RC24999 (W1005-127) May 25, 2010
Mathematics

IBM Research Report

The Quadratic Graver Cone, Quadratic Integer Minimization, and Extensions

Jon Lee
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 218
Yorktown Heights, NY 10598
USA

Shmuel Onn, Lyubov Romanchuk
Technion - Israel Institute of Technology
Haifa, Israel

Robert Weismantel
ETH
Zürich, Switzerland

Research Division
Almaden - Austin - Beijing - Cambridge - Haifa - India - T. J. Watson - Tokyo - Zurich

The Quadratic Graver Cone, Quadratic Integer Minimization, and Extensions

Jon Lee, Shmuel Onn, Lyubov Romanchuk, Robert Weismantel

May 24, 2010

1 Introduction

Consider the general nonlinear integer minimization problem in standard form,

$$\min \{f(x) \ : \ x \in \mathbb{Z}^n \, , \ Ax = b \, , \ l \leq x \leq u\} \, , \tag{1}$$

with $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$, $l, u \in \mathbb{Z}^n_\infty$ with $\mathbb{Z}_\infty := \mathbb{Z} \uplus \{\pm\infty\}$, and $f : \mathbb{R}^n \to \mathbb{R}$.

It is well known to be NP-hard already for linear functions. However, recently it was shown that, if the *Graver basis* $\mathcal{G}(A)$ of A is given as part of the input, then the problem can be solved in polynomial time for the following classes of functions. First, in [1], for composite concave functions $f(x) = g(Wx)$, with $W \in \mathbb{Z}^{d \times n}$, $g : \mathbb{R}^d \to \mathbb{R}$ concave, and d fixed. Second, in [3], for separable convex functions $f(x) = \sum_i f_i(x_i)$ with each f_i univariate convex, and in particular for linear functions $f(x) = w^\intercal x$. While the Graver basis is a complex object, it can be computed in polynomial time from A for many natural and useful classes of matrices as demonstrated in [1, 3]. Moreover, the results of [2] imply that there is a parameterized scheme that enables to construct increasingly better approximations of the Graver basis of any matrix A and obtain increasingly better approximations to problem (1), see [4] for details.

In this article we continue this line of investigation and consider problem (1) for quadratic functions $f(x) = x^\intercal V x + w^\intercal x + a$ with $V \in \mathbb{R}^{n \times n}$, $w \in \mathbb{R}^n$, and $a \in \mathbb{R}$. We also discuss extensions to multivariate polynomial functions of arbitrary degree.

We begin by noting that problem (1) remains NP-hard even if the Graver basis is part of the input and even if the objective function is quadratic convex of rank 1.

Proposition 1.1 *It is NP-hard to determine the optimal value of the problem*

$$\min \left\{x^\intercal V x + w^\intercal x + a \ : \ x \in \mathbb{Z}^n \, , \ Ax = b \, , \ l \leq x \leq u\right\} \tag{2}$$

even when $\mathcal{G}(A)$ is given and the function is convex quadratic with matrix $V = vv^\intercal$.

Proof. Let $v \in \mathbb{Z}^n_+$ and $v_0 \in \mathbb{Z}_+$ be input to the *subset sum* problem of deciding if there exists $x \in \{0,1\}^n$ with $v^\intercal x = v_0$. Let $A := 0$ be the zero $1 \times n$ matrix, whose Graver basis $\mathcal{G}(A) = \{\pm \mathbf{1}_i \ : \ i = 1, \ldots, n\}$ consists of the n unit vectors and their

negations. Let $l := 0$ and $u := \mathbf{1}$ be the zero and all-ones vectors in $\mathbb{Z}^n$, and let $b := 0$ in $\mathbb{Z}^m$. Let $V := vv^\intercal$, $w := -2v_0v$, and $a := v_0^2$. Then problem (2) becomes

$$\min\left\{\left(v^\intercal x - v_0\right)^2 \ : \ x \in \{0,1\}^n\right\},$$

whose optimal value is 0 if and only if there is a subset sum, proving the claim. □

This shows that to solve problem (2) in polynomial time, even when the Graver basis is given, some restrictions on the class of quadratic functions must be enforced.

In Section 2 we introduce the *quadratic Graver cone* $\mathcal{Q}(A)$, which is a cone of $n \times n$ matrices defined via the Graver basis of A, and the *diagonal Graver cone* $\mathcal{D}(A)$ which is the diagonal projection of $\mathcal{Q}(A)$ into $\mathbb{R}^n_+$. We discuss some elementary properties of these cones and their duals $\mathcal{Q}^*(A)$ and $\mathcal{D}^*(A)$ and give some examples.

In Section 3 we prove the following algorithmic result about the solvability of problem (1) for every quadratic function (possibly indefinite, neither convex nor concave) whose defining matrix lies in the dual quadratic Graver cone.

Theorem 1.2 *There is an algorithm that, given $\mathcal{G}(A)$, solves the quadratic problem*

$$\min\left\{x^\intercal Vx + w^\intercal x + a \ : \ x \in \mathbb{Z}^n\,,\ Ax = b\,,\ l \le x \le u\right\} \tag{3}$$

in polynomial time for every integer matrix V lying in the cone $\mathcal{Q}^*(A)$ dual to $\mathcal{Q}(A)$.

We point out that, in practice, the algorithm that underlies Theorem 1.2 can be applied to any quadratic function. The algorithm will always stop and output a feasible solution if one exists, which can be used as an approximation of the optimal one. And, whenever V lies in $\mathcal{Q}^*(A)$, the solution produced will be true optimal.

As a special case we obtain the following result on separable quadratic functions.

Theorem 1.3 *There is an algorithm that, given $\mathcal{G}(A)$, solves the separable problem*

$$\min\{\sum_{i=1}^n \left(v_ix_i^2 + w_ix_i + a_i\right) \ : \ x \in \mathbb{Z}^n\,,\ Ax = b\,,\ l \le x \le u\} \tag{4}$$

in polynomial time for every integer vector v lying in the cone $\mathcal{D}^*(A)$ dual to $\mathcal{D}(A)$. In particular, this applies to any convex separable quadratic, that is, with $v \in \mathbb{Z}^n_+$.

In particular, Theorem 1.3 enables us to solve the problem with any linear objective function $f(x) = w^\intercal x$, which is the special case with $v = 0$, which is always in $\mathcal{D}^*(A)$.

In Section 4 we proceed with a discussion of the relation between the dual quadratic Graver cone $\mathcal{Q}^*(A)$ and the cone $\mathcal{S}^n_+$ of symmetric positive semidefinite matrices, and establish Theorem 4.2 which provides a characterization, in terms of their matroids only, of those matrices A for which the dual diagonal Graver cone $\mathcal{D}^*(A)$ strictly contains $\mathbb{R}^n_+$ and for which Theorem 1.3 assures efficient solution of problem (4) for all separable convex as well as some nonconvex quadratic functions.

In the final Section 5 we extend our results to multivariate polynomial functions of arbitrary degree. We define a hierarchy of higher degree analogues $\mathcal{P}_k(A)$ of the quadratic Graver cone, and show that the iterative algorithm of Theorem 1.2 solves the polynomial integer minimization problem (1) in polynomial time for every degree d form f that lies in a cone $\mathcal{K}_d(A)$ defined in terms of the dual Graver cones $\mathcal{P}^*_k(A)$.

Theorem 1.4 *For every fixed d there is an algorithm that, given $\mathcal{G}(A)$, solves*

$$\min\{f(x) \ : \ x \in \mathbb{Z}^n\,,\ Ax = b\,,\ x \geq 0\} \tag{5}$$

in polynomial time for every degree d integer homogenous polynomial f in $\mathcal{K}_d(A)$.

2 The quadratic and diagonal Graver cones

We begin with some notation. The inner product of two $m \times n$ matrices U, V is $U \cdot V := \sum_{i,j} U_{i,j} V_{i,j}$. The diagonal of $n \times n$ matrix V is the vector $v := \mathrm{diag}(V) \in \mathbb{R}^n$ defined by $v_i := V_{i,i}$ for all i. For $u \in \mathbb{R}^n$ we denote by $U := \mathrm{Diag}(u)$ the $n \times n$ diagonal matrix with $\mathrm{diag}(U) = u$. The *pointwise product* of vectors $g, h \in \mathbb{R}^n$ is the vector $g \circ h$ in $\mathbb{R}^n$ with $(g \circ h)_i := g_i h_i$ for all i. Note that g, h lie in the same orthant of $\mathbb{R}^n$ if and only if $g \circ h \geq 0$. The *tensor product* of $g, h \in \mathbb{R}^n$ is the $n \times n$ matrix $g \otimes h = gh^\intercal$ with $(g \otimes h)_{i,j} := (gh^\intercal)_{i,j} = g_i h_j$ for all i, j. We will use the notation $g \otimes h$ and $gh^\intercal$ interchangeably as we find appropriate. Note that for all $g, h \in \mathbb{R}^n$ and $V \in \mathbb{R}^{n \times n}$, we have $g \circ h = \mathrm{diag}(g \otimes h)$ and $(g \otimes h) \cdot V = g^\intercal V h$.

