Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 50 (2009), No. 2, 521-531.

On the Graver Complexity of Codimension 2 Matrices

Kristen A. Nairn

College of St. Benedict, MN, USA
e-mail: knairn@csbsju.edu

Abstract. In this paper we describe how the inherent geometric properties of the Graver bases of integer matrices of the form $\{(1,0),(1,a),(1,b),(1,a+b)\}$ with $a,b \in \mathbb{Z}^+$ enable us to determine that the Graver complexity of the more general matrix $\mathcal{A} = \{(1,i_1),(1,i_2),(1,i_3),(1,i_4)\}$ associated to a monomial curve in $\mathbb{P}^3$ can be bounded as a linear relation of the entries of $\mathcal{A}$.

MSC 2000: 14M25 (primary); 52B20, 13P99 (secondary)
Keywords: Graver complexity, Hilbert bases, monomial curves

1. Introduction

Vector configurations of the form $\mathcal{A} = \{(1,i_1),(1,i_2),(1,i_3),(1,i_4)\}$ with $0 \le i_1 < i_2 < i_3 < i_4$ define a toric ideal whose projective toric variety is a monomial space curve in $\mathbb{P}^3$ [2]. We will study matrices of this form and use the well-known result that any minimal generating set of binomial generators of a Lawrence ideal is the Graver basis of this defining ideal [16] in order to determine some geometric properties of the Graver basis of $\mathcal{A}$ as well as an upper bound on the Graver complexity of $\mathcal{A}$. For $\mathbf{u},\mathbf{v} \in \mathbb{R}^n$, define the relation $\sqsubseteq$ on $\mathbb{R}^n$ by $\mathbf{u} \sqsubseteq \mathbf{v}$ if $u^{(i)}v^{(i)} \ge 0$ and $|u^{(j)}| \le |v^{(j)}|$ for every component $1 \le j \le n$. We say that $\mathbf{u}$ *reduces* $\mathbf{v}$ if $\mathbf{u} \sqsubseteq \mathbf{v}$. Let O_ρ denote an orthant in $\mathbb{R}^n$ where $\rho \in \{+,-\}^n$ and let $C_\rho = \ker_{\mathbb{Z}}(\mathcal{A}) \cap O_\rho$ be a pointed polyhedral cone. Let $\mathcal{H}_\rho$ be the Hilbert basis of C_ρ as in [15]. The *Graver basis*, $\mathcal{G}r(\mathcal{A}) = \bigcup_\rho \mathcal{H}_\rho \backslash \{0\}$, of a matrix $\mathcal{A}$ is the set of nonzero minimal elements in the poset $\{\mathcal{H}_\rho, \sqsubseteq\}$ for each cone C_ρ.

Given a vector $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{R}^n$ the 1-*norm* of $\mathbf{u}$ is $\|\mathbf{u}\|_1 = \sum_{i=1}^n |u_i|$. The following result from Santos-Sturmfels [14] provides an explicit formula for computing the Graver complexity of a $d \times n$ integer vector configuration $\mathcal{A} = (a_1 a_2 \cdots a_n) \subseteq \mathbb{Z}^{d\times n}$ without using higher-dimensional Lawrence configurations:

Theorem 1.1. *The Graver complexity of a vector configuration $\mathcal{A} = (a_1 a_2 \cdots a_n) \subseteq \mathbb{Z}^{d\times n}$ is the maximum* 1*-norm of the elements of the Graver basis of the Graver basis of $\mathcal{A}$.*

If one takes as column vectors the Graver basis of $\mathcal{A}$, the Graver basis of this new matrix is the Graver of the Graver basis, $\mathcal{G}r(\mathcal{G}r(\mathcal{A}))$. Define the non-unique element $\psi \in \mathcal{G}r(\mathcal{G}r(\mathcal{A}))$ with maximal 1-norm as the *Graver representative.* Since there is the natural identification of Graver basis elements as exponent vectors of binomials in some polynomial ring, taking the 1-norm of a Graver representative tells us the degree of a Graver basis element [16]. Note that the Graver complexity of the 2×3 case $\mathcal{A} = \{(1,0),(1,a),(1,b)\}$ is uninteresting since $(b-a,-b,a)$ is the unique element (up to sign) in $\ker_{\mathbb{Z}}(\mathcal{A})$. Thus the kernel of $\mathcal{G}r(\mathcal{G}r(\mathcal{A}))$ is trivial.

In general, it is not clear how the degree of the generators of the homogeneous ideal $I_{\mathcal{A}} = \langle \mathbf{x}^\alpha - \mathbf{x}^\beta \colon \alpha, \beta \in \mathbb{N}^n,\ \alpha - \beta \in \ker_{\mathbb{Z}}(\mathcal{A})\rangle$ is related to the matrix $\mathcal{A}$. L'vovsky [9] showed that the toric ideal $I_{\mathcal{A}}$ defined by a $2 \times n$ integer matrix $\mathcal{A} = \{(1,i_1),(1,i_2),\ldots,(1,i_{n-1}),(1,i_n)\}$ with $0 \le i_1 < i_2 < \cdots < i_n$ is generated by elements of degree at most the sum of the two largest consecutive differences $i_k - i_{k-1}$. Thus, if $\delta_k = i_k - i_{k-1}$, where $1 \le k \le n$, then the maximal degree of the generators for the monomial curve ideal $I_{\mathcal{A}}$ is $\max\{\delta_k + \delta_j\}$ for $1 \le k < j \le n$. We remark that the Graver complexity is not necessarily the regularity of the ideal $I_{\mathcal{A}}$. For example, the Graver complexity of the twisted cubic curve represented by the matrix $\mathcal{A} = \{(1,0),(1,1),(1,2),(1,3)\}$ is $g(\mathcal{A}) = 6$; however, the regularity of the ideal is $\operatorname{reg}(I_{\mathcal{A}}) = 2$.

