Bulletin of the Iranian Mathematical Society Vol. 39 *No.* 5 (*2013*), *pp 893-901.*

A DEGREE BOUND FOR THE GRAVER BASIS OF NON-SATURATED LATTICES

H. SABZROU

Communicated by Ali Reza Ashrafi

Abstract. Let L be a lattice in $\mathbb{Z}^n$ of dimension m. We prove that the total degree of any Graver element of L is not greater than $m(n-m+1)MD$, where the integer M is defined by the set of circuits of L, and the integer D is defined by the saturation of L. The case $M = 1$ occurs precisely when L is saturated, and in this case the bound is a reformulation of a well-known bound given by several authors. As a corollary, we show that the Castelnuovo-Mumford regularity of the corresponding lattice ideal I_L is not greater than $\frac{1}{2}m(n-1)(n-m+1)MD$.

1. Introduction

Let $\mathbb{k}$ be a field, $R = \mathbb{k}[\mathbf{x}] := \mathbb{k}[x_1, \ldots, x_n]$ the polynomial ring in n indeterminates, and L a lattice, i.e. a $\mathbb{Z}$-module, in $\mathbb{Z}^n$. Each monomial $\mathbf{x}^{\mathbf{u}} := x_1^{u_1} \cdots x_n^{u_n}$ in R can be identified with vector $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{N}^n$ where $\mathbb{N}$ stands for the set of non-negative integers. For each vector $\mathbf{u} := (u_1, \ldots, u_n) \in \mathbb{Z}^n$, the set $\operatorname{supp}(\mathbf{u}) := \{i \mid u_i \neq 0\}$ is called the support of $\mathbf{u}$. Every vector $\mathbf{u} \in \mathbb{Z}^n$ can be written uniquely as $\mathbf{u} = \mathbf{u}^+ - \mathbf{u}^-$ where $\mathbf{u}^+$ and $\mathbf{u}^-$ are nonnegative and have disjoint supports. For the lattice L, the binomial ideal $I_L := \langle \mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} \mid \mathbf{u} \in L \rangle$ is the corresponding lattice ideal in R.

MSC(2010): Primary: 13P10; Secondary: 14M25, 90C10.
Keywords: Non-saturated lattices, Graver bases.
Received: 13 October 2011, Accepted: 15 August 2012.

An element $\mathbf{u} \in L$ is called primitive if there exists no other element $\mathbf{v} \in L \setminus \{0, \mathbf{u}\}$ such that $\mathbf{v}^+ \leq \mathbf{u}^+$, and $\mathbf{v}^- \leq \mathbf{u}^-$ where $\leq$ is the usual coordinatewise order on $\mathbb{Z}^n$. The set of all primitive elements of L is called the Graver basis of L and is denoted by Gr_L. Since the elements $\mathbf{u} \in L$ correspond to the pure binomials $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} \in I_L$, we can rephrase this definition in terms of pure binomials as follows. A binomial $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} \in I_L$ is called primitive if there exists no other binomial $\mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-} \in I_L$ such that $\mathbf{x}^{\mathbf{v}^+}$ divides $\mathbf{x}^{\mathbf{u}^+}$ and $\mathbf{x}^{\mathbf{v}^-}$ divides $\mathbf{x}^{\mathbf{u}^-}$. The set of all primitive binomials in I_L is again called the Graver basis of I_L and is denoted by Gr_L.

Graver bases first appeared as a universal test set for integer programming problems [5]. Since then, they have been utilized for counting lattice points of polyhedra, finding the Hilbert basis of a given cone, they are related to the transportation problem and the knapsack problem [8]. They also contain other important finite bases in L: lattice basis $\subseteq$ Markov basis $\subseteq$ Gröbner basis $\subseteq$ universal Gröbner basis $\subseteq$ Graver basis, where the definitions of the undefined concepts can be found in [4, Section 1.3].

When L is saturated, there is a well-known bound on the total degree of the Graver elements in I_L. This bound was obtained by many different people from very diverse areas [2, 3, 7, 9]. In this paper we generalize the version given in [9, Theorem 4.7] to the non-saturated lattices. In fact, for a lattice L in $\mathbb{Z}^n$ of dimension m, we prove that the total degree of any Graver element of L is not greater than $m(n-m+1)MD$, where M and D are integer constants defined by the set of circuits of L, and by a defining matrix of the lattice $\widetilde{L}$, the saturation of L, respectively (cf. Theorem 2.10). As shown in Theorem 2.8 (cf. Remark 2.9), the integers D and M are basis-independent in the sense that choosing a different basis for $\widetilde{L}$ (resp. L) will result in the same D (resp. M). As a corollary, we will show that the Castelnuovo-Mumford regularity of the ideal I_L is not greater than $\frac{1}{2}m(n-1)(n-m+1)MD$ (cf. Corollary 2.11).

