Integer matrices that are not copositive have certificates of less than quadratic complexity

Timo Hirscher

May 7, 2014

Abstract

A symmetric matrix $M$ in $\mathbb{R}^{n \times n}$ is called copositive if the corresponding quadratic form $Q(x) = x^T M x$ is non-negative on the closed first orthant $\mathbb{R}_{\geq 0}^n$. If the matrix fails to be copositive there exists some certificate $x \in \mathbb{R}_{\geq 0}^n$ for which the quadratic form is negative. Due to the scaling property $Q(\lambda x) = \lambda^2 Q(x)$ for $\lambda \in \mathbb{R}$, we can find such certificates in every neighborhood of the origin but their properties depend on $M$ of course and are hard to describe. If $M$ is an integer matrix however, we are guaranteed certificates of a complexity that is at most a constant times the binary encoding length of the matrix raised to the power $\frac{3}{2}$.

1 Introduction

Let $M = (m_{ij})_{i,j} \in \mathbb{R}^{n \times n}$ be a symmetric real-valued matrix. As is known $M$ is called positive semi-definite if all its eigenvalues are non-negative or equivalently the corresponding quadratic form is non-negative, i.e. $Q(x) := x^T M x \geq 0$ for all vectors $x \in \mathbb{R}^n$.

$M$ is in turn called copositive if this condition holds true for all vectors with non-negative entries, i.e.

$$x^T M x \geq 0 \text{ for all vectors } x \in \mathbb{R}_{\geq 0}^n.$$  (1)

Obviously, positive semi-definite matrices are copositive, as are all symmetric non-negative matrices, since $m_{ij} \geq 0$ for all $1 \leq i, j \leq n$ implies (1).

However, there are symmetric non-negative matrices, which are not positive semi-definite. Hence copositive matrices are a proper subset of all symmetric matrices (having negative diagonal entries trivially renders copositivity impossible) and a proper superset of the positive semi-definite matrices in $\mathbb{R}^{n \times n}$ for $n \geq 2$. For $n = 1$ positive semi-definiteness and copositivity correspond to non-negativity and are thus equivalent.

$$M := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
has eigenvalues \{-1, 1\} but is non-negative showing that in \(\mathbb{R}^{2 \times 2}\) copositivity is strictly weaker than positive semi-definiteness. Putting \(M\) as upper left corner in an \(n \times n\) zero matrix will establish the same for higher dimensions.

Murty and Kabadi showed that it is an NP-complete problem to decide whether a given symmetric matrix is copositive or not. They actually showed this for integer matrices (see [4]).

2 Finding relatively simple certificates

The main result to be established is the following statement about the complexity of certificates for integer matrices which are not copositive:

**Theorem 2.1**

Let \(M \in \mathbb{Z}^{n \times n}\) be a symmetric integer-valued matrix. If there exists some \(x \in \mathbb{R}_{\geq 0}^n\) such that \(x^T M x < 0\), i.e. a certificate for \(M\) not being copositive, a vector \(y \in \mathbb{R}_{\geq 0}^n\) can be found such that \(y^T M y < 0\) and the binary encoding length of \(y\) is at most \(17\) times that of \(M\) to the power \(\frac{3}{2}\).

On the way to achieve this result a couple of lemmas are needed, some of which were already sketched by Murty and Kabadi.

**Lemma 1**

Given \(M \in \mathbb{R}^{n \times n}\), a symmetric real-valued matrix, let us define the following minimization problem:

\[
\begin{align*}
\text{minimize} & \quad Q(x) = x^T M x \\
\text{subject to} & \quad x \in [0, 1]^n.
\end{align*}
\]  

(2)

For an optimal solution \(\bar{x}\) to (2), there exist vectors \(\bar{y}, \bar{u}, \bar{v} \in \mathbb{R}^n_{\geq 0}\) such that

\[
\begin{bmatrix}
\bar{u} \\
\bar{v}
\end{bmatrix} - \begin{bmatrix}
M & I \\
-I & 0
\end{bmatrix} \cdot \begin{bmatrix}
\bar{x} \\
\bar{y}
\end{bmatrix} = \begin{bmatrix}
0 \\
e
\end{bmatrix}
\quad \text{and}
\]

(3)

\[
\begin{bmatrix}
\bar{u}^T \\
\bar{v}^T
\end{bmatrix} \cdot \begin{bmatrix}
\bar{x} \\
\bar{y}
\end{bmatrix} = 0,
\]

(4)

where \(I\) denotes the \(n \times n\) identity matrix and \(e \in \mathbb{R}^n\) the vector of all ones.

