x_{ij}x_{kl} &\to x_{1j}x_{s1}x_{i1}x_{kl} \to x_{sj}x_{11}x_{i1}x_{kl} \to x_{sj}x_{1l}x_{i1}x_{k1} \\ &\to x_{sj}x_{11}x_{il}x_{k1} \to x_{s1}x_{1j}x_{il}x_{k1} \to x_{s1}x_{11}x_{il}x_{kj}. \end{aligned}$$

This shows that $x_{11}x_{s1} \cdot (x_{ij}x_{kl} - x_{il}x_{kj}) \in I_{\mathcal{B}_{cor}}$. Applying (3.5) to $(a-s) \times (b-1)$-matrices, we conclude that $x_{11}^2 I_{2,2} \subset in_<(I_{\mathcal{B}_{cor}})$ and $x_{11}x_{s1}I_{s,2} \subset in_<(I_{\mathcal{B}_{cor}})$ for $s \geq 2$. By symmetry, we also obtain $x_{11}x_{1t}I_{2,t} \subset in_<(I_{\mathcal{B}_{cor}})$ for $t \geq 2$. It is evident that $R'C' \subset in_<(I_{\mathcal{B}_{cor}})$. We have shown that the right side of (3.8) lies in the left side.

The inclusion $\supseteq$ in (3.4) is clear. To prove equality in both (3.4) and (3.8), it suffices to show that the right side of (3.8) contains the left side in (3.4), i.e.,

$$\begin{aligned} I_{1,1} \cap R \cap C \cap (R+C)^2 \quad &\subseteq \\ R'C' + x_{11}^2 I_{2,2} + \sum_{t \geq 2} x_{11}x_{1t}I_{2,t} &+ \sum_{s \geq 2} x_{11}x_{s1}I_{s,2} + M. \end{aligned}$$

Let m be a monomial in $I_{1,1} \cap R \cap C \cap (R+C)^2$. If m is not divisible by x_{11}, then since $m \in R \cap C$ we must have $m \in R' \cap C' = R'C'$. Thus we may suppose that x_{11} divides m. If m is not divisible by x_{11}^2, then since $m \in (R+C)^2$ we must have $m \in R'$ or $m \in C'$, say m is divisible by $x_{11}x_{1t}$ for some t. Since $m \in I_{1,1}$ as well, we see that either:

- m is also divisible by x_{su} for some $s > 1$ and $u < t$, in which case $m \in M$, or else
- m is also divisible by $x_{su}x_{vw}$ with $s > v > 1$, $t \leq u < w$, in which case $m \in x_{11}x_{1t}I_{2,t}$.

In either case m lies in the desired sum. Now consider the case where x_{11}^2 divides m. Since $m \in I_{1,1}$, m is also divisible by a product of the form $x_{ij}x_{kl}$ with $i < j$, $k > l$. If $i = l = 1$, then $m \in R'C'$. If exactly one of i or l equals 1, then $m \in M$. If both $i > 1$ and $l > 1$ then $m \in x_{11}^2 I_{2,2}$, and we are done.

Finally, we show that the intersection in (3.3) is irredundant. It suffices to show this for $a = b = 3$. In this special case the monomial ideal (3.8) equals

$$\begin{aligned} in_{\prec}(I_{\mathcal{B}_{cor}}) = \langle\, & x_{12}x_{21}, x_{13}x_{21}, x_{12}x_{31}, x_{13}x_{31}, x_{11}^2x_{23}x_{32}, x_{11}x_{12}x_{23}x_{32}, \\ & x_{11}x_{21}x_{23}x_{32}, x_{11}x_{22}x_{31}, x_{11}x_{23}x_{31}, x_{11}x_{13}x_{22}, x_{11}x_{13}x_{32} \,\rangle. \end{aligned} \tag{3.9}$$