For $\mathbf{u} \in \mathbb{R}^n$, the *support* of $\mathbf{u}$ is $\operatorname{supp}(\mathbf{u}) = \{i \colon u_i \neq 0\}$. A vector $\mathbf{u} \in \ker(\mathcal{A})$ is called a *circuit* of $\mathcal{A}$ if $\operatorname{supp}(\mathbf{u})$ is minimal with respect to inclusion and the coordinates of $\mathbf{u}$ are relatively prime. Denote by $\mathcal{C}(\mathcal{A})$ the set of all circuits of a $d \times n$ matrix $\mathcal{A}$. We may define the 1-norm of a nonzero vector $\mathbf{u} \in \ker(\mathcal{A})$ by applying Cramer's rule to the $d \times (d+1)$ submatrices of $\mathcal{A} \subseteq \mathbb{Z}^{d\times n}$:

$$\|\mathbf{u}\|_1 = \sum_{j=1}^{d+1} (-1)^j \mathcal{D}(a_{i_1}, \ldots, a_{i_{j-1}}, a_{i_{j+1}}, \ldots, a_{i_{d+1}}) \cdot e_{i_j}.$$

Circuits defined by Cramer's rule are called *true circuits*, denoted by $\mathcal{TC}(\mathcal{A})$.

Example. Consider $\mathcal{A} = \{(1,0),(1,3),(1,4),(1,6)\}$. Using 4ti2 [5], we find that the circuits for $\mathcal{A}$ are $\mathcal{C}(\mathcal{A}) = \{c_1 = (0,2,-3,1), c_2 = (1,-2,0,1), c_3 = (1,0,-3,2), c_4 = (1,-4,3,0)\}$ and the true circuits are $\mathcal{TC}(\mathcal{A}) = \{c_1, 3c_2, 2c_3, c_4\}$.

Denote by $\operatorname{maxg}(\mathcal{A}) = \max\{\|\mathbf{u}\|_1 \colon \mathbf{u} \in \mathcal{G}r(\mathcal{A})\}$ the elements in the Graver basis of $\mathcal{A}$ with maximal 1-norm. For a homogenous toric ideal $I_{\mathcal{A}} \subset S = k[x_1, \ldots, x_n]$, Hosten [8] proved that $\operatorname{reg}(I_{\mathcal{A}}) \le \frac{n}{2}\operatorname{maxg}(\mathcal{A})$ where $\operatorname{reg}(I_{\mathcal{A}})$ is the Castelnuovo-Mumford regularity determined by its minimal free resolution. It is necessary to define the maximal 1-norm of the true circuits in order to get a bound on maxg($\mathcal{A}$) [8]. Thus to give the bound on the total degree of the Graver basis elements for codim 2 matrices, we utilize the geometric relationship between circuits in a Gale dual diagram and circuits in the Graver basis for $\mathcal{A}$.

Definition 1.2. [12] *Let $\mathcal{A}$ be a 2×4 integer matrix and let $B = (a_1, a_2)^T$ be the 4×2 matrix whose columns are a basis of $\mathcal{L}(\mathcal{A})$. The Gale diagram $G_{\mathcal{L}}$ of $\mathcal{A}$ is the collection of row vectors $\mathbf{b}_i = (b_{i1}, b_{i2})$ which is unique up to the action of $SL_2(\mathbb{Z})$. We are interested in the Gale dual diagram, $G_{\mathcal{L}}{}^* = \{b_1^*, b_2^*, b_3^*, b_4^*\}$, where each $b_i^* = (-b_{i2}, b_{i1}) \in \mathbb{Z}^2$.*

The four row vectors in $G_{\mathcal{L}}{}^*$ correspond to the circuits in the Graver basis $\mathcal{G}r(\mathcal{A})$ for the matrix $\mathcal{A}$ and are extremal rays dividing $\mathbb{R}^2$ into eight cones. The remaining vectors of $\mathcal{G}r(\mathcal{A})$ are elements in the Hilbert basis of the cones defined by these rays. If b_1^*, b_2^* are two vectors defining a cone $C = \text{cone}(b_1^*, b_2^*)$ and if $\det(b_1 b_2) = 1$, then the cone is unimodular and thus there is exactly one lattice point in the interior of the parallelogram spanned by these two vectors.