Any quadratic function $f(x) = x^\intercal V x + w^\intercal x + a$ has an equivalent description $f(x) = x^\intercal U x + w^\intercal x + a$ with $U := \frac{1}{2}(V + V^\intercal)$ symmetric matrix. We therefore can and will be working with symmetric matrices which are much better behaved than arbitrary square matrices. We denote by $\mathcal{S}^n \subset \mathbb{R}^{n \times n}$ the linear subspace of symmetric $n \times n$ matrices. A *cone* is a subset $\mathcal{P}$ of real vector space such that $\alpha x + \beta y \in \mathcal{P}$ for all $x, y \in \mathcal{P}$ and $\alpha, \beta \in \mathbb{R}_+$. The *cone generated* by a set $\mathcal{V}$ of vectors is the set $\mathrm{cone}(\mathcal{V})$ of nonnegative linear combinations of finitely many vectors from $\mathcal{V}$. In particular, $\mathrm{cone}(\emptyset) := \{0\}$. We will be using cones $\mathcal{D} \subseteq \mathbb{R}^n$ of vectors and cones $\mathcal{Q} \subseteq \mathcal{S}^n$ of $n \times n$ symmetric matrices. The *dual* of a cone $\mathcal{D} \subseteq \mathbb{R}^n$ and the (symmetric) *dual* of a cone $\mathcal{Q} \subseteq \mathcal{S}^n$ are, respectively, the cones

$$\mathcal{D}^* \ := \ \{v \in \mathbb{R}^n \ : \ u^\intercal v \geq 0\,,\ u \in \mathcal{D}\}, \quad \mathcal{Q}^* \ := \ \{V \in \mathcal{S}^n \ : \ U \cdot V \geq 0\,,\ U \in \mathcal{Q}\}.$$

Duality reverses inclusions, that is, if $\mathcal{P} \subseteq \mathcal{K}$ are cones in $\mathbb{R}^n$ or $\mathcal{S}^n$ then $\mathcal{K}^* \subseteq \mathcal{P}^*$.

We proceed with the definition of the Graver basis of an integer matrix. The lattice of an integer $m \times n$ matrix A is the set $\mathcal{L}(A) := \{x \in \mathbb{Z}^n \ : \ Ax = 0\}$. We denote by $\mathcal{L}^*(A)$ the set of nonzero elements in $\mathcal{L}(A)$. We use a partial order $\sqsubseteq$ on $\mathbb{R}^n$ which extends the coordinate-wise partial order $\leq$ on the nonnegative orthant $\mathbb{R}^n_+$ and is defined as follows. For $x, y \in \mathbb{R}^n$ we write $x \sqsubseteq y$ and say that x is *conformal* to y if $x \circ y \geq 0$ (that is, x, y lie in the same orthant) and $|x_i| \leq |y_i|$ for all i. We write $x \sqsubset y$ if $x \sqsubseteq y$ and $x \neq y$. A simple extension of the classical Gordan Lemma implies that every subset of $\mathbb{Z}^n$ has finitely many $\sqsubseteq$-minimal elements.

Definition 2.1 The *Graver basis* of an integer matrix A is defined to be the finite set $\mathcal{G}(A) \subset \mathbb{Z}^n$ of $\sqsubseteq$-minimal elements in $\mathcal{L}^*(A) = \{x \in \mathbb{Z}^n \ : \ Ax = 0,\ x \neq 0\}$.

In this article we introduce the following objects defined via the Graver basis.

Definition 2.2 The *quadratic Graver cone* of an integer $m \times n$ matrix A is defined to be the cone $\mathcal{Q}(A) \subseteq \mathcal{S}^n$ of $n \times n$ matrices generated by the matrices $g \otimes h + h \otimes g$ over all pairs of distinct elements $g, h \in \mathcal{G}(A)$ that lie in the same orthant, that is,

$$\mathcal{Q}(A) \;:=\; \text{cone}\,\{g \otimes h + h \otimes g \;:\; g, h \in \mathcal{G}(A)\,,\; g \neq h\,,\; g \circ h \geq 0\} \;\subseteq\; \mathcal{S}^n\;.$$

The *dual quadratic Graver cone* is its (symmetric) dual $\mathcal{Q}^*(A)$ in $\mathcal{S}^n$ given by

$$\begin{aligned} \mathcal{Q}^*(A) &= \{V \in \mathcal{S}^n \;:\; U \cdot V \geq 0\,,\;\; U \in \mathcal{Q}(A)\} \\ &= \{V \in \mathcal{S}^n \;:\; (gh^{\intercal} + hg^{\intercal}) \cdot V \;\geq\; 0\,,\;\; g, h \in \mathcal{G}(A)\,,\; g \neq h\,,\; g \circ h \geq 0\} \\ &= \{V \in \mathcal{S}^n \;:\; g^{\intercal} V h \;\geq\; 0\,,\;\; g, h \in \mathcal{G}(A)\,,\; g \neq h\,,\; g \circ h \geq 0\}. \end{aligned} \tag{6}$$

We are also interested is the following cone of diagonals of matrices in $\mathcal{Q}(A)$.

Definition 2.3 The *diagonal Graver cone* of A is the cone of nonnegative vectors

$$\mathcal{D}(A) \;:=\; \text{cone}\,\{g \circ h \;:\; g, h \in \mathcal{G}(A)\,,\; g \neq h\,,\; g \circ h \geq 0\} \;\subseteq\; \mathbb{R}^n_+\;.$$

The *dual diagonal Graver cone* is its dual $\mathcal{D}^*(A)$ in $\mathbb{R}^n$ given by

$$\begin{aligned} \mathcal{D}^*(A) &= \{v \;:\; u^{\intercal} v \geq 0\,,\;\; u \in \mathcal{D}(A)\} \\ &= \{v \;:\; (g \circ h)^{\intercal} v \;\geq\; 0\,,\;\; g, h \in \mathcal{G}(A)\,,\; g \neq h\,,\; g \circ h \geq 0\} \\ &= \{v \;:\; \sum g_i h_i v_i \;\geq\; 0\,,\;\; g, h \in \mathcal{G}(A)\,,\; g \neq h\,,\; g \circ h \geq 0\}. \end{aligned} \tag{7}$$

The following lemma provides some basic relations among the above cones and more. All inclusions can be strict, as is demonstrated in Examples 2.5 and 2.6 below. In particular, it is interesting to note that $\mathcal{D}(A)$ is the diagonal projection of $\mathcal{Q}(A)$, but $\mathcal{D}^*(A)$ is generally strictly contained in the diagonal projection of $\mathcal{Q}^*(A)$.

Lemma 2.4 *The quadratic and diagonal Graver cones and their duals satisfy*

$$\begin{aligned} \mathbb{R}^n_+ \;\supseteq\; \mathcal{D}(A) \;&=\; \{\text{diag}(U) \;:\; U \in \mathcal{Q}(A)\} \;\supseteq\; \{u \;:\; \text{Diag}(u) \in \mathcal{Q}(A)\}\,, \\ \mathbb{R}^n_+ \;\subseteq\; \mathcal{D}^*(A) \;&=\; \{v \;:\; \text{Diag}(v) \in \mathcal{Q}^*(A)\} \;\subseteq\; \{\text{diag}(V) \;:\; V \in \mathcal{Q}^*(A)\}\,. \end{aligned} \tag{8}$$

Proof. First, $\mathcal{D}(A) \subseteq \mathbb{R}^n_+$ because it is generated by nonnegative vectors. Therefore $\mathcal{D}^*(A) \supseteq (\mathbb{R}^n_+)^* = \mathbb{R}^n_+$. To establish the top equality note that the following are equivalent: $u \in \mathcal{D}(A)$; $u = \sum_k \mu_k (g_k \circ h_k)$ for some suitable $\mu_k \geq 0$, $g_k, h_k \in \mathcal{G}(A)$; $u = \text{diag}(U)$ with $U = \frac{1}{2}\sum_k \mu_k (g_k \otimes h_k + h_k \otimes g_k)$; and $u = \text{diag}(U)$ with $U \in \mathcal{Q}(A)$. To establish the bottom equality note that the following are equivalent: $v \in \mathcal{D}^*(A)$; $(g \circ h)^{\intercal} v \geq 0$ for all suitable $g, h \in \mathcal{G}(A)$; $V = \text{Diag}(v)$ with $g^{\intercal} V h \geq 0$ for all g, h; and $V = \text{Diag}(v)$ with $V \in \mathcal{Q}^*(A)$. The two remaining inclusions on the right-hand sides follow from $\text{diag}(\text{Diag}(x)) = x$. This completes the proof of the lemma. □

The next two examples show that all inclusions in Lemma 2.4 can be strict.