1.1. **Notation and Conventions.** Let m and n be two positive integers. We denote by I_n the identity matrix of size n. For an integer $n \times m$ matrix B, we denote by $C(B)$ and $D(B)$, the greatest common divisor and the maximum of the absolute values of all maximal minors of B, respectively. The integer $C(B)$ is called the content of the matrix B. If B is over a field, and $1 \leq i_1 < \cdots < i_s \leq n$ and $1 \leq j_1 < \cdots < j_t \leq m$

are arbitrary integer sequences, we denote by $B[{}_{i_1,\dots,i_s}|{}_{j_1,\dots,j_t}]$ the submatrix of B whose rows and columns correspond to $i_1,\dots,i_s$ and $j_1,\dots,j_t$, respectively. The submatrix of B obtained by deleting the rows and columns corresponding to $i_1,\dots,i_s$ and $j_1,\dots,j_t$, respectively, will be denoted by $B({}_{i_1,\dots,i_s}|{}_{j_1,\dots,j_t})$.

2. The main result

Let L be a lattice in $\mathbb{Z}^n$ of dimension m. An integer $n \times m$ matrix B of rank m whose columns generate L as a lattice, is called a defining matrix for L. Such a matrix is of course not unique, but one can see that it is unique up to the action of the general linear group $\mathrm{GL}_m(\mathbb{Z})$. For the lattice L, the lattice $\widetilde{L} := (L \otimes_{\mathbb{Z}} \mathbb{Q}) \cap \mathbb{Z}^n$ is called the saturation of L. In fact, $\widetilde{L}$ is the set of all $\mathbf{u} \in \mathbb{Z}^n$ for which $r\mathbf{u} \in L$ for some positive integer r. In general, we have $\widetilde{L} \supseteq L$, and if the equality occurs, we say that L is saturated.

Proposition 2.1. *Let L be a lattice in $\mathbb{Z}^n$ of dimension m, and B a defining matrix of L. The following conditions are equivalent.*

(1) *L is saurated.*
(2) *The abelian group $\mathbb{Z}^n/L$ is torsion free.*
(3) *There exists an integer $(n-m) \times n$ matrix A such that $L = \ker_{\mathbb{Z}}(A)$.*
(4) *$C(B)$, the content of B, equals 1.*

Proof. (1) $\Leftrightarrow$ (2), (3) $\Rightarrow$ (1): Trivial.

(1) $\Rightarrow$ (3): Since $\mathbb{Z}$ is a PID, and $\mathbb{Z}^n$ is a free $\mathbb{Z}$-module, there exist a basis $\{\mathbf{u}_1,\dots,\mathbf{u}_n\}$ for $\mathbb{Z}^n$, and integers $c_1,\dots,c_m$ such that $\{c_1\mathbf{u}_1,\dots,c_m\mathbf{u}_m\}$ is a basis for L. Since L is saturated, $c_i\mathbf{u}_i \in L$ implies that $\mathbf{u}_i \in L$ for $i = 1,\dots,m$. It follows that $\{\mathbf{u}_{m+1}+L,\dots,\mathbf{u}_n+L\}$ is a basis for $\mathbb{Z}^n/L$, and so $\mathbb{Z}^n/L \simeq \mathbb{Z}^{n-m}$, as required.