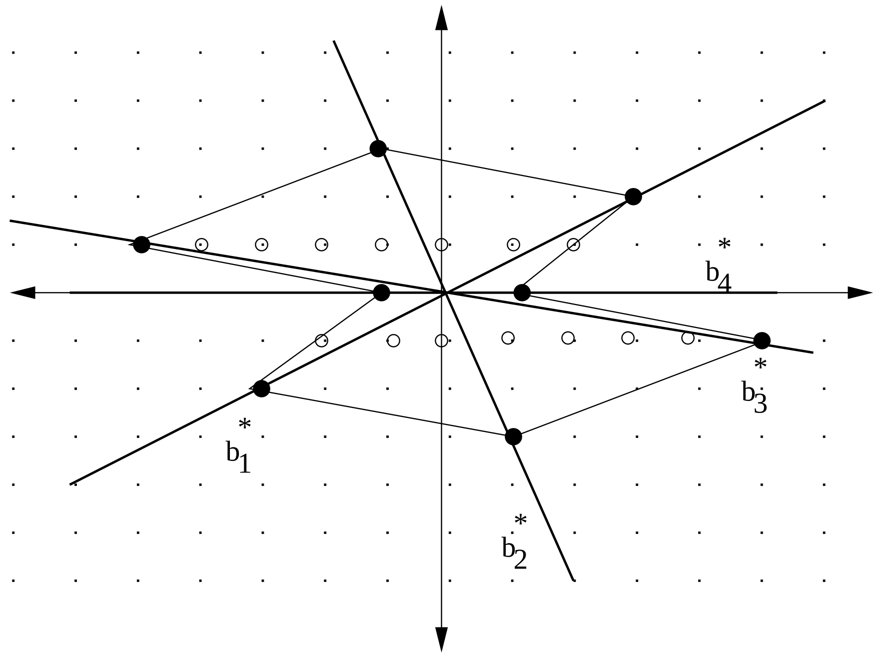

Figure 1. The Gale dual diagram for $\mathcal{A} = \{(1,0),(1,1),(1,3),(1,14)\}$

Example. The matrix $\mathcal{A} = \{(1,0),(1,1),(1,3),(1,14)\}$. Using *4ti2* [5], the minimal generators for the toric ideal are $I_{\mathcal{A}} = \langle(-2,3,-1,0),\ (3,1,-5,1)\rangle$. Thus the Gale dual diagram is defined by the 4×2 matrix

$$G_{\mathcal{L}}{}^* = \begin{pmatrix} -3 & -1 & 5 & -1 \\ -2 & 3 & -1 & 0 \end{pmatrix}^T = \left(b_1^*, b_2^*, b_3^*, b_4^*\right)^T$$

see Figure 1. The extremal rays defining each 2-dimensional cone correspond to the circuits in the Graver basis and the minimal lattice points in the interior of the cones are Hilbert basis elements. Thus finding a bound on the circuits $\mathcal{C}(\mathcal{A})$ would be meaningful. It is important to distinguish the cases where the circuits of the Graver basis of a matrix $\mathcal{A}$ are the true circuits. We will do this using Gale dual diagrams.

Lemma 1.3. *Let $\mathcal{A} = \{(1,0),(1,a),(1,b),(1,a+b)\} \subseteq \mathbb{Z}^{2\times 4}$ where $0 < a < b$ and the differences of integers in the second row of $\mathcal{A}$ are pairwise co-prime. The circuits of $\mathcal{A}$ are the true circuits.*

Proof. Let $c = a+b$. By Cramer's rule [15] the 2×2 minors of $\mathcal{A}$ determine the circuits

$$\mathcal{C}(\mathcal{A}) = \{(0, b-c, c-a, a-b), (b-c, 0, c, -b), (a-c, c, 0, -a), (a-b, b, -a, 0)\}$$

whose pairwise differences are co-prime. Therefore the circuits for $\mathcal{A}$ are the true circuits. □

Corollary 1.4. *For $\mathbf{u} \in \mathcal{G}r(\mathcal{A})$ the maximal 1-norm of true circuits is $2(a+b)$.*

Using matrices of the form $\mathcal{A} = \{(1,0),(1,a),(1,b),(1,a+b)\}$ where $0 < a < b$ allows us to further reduce the computation of the Graver complexity. Theorem 2.3 shows that in order to compute the Graver complexity of matrices of this form it is sufficient to find the maximal 1-norm of the Graver basis elements for the matrix $B_c = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 0 \\ 0 & 1 & 2 & \cdots & c & 1 \end{pmatrix}$, where $c = a+b$. In [6], we showed that the maximal 1-norm of the Graver basis elements for B_c is $2c$. We define what it means for a Graver basis to be *covered by circuits* and prove in Theorem 2.6 that the region bounded by the circuits for matrices of this particular form have area $2c$. Although the Graver basis of $\mathcal{A}$ is covered by circuits, the Graver basis of the Graver basis of $\mathcal{A}$ is not covered by circuits (Theorem 2.8). Therefore, we must assume

Conjecture 1.5. True Circuit Conjecture (Hosten [8, 2.2.10]). *The 1-norm of a Graver basis element $\mathcal{G}r(\mathcal{A})$ is bounded by the 1-norm of a true circuit.*

In order to prove our main result that the Graver complexity of a homogeneous codim 2 matrix can be bounded in terms of a linear relation on the entries of $\mathcal{A}$:

Theorem 1.6. *Let $\mathcal{A}$ be the homogeneous 2×4 matrix of the form $\mathcal{A} = \{(1,i_1),(1,i_2),(1,i_3),(1,i_4)\}$ such that $0 \le i_1 < i_2 < i_3 < i_4$. Then assuming the true circuit conjecture the Graver complexity $g(\mathcal{A})$ is bounded above by the maximal 1-norm of the true circuits of $\mathcal{A}$ by $\max\{i_2+i_3+i_4-3i_1, 3i_4-i_1-i_2-i_3\}$. If, in addition, the set of integers $\{i_2-i_1, i_3-i_1, i_4-i_1, i_3-i_2, i_4-i_2, i_4-i_3\}$ is pairwise co-prime, then the bound is tight.*