Example 2.5 *Consider the zero $1 \times n$ matrix $A := 0$, whose Graver basis is given by $\mathcal{G}(A) = \{\pm \mathbf{1}_i \;:\; i = 1, \ldots, n\}$. Then $g \circ h = 0$ is the zero vector for all distinct $g, h \in \mathcal{G}(A)$ in the same orthant. So the diagonal Graver cone and its dual are $\mathcal{D}(A) = \{0\} \subsetneq \mathbb{R}^n_+$ and $\mathcal{D}^*(A) = \mathbb{R}^n \supsetneq \mathbb{R}^n_+$ so the left inclusions in (8) are strict.*

Example 2.6 *Consider the* 1×3 *matrix* $A := (1\ \ 1\ \ 1)$ *with Graver basis* $\mathcal{G}(A) = \pm\{(1,-1,0),(1,0,-1),(0,1,-1)\}$. *The quadratic Graver cone and its dual satisfy*

$$\mathcal{Q}(A) \;=\; \text{cone}\left\{\begin{pmatrix} 2 & -1 & -1 \\ -1 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 1 \\ -1 & 2 & -1 \\ 1 & -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & -1 \\ -1 & -1 & 2 \end{pmatrix}\right\},$$

$$\begin{aligned} \mathcal{Q}^*(A) \;&=\; \left\{\begin{pmatrix} a & d & e \\ d & b & f \\ e & f & c \end{pmatrix} \;:\; \begin{array}{rcl} a-d-e+f & \geq & 0 \\ b-d+e-f & \geq & 0 \\ c+d-e-f & \geq & 0 \end{array}\right\} \\ &\supseteq\; \left\{\begin{pmatrix} 2a & a+b & a+c \\ a+b & 2b & b+c \\ a+c & b+c & 2c \end{pmatrix} \;:\; a,b,c \in \mathbb{R}\right\}. \end{aligned} \tag{9}$$

The diagonal Graver cone and its dual are $\mathcal{D}(A) = \mathbb{R}^n_+$ *and* $\mathcal{D}^*(A) = \mathbb{R}^n_+$. *Therefore, the top and bottom inclusions on the right-hand side of equation (8) are strict,*

$$\mathcal{D}(A) = \mathbb{R}^n_+ \;\supsetneq\; \{0\} \;=\; \{u \;:\; \text{Diag}(u) \in \mathcal{Q}(A)\},$$

$$\mathcal{D}^*(A) = \mathbb{R}^n_+ \;\subsetneq\; \mathbb{R}^n \;=\; \{\text{diag}(V) \;:\; V \in \mathcal{Q}^*(A)\}.$$

3 Quadratic integer minimization

We proceed to establish our algorithmic Theorems 1.2 and 1.3. We focus on the situation of finite feasible sets, which is natural in most applications. But we do allow the lower and upper bounds $l, u \in \mathbb{Z}^n_\infty$ to have infinite components for flexibility of modeling (for instance, it is quite common in applications to have $l_i = 0$ and $u_i = \infty$ for all i, with the resulting feasible set typically still finite). We also require our algorithms to identify and properly stop when the set is infinite. So in all algorithmic statements, an algorithm is said to *solve* a (nonlinear) discrete optimization problem, if for every input, it either finds an optimal solution, or asserts that the problem is infeasible or the feasible set is infinite. We begin with a simple lemma that shows that we can quickly minimize a given quadratic function in a given direction.

Lemma 3.1 *There is an algorithm that, given bounds* $l, u \in \mathbb{Z}^n_\infty$, *direction* $g \in \mathbb{Z}^n$, *point* $z \in \mathbb{Z}^n$ *with* $l \leq z \leq u$, *and quadratic function* $f(x) = x^\intercal V x + w^\intercal x + a$ *with* $V \in \mathbb{Z}^{n\times n}$, $w \in \mathbb{Z}^n$, *and* $a \in \mathbb{Z}$, *solves in polynomial time the univariate problem*

$$\min\{f(z+\mu g) \;:\; \mu \in \mathbb{Z}_+\,,\; l \leq z+\mu g \leq u\}. \tag{10}$$

Proof. Let $S := \{\mu \in \mathbb{Z}_+ : l \leq z + \mu g \leq u\}$, and let $s := \sup S$ which is easy to determine. If $s = \infty$ then we conclude that S is infinite and stop. Otherwise we need to minimize the univariate quadratic function $h(\mu) := f(z+\mu g) = h_2\mu^2 + h_1\mu + h_0$ with $h_2 := g^\intercal V g$, $h_1 := z^\intercal V g + g^\intercal V z + w^\intercal g$, and $h_0 := z^\intercal V z + w^\intercal z + a$ over $S = \{0, 1, \ldots, s\}$. If $h_2 \leq 0$, then h is concave, and the minimum over S is attained

at $\mu = 0$ or $\mu = s$. If $h_2 > 0$ then h is convex with real minimum at $\mu^* := -\frac{h_1}{2h_2}$. Then minimizing h over S reduces to minimizing h over $S \cap \{0, \lfloor \mu^* \rfloor, \lceil \mu^* \rceil, s\}$. □

A finite sum $u := \sum_i v_i$ of vectors in $\mathbb{R}^n$ is called *conformal* if $v_i \sqsubseteq u$ for all i, and hence all summands lie in the same orthant. The following lemma shows that quadratic f with defining matrix in the dual quadratic Graver cone is supermodular on conformal sums of nonnegative combinations of elements of the Graver basis.

Lemma 3.2 *Let A be any integer $m \times n$ matrix with quadratic Graver cone $\mathcal{Q}(A)$. Let $f : \mathbb{R}^n \to \mathbb{R}$ be any quadratic function $f(x) = x^\intercal V x + w^\intercal x + a$ with $V \in \mathcal{Q}^*(A)$. Let $x \in \mathbb{R}^n$ be any point, and let $\sum \mu_i g_i$ be any conformal sum in $\mathbb{R}^n$ with $g_i \in \mathcal{G}(A)$ distinct elements in the Graver basis of A and $\mu_i \geq 0$ nonnegative scalars. Then*

$$\Delta \;:=\; \left(f\left(x + \sum \mu_i g_i\right) - f(x)\right) \;-\; \sum \left(f\left(x + \mu_i g_i\right) - f(x)\right) \;\geq\; 0.$$

Proof. We have

$$f\left(x + \sum \mu_i g_i\right) - f(x) = \sum x^\intercal V \mu_j g_j + \sum \mu_i g_i^\intercal V x + \sum_{i,j} \mu_i g_i^\intercal V \mu_j g_j + \sum w^\intercal \mu_i g_i \;,$$

and

$$\sum \left(f(x + \mu_i g_i) - f(x)\right) \;=\; \sum \left(x^\intercal V \mu_i g_i + \mu_i g_i^\intercal V x + \mu_i g_i^\intercal V \mu_i g_i + w^\intercal \mu_i g_i\right).$$

Therefore we obtain

$$\Delta \;=\; \sum_{i,j} \mu_i g_i^\intercal V \mu_j g_j - \sum \mu_i g_i^\intercal V \mu_i g_i \;=\; \sum_{i \neq j} \mu_i g_i^\intercal V \mu_j g_j \;=\; \sum_{i \neq j} \mu_i \mu_j g_i^\intercal V g_j \;\geq 0,$$

because $g_i, g_j \in \mathcal{G}(A)$ satisfy $g_i \circ g_j \geq 0$ and $g_i \neq g_j$ for $i \neq j$, and V is in $\mathcal{Q}^*(A)$. □

We need two more useful properties of Graver bases. First we need the following integer analogue of Carathéodory's theorem of [6] which we state without proof.

Lemma 3.3 *Let A be an integer $m \times n$ matrix, and let $\mathcal{G}(A)$ be its Graver basis. Then every $x \in \mathcal{L}^*(A)$ is a conformal sum $x = \sum_{i=1}^t \mu_i g_i$ that involves $t \leq 2n - 2$ Graver basis elements $g_i \in \mathcal{G}(A)$ and nonnegative integer coefficients $\mu_i \in \mathbb{Z}_+$.*

The next lemma provides a Graver basis criterion for finiteness of integer programs.