(1) $\Leftrightarrow$ (4): [8, Corollary 4.1c]. □

Definition 2.2. *Let L be a lattice in $\mathbb{Z}^n$. A non-zero element $\mathbf{u} \in L$ is said to be a circuit if the support of $\mathbf{u}$ is minimal with respect to inclusion and $\frac{1}{d}\mathbf{u} \notin L$ for any positive integer $d \neq 1$.*

Remark 2.3. *Definition 2.2 agrees with the original definition of a circuit where the lattice L is assumed to be saturated. Indeed, if L is saturated, then a non-zero element $\mathbf{u} \in L$ is circuit if* $\mathrm{supp}(\mathbf{u})$ *is minimal, and the coordinates of $\mathbf{u}$ are relatively prime.*

Proposition 2.4. *There is a one to one correspondence between the circuits of L and those of $\widetilde{L}$.*

Proof. Let $\mathbf{v}$ be a circuit of L. Since $L \subseteq \widetilde{L}$, and $\widetilde{L}$ is saturated, then $\frac{1}{\gcd(\mathbf{v})}\mathbf{v} \in \widetilde{L}$. On the contrary suppose that $\frac{1}{\gcd(\mathbf{v})}\mathbf{v}$ is not a circuit in $\widetilde{L}$, then there exists $\mathbf{v}' \in \widetilde{L}$ such that $\operatorname{supp}(\mathbf{v}') \subsetneqq \operatorname{supp}(\frac{1}{\gcd(\mathbf{v})}\mathbf{v})$. Since $\mathbf{v}' \in \widetilde{L}$, there exits a positive integer m such that $m\mathbf{v}' \in L$ and $\operatorname{supp}(m\mathbf{v}') = \operatorname{supp}(\mathbf{v}') \subsetneqq \operatorname{supp}(\frac{1}{\gcd(\mathbf{v})}\mathbf{v}) = \operatorname{supp}(\mathbf{v})$. This contradicts the assumption that $\mathbf{v}$ is a circuit in L.

Conversely, if $\mathbf{v} \in \widetilde{L}$ is circuit, and m is the smallest positive integer such that $m\mathbf{v} \in L$, then $m\mathbf{v}$ is circuit in L because otherwise there exists $\mathbf{v}' \in L \subseteq \widetilde{L}$ such that $\operatorname{supp}(\mathbf{v}') \subsetneqq \operatorname{supp}(m\mathbf{v}) = \operatorname{supp}(\mathbf{v})$ which is impossible. □

Remark 2.5. *Let L be a lattice in $\mathbb{Z}^n$. By Proposition 2.4, and* [9, Lemma 4.9]*, the set of all circuits of L is finite. One of the main reasons that the finite set of circuits is useful, is Proposition 2.6 below, which shows that this set is a special generating set of L. Here we need to recall that a vector $\mathbf{u} \in L$ is* conformal *to a vector $\mathbf{v} \in L$ if* $\operatorname{supp}(\mathbf{u}^+) \subseteq \operatorname{supp}(\mathbf{v}^+)$ *and* $\operatorname{supp}(\mathbf{u}^-) \subseteq \operatorname{supp}(\mathbf{v}^-)$.

Proposition 2.6. *Let L be a lattice in $\mathbb{Z}^n$ of dimension m. Then for every vector $\mathbf{v} \in L$, there exist non-negative rational coefficients $\lambda_1, \ldots, \lambda_m$, and circuits $\mathbf{v}_1, \ldots, \mathbf{v}_m$ in L such that $\mathbf{v} = \lambda_1\mathbf{v}_1 + \cdots + \lambda_m\mathbf{v}_m$, and each $\mathbf{v}_i$ is conformal to $\mathbf{v}$. If in addition $\mathbf{v}$ is primitive, then $\lambda_i \leq 1$ for each i.*

Proof. Since $\mathbf{v} \in L \subseteq \widetilde{L}$, it follows from [9, Lemma 4.10] that there exist non-negative rational coefficients $\lambda'_1, \ldots, \lambda'_m$ and circuits $\mathbf{v}'_1, \ldots, \mathbf{v}'_m \in \widetilde{L}$ such that $\mathbf{v} = \lambda'_1\mathbf{v}'_1 + \cdots + \lambda'_m\mathbf{v}'_m$ and each $\mathbf{v}'_i$ is conformal to $\mathbf{v}$. Let $\mathbf{v}_i := m_i\mathbf{v}'_i$ where m_i is the smallest positive integer such that $m_i\mathbf{v}'_i \in L$, and $\lambda_i := \lambda'_i/m_i$. Then by Proposition 2.4, $\mathbf{v}_i$ is a circuit of L, and we have $\mathbf{v} = \lambda_1\mathbf{v}_1 + \cdots + \lambda_m\mathbf{v}_m$ as requested. The fact that each $\mathbf{v}_i$ is conformal to $\mathbf{v}$ implies that $\mathbf{v}^+ = \lambda_1\mathbf{v}_1^+ + \cdots + \lambda_m\mathbf{v}_m^+$, and $\mathbf{v}^- = \lambda_1\mathbf{v}_1^- + \cdots + \lambda_m\mathbf{v}_m^-$. Suppose the contrary that $\lambda_i > 1$ for some i. Then $\lambda_i = k + \lambda'_i$ where $k \geq 1$ is an integer and $0 \leq \lambda'_i \leq 1$. Therefore $\mathbf{v}^+ - k\mathbf{v}_i^+$ and $\mathbf{v}^- - k\mathbf{v}_i^-$ are non-negative vectors. Hence $\mathbf{v}_i^+ \leq \mathbf{v}^+$ and $\mathbf{v}_i^- \leq \mathbf{v}^-$, contradicting the fact that $\mathbf{v}$ is primitive. □