**Proof:** First of all, \([0, 1]^n\) is bounded and closed, hence compact, and the quadratic form \(Q\) a continuous function on \(\mathbb{R}^n\). Therefore it attains its minimum \(\gamma := \min_{x \in [0, 1]^n} Q(x) \in \mathbb{R}\) and (2) has an optimal solution.

Let \(\bar{x} \in [0, 1]^n\) be such that \(Q(\bar{x}) = \gamma\). From quadratic programming, it is known that an optimal solution \(\bar{x}\) to the quadratic problem

\[
\begin{align*}
\text{minimize} & \quad Q(x) = c^T x + \frac{1}{2} x^T D x \\
\text{subject to} & \quad A x \geq b \\
\text{and} & \quad x \in \mathbb{R}^n_{\geq 0},
\end{align*}
\]

(5)
where \( b, c \in \mathbb{R}^n \) and \( A, D \in \mathbb{R}^{n \times n} \), is also an optimal solution to the linear program

\[
\begin{aligned}
\text{minimize} & \quad (c^T + \bar{x}^T D)x \\
\text{subject to} & \quad Ax \geq b \\
\text{and} & \quad x \in \mathbb{R}_{\geq 0}^n.
\end{aligned}
\]

(6)

see for example Thm. 1.12 in [2]. It is easy to check that (2) is equivalent to (5) if we choose \( c = 0 \), \( D = M \), \( A = -I \) and \( b = -e \). Proceeding to the linear program, it is thus equivalent to

\[
\begin{aligned}
\text{maximize} & \quad -\bar{x}^T M x \\
\text{subject to} & \quad -x \geq -e \\
\text{and} & \quad x \in \mathbb{R}_{\geq 0}^n.
\end{aligned}
\]

(7)

consequently having the value \(-\gamma\). Rewritten as cone program, this reads

\[
\begin{aligned}
\text{maximize} & \quad \langle -M \bar{x}, x \rangle \\
\text{subject to} & \quad e - I y + M \bar{x} \in \mathbb{R}_{\geq 0}^n \\
\text{and} & \quad y \in \mathbb{R}_{\geq 0}^n.
\end{aligned}
\]

(8)

Noting that we have interior points, e.g. \( x = \frac{1}{2} e \), and that the cone \( \mathbb{R}_{\geq 0}^n \) is self-dual allows for another transformation. Duality theory tells us that the dual problem

\[
\begin{aligned}
\text{minimize} & \quad \langle e, y \rangle \\
\text{subject to} & \quad I y + M \bar{x} \in \mathbb{R}_{\geq 0}^n \\
\text{and} & \quad y \in \mathbb{R}_{\geq 0}^n.
\end{aligned}
\]

(9)

is also feasible and has the same value \(-\gamma\), see for example Thm. 4.7.1 in [1]. If we denote an optimal solution to the dual problem by \( \bar{y} \) and let \( \bar{u} := \bar{y} + M \bar{x}, \bar{v} := e - \bar{x} \), we have indeed \( \bar{u}, \bar{v}, \bar{x}, \bar{y} \in \mathbb{R}_{\geq 0}^n \),

\[
\begin{aligned}
\left( \bar{u} \quad \bar{v} \right) = \left( \begin{array}{cc}
M & I \\
-I & 0
\end{array} \right) \cdot \left( \begin{array}{c}
\bar{x} \\
\bar{y}
\end{array} \right) = \left( \begin{array}{c}
0 \\
e
\end{array} \right)
\end{aligned}
\]