The following "witnesses" show that each of the four primary components in

(3.3) is needed:

$$x_{11}^2,\quad x_{31}\cdot(x_{21}x_{32}-x_{22}x_{31}),\quad x_{13}\cdot(x_{13}x_{22}-x_{12}x_{23}),\quad x_{11}\cdot(x_{22}x_{33}-x_{23}x_{32}).$$

The intersection of any three of the ideals on the right side of (3.3) contains one the four polynomials listed. But none of these four is in $I_{\mathcal{B}_{cor}}$ because none of their terms lies in (3.9). This completes the proof of Theorem 3.2. ■

Remark 3.4. In general when we have a primary decomposition $I = \cap_j I_j$ in a polynomial ring with a term order $<$, then $in_>(I) \subseteq \cap_j in_>(I_j)$, but the two sides will usually not be equal. For a simple example, suppose that $x < y$ are indeterminates, and consider

$$\langle x^2\rangle \;=\; in_<\langle x^2-y^2\rangle \quad\neq\quad \langle x\rangle\cap\langle x\rangle \;=\; in_<\langle x-y\rangle \cap in_<\langle x+y\rangle.$$

But in the setting of Theorem 3.1 a small miracle occurs and the corresponding intersections of initial ideals are equal for the right choice of term order. It would be interesting to understand when such things happen in general.

Remark 3.5. The referee suggested an alternate approach to the proof of Theorem 3.2 which simplifies the computations but yields a little less: Write J for the ideal on the right hand side of equation 3.3. As J is obviously contained in $I_{\mathcal{B}_{cor}}$, it suffices to prove $I_{\mathcal{B}_{cor}} \subseteq J$. It is easy to see that the two ideals become equal after adding (x_{11}) to both sides, so it suffices to show that

$$x_{11}(J : x_{11}) \subseteq I_{\mathcal{B}_{cor}}.$$

Using the computation of the initial ideal of $I_{\mathcal{B}_{cor}} + R^2 + C^2$ in the proof above one can prove that $(I_{\mathcal{B}_{cor}} + R^2 + C^2) : x_{11} = R + C$, and it follows that $(J : x_{11}) = I_{\mathcal{L}} \cap (R+C)$. Thus it suffices to show that $x_{11}(I_{\mathcal{L}}\cap(R+C)) \subseteq I_{\mathcal{B}_{cor}}\ldots$

4. Adjacent minors

Another natural basis for the lattice $\mathcal{L}$ in Section 3 is the set $\mathcal{B}_{adj}$ of adjacent 2×2-minors. Here the situation is more complicated than before. Let us examine the case $a = b = 4$ in detail. The adjacent 2×2-moves for 4×4-matrices are encoded by the ideal

$$\begin{aligned} I \;:=\; I_{\mathcal{B}_{adj}} \;=\; \langle & x_{12}x_{21}-x_{11}x_{22},\, x_{13}x_{22}-x_{12}x_{23},\, x_{14}x_{23}-x_{13}x_{24},\\ & x_{22}x_{31}-x_{21}x_{32},\, x_{23}x_{32}-x_{22}x_{33},\, x_{24}x_{33}-x_{23}x_{34},\\ & x_{32}x_{41}-x_{31}x_{42},\, x_{33}x_{42}-x_{32}x_{43},\, x_{34}x_{43}-x_{33}x_{44}\rangle. \end{aligned}$$

Two nonnegative integer 4×4-matrices (a_{ij}) and (b_{ij}) with the same row and column sums can be connected by a sequence of adjacent 2×2-moves if and only if the binomial

$$\prod_{1\le i,j\le 4} x_{ij}^{a_{ij}} \quad - \quad \prod_{1\le i,j\le 4} x_{ij}^{b_{ij}}$$

lies in the ideal I, by Corollary 2.1.