The next elementary lemma is a folklore result in linear algebra. We present a proof for it for the convenience of the reader.

Lemma 2.7. *Let M be a $n \times n$ matrix over a field partitioned as*

$$M = \left[\begin{array}{c|c} I_d & C \\ \hline -C^T & I_{n-d} \end{array}\right]$$

where C is a $d \times (n-d)$ matrix, and C^T is the transpose of C. Then

$$\det M({\scriptstyle 1,\dots,d|j_1,\dots,j_d}) = (-1)^{1+\cdots+d+j_1+\cdots+j_d} \det M[{\scriptstyle 1,\dots,d|j_1,\dots,j_d}].$$

Proof. We consider the submatrix $N := M[{\scriptstyle 1,\dots,d|j_1,\dots,j_d}]$ of M, and assume that $1 \le j_1 < \cdots < j_\ell \le d < j_{\ell+1} < \cdots < j_d \le n$. Let $\{j'_1, \dots, j'_\ell\}$ be a subset of $\{j_1, \dots, j_d\}$ such that $j'_1 < \cdots < j'_\ell$. If $(j_1, \dots, j_\ell) \neq (j'_1, \dots, j'_\ell)$, then one of the columns of the matrix $N({\scriptstyle j_1,\dots,j_\ell|j'_1,\dots,j'_\ell})$ is a part of a column of N indexed by one of $j_1 \dots, j_\ell$, and is zero. Hence, in this case, we have $\det N({\scriptstyle j_1,\dots,j_\ell|j'_1,\dots,j'_\ell}) = 0$. On the other hand, if $(j_1, \dots, j_\ell) = (j'_1, \dots, j'_\ell)$, then $\det N[{\scriptstyle j_1,\dots,j_\ell|j'_1,\dots,j'_\ell}] = \det I_\ell = 1$, and $N({\scriptstyle j_1,\dots,j_\ell|j'_1,\dots,j'_\ell}) = M[\sigma_1|\sigma_2]$ where $\sigma_1 := \{1, \dots, d\} \setminus \{j_1, \dots, j_\ell\}$ and $\sigma_2 := \{j_{\ell+1}, \dots, j_d\}$. Thus using the Laplace expansion for the matrix N with respect to the rows indexed by $j_1, \dots, j_\ell$, we have

$$\det M[{\scriptstyle 1,\dots,d|j_1,\dots,j_d}] = \det N = (-1)^{1+\cdots+\ell+j_1+\cdots+j_\ell} \det M[\sigma_1|\sigma_2].$$

Now let $N' := M({\scriptstyle 1,\dots,d|j_1,\dots,j_d})$, and $\{j'_1, \dots, j'_{d-\ell}\}$ be a subset of $\{1, \dots, n\}$ such that $j'_1 < \cdots < j'_{d-\ell}$ and $j'_i \notin \{j_1, \dots, j_d\}$. If the columns of N' indexed by $j'_1, \dots, j'_{d-\ell}$ are not the first $d - \ell$ columns of N', then the matrix $N'[{\scriptstyle j_{\ell+1}-d,\dots,j_d-d|j'_1,\dots,j'_{d-\ell}}]$ has at least one zero column which implies $\det N'[{\scriptstyle j_{\ell+1}-d,\dots,j_d-d|j'_1,\dots,j'_{d-\ell}}] = 0$. On the other hand, if the columns of N' indexed by $j'_1, \dots, j'_{d-\ell}$ are the first $d - \ell$ columns of N', then we have $\det N'({\scriptstyle j_{\ell+1}-d,\dots,j_d-d|j'_1,\dots,j'_{d-\ell}}) = 1$ and

$$\det N'[{\scriptstyle j_{\ell+1}-d,\dots,j_d-d|j'_1,\dots,j'_{d-\ell}}] = \det N'[{\scriptstyle j_{\ell+1}-d,\dots,j_d-d|1,\dots,d-\ell}].$$