and

\[
\left( \begin{array}{c}
\bar{u}^T \\
\bar{v}^T
\end{array} \right) \cdot \left( \begin{array}{c}
\bar{x} \\
\bar{y}
\end{array} \right) = \bar{y}^T \bar{x} + \bar{x}^T M \bar{x} + e^T \bar{y} - \bar{x}^T \bar{y} = \gamma - \gamma = 0,
\]

which establishes the claim. \qed

For a system of linear equations in non-negative variables such as

\[
\begin{aligned}
As & = b \\
s & \in \mathbb{R}_{\geq 0}^l
\end{aligned}
\]

(10)

where \( A = (A_1, \ldots, A_l) \in \mathbb{R}^{k \times l} \), \( b \in \mathbb{R}^k \), a vector \( s \in \mathbb{R}^l \) is called a solution if \( As = b \), feasible if \( s \in \mathbb{R}_{\geq 0}^l \) and a basic feasible solution (abbreviated: BFS) if it satisfies (10) and the set of columns \( \{ A_j, s_j > 0 \} \) is linearly independent. Thm. 3.1 in [3] states that the basic feasible solutions are precisely the extreme points of the convex set of feasible solutions.
Lemma 2
Let $M \in \mathbb{R}^{n \times n}$ again be a symmetric real-valued matrix and consider the system of linear equations in non-negative variables

$$A \mathbf{s} = \mathbf{b}, \quad \text{where } A := \begin{pmatrix} -M & -I & I & I \\ -I & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \in \mathbb{R}^{2n \times 4}, \quad \mathbf{b} := \begin{pmatrix} 0 \\ e \end{pmatrix} \in \mathbb{R}^{2n}. \tag{11}$$

Then there exist $\bar{\mathbf{u}}, \bar{\mathbf{v}}, \bar{\mathbf{x}}, \bar{\mathbf{y}} \in \mathbb{R}_{\geq 0}^n$ such that

$$\mathbf{s} := \begin{pmatrix} \bar{\mathbf{x}} \\ \bar{\mathbf{y}} \\ \bar{\mathbf{u}} \\ \bar{\mathbf{v}} \end{pmatrix}$$

is a BFS to (11) and (4) is also satisfied.

**Proof:** First note that being a solution of (11) is equivalent to (3). Furthermore, from (3) and (4) it follows (by multiplying (3) with $(\bar{\mathbf{x}}^T, \bar{\mathbf{y}}^T)$ from the left):

$$-\bar{\mathbf{x}}^T M \bar{\mathbf{x}} = \bar{\mathbf{y}}^T e. \tag{12}$$

With $\bar{\mathbf{x}}^{(0)}$ being an optimal solution to problem (2) and the corresponding vectors $\bar{\mathbf{u}}^{(0)}, \bar{\mathbf{v}}^{(0)}, \bar{\mathbf{y}}^{(0)} \in \mathbb{R}_{\geq 0}^n$ defined as in the foregoing lemma, we know that

$$\mathbf{s}^{(0)} := \begin{pmatrix} \bar{\mathbf{x}}^{(0)} \\ \bar{\mathbf{y}}^{(0)} \\ \bar{\mathbf{u}}^{(0)} \\ \bar{\mathbf{v}}^{(0)} \end{pmatrix}$$

is a solution to (11) which also satisfies (4). However, it is not guaranteed that this is an extreme point in the set of feasible solutions.

If not, we proceed as follows:
Assume $\mathbf{s}^{(0)}$ is no extreme point, then there exist distinct feasible solutions $\mathbf{t}^{(1)}, \mathbf{t}^{(2)}$ and $\alpha \in (0, 1)$ s.t. $\mathbf{s}^{(0)} = \alpha \mathbf{t}^{(1)} + (1 - \alpha) \mathbf{t}^{(2)}$. From (4) and the non-negativity, $\bar{\mathbf{u}}^{(0)}, \bar{\mathbf{v}}^{(0)}, \bar{\mathbf{x}}^{(0)}, \bar{\mathbf{y}}^{(0)} \in \mathbb{R}_{\geq 0}^n$, it follows that only one coordinate in each of the pairs