Proposition 4.1. *Two non-negative integer 4×4-matrices with the same row and column sums can be connected by a sequence of adjacent 2×2-moves if both of them satisfy the following six inequalities:*
(i) $a_{21}+a_{22}+a_{23}+a_{24} \ \ge 2$;
(ii) $a_{31}+a_{32}+a_{33}+a_{34} \ \ge 2$;
(iii) $a_{12}+a_{22}+a_{32}+a_{42} \ \ge 2$;
(iv) $a_{13}+a_{23}+a_{33}+a_{43} \ \ge 2$;
(v) $a_{12}+a_{22}+a_{23}+a_{24}+a_{31}+a_{32}+a_{33}+a_{43} \ \ge 1$;
(vi) $a_{13}+a_{21}+a_{22}+a_{23}+a_{32}+a_{33}+a_{34}+a_{42} \ \ge 1$.

We remark that these sufficient conditions remain valid if (at most) one of the four inequalities "≥ 2" is replaced by "≥ 1". No further relaxation of the conditions (i)–(vi) is possible, as is shown by the following two pairs of matrices, which are disconnected:

$$\begin{pmatrix} 0&0&0&0\\ 0&1&1&0\\ 0&1&0&0\\ 0&0&0&1 \end{pmatrix} \leftrightarrow \begin{pmatrix} 0&0&0&0\\ 0&0&1&1\\ 0&1&0&0\\ 0&1&0&0 \end{pmatrix} \text{ and } \begin{pmatrix} 0&0&1&0\\ 1&1&0&0\\ 0&0&0&2\\ 0&0&0&0 \end{pmatrix} \leftrightarrow \begin{pmatrix} 0&0&0&1\\ 0&0&1&1\\ 1&1&0&0\\ 0&0&0&0 \end{pmatrix}.$$

The necessity of conditions (v) and (vi) is seen from the disconnected matrices

$$\begin{pmatrix} n&n&0&n\\ 0&0&0&n\\ n&0&0&0\\ n&0&n&n \end{pmatrix} \leftrightarrow \begin{pmatrix} n&0&n&n\\ n&0&0&0\\ 0&0&0&n\\ n&n&0&n \end{pmatrix} \qquad \text{for any integer} \quad n\ge 0.$$

Proof of Proposition 4.1 Let $I_{\mathcal{L}}$ be the prime ideal generated by all 36 2×2-minors of a 4×4-matrix (x_{ij}) of indeterminates. Define also the primes

$$\begin{aligned} C_1 \ &:= \ \langle x_{12},x_{22},x_{23},x_{24},x_{31},x_{32},x_{33},x_{43}\rangle \quad \text{and} \\ C_2 \ &:= \ \langle x_{13},x_{21},x_{22},x_{23},x_{32},x_{33},x_{34},x_{42}\rangle. \end{aligned}$$

Using a computer algebra system – such as MACAULAY – it can be verified easily that

$$\begin{aligned} I_{\mathcal{L}} \ \cap \ C_1 \cap C_2 \cap \langle x_{21},x_{22},x_{23},x_{24}\rangle \ \cap \ \langle x_{31},x_{32},x_{33},x_{34}\rangle^2 \\ \cap \ \langle x_{12},x_{22},x_{32},x_{42}\rangle^2 \ \cap \ \langle x_{13},x_{23},x_{33},x_{43}\rangle^2 \quad \subseteq \quad I_{\mathcal{B}_{adj}}. \end{aligned} \tag{4.1}$$

This containment of ideals implies Proposition 4.1. ■

For completeness we describe the primary decomposition of $I = I_{\mathcal{B}_{adj}}$. This is a good test case for implementations of (binomial) primary decomposition. Consider the prime ideals

$$A \quad := \quad \langle\, x_{12}x_{21} - x_{11}x_{22}, x_{13}, x_{23}, x_{31}, x_{32}, x_{33}, x_{43}\,\rangle \qquad \text{and}$$

$$\begin{aligned} B \;:=\; \langle\, & x_{11}x_{22} - x_{12}x_{21}, x_{11}x_{23} - x_{13}x_{21}, x_{11}x_{24} - x_{14}x_{21}, x_{12}x_{23} - x_{13}x_{22},\\ & x_{12}x_{24} - x_{14}x_{22}, x_{13}x_{24} - x_{14}x_{23}, x_{31}, x_{32}, x_{33}, x_{34}\rangle. \end{aligned}$$