Thus the Laplace expansion for the matrix N' with respect to the rows $j_{\ell+1}-d, \dots, j_d-d$ implies $\det N' = (-1)^{(j_{\ell+1}-d)+\cdots+(j_d-d)+1\cdots+(d-\ell)} \det P$ where $P = -C^T[{\scriptstyle j_{\ell+1}-d,\dots,j_d-d|\{1,\dots,d\}\setminus\{j_1,\dots,j_\ell\}}] = -M[\sigma_1|\sigma_2]^T$. Therefore we have

$$\begin{aligned}
\det N' &= (-1)^{(j_{\ell+1}-d)+\cdots+(j_d-d)+1\cdots+(d-\ell)}(-1)^{d-\ell} \det M[\sigma_1|\sigma_2] \\
&= (-1)^{j_{\ell+1}+\cdots+j_d+d(d-\ell)+1+\cdots+(d-\ell)+(d-\ell)} \det M[\sigma_1|\sigma_2] \\
&= (-1)^{(j_1+\cdots+j_d)+(1+\cdots+d)+(j_1+\cdots+j_\ell)+(1+\cdots+\ell)} \det M[\sigma_1|\sigma_2] \\
&= (-1)^{j_1+\cdots+j_d+1+\cdots+d} \det N
\end{aligned}$$

where the second equality holds because $(-1)^{-d(d-\ell)} = (-1)^{d(d-\ell)}$, and the third equality holds because the sum of the exponents of (-1) on both sides of the equality is even. $\square$

Theorem 2.8. *Let m, n be two integers with $0 < m < n$, B an integer $n \times m$ matrix with $\operatorname{rank}(B) = m$, and A an integer $d \times n$ matrix with $d := \operatorname{rank}(A) = n - m$ such that the sequence $0 \longrightarrow \mathbb{Z}^m \xrightarrow{B} \mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^d$ of abelian groups is exact. Let $\sigma := \{j_1, \ldots, j_d\}$ be a subset of $\{1, \ldots, n\}$ with $j_1 < \cdots < j_d$, and $\bar{\sigma}$ be its complement. Then*

$$\det A[{\scriptstyle 1,\ldots,d}|\sigma] = (-1)^{1+\cdots+d+j_1+\cdots+j_d} C(A) \det B[\bar{\sigma}|{\scriptstyle 1,\ldots,m}].$$

Consequently, $D(A) = C(A)D(B)$, and if B' is another matrix with the same property as B, then $C(B) = C(B')$ and $D(B) = D(B')$.

Proof. We consider the $n \times n$ partitioned matrix

$$M = \left[\frac{A}{B^T}\right]$$

over the field of rational numbers. Since the matrix B^T is full row rank, there exists an integer sequence $1 \le i_1 < \cdots < i_d \le n$ such that $\det M({\scriptstyle 1,\ldots,d}|{\scriptstyle i_1,\ldots,i_d}) \neq 0$. Without loss of generality, we assume that $(i_1, \ldots, i_d) = (1, \ldots, d)$. Let $\alpha := \det M({\scriptstyle 1,\ldots,d}|{\scriptstyle 1,\ldots,d})$, and $\beta := \det M[{\scriptstyle 1,\ldots,d}|{\scriptstyle 1,\ldots,d}]$. For any sequence $1 \le j_1 < \cdots < j_d \le n$, we claim that

$$\det M[{\scriptstyle 1,\ldots,d}|{\scriptstyle j_1,\ldots,j_d}] = (-1)^{1+\cdots+d+j_1+\cdots+j_d} \frac{\beta}{\alpha} \det M({\scriptstyle 1,\ldots,d}|{\scriptstyle j_1,\ldots,j_d}).$$

To prove the claim, we note that the equality remains unchanged when we apply the elementary row operations to the first d rows or the second $n - d$ rows. Note that, for example, permuting two of the first d rows changes the sign of β as well as $\det M[{\scriptstyle 1,\ldots,d}|{\scriptstyle j_1,\ldots,j_d}]$. Hence using the hypotheses on the matrices A and B, we may assume that

$$M = \left[\begin{array}{c|c} I_d & C \\ \hline -C^T & I_{n-d} \end{array}\right].$$