Lemma 3.4 *Let $\mathcal{G}(A)$ be the Graver basis of matrix A, and let $l, u \in \mathbb{Z}^n_\infty$. If there is some $g \in \mathcal{G}(A)$ satisfying $g_i \leq 0$ whenever $u_i < \infty$ and $g_i \geq 0$ whenever $l_i > -\infty$ then every set of the form $S := \{x \in \mathbb{Z}^n \,:\, Ax = b\,,\; l \leq x \leq u\}$ is either empty or infinite, whereas if there is no such g, then every set S of this form is finite. Clearly, given the Graver basis, the existence of such g can be checked in polynomial time.*

Proof. Suppose there is such g and consider such S containing a point x. Then for all $\lambda \in \mathbb{Z}_+$ we have $l \le x+\lambda g \le u$ and $A(x+\lambda g) = Ax = b$, and hence $x+\lambda g \in S$ so S is infinite. Next suppose S is infinite. Then $P := \{x \in \mathbb{R}^n : Ax = b,\, l \le x \le u\}$ is unbounded, and hence has a recession vector, which we may assume is integer, that is, a nonzero h such that $x + \alpha h \in P$ for all $x \in P$ and $\alpha \ge 0$. Then $h \in \mathcal{L}^*(A)$ and $h_i \le 0$ whenever $u_i < \infty$ and $h_i \ge 0$ whenever $l_i > -\infty$. By Lemma 3.3, the vector h is a conformal sum $h = \sum g_i$ of vectors $g_i \in \mathcal{G}(A)$, each of which also satisfies $g_i \le 0$ whenever $u_i < \infty$ and $g_i \ge 0$ whenever $l_i > -\infty$, providing such g. □

Next we prove the main lemma underlying our algorithm, which shows that, given the Graver basis, and an initial feasible point, we can minimize a quadratic function with defining matrix in the dual quadratic Graver cone in polynomial time.

Lemma 3.5 *There is an algorithm that, given $A \in \mathbb{Z}^{m\times n}$, its Graver basis $\mathcal{G}(A)$, bounds $l, u \in \mathbb{Z}^n_\infty$, point $z \in \mathbb{Z}^n$ with $l \le z \le u$, and quadratic $f(x) = x^{\mathsf{T}} V x + w^{\mathsf{T}} x + a$ with integer $V \in \mathcal{Q}^*(A)$, $w \in \mathbb{Z}^n$, and $a \in \mathbb{Z}$, solves in polynomial time the program*

$$\min\{f(x) = x^{\mathsf{T}} V x + w^{\mathsf{T}} x + a \;:\; x \in \mathbb{Z}^n\,,\; Ax = b\,,\; l \le x \le u\}\;, \quad b := Az\;. \tag{11}$$

Proof. First, apply the algorithm of Lemma 3.4 to $\mathcal{G}(A)$ and l, u and either detect that the feasible set is infinite and stop, or conclude it is finite and continue. Next produce a sequence of feasible points $x_0, x_1, \ldots, x_s$ with $x_0 := z$ the given input point, as follows. Having obtained x_k, solve the minimization problem

$$\min\{f(x_k + \mu g) \;:\; \mu \in \mathbb{Z}_+\,,\; g \in \mathcal{G}(A)\,,\; l \le x_k + \mu g \le u\,\} \tag{12}$$

by applying the algorithm of Lemma 3.1 for each $g \in \mathcal{G}(A)$. If the minimal value in (12) satisfies $f(x_k + \mu g) < f(x_k)$ then set $x_{k+1} := x_k + \mu g$ and repeat, else stop and output the last point x_s in the sequence. Now, $Ax_{k+1} = A(x_k + \lambda g) = Ax_k = b$ by induction on k, so each x_k is feasible. Because the feasible set is finite and the x_k have decreasing objective values and hence distinct, the algorithm terminates.

We now show that the point x_s output by the algorithm is optimal. Let x^* be any optimal solution to (11). Consider any point x_k in the sequence, and suppose that it is not optimal. We claim that a new point x_{k+1} will be produced and will satisfy

$$f(x_{k+1}) - f\,(x^*) \;\le\; \frac{2n-3}{2n-2}\,(f(x_k) - f(x^*))\,. \tag{13}$$

By Lemma 3.3, we can write the difference $x^* - x_k = \sum_{i=1}^t \mu_i g_i$ as conformal sum involving $1 \le t \le 2n-2$ elements $g_i \in \mathcal{G}(A)$ with all $\mu_i \in \mathbb{Z}_+$. By Lemma 3.2,

$$f(x^*) - f\,(x_k) \;=\; f\left(x_k + \sum_{i=1}^t \mu_i g_i\right) - f(x_k) \;\ge\; \sum_{i=1}^t (f\,(x_k + \mu_i g_i) - f(x_k))\,.$$

Adding $t\,(f(x_k) - f(x^*))$ on both sides and rearranging terms, we obtain

$$\sum_{i=1}^t (f\,(x_k + \mu_i g_i) - f(x^*)) \;\le\; (t-1)\,(f(x_k) - f(x^*))\,.$$

Therefore there is some summand on the left-hand side satisfying

$$f\left(x_k+\mu_i g_i\right)-f(x^*) \;\le\; \frac{t-1}{t}\left(f(x_k)-f(x^*)\right) \;\le\; \frac{2n-3}{2n-2}\left(f(x_k)-f(x^*)\right).$$

So the point $x_k+\mu g$ attaining minimum in (12) satisfies

$$f(x_k+\mu g)-f(x^*) \;\le\; f\left(x_k+\mu_i g_i\right)-f(x^*) \;\le\; \frac{2n-3}{2n-2}\left(f(x_k)-f(x^*)\right),$$

and so indeed $x_{k+1}:=x_k+\mu g$ will be produced and will satisfy (13). This shows that the last point x_s produced and output by the algorithm is indeed optimal.

We proceed to bound the number s of points. Consider any $i<s$ and the intermediate non-optimal point x_i in the sequence produced by the algorithm. Then $f(x_i)>f(x^*)$ with both values integer, and so repeated use of (13) gives

$$\begin{aligned} 1\le f(x_i)-f(x^*) &= \prod_{k=0}^{i-1}\frac{f(x_{k+1})-f(x^*)}{f(x_k)-f(x^*)}\left(f(x)-f(x^*)\right) \\ &\le \left(\frac{2n-3}{2n-2}\right)^{i}\left(f(x)-f(x^*)\right), \end{aligned}$$

and therefore

$$i \;\le\; \left(\log\frac{2n-2}{2n-3}\right)^{-1}\log\left(f(x)-f(x^*)\right).$$

Therefore the number s of points produced by the algorithm is at most one unit larger than this bound, and using a simple bound on the logarithm, we obtain

$$s \;=\; O\left(n\log(f(x)-f(x^*))\right).$$

Thus, the number of points produced and the total running time are polynomial. □

Next we show that, given the Graver basis, we can also find an initial feasible point for assert that the given set is empty or infinite, in polynomial time.

Lemma 3.6 *There is an algorithm that, given integer $m\times n$ matrix A, its Graver basis $\mathcal{G}(A)$, $l,u\in\mathbb{Z}^n_\infty$, and $b\in\mathbb{Z}^m$, in polynomial time, either finds a feasible point in the set $S:=\{x\in\mathbb{Z}^n\,:\,Ax=b,\,l\le x\le u\}$ or asserts that S is empty or infinite.*

Proof. Assume that $l\le u$ and that $l_j<\infty$ and $u_j>-\infty$ for all j, because otherwise there is no feasible point. Also assume that there is no $g\in\mathcal{G}(A)$ satisfying $g_j\le 0$ whenever $u_j<\infty$ and $g_j\ge 0$ whenever $l_j>-\infty$, because otherwise S is empty or infinite by Lemma 3.4. Now, either detect there is no integer solution to the system of equations $Ax=b$ (without the lower and upper bound constraints) and stop, or determine some such solution $x\in\mathbb{Z}^n$ and continue; it is well known that this can be done in polynomial time, say, using the Hermite normal form of A, see [5]. Let

$$I \;:=\; \{j\,:\,l_j\le x_j\le u_j\} \;\subseteq\; \{1,\ldots,n\}$$

be the set of indices of entries of x that satisfy their lower and upper bounds. While $I \subsetneq \{1,\ldots,n\}$ repeat the following procedure. Pick any index $i \notin I$. Then either $x_i < l_i$ or $x_i > u_i$. We describe the procedure only in the former case, the latter being symmetric. Update the lower and upper bounds by setting

$$\hat{l}_j \ := \ \min\{l_j, x_j\}\,, \qquad \hat{u}_j \ := \ \max\{u_j, x_j\}\,, \qquad j = 1,\ldots,n\ .$$

Solve in polynomial time the following linear integer program, for which x is feasible,

$$\max\{z_i \ : \ z \in \mathbb{Z}^n\,,\ Az = b\,,\ \hat{l} \le z \le \hat{u}\,,\ z_i \le u_i\}, \tag{14}$$

by applying the algorithm of Lemma 3.5 using the function $f(z) := z^{\intercal} 0 z + \mathbf{1}_i^{\intercal} z + 0$ with $V = 0$ the zero matrix which is always in $\mathcal{Q}^*(A)$. Now $\hat{l}_j > -\infty$ if and only if $l_j > -\infty$, and $\hat{u}_j < \infty$ if and only if $u_j < \infty$. So there is no $g \in \mathcal{G}(A)$ satisfying $g_j \le 0$ whenever $\hat{u}_j < \infty$ and $g_j \ge 0$ whenever $\hat{l}_j > -\infty$, and hence the feasible set of (14) is finite by Lemma 3.4 and has an optimal solution z. If $z_i < l_i$ then assert that the set S is empty and stop. Otherwise, set $x := z$, $I := \{j \ : \ l_j \le x_j \le u_j\}$, and repeat. Note that in each iteration, the cardinality of I increases by at least one. Therefore, after at most n iterations, either the algorithm detects infeasibility, or $I = \{1,\ldots,n\}$ is obtained, in which case the current point x is feasible. □

We are now in position to establish our theorem.