$$\{(\bar{x}_i^{(0)}, \bar{u}_i^{(0)}), (\bar{y}_i^{(0)}, \bar{v}_i^{(0)}); \ 1 \leq i \leq n\}$$

can be strictly positive. If one writes

$$\mathbf{t}^{(i)} := \begin{pmatrix} \mathbf{x}^{(i)} \\ \mathbf{y}^{(i)} \\ \mathbf{u}^{(i)} \\ \mathbf{v}^{(i)} \end{pmatrix} \text{ for } i = 1, 2,$$

the non-negativity of $\mathbf{t}^{(1)}, \mathbf{t}^{(2)}$ and $\alpha \in (0, 1)$ together imply that $s_j^{(0)} = 0$ forces $t_j^{(1)} = t_j^{(2)} = 0$. Hence the orthogonality relation from (4) also holds for both
Consequently, we get

\[
(\bar{x}^{(0)})^T M \bar{x}^{(0)} = -e^T \bar{y}^{(0)} = \alpha \cdot (\bar{x}^{(1)})^T M \bar{x}^{(1)} + (1 - \alpha) \cdot (\bar{x}^{(2)})^T M \bar{x}^{(2)} \\
\geq (\bar{x}^{(0)})^T M \bar{x}^{(0)}
\]

by optimality of \(\bar{x}^{(0)}\), where the first and third equality follow from the consideration in (12). This implies \((x^{(i)})^T M x^{(i)} = (\bar{x}^{(0)})^T M \bar{x}^{(0)}\), i.e. \(t^{(1)}, t^{(2)}\) also feature optimal solutions to (2) in their first \(n\) coordinates.

Define the line \(l : s(r) = s^{(0)} + r \cdot (t^{(2)} - t^{(1)})\), \(r \in \mathbb{R}\). Linearity guarantees that every

\[
s = \begin{pmatrix} x \\ y \\ u \\ v \end{pmatrix} \in l \cap \mathbb{R}^{4n}_{\geq 0}
\]

is a feasible solution to (11) which also satisfies (4), because \(s_j^{(0)} = 0\) implies \(s_j = 0\). As above, from this we can deduce

\[
x^T M x = -e^T y = -e^T \bar{y}^{(0)} + r \cdot (e^T y^{(2)} + e^T y^{(1)}) = (\bar{x}^{(0)})^T M \bar{x}^{(0)},
\]

i.e. \(x\) is another optimal solution to (2).

Since \(t^{(1)} \neq t^{(2)}\), \(r\) can be chosen in such a way that

\[
s = s^{(0)} + r \cdot (t^{(2)} - t^{(1)}) \in \mathbb{R}^{4n}_{\geq 0}
\]

and there exists some index \(j\) with \(s_j = 0 \neq s_j^{(0)}\).

Use this feasible solution to define \(s^{(1)} := s\). As \(s^{(0)}\) has not more than \(2n\) non-zero coordinates, this procedure (when iterated) must stop, yielding a point \(s^{(k)} \in \mathbb{R}^{4n}_{\geq 0}\) that is an extreme point in the set of feasible solutions to (11). It will also satisfy (4), which in turn implies that \(\bar{x}^{(k)}\) is again optimal for (2). \(\square\)

**Lemma 3**

Let \(M \in \mathbb{Z}^{n \times n}\) now be a symmetric integer-valued matrix. The optimal value in (2) is either 0 (iff \(M\) is copositive) or at most \(-2^{-2L+1}\), where \(L\) denotes the binary encoding length of \(M\).