Therefore the claim follows from Lemma 2.7. Now let $\gamma := \gcd(\alpha, \beta)$. By the claim α/γ divides $\det M({\scriptstyle 1,\ldots,d}|{\scriptstyle j_1,\ldots,j_d})$ for all sequences $1 \le j_1 < \cdots < j_d \le n$. Since the lattice $L = \ker_{\mathbb{Z}}(A) = \operatorname{Im}_{\mathbb{Z}}(B)$ is saturated, it follows from Proposition 2.1 that $\alpha/\gamma = 1$ which implies that $\beta = \alpha\beta'$ for some integer β'. Therefore

$$\det M[{\scriptstyle 1,\ldots,d}|{\scriptstyle j_1,\ldots,j_d}] = (-1)^{1+\cdots+d+j_1+\cdots+j_d} \beta' \det M({\scriptstyle 1,\ldots,d}|{\scriptstyle j_1,\ldots,j_d}).$$

Since $\gcd(M(_{1,\dots,d}|_{j_1,\dots,j_d}) \mid {}_{1\le j_1<\cdots<j_d\le n}) = 1$, we conclude $\beta' = C(A)$. □

Remark 2.9. *Let L be a lattice in $\mathbb{Z}^n$ of dimension m, and B a defining matrix of $\widetilde{L}$. Then by Theorem 2.8, the integer $D(B)$ does not depend on B and hence we can set $D(\widetilde{L}) := D(B)$. Furthermore, if L is saturated, we may assume that $L = \ker_{\mathbb{Z}}(A)$ for some integer $(n-m)\times n$ matrix A, by Proposition 2.1. We may also assume that $C(A) = 1$, by* [6, Propositions 1.1 and 1.2]. *Hence, in this case, $D(L) = D(A)$, by Theorem 2.8.*

Theorem 2.10. *Let L be a lattice in $\mathbb{Z}^n$ of dimension m, M the maximum of the values* $\gcd(\mathbf{v})$ *where* $\mathbf{v}$ *runs over the set of circuits of L, and $D := D(\widetilde{L})$. Then the total degree of any Graver element of L is less than or equal to $m(n-m+1)MD$. Furthermore, $M = 1$ if and only if L is saturated.*

Proof. Let $\mathbf{v}$ be a circuit in L. Then by Proposition 2.4, $\mathbf{v} = \gcd(\mathbf{v})\mathbf{v}'$ where $\mathbf{v}'$ is a circuit of $\widetilde{L}$. Therefore, $\|\mathbf{v}\|_1 = \gcd(\mathbf{v})\|\mathbf{v}'\|_1$ where $\|\mathbf{v}\|_1$ is the sum of the absolute values of coordinates of $\mathbf{v}$. Then

$$\|\mathbf{v}\|_1 \le \gcd(\mathbf{v})(n-m+1)D \le M(n-m+1)D$$

where the first inequality holds by Remark 2.9, and [9, Lemma 4.8, 4.9]. Let $\mathbf{v} \in L$ be a Graver element, i.e. a primitive vector of L. By Theorem 2.6, there exist non-negative rational coefficients $\lambda_1,\dots,\lambda_m$, and circuits $\mathbf{v}_1,\dots,\mathbf{v}_m$ in L such that $\mathbf{v} = \lambda_1\mathbf{v}_1 + \cdots + \lambda_m\mathbf{v}_m$ and $\lambda_i \le 1$. Therefore

$$\|\mathbf{v}\|_1 \le \sum_{i=1}^{m} \lambda_i\|\mathbf{v}_i\|_1 \le \sum_{i=1}^{m} \|\mathbf{v}_i\|_1 \le m(n-m+1)MD.$$

Since the degree of $\mathbf{v}$ or equivalently the degree of $\mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-}$ is equal to $\max\{\|\mathbf{v}^+\|_1, \|\mathbf{v}^-\|_1\}$, the first part follows.