To clarify the notion of pairwise co-prime consider the matrix $\mathcal{A} = \{(1,0),(1,a),(1,b),(1,c)\}$. We require that a, b, c are pairwise co-prime in addition to their differences being pairwise co-prime. For example, consider the matrix associated to the twisted cubic curve $\mathcal{A} = \{(1,0),(1,1),(1,2),(1,3)\}$. Each difference is pairwise co-prime and hence the Graver complexity bound is tight. However, for the matrix $\mathcal{A} = \{(1,0),(1,1),(1,2),(1,6)\}$ the theorem gives the bound $g(\mathcal{A}) \leq 15$ whereas the Graver complexity is 10 with Graver representative $\psi = (0,4,-5,0,0,0,1)$ using $4ti2$.

2. Geometric structure for $\mathcal{A} = \{(1,0),(1,a),(1,b),(1,c)\}$

To determine the generating elements for the Graver basis of $\mathcal{A}$ we perform column operations on the Hermite normal form of $\mathcal{A}$ to obtain the column vector $\lambda = (1,-1,-1,1)$. Using the unimodular matrix and the vector λ to transform any vector v in the kernel of $\mathcal{A}$ into a vector with a zero third component, we obtain a unique minimal generator $h = (b,-(a+b),0,a)$ and thus

Lemma 2.1. *The kernel of the matrix $\mathcal{A} = \{(1,0),(1,a),(1,b),(1,a+b)\}$ with $0 < a < b$ is generated by $\lambda = (1,-1,-1,1)$ and $h = (b,-(a+b),0,a)$.*

Lemma 2.2. *The matrix $\mathcal{A} = \{(1,0),(1,a),(1,b),(1,a+b)\}$ with $0 < a < b$ has Graver basis $\mathcal{G}r(\mathcal{A}) = \pm\{h, h+\lambda, h+2\lambda, \dots, h+(a+b)\lambda, \lambda\}$, where $h = (b,-(a+b),0,a)$ and $\lambda = (-1,1,1,-1)$.*

Proof. The lattice associated to the kernel of $\mathcal{A}$ is generated by $h = (b,-(a+b),0,a)$ and $\lambda = (-1,1,1,-1)$. Notice that the set $\mathcal{G}r(\mathcal{A})$ in the hypothesis generates $\ker_{\mathbb{Z}}(\mathcal{A})$ because it contains λ, h. Using Algorithm 2.7.1 in Hemmecke [4] (or Pottier [13]), we must show this set is a minimal set of irreducible vectors. Notice that $h \sqsubseteq h - \lambda = (b+1,-(a+b+1),-1,a+1)$ and that $h+(a+b)\lambda = (-a,0,a+b,-b) \sqsubseteq (h-(a+b)\lambda)+\lambda = (a+2b-1,-2(a+b)+1,-(a+b)+1,2a+b-1)$. The difference of any two elements in the set $\mathcal{G}r(\mathcal{A})$ is some multiple of λ so there are no new elements obtained from taking differences of the sets. It remains to consider possible sums of elements in the generating set and determine whether or not these sums are irreducible. Consider the sum of any two elements in the set $\mathcal{G}r(\mathcal{A})$, say $h+p\lambda+h+q\lambda = 2h+(p+q)\lambda$. If we find an element $h+r\lambda \sqsubseteq 2h+(p+q)\lambda$ then $2h+(p+q)\lambda$ is reducible.

There is a structure to the set $\mathcal{G}r(\mathcal{A})$. The generators λ, h define a line of negative slope (see Figure 2). None of the elements on this line are divisible by the other elements and therefore they are minimal. If $2 \mid (p+q)$ then take $r = \frac{p+q}{2}$ and hence $h+r\lambda = 2h+(p+q)\lambda \sqsubseteq 2h+(p+q)\lambda$. If 2 does not divide $p+q$, take $r = \frac{p+q\pm 1}{2}$. Then $h+r\lambda = 2h+(p+q\pm 1)\lambda$ where $p+q\pm 1$ is even and we use the first case. Thus we have found an r dividing the sum of any two elements in $\mathcal{G}r(\mathcal{A})$ so that element is not minimal. $\square$

The next theorem gives an important geometric property of the Graver basis:

Theorem 2.3. *Given the matrix $\mathcal{A} = \{(1,0),(1,a),(1,b),(1,a+b)\}$ satisfying $0 < a < b$, the Graver complexity $g(\mathcal{A})$ is equal to the maximal 1-norm of a Graver basis element of* $B_c = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 0 \\ 0 & 1 & 2 & \cdots & c & 1 \end{pmatrix}$, *where $c = a+b$.*

Proof. By Lemma 2.2,

$$\mathcal{G}r(\mathcal{A}) = \{h, h+\lambda, h+2\lambda, \dots, h+(a+b)\lambda, \lambda\},$$

where $h = (b, -(a+b), 0, a)$ and $\lambda = (-1, 1, 1, -1)$.