Theorem 1.2 *There is an algorithm that, given $A \in \mathbb{Z}^{m\times n}$, its Graver basis $\mathcal{G}(A)$, bounds $l, u \in \mathbb{Z}^n_\infty$, $b \in \mathbb{Z}^m$, integer matrix $V \in \mathcal{Q}^*(A)$ in the dual quadratic Graver cone, $w \in \mathbb{Z}^n$, and $a \in \mathbb{Z}$, solves in polynomial time the quadratic integer program*

$$\min\{x^{\intercal} V x + w^{\intercal} x + a \ : \ x \in \mathbb{Z}^n\,,\ Ax = b\,,\ l \le x \le u\}.$$

Proof. Use the algorithm underlying Lemma 3.6 to either detect that the problem is infeasible or that the feasible set is infinite and stop, or obtain a feasible point and use the algorithm underlying Lemma 3.5 to obtain an optimal solution. □

An important immediate consequence of Theorem 1.2 is that we can efficiently minimize separable quadratic functions defined by vectors in the dual diagonal Graver cone. In particular, it applies to every convex separable quadratic function (which can also be deduced from the results of [3] on separable convex functions).

Theorem 1.3 *There is an algorithm that, given $A \in \mathbb{Z}^{m\times n}$, its Graver basis $\mathcal{G}(A)$, bounds $l, u \in \mathbb{Z}^n_\infty$, $b \in \mathbb{Z}^m$, integer vector $v \in \mathcal{D}^*(A)$ in the dual diagonal Graver cone, and $w, a \in \mathbb{Z}^n$, solves in polynomial time the separable quadratic program*

$$\min\{\sum_{i=1}^{n} \left(v_i x_i^2 + w_i x_i + a_i\right) \ : \ x \in \mathbb{Z}^n\,,\ Ax = b\,,\ l \le x \le u\}.$$

In particular, this applies to any convex separable quadratic, that is, with $v \in \mathbb{Z}^n_+$.

Proof. First, for any $v \in \mathcal{D}^*(A)$ we have $V := \mathrm{Diag}(v) \in \mathcal{Q}^*(A)$ by Lemma 2.4. Hence, by Theorem 1.2, we can minimize in polynomial time the quadratic function

$$\sum_{i=1}^{n} \left(v_i x_i^2 + w_i x_i + a_i \right) \;=\; x^{\intercal} V x + w^{\intercal} x + \sum_{i=1}^{n} a_i \;.$$

Second, if the separable quadratic function is convex, which is equivalent to its defining vector v being nonnegative, then $v \in \mathbb{R}^n_+ \subseteq \mathcal{D}^*(A)$ by Lemma 2.4 again. Hence the second statement of the theorem now follows from the first statement. □

4 Nonconvex solvable quadratics and matroids

Consider the quadratic minimization problem, with the Graver basis of A given,

$$\min \left\{ f(x) = x^{\intercal} V x + w^{\intercal} x + a \;:\; x \in \mathbb{Z}^n \,,\; Ax = b \,,\; l \leq x \leq u \right\}. \qquad (15)$$

The function f is convex if and only if its defining matrix V is positive semidefinite, that is, if $x^{\intercal} V x \geq 0$ for all $x \in \mathbb{R}^n$. Let $\mathcal{S}^n_+ \subset \mathcal{S}^n$ denote the cone of symmetric positive semidefinite matrices. Now, on the one hand, if $V \in \mathcal{Q}^*(A)$ then, by Theorem 1.2, we can solve problem (15) efficiently. On the other hand, if $V \in \mathcal{S}^n_+$ then f is convex, and problem (15) may seem to be easier, but remains NP-hard even for rank-1 matrices $V = vv^{\intercal} \in \mathcal{S}^n_+$ by Proposition 1.1. So it is unlikely that $\mathcal{Q}^*(A)$ contains $\mathcal{S}^n_+$, and it is interesting to consider the relation between these matrix cones.

For this, we need a couple of basic facts about positive semidefinite matrices. First, Note that for any vector $u \in \mathbb{R}^n$, the rank-1 matrix $uu^{\intercal}$ is in $\mathcal{S}^n_+$ because $x^{\intercal}(uu^{\intercal})x = (u^{\intercal}x)^2 \geq 0$ for all $x \in \mathbb{R}^n$, whereas for any two linearly independent vectors $g, h \in \mathbb{R}^n$, the rank-2 matrix $gh^{\intercal} + hg^{\intercal}$ is in $\mathcal{S}^n \backslash \mathcal{S}^n_+$ because there is an $x \in \mathbb{R}^n$ with $g^{\intercal}x = 1$ and $h^{\intercal}x = -1$ and hence $x^{\intercal}(gh^{\intercal} + hg^{\intercal})x = 2(g^{\intercal}x)(h^{\intercal}x) = -2 < 0$. Second, the cone of symmetric positive semidefinite matrices is self dual, that is, $(\mathcal{S}^n_+)^* = \mathcal{S}^n_+$. To see this, note that if $U \in \mathcal{S}^n \setminus \mathcal{S}^n_+$ then there is an $x \in \mathbb{R}^n$ with $(x \otimes x) \cdot U = x^{\intercal} U x < 0$ so $U \notin (\mathcal{S}^n_+)^*$; and if $V \in \mathcal{S}^n_+$ has rank r, then $V = \sum_{i=1}^{r} x_i \otimes x_i$ for some $x_i \in \mathbb{R}^n$ and hence $U \cdot V = \sum_{i=1}^{r} x_i^{\intercal} U x_i \geq 0$ for all $U \in \mathcal{S}^n_+$, so $V \in (\mathcal{S}^n_+)^*$.

So we can conclude the following. In the rare situation where each orthant of $\mathbb{R}^n$ contains at most one element of $\mathcal{G}(A)$, we have $\mathcal{Q}(A) = \{0\}$ and $\mathcal{Q}^*(A) = \mathcal{S}^n$, so Theorem 1.2 enables to solve problem (15) for any quadratic function. In the more typical situation, where some orthant does contain two elements $g, h \in \mathcal{G}(A)$, the corresponding generator of $\mathcal{Q}(A)$ satisfies $gh^{\intercal} + hg^{\intercal} \in \mathcal{S}^n \backslash \mathcal{S}^n_+$ and hence $\mathcal{Q}(A) \nsubseteq \mathcal{S}^n_+$. By self duality of $\mathcal{S}^n_+$, we obtain $\mathcal{S}^n_+ = (\mathcal{S}^n_+)^* \nsubseteq \mathcal{Q}^*(A)$. So we cannot solve problem (15) for all convex quadratics, reflecting the NP-hardness of the convex problem. But we do typically also have $\mathcal{Q}^*(A) \nsubseteq \mathcal{S}^n_+$, that is, we can solve problem (15) in polynomial time for various nonconvex quadratics. For instance, in Example 2.6, the matrix in (9) is not positive semidefinite for all $a, b, c < 0$. Moreover, by Lemma 2.4, $\mathbb{R}^n_+ \subseteq \mathcal{D}^*(A) = \{v \,:\, \mathrm{Diag}(v) \in \mathcal{Q}^*(A)\}$, so $\mathcal{Q}^*(A) \backslash \mathcal{S}^n_+ \neq \emptyset$ whenever $\mathcal{D}^*(A) \backslash \mathbb{R}^n_+ \neq \emptyset$.

We proceed to discuss this diagonal case, where the function f is defined by a diagonal matrix $V = \mathrm{Diag}(v)$ for some $v \in \mathbb{R}^n$, that is, f is separable of the form

$f(x) = \sum_i (v_i x_i^2 + w_i x_i + a_i)$. In this case, f is convex if and only if v is nonnegative. As noted in Lemma 2.4, the dual diagonal Graver cone $\mathcal{D}^*(A)$ always contains the nonnegative orthant $\mathbb{R}^n_+$. We proceed to characterize those matrices A for which this inclusion is strict, so that $\mathcal{D}^*(A) \setminus \mathbb{R}^n_+ \neq \emptyset$ and Theorem 1.3 enables to solve problem (15) in polynomial time also for various nonconvex separable quadratics.