To prove the last part, we note that if $M = 1$, then by Proposition 2.4, the sets of circuits of L and $\widetilde{L}$ coincide. Hence by Proposition 2.6, we have $L = \widetilde{L}$, as required. The converse is also obvious. □

Let I be a homogeneous ideal in the polynomial ring $R = \Bbbk[x_1,\dots,x_n]$ graded with $\deg(x_i) = 1$ for $i = 1,\dots,n$. Then the ith Betti number of the ideal I in degree j is defined to be the vector space dimension $\dim_{\Bbbk} \operatorname{Tor}_i(\Bbbk, I)_j$ and is denoted by $\beta_{i,j}(I)$. The integer $\operatorname{reg}(I) := \max\{j-$

$i \mid \beta_{i,j}(I) \neq 0\}$ is called the Castelnuovo-Mumford regularity of I, and is an important measure of the complexity of I.

Corollary 2.11. *Let I_L be a homogeneous lattice ideal in $R = \Bbbk[x_1, \ldots, x_n]$ where L is a lattice in $\mathbb{Z}^n$ of dimension m. Then we have the inequality*

$$\operatorname{reg}(I_L) \leq \frac{1}{2} m(n-1)(n-m+1)MD$$

where $\operatorname{reg}(I_L)$ is the Caselnuovo-Mumford regularity of I_L, and the constants M and D are as in Theorem 2.10.

Proof. Let $p := \frac{1}{2} m(n-m+1)MD$, and $\mathbf{u} \in L$ a Graver element of L. Since I_L is homogeneous, it follows from Theorem 2.10 that $\|\mathbf{u}^+\|_1 = \|\mathbf{u}^-\|_1 \leq p$. Let $<$ be a term order. Since the Graver basis contains the universal Gröbner basis, it follows that p is an upper bound for the degree of any minimal monomial generator of $\operatorname{in}_<(I_L)$. By the Taylor resolution [1, Section 2], we have $\beta_{i,j}(\operatorname{in}_<(I_L)) = 0$ for $j > (i+1)p$. Since $\beta_{i,j}(I_L) \leq \beta_{i,j}(\operatorname{in}_<(I_L))$, we have $\beta_{i,j}(I_L) = 0$ for $j > (i+1)p$. Hence

$$\begin{aligned} \operatorname{reg}(I_L) &\leq \max\{(i+1)p - i \mid 0 \leq i \leq \operatorname{pd}_R(I_L)\} \\ &\leq (\operatorname{pd}_R(I_L) + 1)p \\ &\leq \operatorname{pd}_R(R/I_L)p. \end{aligned}$$

Therefore $\operatorname{reg}(I_L) \leq \operatorname{pd}_R(R/I_L)p$. Since each monomial is regular over R/I_L, we have $\operatorname{depth}(R/I_L) > 0$ which implies that $\operatorname{pd}_R(R/I_L) \leq n - 1$. □

Acknowledgments

This research was supported by a grant from the Research Council of University of Tehran.

References

[1] D. Bayer, I. Peeva and B. Sturmfels, Monomial resolutions, *Math. Res. Lett.* **5** (1998), no. 1-2, 31–46

[2] I. Borosh and L. B. Treybig, Bounds on positive integral solutions of linear Diophantine equations, *Proc. Amer. Math. Soc.* **55** (1976), no. 2, 299–304.

[3] E. Domenjoud, Solving Systems of Linear Diophantine Equations: An Algebraic Approach, Mathematical Foundations of Computer Science, 141–150, Lecture Notes in Comput. Sci., 520, Springer, Berlin, 1991.

[4] M. Drton, B. Sturmfels and S. Sullivant, Lectures on Algebraic Statistics, Birkhäuser Verlag, Basel, 2009.
[5] J. Graver, On the foundations of linear and integer linear programming, I, *Math. Programming* **9** (1975), no. 2, 207–226.
[6] H. Ohsugi and T. Hibi, Centrally symmetric configurations of integer matrices, `arXiv:1105.4322v1` (2001).
[7] L. Pottier, Minimal Solutions of Linear Diophantine Systems: Bounds and Algorithms, Rewriting Techniques and Applications, 162–173, Lecture Notes in Comput. Sci., 488, Springer, Berlin, 1991.
[8] A. Schrijver, Theory of Linear and Integer Programming, Wiley-Interscience Series in Discrete Mathematics, John Wiley & Sons, Chichester, 1986.
[9] B. Sturmfels, Gröbner Bases and Convex Polytopes, University Lecture Series, 8, Amer. Math. Soc., Providence, 1996.

Hossein Sabzrou
Department of Mathematics, University of Tehran, P.O. Box 14155-6455, Tehran, Iran
Email: sabzrou@ut.ac.ir