Rotating and reflecting the matrix (x_{ij}), we find eight ideals $A_1, A_2, \ldots, A_8$ equivalent to A and four ideals B_1, B_2, B_3, B_4 equivalent to B. Note that A_i has codimension 7 and degree 2, B_j has codimension 7 and degree 4, and C_k has codimension 8 and degree 1, while P has codimension 9 and degree 20.

Proposition 4.1. *The minimal associated primes of the binomial ideal I are the* 15 *primes A_i, B_j, C_j and P. Each of these occurs with multiplicity one in I, so that*

$$\mathit{Rad}(I) \quad = \quad A_1 \cap A_2 \cap \cdots \cap A_8 \,\cap\, B_1 \cap B_2 \cap B_3 \cap B_4 \,\cap\, C_1 \cap C_2 \,\cap\, P.$$

In particular, both I and its radical $\mathit{Rad}(I)$ have codimension 7 *and degree* 32.

We next list the embedded components of I. Our first primary ideal is

$$D := \Big(\big(I + \langle x_{13}^2, x_{23}^2, x_{31}^2, x_{32}^2, x_{33}^2, x_{34}^2, x_{43}^2\rangle\big) \;:\; x_{11}x_{12}x_{14}x_{21}x_{22}x_{24}x_{41}x_{42}x_{44}\Big).$$

Its radical $\mathit{Rad}(D)$ is a prime of codimension 10 and degree 5. (Commutative algebra experts will notice that $\mathit{Rad}(D)$ is a *ladder determinantal ideal.*) Up to symmetry, there are four such ideals D_1, D_2, D_3, D_4.

Our second type of primary ideal is $E :=$

$$\big(\big[I + \langle x_{12}^2, x_{21}^2, x_{22}^2, x_{23}^2, x_{24}^2, x_{32}^2, x_{33}^2, x_{34}^2, x_{42}^2, x_{43}^2\rangle\big] : (x_{11}x_{13}x_{14}x_{31}x_{41}x_{44})^2\big).$$

Its radical $\mathit{Rad}(E)$ is a monomial prime of codimension 1. Up to symmetry, there are eight such primary ideals $E_1, E_2, \ldots, E_8$.

Our third type of primary ideal has codimension 11. We set $F :=$

$$\big(\big[\,I + \langle x_{12}^3, x_{13}^3, x_{22}^3, x_{23}^3, x_{31}^3, x_{32}^3, x_{33}^3, x_{34}^3, x_{42}^3, x_{43}^3\rangle\big] : (x_{11}x_{14}x_{21}x_{24}x_{41}x_{44})^2\big).$$

The radical of F is the degree 2 prime

$$Rad(F) \;=\; (x_{11}x_{24} - x_{21}x_{14},\, x_{12}, x_{13}, x_{22}, \,\ldots\,,\, x_{43}).$$

Up to symmetry, there are four such primary ideals F_1, F_2, F_3, F_4.

Our last primary ideal has codimension 12. It is unique up to symmetry.

$$G \;:=\; \big(\, [I + \langle x_{12}^5, x_{13}^5, x_{21}^5, x_{22}^5, x_{23}^5, x_{24}^5, x_{31}^5, x_{32}^5, x_{33}^5, x_{34}^5, x_{42}^5, x_{43}^5 \rangle] \\ : (x_{11}x_{14}x_{41}x_{44})^5 \,\big).$$

In summary, we have the following theorem, which can be checked by MACAULAY:

Theorem 4.2. *The ideal I has precisely 32 associated primes, 15 minimal and 17 embedded. Using the decomposition in Proposition 2, we get the minimal primary decomposition*

$$I \;=\; Rad(I) \cap D_1 \cap D_2 \cap D_3 \cap D_4 \cap E_1 \cap E_2 \cap \cdots \cap E_8 \cap F_1 \cap F_2 \cap F_3 \cap F_4 \cap G.$$

It remains an open problem to find a primary decomposition for the ideal of adjacent 2×2-minors for larger sizes. We do not even have a reasonable conjecture for generalizing the result in Proposition 4.1.