Now let $c = (a+b)$ and let $(\alpha_0, \alpha_1, \dots, \alpha_c, \beta) \in \ker(\mathcal{G}r(\mathcal{A}))$ which is the case if and only if

$$\left(\sum_{i=0}^{c} \alpha_i\right) h + \left(\sum_{i=0}^{c} i\alpha_i + \beta\right) \lambda = 0. \tag{1}$$

Since h and λ are linearly independent, this implies that the coefficients in (1) must vanish. Therefore, the kernel of $\mathcal{G}r(\mathcal{A})$ is the same as the kernel of the matrix B_c implying $\mathcal{G}r(\mathcal{G}r(\mathcal{A})) = \mathcal{G}r(B_c)$, and the result follows. $\square$

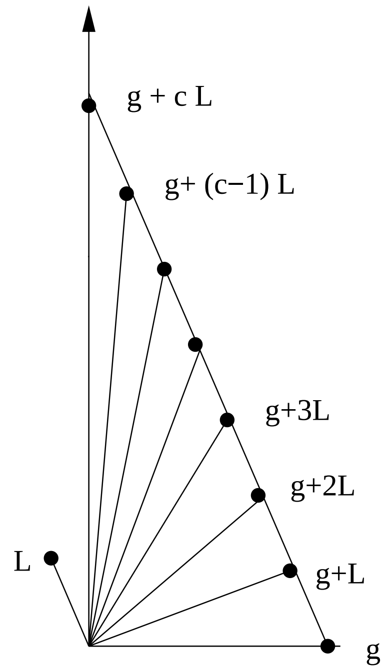

Figure 2. Graver basis of $\mathcal{A} = \{(1,0), (1,a), (1,b), (1,a+b)\}$

We make the following definition which will be useful in characterizing the Graver basis.

Definition 2.4. *The Graver basis for an integer $d \times n$ matrix $\mathcal{A}$ is covered by circuits if, in each orthant, the Hilbert basis of that orthant lies in the simplex spanned by the circuits defining that orthant.*

For example, the extremal rays have largest 1-norm in each cone in the Gale dual diagram in Figure 1 of the matrix $\{(1,0), (1,1), (1,3), (1,14)\}$. Matrices of the form $\{(1,0), (1,a), (1,b), (1,c)\}$ where $0 < a < b < c$ and the differences of

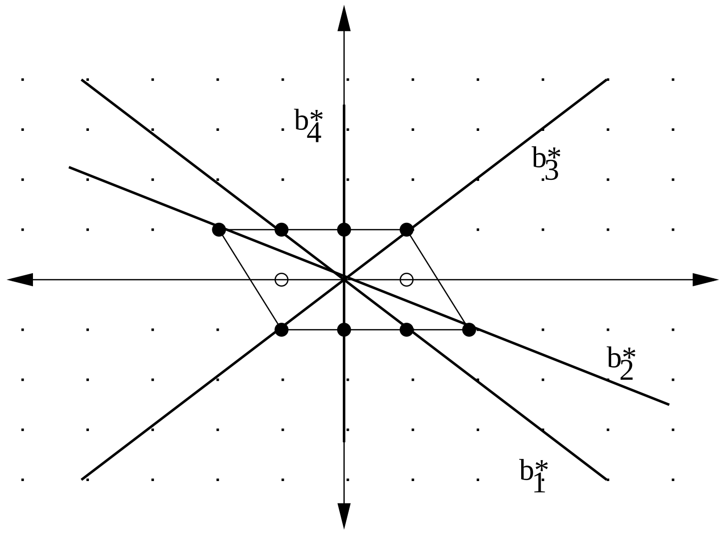

Figure 3. Gale dual diagram for $\{(1,0),(1,1),(1,2),(1,3)\}$

the numbers in the second row of $\mathcal{A}$ are pairwise co-prime have a unique form of Gale dual diagram; see Figure 3 for the Gale dual diagram of the matrix $\{(1,0),(1,1),(1,2),(1,3)\}$ representing the twisted cubic curve in $\mathbb{P}^3$.

By Lemma 1.3, the maximal 1-norm for elements in the Graver basis is $2(a+b)$ and is taken on by a circuit. Therefore

Theorem 2.5. *Given* $\mathcal{A} = \{(1,0),(1,a),(1,b),(1,c)\}$ *satisfying* $0 < a < b,\ c = a+b$ *and the differences of entries in the second row of* $\mathcal{A}$ *are pairwise co-prime, the Graver basis* $\mathcal{G}r(\mathcal{A})$ *of the matrix is covered by circuits.*

The following theorem describes a relationship between the maximum 1-norm of elements in the Graver basis and the area of the region bounded by the circuits in the Gale diagram:

Theorem 2.6. *Given the matrix* $\mathcal{A} = \{(1,0),(1,a),(1,b),(1,c)\}$ *satisfying* $0 < a < b,\ c = a+b$ *and the differences of entries in the second row of* $\mathcal{A}$ *are pairwise co-prime, the region bounded by the circuits in* $\mathbb{R}^2$ *has area* $2c$.

Proof. Construct ${G_{\mathcal{L}}}^*$. From Theorem 2.5, for each cone there is at least one of the vectors defining the extremal rays that has norm greater than or equal to any other element restricted to that cone. Denote by $\mathcal{P}$ the region formed from connecting the lattice points corresponding to the circuits of $\mathcal{G}r(\mathcal{A})$. Since these vectors of ${G_{\mathcal{L}}}^*$ define a central hyperplane arrangement, there is symmetry about the origin. Hence $\mathcal{P}$ is a parallelogram and it is defined by those vectors in ${G_{\mathcal{L}}}^*$ with the largest norms. We claim the area of the parallelogram is $2c$.