**Proof:** The statement about a copositive matrix \(M\) follows directly from the definition and \(0^T M 0 = 0\).

In the other case, let

\[
s := \begin{pmatrix} \bar{x} \\ \bar{y} \\ \bar{u} \\ \bar{v} \end{pmatrix}
\]

be as guaranteed by the above lemma, which means among other things that \(\bar{x}\) is optimal for (2). Since \(s = (s_j)_{j=1}^{4n}\) is a BFS to (11), the set \(S := \{A_j, s_j > 0\}\)
of not more than $2n$ columns is linearly independent. The matrix $A$ clearly has rank $2n$, we can thus choose additional columns to get a superset of $S$ which forms a base of $\mathbb{R}^{2n}$. Deleting the unchosen columns in $A$ and corresponding zero entries in $s$ gives an invertible $2n \times 2n$ submatrix $B$ of $A$ and a subvector $\tilde{s} \in \mathbb{R}^{2n}_+$ of $s$ such that $B\tilde{s} = b$. Cramer’s rule applies and gives

$$
\tilde{s}_i = \frac{\det(B_i, b)}{\det B},
$$

where $(B_i, b)$ denotes the matrix in which the $i$th column of $B$ has been replaced by $b$. The fact that all entries in $A$, hence $B$, and $b$ are integers, implies that the determinants in (13) are integers too and $\det B \neq 0$ as $B$ is invertible. Consequently, the non-zero entries of $s$ are at least $|\det B| - 1$ due to non-negativity and $\det(B_i, b) \in \mathbb{Z}$.

To finish off the proof of this lemma, whose final part is essentially a concatenation of ideas from section 15.2 in [3], it is left to show that $|\det B| \leq 2^{2L-1}$, since as in the foregoing lemma, we have $\tilde{x}^T M\tilde{x} = -e^T \tilde{y}$. So in the case of $M$ not being copositive, the left hand side is negative forcing positive entries in $\tilde{y}$, hence $s$ hence $\tilde{s}$. Those are in turn at least $|\det B| - 1$, which by non-negativity of $\tilde{y}$ implies $\tilde{x}^T M\tilde{x} \leq -|\det B|^{-1}$.

First of all, the binary encoding length of the original matrix has to be determined. Clearly, the symmetry allows to encode the upper triangular part only. To store $M$ in the upper triangular part of an $n \times n$ array we need

$$
L := \sum_{1 \leq i \leq j \leq n} \left( \left\lceil \log_2(|m_{ij}| + 1) \right\rceil + 1 \right)
$$

bits, since $\left\lceil \log_2(|m_{ij}| + 1) \right\rceil$ bits are needed to represent $|m_{ij}|$ if larger than 0 and one bit for its sign, just one bit if $m_{ij} = 0$.

Having the form of $A$ in mind (see (11)), we can expand the determinant of the submatrix $B$ with respect to first columns to the right then rows below $M$ in $A$ such that $\det(B) = \pm \det(B')$, where $B'$ is a $l \times l$ submatrix of $M$. If $S_l$ denotes the group of permutations on $\{1, \ldots, l\}$ and $B' = (b_{ij})_{i,j}$, one gets using Leibniz’ formula:

$$
|\det(B')| = \left| \sum_{\sigma \in S_l} (-1)^{\text{sgn}(\sigma)} b_{1, \sigma(1)} \cdots b_{l, \sigma(l)} \right|
\leq \sum_{\sigma \in S_l} |b_{1, \sigma(1)}| \cdots |b_{l, \sigma(l)}| \leq \prod_{i=1}^l (|b_{i1}| + \ldots + |b_{il}|)
\leq \prod_{i=1}^n (|m_{i1}| + \ldots + |m_{in}|) \leq \prod_{1 \leq i,j \leq n} (|m_{ij}| + 1)
\leq 2^{2L-1},
$$

where the last inequality follows directly from the consideration in (14).
Having prepared all those auxiliary results, we can finally proceed to proving the central conclusion.