In the special case $a = 2$ the ideal $I_{\mathcal{B}_{adj}}$ is radical and has a nice explicit prime decomposition. We shall present this decomposition using a slightly simplified notation. We write I as the ideal generated by the following n binomials in $2n+2$ variables:

$$x_{i-1} \cdot y_i \;-\; x_i \cdot y_{i-1} \qquad (i = 1, 2, \ldots, n). \tag{4.2}$$

Let $f(n)$ denote the n-th *Fibonacci number*, which is defined recursively by $f(0) = f(1) = 1$ and $f(n) = f(n-1) + f(n-2)$.

Theorem 4.3. *The ideal I of adjacent 2×2-minors of a generic $2 \times (n+1)$-matrix is the intersection of $f(n)$ prime ideals; in particular, I is radical.*

Proof. The ideal I is a complete intersection, which means I has codimension n and degree 2^n. (To see this note that the left hand terms in (4.2) are pairwise relatively prime. They are the leading terms in the lexicographic order.) By Macaulay's Unmixedness Theorem [Eis, Corollary 18.14], every associated prime of I is minimal and has codimension n.

Let $\mathcal{D}(n)$ denote the set of all subsets of $\{1, 2, \ldots, n-1\}$ which do not contain two consecutive integers. The cardinality of $\mathcal{D}(n)$ equals the Fibonacci number $f(n)$. For instance, $\mathcal{D}(4) = \big\{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1,3\}, \{1,4\}, \{2,4\}\big\}$. For each element S we define a binomial ideal I_S in $k[x_0, \ldots, x_n, y_0, \ldots, y_n]$.

The generators of I_S are the variables x_i and y_i for all $i \in S$, and the binomials $x_j y_k - x_k y_j$ for all $j, k \notin S$ such that no element of S lies between j and k. It is easy to see that I_S is a prime ideal of codimension n. Moreover, I_S contains I, and therefore I_S is a minimal prime of I. We claim that

$$I \quad = \quad \bigcap_{S \in \mathcal{D}(n)} I_S \tag{4.3}$$

In view of Macaulay's Unmixedness Theorem, it suffices to prove the identity

$$\sum_{S \in \mathcal{D}(n)} degree(I_S) \quad = \quad 2^n \tag{4.4}$$

First note that $I_\emptyset$ is the determinantal ideal $\langle x_i y_j - x_i x_j \,:\, 0 \leq i < j \leq n \rangle$. It is known (see e.g. [Har, Example 19.10]) that the degree of $I_\emptyset$ equals $n+1$. Using the same fact for matrices of smaller size, we find that, for S non-empty, the degree of I_S equals the product

$$i_1 \cdot (i_2 - i_1 + 1) \cdot (i_3 - i_2 + 1) \cdots (i_r - i_{r-1} + 1) \cdot i_r \quad \text{where} \quad S = \{i_1 < i_2 < \cdots < i_r\}. \tag{4.5}$$

Consider the surjection $\phi \,:\, 2^{\{1,\ldots,n\}} \to \mathcal{D}(n)$ defined by $\phi(\{j_1 < j_2 < \cdots < j_r\}) = \{j_{r-1}, j_{r-3}, j_{r-5}, \ldots\}$. The product in (4.5) is the cardinality of the inverse image $\phi^{-1}(S)$. This proves $\sum_{S \in \mathcal{D}(n)} \#(\phi^{-1}(S)) \;=\; 2^n$, which implies (4.4) and hence Theorem 4.3. ∎