From above, the vector $\lambda = (1,-1,-1,1)$ lies in the kernel of $\mathcal{A}$ and we may take any other vector in $\mathcal{G}r(\mathcal{A})$ that is nonconformal to λ as the other vector defining ${G_{\mathcal{L}}}^*$. The Gale diagram is determined by two vectors of minimal length. Using the λ, g_0 previously determined, choose λ and the vector $v = (b,-c,0,a)+$

$2\lambda = (b-2, -c+2, 2, a-2)$ to define $G_{\mathcal{L}}$. From the set of vectors in ${G_{\mathcal{L}}}^*$, the two of largest norms are $\{\pm(-1, c-2), \pm(-1,-2)\}$ and these define the parallelogram determining the area $2 \cdot (c-2+2) = 2c$. $\square$

The Graver basis for arbitrary matrices $\mathcal{A} = \{(1,i_1),(1,i_2),(1,i_3),(1,i_4)\}$ with $0 \le i_1 < i_2 < i_3 < i_4$ is also covered by circuits but the Gale dual diagram does not have the same nice symmetry. Let $N := \mathbb{Z}^2$ and let $\sigma = \mathrm{cone}(c_1, c_2)$ be a strongly convex rational polyhedral cone in $N_{\mathbb{R}} := N \otimes_{\mathbb{Z}} \mathbb{R}$ with $\dim(\sigma) = 2$. We define a *corner* in σ as an interior Hilbert basis element h whose 1-norm satisfies $\| h\|_1 \le \min\{\|c_1\|_1, \|c_2\|_1\}$. Therefore

Theorem 2.7. *For matrices* $\mathcal{A} = \{(1,i_1),(1,i_2),(1,i_3),(1,i_4)\}$ *satisfying* $0 \le i_1 < i_2 < i_3 < i_4$ *the Graver basis* $\mathcal{G}r(\mathcal{A})$ *is covered by circuits.*

Proof. Let $\{b_1^*, \ldots, b_4^*\} \in {G_{\mathcal{L}}}^*$ be the row vectors defining the Gale dual diagram. Oda ([11, Proposition 1.19]) proved that every two consecutive vectors in ${G_{\mathcal{L}}}^*$ define $\mathrm{cone}(b_i^*, b_{i+1}^*)$ whose interior Hilbert basis elements h lie on the boundary polygon. Therefore $\|h\|_1 \le \max\{\|b_i^*\|_1,\ \|b_{i+1}^*\|_1\}$. Since this is true for every i, the result follows. $\square$

This proof fails for dimensions greater than 2.

Theorem 2.8. *The circuits of a* $2 \times (c+2)$, $c \ge 3$, *integer matrix* B_c *are not the true circuits for* B_c.

Proof. By Cramer's rule, the possible 2×2 minors of B_c define the true circuits $\mathcal{TC}(B_c)$. Thus there are three cases of circuits to consider.

Case 1: The true circuit is defined by any three consecutive nonzero coordinates

$$(0, \ldots, \begin{vmatrix} 1 & 1 \\ s & s+1 \end{vmatrix}, \begin{vmatrix} 1 & 1 \\ s-1 & s+1 \end{vmatrix}, \begin{vmatrix} 1 & 1 \\ s-1 & s \end{vmatrix}, 0, \ldots)$$

which is the vector $(0, \ldots, 1, 2, 1, 0, \ldots)$ and thus the g.c.d. of the coordinates is one.

Case 2: The true circuit is defined by any two consecutive nonzero coordinates and one separate $(0, \ldots, s, s+1, 0, \ldots, k, \ldots, 0)$

$$(0, \ldots, \begin{vmatrix} 1 & 1 \\ s+1 & k \end{vmatrix}, \begin{vmatrix} 1 & 1 \\ s & k \end{vmatrix}, 0, \ldots, \begin{vmatrix} 1 & 1 \\ s & s+1 \end{vmatrix}, \ldots, 0)$$

which is the vector $(0, \ldots, k-s-1, k-s, 0, \ldots, 1, \ldots, 0)$ and the g.c.d. of the components is one.

Case 3: All three nonzero coordinates are separate $(0, \ldots, s, \ldots, 0, t, 0, \ldots, k, 0, \ldots)$ where $s < t < k$.

$$(0, \ldots, \begin{vmatrix} 1 & 1 \\ t & k \end{vmatrix}, \ldots, 0, \begin{vmatrix} 1 & 1 \\ s & k \end{vmatrix}, 0, \ldots, \begin{vmatrix} 1 & 1 \\ s & t \end{vmatrix}, 0, \ldots)$$

which is the vector $(0,\ldots,k-t,\ldots,0,k-s,0,\ldots,t-s,0,\ldots)$. If the s,t,k are all even, then the g.c.d. of the components is not equal to one. However, when the s,t,k are all odd, the g.c.d. is equal to one or more. Thus having s,t,k all odd is not sufficient to have the g.c.d. of the coordinates equal to one. Therefore, the true circuits are not equal to the circuits. $\square$

For example, in B_{11}, $\begin{vmatrix} 1 & 1 \\ 11 & 9 \end{vmatrix} = 2$, $\begin{vmatrix} 1 & 1 \\ 11 & 3 \end{vmatrix} = 8$, $\begin{vmatrix} 1 & 1 \\ 9 & 3 \end{vmatrix} = 6$. The g.c.d. is 2.