For this we need a few more definitions. A *circuit* of an integer matrix A is an element $c \in \mathcal{L}^*(A)$ whose support $\mathrm{supp}(c)$ is minimal under inclusion and whose entries are relatively prime. We denote the set of circuits of A by $\mathcal{C}(A)$. It is easy to see that for every integer matrix A, the set of circuits is contained in the Graver basis, that is, $\mathcal{C}(A) \subseteq \mathcal{G}(A)$. Recall that a finite sum $u := \sum_i v_i$ of vectors in $\mathbb{R}^n$ is *conformal* if $v_i \sqsubseteq u$ for all i, and hence all summands lie in the same orthant. The following property of circuits is well known. For a proof see, for instance, [4] or [7].

Lemma 4.1 *Let A be an integer matrix. Then every $x \in \mathcal{L}^*(A)$ is a conformal sum $x = \sum_i \alpha_i c_i$ involving circuits $c_i \in \mathcal{C}(A)$ and nonnegative real coefficients $\alpha_i \in \mathbb{R}_+$.*

It turns out that the matroid of linear dependencies on the columns of the integer $m \times n$ matrix A (over the reals or integers) plays a central role in the characterization we are heading for. A *matroid-circuit* is any set $C \subseteq \{1, \ldots, n\}$ that is the support $C = \mathrm{supp}(c)$ of some circuit $c \in \mathcal{C}(A)$ of A. Note that a circuit c is in $\mathcal{C}(A)$ if and only if its antipodal $-c$ is, and if $c, e \in \mathcal{C}(A)$ are circuits with $c \neq \pm e$ then $\mathrm{supp}(c) \neq \mathrm{supp}(e)$. We denote the set of matroid-circuits of A, that is, the set of supports of circuits in $\mathcal{C}(A)$, by $\mathcal{M}(A) := \{\mathrm{supp}(c) \,:\, c \in \mathcal{C}(A)\}$, and refer to it simply as the *matroid* of A. For instance, for the 1×3 matrix $A := (1 \;\; 2 \;\; 1)$ we have

$$\mathcal{C}(A) \;=\; \pm\{(2,-1,0),(0,-1,2),(1,0,-1)\}\,, \quad \mathcal{M}(A) \;=\; \{\{1,2\},\{2,3\}),\{1,3\}\}\,.$$

We now characterize those matrices A for which $\mathcal{D}^*(A)$ strictly contains $\mathbb{R}^n_+$.

Theorem 4.2 *The dual diagonal Graver cone of every integer $m \times n$ matrix A satisfies $\mathcal{D}^*(A) \supseteq \mathbb{R}^n_+$, and the inclusion is strict if and only if there is $1 \leq k \leq n$ such that $C \cap E \neq \{k\}$ for every two distinct matroid-circuits $C, E \in \mathcal{M}(A)$ of A.*

Proof. We prove the dual statements about the diagonal Graver cone. By definition $\mathcal{D}(A) \subseteq \mathbb{R}^n_+$, and the inclusion is strict if and only if some unit vector $\mathbf{1}_k$ is not in $\mathcal{D}(A)$. Therefore it suffices to prove that, for any $1 \leq k \leq n$, we have $\mathbf{1}_k \in \mathcal{D}(A)$ if and only if there are two distinct matroid-circuits $C, E \in \mathcal{M}(A)$ with $C \cap E = \{k\}$.

Suppose first $C, E \in \mathcal{M}(A)$ are distinct matroid-circuits with $C \cap E = \{k\}$. Then there are $c, e \in \mathcal{C}(A)$ with $c \neq \pm e$ such that $\mathrm{supp}(c) = C$ and $\mathrm{supp}(e) = E$. Replacing e by $-e \in \mathcal{C}(A)$ if necessary we may assume that $c_k e_k > 0$. Then $c \circ e \geq 0$, $c \neq e$, and $c, e \in \mathcal{G}(A)$ imply that $c \circ e = c_k e_k \mathbf{1}_k$ is a generator of $\mathcal{D}(A)$, and hence $\mathbf{1}_k \in \mathcal{D}(A)$. Conversely, suppose $\mathbf{1}_k \in \mathcal{D}(A)$. Because $\mathcal{D}(A) \subseteq \mathbb{R}^n_+$, some nonnegative multiple of $\mathbf{1}_k$ must be one of the generators. So there are $g, h \in \mathcal{G}(A)$ with $g \circ h \geq 0$ and $g \neq h$ such that $g \circ h$ is a nonnegative multiple of $\mathbf{1}_k$, and hence $\mathrm{supp}(g) \cap \mathrm{supp}(h) = \{k\}$. By Lemma 4.1 we have $g = \sum_i \alpha_i c_i$ and $h = \sum_j \alpha_j e_j$ conformal sums of circuits with nonnegative coefficients. Then $\mathrm{supp}(g) = \cup \mathrm{supp}(c_i)$ and $\mathrm{supp}(h) = \cup \mathrm{supp}(e_j)$, and hence there are c_i and e_j among these circuits such

that $\mathrm{supp}(c_i) \cap \mathrm{supp}(e_j) = \{k\}$. Let $C := \mathrm{supp}(c_i)$ and $E := \mathrm{supp}(e_j)$ be the corresponding matroid-circuits of A. It remains to show that C and E are distinct. Suppose indirectly that $C = E$. Then $C = E = C \cap E = \{k\}$. This implies that the k-th column of A is 0 and $c_i = e_j = \pm \mathbf{1}_k$. But then $c_i \sqsubseteq g$ and $e_j \sqsubseteq h$, and therefore $g = c_i = e_j = h$ which is a contradiction. So $C \neq E$, and the proof is complete. □

It is interesting to emphasize that the characterization in Theorem 4.2 is in terms of only the matroid of A, that is, the linear dependency structure on the columns of A. The algorithm of Theorem 1.3 enables to solve in polynomial time the program

$$\min\{\sum_{i=1}^{n} \left(v_i x_i^2 + w_i x_i + a_i\right) \ : \ x \in \mathbb{Z}^n \,,\ Ax = b \,,\ l \leq x \leq u\}$$

for all separable quadratics with $v \in \mathcal{D}^*(A)$ and in particular for all separable convex quadratic functions with $v \in \mathbb{R}^n_+$. So the algorithm can solve the program moreover for some separable nonconvex quadratic functions precisely when the matroid of A satisfies the criterion of Theorem 4.2. Here are some concrete simple examples.

Example 4.3 *Consider again Example 2.5 with $A := 0$ the zero $1 \times n$ matrix having Graver basis $\mathcal{G}(A) = \{\pm \mathbf{1}_i \ : \ i = 1, \ldots, n\}$. Then the set of matroid-circuits of A is $\mathcal{M}(A) = \{\{1\}, \ldots, \{n\}\}$. Therefore $C \cap E = \emptyset$ for all distinct $C, E \in \mathcal{M}(A)$ and the condition of Theorem 4.2 trivially holds, so $\mathcal{D}^*(A) \supsetneq \mathbb{R}^n_+$. In fact, here $\mathcal{D}^*(A) = \mathbb{R}^n$.*

Example 4.4 Directed graphs. *Let G be a directed graph, and let A be its $V \times E$ incidence matrix, with $A_{v,e} := 1$ if vertex v is the head of directed edge e, $A_{v,e} := -1$ if v is the tail of e, and $A_{v,e} := 0$ otherwise. The set $\mathcal{M}(A)$ of matroid-circuits consists precisely of all subsets $C \subseteq E$ that are circuits of the undirected graph underlying G. The set $\mathcal{C}(A)$ of circuits consists of all vectors $c \in \{-1, 0, 1\}^E$ obtained from some matroid circuit $C \subseteq E$ by choosing any of its two orientations and setting $c_e := 1$ if directed edge $e \in C$ agrees with the orientation, $c_e := -1$ if e disagrees, and $c_e := 0$ if $e \notin C$. The Graver basis is equal to the set of circuits, $\mathcal{G}(A) = \mathcal{C}(A)$. By Theorem 4.2 we have $\mathcal{D}^*(A) \supsetneq \mathbb{R}^E_+$ if and only if there is an edge $e \in E$ such that no two distinct circuits C, C' of the underlying undirected graph satisfy $C \cap C' = \{e\}$.*

Example 4.5 Generic Matrices. *Let A be a generic integer $m \times n$ matrix, that is, a matrix for which every set of m columns is linearly independent, say, the matrix defined by $A_{i,j} := j^i$ for all i, j, whose columns are distinct points on the moment curve in $\mathbb{R}^m$. Then the matroid of A is uniform, that is, its matroid-circuits are exactly all $(m+1)$-subsets of $\{1, \ldots, n\}$. Suppose $n \leq 2m$. Then every distinct $C, E \in \mathcal{M}(A)$ satisfy $|C \cap E| \geq 2$, and hence $\mathcal{D}^*(A) \supsetneq \mathbb{R}^n_+$ by Theorem 4.2. So, by Theorem 1.2,*

$$\min\{\sum_{i=1}^{n} \left(v_i x_i^2 + w_i x_i + a_i\right) \ : \ x \in \mathbb{Z}^n \,,\ Ax = b \,,\ l \leq x \leq u\}$$

can be solved in polynomial time for all such A, all $b \in \mathbb{Z}^m$ and $l, u \in \mathbb{Z}^n_\infty$, all convex and some nonconvex separable quadratic functions defined by data $v, w, a \in \mathbb{Z}^n$.