5. Circuit walks

Let $\mathcal{A}$ be a $d \times n$-integer matrix of rank d. The integer kernel of $\mathcal{A}$ is a sublattice $\mathcal{L}$ in $\mathbf{Z}^n$ of rank $n-d$. In this case $\mathcal{L}$ is saturated and hence $I_\mathcal{L}$ is a prime ideal. A non-zero vector $\mathbf{u} = (u_1, \ldots, u_n)$ in $\mathcal{L}$ is called a *circuit* if its coordinates u_i are relatively prime and its support $supp(\mathbf{u}) = \{\, i \,:\, u_i \neq 0\}$ is minimal with respect to inclusion. In this section we discuss the walk defined by the set $\mathcal{C}$ of all circuits in $\mathcal{L}$. This makes sense for two reasons:

- The lattice $\mathcal{L}$ is generated by the circuits, i.e., $\mathbf{Z}\mathcal{C} \;=\; \mathcal{L}$ (see e.g. [ES, Lemma 8.8]).
- The circuits can be computed easily from the matrix $\mathcal{A}$.

Here is a simple algorithm for computing $\mathcal{C}$. (See [BM] for a more sophisticated approach.) Initialize $\mathcal{C} := \emptyset$. For any $(d+1)$-subset $\tau = \{\tau_1, \ldots, \tau_{d+1}\}$ of $\{1, \ldots, n\}$ form the vector

$$C_\tau \quad = \quad \sum_{i=1}^{d+1} (-1)^i \cdot det(\mathcal{A}_{\tau \backslash \{\tau_i\}}) \cdot \mathbf{e}_{\tau_i},$$

where $\mathbf{e}_j$ denotes the j-th unit vector and $\mathcal{A}_\sigma$ denote the submatrix of $\mathcal{A}$ with column indices σ. If C_τ is non-zero then remove common factors from its coordinates. The resulting vector is a circuit and all circuits are obtained in this manner (see e.g. [Stu, §4]).

Example 5.1. Let $d-2, n=4$ and $\mathcal{A} = \begin{pmatrix} 0 & 2 & 5 & 7 \\ 7 & 5 & 2 & 0 \end{pmatrix}$. Then the set of circuits equals

$$\mathcal{C} \quad = \quad \pm\{\,(3,-5,2,0),\ (5,-7,0,2),\ (2,0,-7,5),\ (0,2,-5,3)\,\}. \qquad (5.1)$$

It is instructive to check that the $\mathbf{Z}$-span of $\mathcal{C}$ equals $\mathcal{L} = ker_{\mathbf{Z}}(\mathcal{A})$. (For instance, try to write $(1,-1,-1,1) \in \mathcal{L}$ as a $\mathbf{Z}$-linear combination of $\mathcal{C}$). We shall derive the following result: *Two $\mathcal{L}$-equivalent non-negative integer vectors (A,B,C,D) and (A',B',C',D') can be connected by the circuits in (5.1) if both of them satisfy the following inequality*

$$min\Big\{max\{A,B,C,D\},\ max\{B,\ \frac{9}{4}C,\ \frac{9}{4}D\},\ max\{\frac{9}{4}A,\ \frac{9}{4}B,\ C\}\Big\} \ \geq\ 9 \quad (5.2)$$

We remark that the following two $\mathcal{L}$-equivalent pairs cannot be connected by circuits:

$$(4,9,0,2) \leftrightarrow (5,8,1,1) \quad \text{and} \quad (1,6,6,1) \leftrightarrow (3,4,4,3) \qquad (5.3)$$