Remark 2.9. For a matrix $\mathcal{A} \subseteq \mathbb{Z}^{2\times n}$, there are $n-2$ generating vectors for the lattice $\mathcal{L}(\mathcal{A})$ and $\binom{n}{n-3}$ true circuits in $\mathcal{G}r(\mathcal{A})$. For example, B_c has $\binom{c+2}{c-1} = \frac{1}{6}(c^3+3c^2+2c)$ true circuits.

For the special case of the codim 2 matrix $B_2 = \{(1,0),(1,1),(1,2),(1,1)\}$ its Graver basis is given by two circuits $\{(0,1,-1,1),(-1,1,0,-1)\}$ that generate a lattice. Thus the Gale dual diagram associated to this lattice is given by the four vectors $\{(1,0),(-1,1),(0,-1),(1,1)\}$ which define unimodular cones. Therefore, every element in $\mathcal{G}r(B_2)$ is a circuit and thus the Graver basis is covered by circuits.

Consider B_3 and look at the orthant defined by the following Graver basis elements $\mathcal{G}r(B_3)$:

$$(1,-2,1,0,0),\ (1,-2,0,1,-1),\ (0,-1,1,0,-1),\ (0,-1,0,1,-1).$$

Write the non-circuit as a linear combination of the three circuits:

$$h = (1,-2,0,1,-1) = 1(1,-2,0,1,-1) + 1(0,1,-1,0,1) + 1(0,-1,0,1,-1)$$

where the height of h is $\text{height}(h) = 3 > 1$. Thus the element h lies outside the simplex defined by the circuits and therefore $\mathcal{G}r(B_3)$ is not covered by circuits. In general, many examples can be found where interior Hilbert basis vectors are not covered by the circuits. Thus we have

Proposition 2.10. *The Graver basis of B_c, $c \geq 3$ is not covered by circuits.*

3. Proof of the main theorem

Since the Graver of the Graver basis of the matrix $\mathcal{A} = \{(1,0),(1,a),(1,b),(1,c)\}$ where $0<a<b$ and $c=a+b$ has kernel isomorphic to the kernel of B_c, we have

Corollary 3.1. *The Graver basis of the Graver basis of $\mathcal{A} = \{(1,0),(1,a),(1,b),(1,c)\}$ where $0<a<b$ and $c=a+b$ is not covered by circuits.*

Therefore, it is necessary to assume the true circuit conjecture in order to prove Theorem 1.6 on the Graver complexity of the codim 2 matrix $\mathcal{A}$. Denote by $\mathcal{C}(\mathcal{C}(\mathcal{A}))$ the vectors in $\mathcal{G}r(\mathcal{G}r(\mathcal{A}))$ that are integer combinations of circuits in $\mathcal{G}r(\mathcal{A})$.

Proposition 3.2. *Let* $\mathcal{A} = \{(1,i_1),(1,i_2),(1,i_3),(1,i_4)\}$*, with* $0 \le i_1 < i_2 < i_3 < i_4$*. Then* $\mathcal{C}(\mathcal{C}(\mathcal{A})) \subseteq \mathcal{C}(\mathcal{G}r(\mathcal{A})^T)$*.*

Remark 3.3. The reverse inclusion is not true. Unfortunately, not every element in $\mathcal{C}(\mathcal{G}r(\mathcal{A})^T)$ arises in this way. The matrix $\{(1,0),(1,2),(1,5),(1,8)\}$ has Graver representatives $(5,-4,0,0,0,0,-1)$, $(0,-3,0,5,0,0,-2)$, $(0,-2,0,0,5,0,-3)$, $(0,-1,0,0,0,5,-4)$ where only $(5,-4,0,0,0,0,-1) \in \mathcal{C}(\mathcal{C}(\mathcal{A}))$.

By Corollary 1.4, the second row entries of $\mathcal{A} = \{(1,0),(1,a),(1,b),(1,c)\}$ were relatively prime and so were their respective differences. Thus, for general matrices $\mathcal{A} = \{(1,0),(1,i_2),(1,i_3),(1,i_4)\}$, with $0 < i_2 < i_3 < i_4$ we expect the property of relatively prime differences to be necessary to obtain a tight bound.

We now prove Theorem 1.6:

Proof. These bounds equivalently hold using $\mathcal{A} = \{(1,0),(1,i_2),(1,i_3),(1,i_4)\}$ such that $0 < i_2 < i_3 < i_4$. The Graver basis $\mathcal{G}r(\mathcal{A})$ is covered by circuits; thus the Graver representative in $\mathcal{G}r(\mathcal{G}r(\mathcal{A}))$ will correspond to an element in $\mathcal{C}(\mathcal{C}(\mathcal{A}))$ by Proposition 3.2. Moreover, since $\mathcal{G}r(\mathcal{G}r(\mathcal{A}))$ is not covered by circuits, we assume the True Circuit Conjecture so that the elements in the Graver basis of the Graver basis are covered by the true circuits of the Graver basis of $\mathcal{A}$. But the Graver basis of $\mathcal{A}$ is covered by circuits; hence $\mathcal{G}r(\mathcal{G}r(\mathcal{A}))$ is covered by the true circuits of the circuits of $\mathcal{A}$. Possible combinations of the numbers in $\mathcal{D}(\mathcal{A}) = \max\{i_1, i_2, i_3, i_4, i_2-i_1, i_3-i_1, i_4-i_1, i_3-i_2, i_4-i_2, i_4-i_3\}$ give the upper bound defined by the maxcircuit$(\mathcal{G}r(\mathcal{A}))$. Thus maxcircuit$(\mathcal{G}r(\mathcal{A})) = \max\{i_1+i_2+i_3+i_4 = i_2-i_1+i_3-i_1+i_4-i_1 = i_2+i_3+i_4-3i_1,\ i_4-i_1+i_4-i_2+i_4-i_3 = 3i_4-i_1-i_2-i_3\}$. Therefore, these give an upper bound for the Graver complexity of $\mathcal{A}$ in terms of the true circuits for $\mathcal{A}$. If all the differences are pairwise co-prime, then $i_2+i_3+i_4-3i_1 = 3i_4-i_1-i_2-i_3$ and the bound is tight. □

For example, consider the matrix $\mathcal{A} = \{(1,0),(1,3),(1,7),(1,8)\}$ which has Graver representative $g = (0,0,8,0,-7,0,0,3)$ with Graver complexity $g(\mathcal{A}) = 18$.

Remark 3.4. The matrix $\{(1,0),(1,1),(1,2),(1,3)\}$ that represents the twisted cubic curve in $\mathbb{P}^3$ has entries whose differences are relatively prime. The Graver representative is $(3,-2,0,0,1)$ which implies that the Graver complexity is $g = 6$ so the bound is tight. However, it is not necessary for the differences of the entries to be co-prime in order to obtain a tight bound. For example, consider $\mathcal{A} = \{(1,0),(1,1),(1,7),(1,9)\}$ where the pairwise differences are not co-prime. The Graver representative is $g = (9,-7,0,0,0,0,0,1)$ and thus the Graver complexity is $g(\mathcal{A}) = 17$ which is a tight bound.

References

[1] Bruns, W.; Herzog, J.: *Cohen-Macaulay rings*. Cambridge Studies in Advanced Mathematics **39**, Cambridge University Press, Cambridge 1993. Zbl 0909.13005

[2] Popescu, S.; Bayer, D.; Sturmfels, B.: *Syzygies of unimodular lawrence ideals*. J. Reine Angew. Math. **534** (2001),169–186. Zbl 1011.13006

[3] Diaconis, P.; Sturmfels, B.: *Algebraic algorithms for sampling from conditional distributions*. Ann. Stat. **26**(1) (1998), 363–397. Zbl 0952.62088

[4] Hemmecke, R.: *On the positive sum property and the computation of Graver test sets*. Mathematical Programming **96** (2003), 247–269.

[5] 4ti2 team: *4ti2 – A software package for algebraic, geometric and combinatorial problems on linear spaces*. Available at www.4ti2.de.

[6] Hemmecke, R.; Nairn, K.: *On the Gröbner Complexity of Matrices*. Journal of Pure and Applied Algebra, (to appear).

[7] Henk, M.; Weismantel, R.: *On Hilbert bases of polyhedral comes*. Result. Math. **32** (1997), 298–303. cf. *The height of minimal bases*. ibidem Zbl 0964.52015

[8] Hosten, S.: *Degrees of Gröbner bases of integer programs*. Thesis, e-print 1997. http://fener.sfsu.edu/∼serkan.

[9] L′vovsky, S.: *On inflection points, monomial curves, and hypersurfaces containing projective curves*. Math. Ann. **306**(4) (1996), 719–735. Zbl 0857.14031

[10] Nairn, K.: *Graver Complexity of Monomial Curves in* $\mathbb{P}^3$. Ph.D. Thesis, Columbia University, 2003.

[11] Oda, T.: *Convex bodies and algebraic geometry*. Ergebnisse der Mathematik und ihrer Grenzgebiete 3. Folge **15**. Springer-Verlag, Berlin 1988. Zbl 0628.52002

[12] Peeva, I.; Sturmfels, B.: *Syzygies of codimension* 2 *lattice ideals*. Math. Z. **229**(1) (1998), 163–194. Zbl 0918.13006

[13] Pottier, L.: *The Euclidean algorithm in dimension* n. In: Y. N. Lakshman (ed.), Proceedings of the 1996 international symposium on symbolic and algebraic computation, ISSAC ’96. New York, NY: ACM Press. 40–42 (1996) Zbl 0919.11088

[14] Santos, F.; Sturmfels, B.: *Higher Lawrence configurations*. J. Comb. Theory, Ser. A **103**(1) (2003), 151–164. Zbl 1036.52018

[15] Schrijver, A.: *Theory of linear and integer programming*. John Wiley & Sons Ltd., Chichester 1986. Zbl 0665.90063

[16] Sturmfels, B.: *Algorithms in invariant theory*. Springer-Verlag, NY 1993. Zbl 0802.13002

[17] Sturmfels, B.: *Gröbner bases and convex polytopes*. American Mathematical Society, Providence, RI, 1996. Zbl 0856.13020

Received June 2, 2008