5 Higher degree polynomial functions

The algorithm that underlies our algorithmic Theorem 1.2 using the Graver basis is conceptually quite simple. First, it finds in polynomial time a feasible point. Then it keeps improving points iteratively, as long as possible, where, at each iteration, it takes the best possible improving step attainable along any Graver basis element. It outputs the last point from which no further Graver improvement is possible.

We now proceed to show that the results of the previous sections can be extended to multivariate polynomials of higher, arbitrary, degree. We will define a hierarchy of cones, and whenever a polynomial function will lie in the corresponding cone, the algorithm outlined above will converge to the optimal solution in polynomial time.

It will be convenient now to make more extensive use of tensor notation, and to work with the tensored, nonsymmetrized form of a polynomial function. We use

$$\otimes_d \mathbb{R}^n \ := \mathbb{R}^n \otimes \cdots \otimes \mathbb{R}^n \ , \quad \otimes_d x \ := \ x \otimes \cdots \otimes x \ , \quad x \in \mathbb{R}^n$$

for the d-fold tensor product of $\mathbb{R}^n$ with itself and for the rank-1 tensor that is the d-fold product of a vector x with itself, respectively. Note that the $(i_1, \ldots, i_d)$-th entry of $\otimes_d x$ is the product $x_{i_1} \cdots x_{i_d}$ of the corresponding entries of x. We denote the standard inner product on the tensor space by

$$\langle U, V \rangle \ := \ \sum_{i_1=1}^{n} \cdots \sum_{i_d=1}^{n} U_{i_1,\ldots,i_d} V_{i_1,\ldots,i_d} \ , \qquad U, V \ \in \ \otimes_d \mathbb{R}^n \ .$$

In particular, in the vector space $\mathbb{R}^n$ we have $\langle x, y \rangle = x^{\intercal} y$ and in the matrix space $\mathbb{R}^n \otimes \mathbb{R}^n$ we have $\langle U, V \rangle = U \cdot V$. Note that for any two rank-1 tensors we have

$$\langle x^1 \otimes \cdots \otimes x^d, y^1 \otimes \cdots \otimes y^d \rangle \ = \ \prod_{k=1}^{d} \langle x^k, y^k \rangle \ .$$

For simplicity, we restrict attention to homogeneous polynomials, also termed *forms*. A form $f(x)$ of degree d in the vector of n variables $x = (x_1, \ldots, x_n)$ can be compactly defined by a single tensor $F \in \otimes_d \mathbb{R}^n$ that collects all coefficients, by

$$f(x) \ := \ \langle F, \otimes_d x \rangle \ = \ \sum_{i_1=1}^{n} \cdots \sum_{i_d=1}^{n} F_{i_1,\ldots,i_d} x_{i_1} \cdots x_{i_d} \ .$$

For instance, the form $f(x) = (x_1 + x_2 + x_3)^3$ of degree $d = 3$ in $n = 3$ variables can be written as $f(x) = \langle F, \otimes_3 x \rangle = \langle \otimes_3 \mathbf{1}, \otimes_3 x \rangle = \langle \mathbf{1}, x \rangle^3$ with $\mathbf{1}$ the all-ones vector in $\mathbb{R}^3$ and $F = \otimes_3 \mathbf{1}$ the all-ones tensor in $\otimes_3 \mathbb{R}^3$, with $F_{i_1,i_2,i_3} = 1$ for $i_1, i_2, i_3 = 1, 2, 3$.

Let A be any integer $m \times n$ matrix, and let $\mathcal{G}(A)$ be its Graver basis. For each degree $d \geq 2$ we now define a cone $\mathcal{P}_d(A)$ in the tensor space $\otimes_d \mathbb{R}^n$ as follows.

Definition 5.1 The *Graver cone of degree d* of an integer $m \times n$ matrix A is the cone $\mathcal{P}_d(A) \subseteq \otimes_d \mathbb{R}^n$ generated by the rank-1 tensors $g^1 \otimes \cdots \otimes g^d$ where the g^i are elements of $\mathcal{G}(A)$ that lie in the same orthant and are not all the same, that is

$$\mathcal{P}_d(A) := \text{cone}\{g^1 \otimes \cdots \otimes g^d \ : \ g^i \in \mathcal{G}(A),\ g^i \circ g^j \geq 0 \text{ for all } i, j,\ g^i \neq g^j \text{ for some } i, j\}.$$

The *dual Graver cone of degree d* is its dual $\mathcal{P}_d^*(A)$ in $\otimes_d\mathbb{R}^n$ given by

$$\mathcal{P}_d^*(A) = \{V \in \otimes_d\mathbb{R}^n \ : \ \langle U, V\rangle \geq 0,\ U \in \mathcal{P}_d(A)\} \ = \ \{V \ : \ \langle g^1 \otimes \cdots \otimes g^d, V\rangle \geq 0, \\ g^i \in \mathcal{G}(A),\ g^i \circ g^j \geq 0 \ \text{ for all } i, j,\ g^i \neq g^j \text{ for some } i, j\}.$$

Note that $\mathcal{P}_2(A)$ is the nonsymmetrized version of $\mathcal{Q}(A)$, that is, $\mathcal{Q}(A) = \mathcal{P}_2(A) \cap \mathcal{S}^n$.

One of the key ingredient in extending our algorithmic results to polynomials of arbitrary degree is the following analogue of Lemma 3.2 which establishes the supermodularity of polynomial functions that lie in suitable cones. We need one more piece of terminology. Let $D := \{1, \ldots, d\}$ and for $0 \leq k \leq d$ let $\binom{D}{k}$ be the set of all k-subsets of D. A k-dimensional *subtensor* of a d-dimensional tensor

$$F \ = \ (F_{i_1,\ldots,i_d} \ : \ 1 \leq i_1, \ldots, i_d \leq n) \ \in \ \otimes_d\mathbb{R}^n$$

is any of the $\binom{d}{k}n^{d-k}$ tensors $T \in \otimes_k\mathbb{R}^n$ obtained from F by choosing $I \in \binom{D}{k}$, letting each index i_j with $j \in I$ vary from 1 to n, and fixing each index i_j with $j \notin I$ at some value between 1 and n. For instance, the k-dimensional tensor obtained by choosing $I = \{1, \ldots, k\}$ and fixing some values $1 \leq i_{k+1}, \ldots, i_d \leq n$ is

$$T \ = \ (T_{i_1,\ldots,i_k} := F_{i_1,\ldots,i_k,i_{k+1},\ldots,i_d} \ : \ 1 \leq i_1, \ldots, i_k \leq n) \ \in \ \otimes_k\mathbb{R}^n \ .$$

For an integer $m \times n$ matrix A, let $\mathcal{K}_d(A) \subseteq \otimes_d\mathbb{R}^n$ be the cone of those tensors F such that, for all $2 \leq k \leq d$, every k-dimensional subtensor of F is in $\mathcal{P}_k^*(A)$.

Lemma 5.2 *Let A be integer $m \times n$ matrix. Let $f : \mathbb{R}^n \to \mathbb{R}$ be degree d form given by $f(x) = \langle F, \otimes_d x\rangle$ with $F \in \mathcal{K}_d(A)$. Let $x \in \mathbb{R}^n_+$ be nonnegative and $\sum_{r=1}^t \mu_r g^r$ conformal sum in $\mathbb{R}^n$ with $g^r \in \mathcal{G}(A)$ distinct and $\mu_r \geq 0$ nonnegative scalars. Then*

$$\Delta \ := \ \left(f\left(x + \sum_{r=1}^t \mu_r g^r\right) - f(x)\right) \ - \ \sum_{r=1}^t \left(f\left(x + \mu_r g^r\right) - f(x)\right) \ \geq \ 0.$$

Proof. To simplify the derivation we assume that all $\mu_r = 1$. The same argument goes through in exactly the same way for arbitrary nonnegative μ_r. For $r = 1, \ldots, t$,

$$\begin{aligned} f(x + g^r) - f(x) \ &= \ \langle F, \otimes_d(x + g^r)\rangle - \langle F, \otimes_d x\rangle \\ &= \ \langle F, g^r \otimes x \otimes \cdots \otimes x\rangle \ + \ \cdots \ + \ \langle F, x \otimes \cdots \otimes x \otimes g^r\rangle \\ &+ \ \sum_{k=2}^d \sum \left\{\langle F, u^1 \otimes \cdots \otimes u^d\rangle \ : \ I \in \binom{D}{k},\ u^i = \left\{ \begin{array}{ll} g^r, & i \in I \\ x, & i \notin I \end{array} \right\}\right. . \end{aligned}$$