To analyze circuit walks in general we consider the *circuit ideal* $I_{\mathcal{C}}$ generated by the binomials $\mathbf{x}^{\mathbf{u}_+} - \mathbf{x}^{\mathbf{u}_-}$ where $\mathbf{u} = \mathbf{u}_+ - \mathbf{u}_-$ runs over all circuits in $\mathcal{L}$. The primary decomposition of circuit ideals was studied in [ES, §8]. We summarize the relevant results. Let $pos(\mathcal{A})$ denote the d-dimensional convex polyhedral cone in $\mathbf{R}^d$ spanned by the column vectors of $\mathcal{A}$. Each face of $pos(\mathcal{A})$ is identified with the subset $\sigma \subset \{1,\ldots,n\}$ consisting of all indices i such that the i-th column of $\mathcal{A}$ lies on that face. If σ is a face of $pos(\mathcal{A})$ then the ideal $I_\sigma := \langle x_i \,:\, i \notin \sigma\rangle + I_{\mathcal{L}}$ is prime. Note that $I_{\{1,\ldots,n\}} = I_{\mathcal{L}}$ and $I_{\{\}} = \langle x_1, x_2, \ldots, x_n\rangle$.

Theorem 5.2. [ES, Theorem 8.3, Example 8.6 and Proposition 8.7]

$$Rad(I_{\mathcal{C}}) \ = \ I_{\mathcal{L}} \quad and \quad Ass(I_{\mathcal{C}}) \ \subseteq \ \big\{\, I_\sigma \,:\, \sigma \textit{ is a face of } pos(\mathcal{A})\big\}.$$

Theorem 8.3 in [ES] gives a procedure for computing a binomial primary decomposition of the circuit ideal $I_{\mathcal{C}}$. This enables us to analyze the connectivity of the circuit walk in terms of the faces of the polyhedral cone $pos(\mathcal{A})$.

Example 5.1. *(continued)* We choose variables a, b, c, d for the four columns of $\mathcal{A}$. The cone $pos(\mathcal{A}) = pos\{(7,0),(5,2),(2,5),(0,7)\}$ equals the positive orthant in $\mathbf{R}^2$. It has one 2-dimensional face, labeled $\{a,b,c,d\}$, two 1-dimensional faces, labeled $\{a\}$ and $\{d\}$ and one 0-dimensional face, labeled $\{\}$. The lattice ideal of $\mathcal{L} = ker_{\mathbf{Z}}(\mathcal{A})$ is the prime ideal

$$I_{\mathcal{L}} \quad = \quad \langle\, ad - bc,\, ac^4 - b^3d^2,\, a^3c^2 - b^5,\, b^2d^3 - c^5,\, a^2c^3 - b^4d\,\rangle.$$

The circuit ideal equals

$$I_{\mathcal{C}} \quad = \quad \langle\, a^3c^2 - b^5,\, a^5d^2 - b^7,\, a^2d^5 - c^7,\, b^2d^3 - c^5\,\rangle.$$

It has the minimal primary decomposition

$$\begin{aligned} I_{\mathcal{C}} \quad = \quad I_{\mathcal{L}} \;&\cap\; \langle\, b^9,\, c^4,\, d^4,\, b^2d^2,\, c^2d^2,\, b^2c^2 - a^2d^2,\, b^5 - a^3c^2\,\rangle \\ &\cap\; \langle\, a^4,\, b^4,\, c^9,\, a^2b^2,\, a^2c^2,\, b^2c^2 - a^2d^2,\, c^5 - b^2d^3\,\rangle \\ &\cap\; \big(\langle a^9, b^9, c^9, d^9\rangle \,+\, I_{\mathcal{C}}\big). \end{aligned}$$

Here the second ideal is primary to $I_{\{a\}} = \langle b,c,d\rangle$ and the third ideal is primary to $I_{\{d\}} = \langle a,b,c\rangle$. The given primary decomposition implies (5.2) because

$$\langle a^9, b^9, c^9, d^9\rangle \;\cap\; \langle b^9,\, c^4,\, d^4\rangle \;\cap\; \langle a^4,\, b^4,\, c^9\rangle \;\cap\; I_{\mathcal{L}} \quad\subset\quad I_{\mathcal{C}}. \tag{5.2$'$}$$