**Proof (of Thm. 2.1):** To begin with, it is obvious that the complexity of $M$ is at least the number of entries necessary to represent it in an array, i.e.

$$L \geq \#\{(i, j), \ 1 \leq i \leq j \leq n\} = \frac{n(n+1)}{2}, \ \text{thus} \ n \leq \sqrt{2L}.$$  

Let $\bar{x}$ be an optimal solution to (2). By the lemma above, we know that the corresponding value of the quadratic form is $Q(\bar{x}) = \bar{x}^T M \bar{x} \leq -2^{-2L+1}$. Denote by $d := \max_{i,j} |m_{ij}|$ the largest entry of $M$ in terms of absolute value and note that $d \in \mathbb{N}$ since $M$ cannot be the zero matrix. Next, let us define $x^* := 2^{2L-1} \cdot \bar{x}$ and finally the vector $y \in \mathbb{R}^n_{\geq 0}$ by

$$y_j := \frac{1}{4dn^2} \lfloor 4dn^2 \cdot x^*_j \rfloor, \ \text{for} \ 1 \leq j \leq n. \quad (15)$$

Let $\| \cdot \|$ denote the Euclidean norm on $\mathbb{R}^n$. Due to $\bar{x} \in [0, 1]^n$ we get $\|\bar{x}\| \leq \sqrt{n}$, $\|x^*\| \leq 2^{2L-1} \sqrt{n}$ and clearly $L \geq \lceil \log_2(d+1) \rceil \geq \log_2 d$.

Note that $y$ is a non-negative rational vector and since every coordinate consists of an integer part in $\{0, \ldots, 2^{2L-1} \}$ and a fractional part which is given by a numerator and denominator in $\{0, \ldots, 4dn^2\}$, its binary complexity is not larger than

$$n \left( \lceil \log_2(2^{2L-1} + 1) \rceil + 2 \left\lceil \log_2(4dn^2 + 1) \right\rceil \right) \leq n \left( 2L + 2 \left\lceil \log_2(4dn^2 + 1) \right\rceil \right) \leq \sqrt{2L} \left( 2L + 2 \left( 2 + \log_2 d + (\log_2 L + 1) + 1 \right) \right) \leq \sqrt{2L} \cdot 12L \leq 17 L^{3/2}. \quad (16)$$

In the before last line the simple estimate $\log x + 1 \leq x$ for $x \geq 0$ and $L \geq 1$ was used.

Finally, it has to be checked that $Q(y) < 0$. The definitions and estimates from above give:

$$\|y\| \leq \|x^* + \frac{1}{4dn^2} e\| \leq 2^{2L-1} \sqrt{n} + \frac{1}{4dn^2} \sqrt{n} \quad \text{and} \quad \|y - x^*\| \leq \frac{1}{4dn^2} \sqrt{n}.$$ 

Furthermore, the eigenvalues of $M$ are all of absolute value at most $dn$, since for every eigenvector $v = (v_i)_{i=1}^n$ corresponding to eigenvalue $\lambda$ the following holds:

$$|\lambda| = \frac{\max_i |(Mv)_i|}{\max_i |v_i|} = \frac{\max_i \left| \sum_{j=1}^n m_{ij} v_j \right|}{\max_i |v_i|} \leq \frac{\max_i \sum_{j=1}^n d |v_j|}{\max_i |v_i|} \leq dn.$$
Consequently, using these estimates we get:

\[
y^T M y = y^T M(y - \mathbf{x}^*) + y^T M \mathbf{x}^*
\]

\[
\leq y^T M(y - \mathbf{x}^*) + (y - \mathbf{x}^+)^T M \mathbf{x}^* + (\mathbf{x}^+)^T M \mathbf{x}^*
\]

\[
\leq (2^{2L-1} \sqrt{n} + \frac{1}{4dn^{3/2}} + \frac{dn}{4dn^{3/2}} + 2^{2L-1} \sqrt{n} - 2^{-2L+1} \cdot 2^{4L-2})
\]

\[
\leq (2^{2L-1} + \frac{1}{4dn^{3/2}}) \cdot \frac{1}{4} + \frac{1}{4} \cdot 2^{2L-1} - 2^{2L-1}
\]

\[
\leq 2^{2L-1} \left(\frac{1}{4} + \frac{1}{4} - 1\right) < 0,
\]