Similarly,

$$\begin{aligned} f\left(x + \sum_{r=1}^t g^r\right) \ - \ f(x) \ &= \ \left\langle F, \otimes_d\left(x + \sum_{r=1}^t g^r\right)\right\rangle - \langle F, \otimes_d x\rangle \\ &= \ \langle F, \sum_{r=1}^t g^r \otimes x \otimes \cdots \otimes x\rangle \ + \ \cdots \ + \ \langle F, x \otimes \cdots \otimes x \otimes \sum_{r=1}^t g^r\rangle \\ &+ \ \sum_{k=2}^d \sum \left\{\langle F, u^1 \otimes \cdots \otimes u^d\rangle \ : \ I \in \binom{D}{k},\ u^i = \left\{ \begin{array}{ll} \sum_{r=1}^t g^r, & i \in I \\ x, & i \notin I \end{array} \right\}\right. . \end{aligned}$$

Therefore,

$$\Delta \;=\; \sum_{k=2}^{d}\sum\left\{\langle F, u^1\otimes\cdots\otimes u^d\rangle \;-\; \sum_{r=1}^{t}\langle F, v^{r,1}\otimes\cdots\otimes v^{r,d}\rangle \;:\; I\in\binom{D}{k}\right., \tag{16}$$
$$\left. u^i=\left\{\begin{array}{ll}\sum_{r=1}^t g^r, & i\in I\\ x, & i\notin I\end{array}\right.,\; v^{r,i}=\left\{\begin{array}{ll} g^r, & i\in I\\ x, & i\notin I\end{array}\right\}.$$

Now, consider any $2\leq k\leq d$ and any $I\in\binom{D}{k}$. For simplicity of the indexation, we assume that $I=\{1,\ldots,k\}$. The derivation for other I is completely analogous. For each choice of indices $1\leq i_{k+1},\ldots,i_d\leq n$ let $T(i_{k+1},\ldots,i_d)$ be the k-dimensional subtensor of F obtained by letting $i_1,\ldots,i_k$ vary and fixing $i_{k+1},\ldots,i_d$ as chosen. Then the corresponding summand of Δ in the expression (16) above satisfies

$$\left\langle F, \otimes_k\left(\sum_{r=1}^t g^r\right)\otimes(\otimes_{d-k}x)\right\rangle \;-\; \sum_{r=1}^t\langle F,(\otimes_k g^r)\otimes(\otimes_{d-k}x)\rangle \tag{17}$$
$$=\;\sum_{i_{k+1}=1}^n\cdots\sum_{i_d=1}^n x_{i_{k+1}}\cdots x_{i_d}\left\langle T(i_{k+1},\ldots,i_d), \otimes_k\left(\sum_{r=1}^t g^r\right)-\sum_{r=1}^t\otimes_k g^r\right\rangle\;.$$

The summand in (17) above which corresponds to $1\leq i_{k+1},\ldots,i_d\leq n$ satisfies

$$\left\langle T(i_{k+1},\ldots,i_d), \otimes_k\left(\sum_{r=1}^t g^r\right)-\sum_{r=1}^t\otimes_k g^r\right\rangle \;= \tag{18}$$
$$\sum\left\{\langle T(i_{k+1},\ldots,i_d), g^{r_1}\otimes\cdots\otimes g^{r_k}\rangle \;:\; 1\leq r_1,\ldots,r_k\leq t,\;\text{ not all } r_i \text{ the same}\right\}.$$

Now, because all the g^r are in the same orthant, and all k-dimensional subtensors of F lie in the dual Graver cone $\mathcal{P}_k^*(A)$, each summand on the right-hand side of (18) above satisfies $\langle T(i_{k+1},\ldots,i_d), g^{r_1}\otimes\cdots\otimes g^{r_k}\rangle\geq 0$, and so the left-hand side of (18) is nonnegative as well. Because $x\in\mathbb{R}^n_+$ is nonnegative, each summand on the right-hand side of (17) above is nonnegative, and so the left-hand side of (17) is nonnegative as well. Because this holds for all $2\leq k\leq d$ and all $I\in\binom{D}{k}$, we obtain that each summand on the right-hand side of (16) is nonnegative, and so $\Delta\geq 0$ as claimed. □

A second key ingredient is the following analogue of Lemma 3.1 which shows that we can efficiently minimize a given form of any fixed degree d in a given direction.

Lemma 5.3 *For every fixed d, there is an algorithm that, given $l,u\in\mathbb{Z}^n_\infty$, $z,g\in\mathbb{Z}^n$ with $l\leq z\leq u$, and $f(x)=\langle F,\otimes_d x\rangle$ with $F\in\otimes_d\mathbb{Z}^n$, solves in polynomial time*

$$\min\{f(z+\mu g)\;:\;\mu\in\mathbb{Z}_+\,,\; l\leq z+\mu g\leq u\}. \tag{19}$$

Proof. Let $S:=\{\mu\in\mathbb{Z}_+ : l\leq z+\mu g\leq u\}$, and let $s:=\sup S$ which is easy to determine. If $s=\infty$ then we conclude that S is infinite and stop. Otherwise we need to minimize the univariate degree d polynomial $h(\mu):=\langle F,\otimes_d(z+\mu g)\rangle=\sum_{i=0}^d h_i\mu^i$, whose coefficients h_i can be easily computed from F, over $S=\{0,1,\ldots,s\}$.

Outline: use repeated bisections and Sturm's theorem which allows us to count the number of real roots of h in any interval using the Euclidean algorithm on $h(\mu) = \sum_{i=0}^{d} h_i \mu^i$ and its derivative $h'(\mu) = \sum_{i=0}^{d-1} (i+1) h_{i+1} \mu^i$, to find intervals $[r_i, s_i]$, $i = 1, \ldots, d$ (possibly with repetitions if h has multiple roots) containing each real root of h, and such that $s_i - r_i < 1$ for all i. Then minimizing h over S reduces to minimizing h over $S \cap \{0, \lceil r_1 \rceil, \lfloor s_1 \rfloor, \ldots \lceil r_d \rceil, \lfloor s_d \rfloor, s\}$. □

We can now establish our theorem on polynomial integer minimization.

Theorem 1.4 *For every fixed d there is an algorithm that, given integer $m \times n$ matrix A, its Graver basis $\mathcal{G}(A)$, $b \in \mathbb{Z}^m$, and degree d integer homogenous polynomial $f(x) = \langle F, \otimes_d x \rangle$ with $F \in \mathcal{K}_d(A)$, solves in polynomial time the polynomial program*

$$\min\{f(x) = \langle F, \otimes_d x \rangle \ : \ x \in \mathbb{Z}^n \,, \ Ax = b \,, \ x \geq 0\}.$$

Proof. First, use the algorithm of Lemma 3.6 to either detect that the problem is infeasible or that the feasible set is infinite and stop, or obtain a feasible point and continue. Now, apply the algorithm of Lemma 3.5 precisely as it is, using the given form $f(x)$ instead of a quadratic. Lemmas 5.2 and 5.3 now assure that the analysis of this algorithm in the proof of Lemma 3.5 carries through precisely as before, and guarantee that the algorithm will find an optimal solution in polynomial time. □

References

[1] De Loera, J., Hemmecke, R., Onn, S., Rothblum, U.G., Weismantel, R.: Convex integer maximization via Graver bases. *J. Pure App. Alg.* 213:1569–1577, 2009.

[2] De Loera, J., Onn, S.: All linear and integer programs are slim 3-way transportation programs. *SIAM J. Optim.* 17: 806–821, 2006.

[3] Hemmecke, R., Onn, S., Weismantel, R.: A polynomial oracle-time algorithm for convex integer minimization. *Math. Prog.* (to appear).

[4] Onn, S.: Nonlinear Discrete Optimization: An Algorithmic Theory, *Nachdiplom Lectures*, ETH Zürich, pp. 1–143.

[5] Schrijver, A.: "Theory of Linear and Integer Programming," 1986. Wiley.

[6] Sebö, A.: Hilbert bases, Carathéodory's theorem and combinatorial optimization. In: Proc. IPCO 1 - 1st Conference on Integer Programming and Combinatorial Optimization, 431–455, 1990. University of Waterloo Press.

[7] Sturmfels, B.: Gröbner Bases and Convex Polytopes. *Univ. Lec. Ser.* Volume 8, 1996. American Mathematical Society.

Jon Lee
IBM T.J. Watson Research Center, Yorktown Heights, USA
jonlee@us.ibm.com

Shmuel Onn
Technion - Israel Institute of Technology, Haifa, Israel
onn@ie.technion.ac.il

Lyubov Romanchuk
Technion - Israel Institute of Technology, Haifa, Israel
lyuba@techunix.technion.ac.il

Robert Weismantel
ETH, Zürich, Switzerland
robert.weismantel@ifor.math.ethz.ch