Returning to our general discussion, Theorem 5.2 implies that for each face σ of the polyhedral cone $pos(\mathcal{A})$ there exists a non-negative integer M_σ such that

$$I_{\mathcal{L}} \;\cap\; \bigcap_{\substack{\sigma \text{ face} \\ \text{of } pos(\mathcal{A})}} \langle\, x_i \,:\, i \notin \sigma\,\rangle^{M_\sigma} \quad\subset\quad I_{\mathcal{C}}. \tag{5.4}$$

Corollary 5.3. *For each proper face σ of the cone $pos(\mathcal{A})$ there is an integer M_σ such that any two $\mathcal{L}$-equivalent vectors $(a_1,\ldots,a_n)$ and $(b_1,\ldots,b_n)$ in $\mathbf{N}^n$ with the property*

$$\sum_{i\notin\sigma} a_i \,\geq\, M_\sigma \quad \textit{and} \quad \sum_{i\notin\sigma} b_i \,\geq\, M_\sigma \quad \textit{for all proper faces } \sigma \textit{ of } pos(\mathcal{A}) \tag{5.4$'$}$$

can be connected by circuits.

This suggests the following research problem.

Problem 5.4. *Find good bounds for the integers M_σ in terms of the matrix $\mathcal{A}$.*

The optimal value of M_σ seems to be related to the singularity of the toric variety defined by $I_{\mathcal{L}}$ along the torus orbit labeled σ: The worse the singularity is, the higher the value of M_σ. It would be very interesting to understand these geometric aspects.

In Example 5.1 we can choose the integers M_σ as follows:

$$M_{\{\}} \;=\; 15 \quad \text{and} \quad M_{\{a\}} \;=\; 11 \quad \text{and} \quad M_{\{d\}} \;=\; 11.$$

These choices are optimal. This is seen from the disconnected pairs in (5.3).

References

[AM] M. F. Atiyah and I. G. Macdonald: *Introduction to Commutative Algebra,* Addison Wesley, Reading MA 1969.

[BM] D. Bayer and I. Morrison: Toric methods for mixed integer programming, in preparation.

[BW] T. Becker, V. Weispfenning: *Gröbner Bases: A Computational Approach to Commutative Algebra*, Graduate Texts in Mathematics, Springer, New York, 1993.

[CLO] D. Cox, J. Little, and D. O'Shea: *Ideals, Varieties, and Algorithms,* Springer-Verlag, NY, 1992.

[DS] P. Diaconis and B. Sturmfels: Algebraic algorithms for sampling from conditional distributions, to appear.

[Eis] D. Eisenbud: *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, NY, 1995.

[ES] D. Eisenbud and B. Sturmfels: Binomial ideals, *Duke Mathematical Journal* **84** (1996) 1–45.

[GL] G. Glonek: Some aspects of log linear models. Thesis, School of Math. Sci., Flinders Univ. of S. Australia, 1987.

[Har] J. Harris: *Algebraic Geometry*, Graduate Texts in Math., Springer, New York, 1992.

[MM] E. Mayr and A. Meyer: The complexity of the word problem for commutative semigroups and polynomial ideals. *Advances in Mathematics* **46** (1982) 305–329.

[Stu] B. Sturmfels: *Gröbner Bases and Convex Polytopes*, American Mathematics Society, Providence, RI, 1995.

[Tho] R.R. Thomas: A geometric Buchberger algorithm for integer programming. *Mathematics of Operations Research* **20** (1995), 864–884.

Dept. of Math., Harvard University, Cambridge MA 02138

Dept. of Math., Brandeis University, Waltham MA 02254
eisenbud@math.brandeis.edu

Dept. of Math., University of California, Berkeley CA 94720
bernd@math.berkeley.edu