where the last line follows from $d \geq 1$, $L \geq 1$. \qed

**Remark**

(a) Choosing the discretization of $\mathbf{x}^*$ finer (i.e. with a spacing of $c \leq \frac{1}{4dn^{3/2}}$ in (15)) will make the above estimate only sharper, but at the same time increase the complexity. Choosing $l \in \mathbb{N}$ minimal s.t. $2^l \geq 4dn^2$ and taking $2^{-l}$ as spacing however, allows to write the fractional part of each coordinate as a sum of negative powers of 2, i.e. $\{2^{-1}, \ldots, 2^{-l}\}$ and thus reducing the summand in the estimate for the binary complexity coming from the pair numerator/denominator from $2 \lceil \log_2(4dn^2) + 1 \rceil$ to $l = \lceil \log_2(4dn^2) + 1 \rceil$. This leads to an overall complexity of not more than $10L^{3/2}$.

(b) To evaluate the sharpness of this result, let us consider the following example. Let $k \in \mathbb{N}$,

\[
M := \begin{pmatrix} 2^{2k+2} & -2^{k+2} \\ -2^{k+2} & 3 \end{pmatrix}
\]

and $Q(x) = x^T M x$ be again the corresponding quadratic form. This means for $x = (1, 0)^T$ one gets the value $Q(x) = 2^{2k+2} > 0$ and for $x = (x, 1)^T$ correspondingly $Q(x) = 2^{2k+2}x^2 - 2^{k+3}x + 3 = 4(2^k x - 1)^2 - 1$.

The latter is smaller than 0 if and only if $x \in (\frac{1}{2^{k+3}}, \frac{3}{2^{k+3}})$. Since $Q(\lambda x) = \lambda^2 Q(x)$ for $\lambda \in \mathbb{R}$, this means that the certificates for $M$ not being copositive lie in the shaded area in the picture to the right.

This however implies that if we consider $y = (p, q)^T \in \mathbb{Q}_{\geq 0}$, a certificate with rational entries, either the denominator appearing in $q$ is at least $2^k$ or the product of the integer part of $p$ and the denominator in $q$ is. Either way, the binary complexity of $y$ is at least $k + 1$. Another look at $M$ reveals that the binary encoding length of this matrix is according to (14) precisely

\[
L = (2k + 4) + (k + 3) + 3 = 3k + 10.
\]

Hence every certificate has a complexity which is at least linear in the encoding length of $M$. 

8
(c) Note that the extra factor $L^{1/2}$ in the estimate for the complexity (16) is coming from the size $n$ of the vector. If we fix the dimension, the result attained in Thm. 2.1 actually is that there exists a certificate with complexity at most $n \cdot 12 L$, which is linear in $L$ and hence up to the constant factor tight according to the above example:

Putting the matrix $M$ as the upper left corner of a zero matrix in $\mathbb{R}^{n \times n}$, for $n \geq 2$, will lead to an encoding length of $3k + 10 + \frac{n}{2}(n+1) - 3$, since only the extra zeros in the upper triangular part have to be encoded. With $n$ fixed, the lower bound on the complexity of a certificate (which is $k + 1 + (n - 2)$ by the same reasoning as above) is still linear in the complexity of $M$.

If however $n$, which is known to be at most $\sqrt{2L}$, is not constant, i.e. in $O(L^0)$, but only in $O(L^\delta)$, $\delta \in (0, \frac{1}{2}]$, the established upper bound is superlinear, namely a constant times $L^{1+\delta}$, and it is not clear whether this is tight.

References

[1] Gärtner, B. and Matoušek, J., “Approximation Algorithms and Semidefinite Programming”, Springer, 2012.

[2] Murty, K.G., “Linear Complementarity, Linear and Nonlinear Programming”, Heldermann Verlag, 1988.

[3] Murty, K.G., “Linear Programming”, Wiley, 1983.

[4] Murty, K.G. and Kabadi, S.N., Some NP-complete problems in quadratic and nonlinear programming, Mathematical Programming, Vol. 39, pp 117-129, 1987.

Timo Hirscher
Department of Mathematical Sciences,
Chalmers University of Technology,
412 96 Gothenburg, Sweden.
hirscher@chalmers.se