Michal Černý

Goffin's algorithm for zonotopes

Kybernetika, Vol. 48 (2012), No. 5, 890--906

Persistent URL: http://dml.cz/dmlcz/143088

GOFFIN'S ALGORITHM FOR ZONOTOPES

Michal Černý

The Löwner–John ellipse of a full-dimensional bounded convex set is a circumscribed ellipse with the property that if we shrink it by the factor n (where n is dimension), we obtain an inscribed ellipse. Goffin's algorithm constructs, in polynomial time, a tight approximation of the Löwner–John ellipse of a polyhedron given by facet description. In this text we adapt the algorithm for zonotopes given by generator descriptions. We show that the adapted version works in time polynomial in the size of the generator description (which may be superpolynomially shorter than the facet description).

Keywords: Löwner–John ellipse, zonotope, Goffin's algorithm, ellipsoid method

Classification: 90C57, 52B12, 52B55, 68U05

1. INTRODUCTION

1.1. Basic definitions and notation

If not said otherwise, vectors are understood as columns. The relation $\leqslant$ between vectors is understood componentwise. The symbol $\mathit{diag}(\xi_1, \ldots, \xi_k)$ denotes the diagonal matrix with diagonal entries $\xi_1, \ldots, \xi_k$. The symbol 1 stands for all-one vector and the symbol $I = \mathit{diag}(1)$ stands for the unit matrix. The symbol e_i denotes the ith column of I. The symbol $\|x\|$ denotes the L_2-norm of a vector x.

The symbol $\mathit{vol}(\cdot)$ denotes volume and the symbol $\mathit{dim}(\cdot)$ denotes dimension. We also use other symbols, such as *convexhull* or *linearhull*, in their obvious meanings.

For a natural number k, let $\mathit{size}(k) := \lceil \log_2(k+1) \rceil$ denote the length of its binary representation; clearly it holds $\mathit{size}(k) \approx \log_2 k$. For a rational number $r = \pm\frac{p}{q}$, where p and q are natural numbers (with p possibly zero), we define $\mathit{size}(r) = 1 + \mathit{size}(p) + \mathit{size}(q)$. For a rational matrix A, the symbol $\mathit{size}(A)$ denotes the sum of *size*s of all entries of A. (The *size* of a rational vector is a special case of *size* of a rational matrix.) If $a_1, \ldots, a_\ell$ is a list of objects, then $\mathit{size}(a_1, \ldots, a_\ell) = \sum_{i=1}^{\ell} \mathit{size}(a_i)$.

We will need the observation that "if only few bits are available, then we can write down neither too big nor too small numbers": for a rational number $r > 0$ with $\mathit{size}(r) \leqslant L$ we have

$$2^{-L} \leqslant r \leqslant 2^{L}. \tag{1}$$

Recall that every positive definite matrix E has a unique positive definite *root* $E^{1/2}$.

A positive definite matrix $E \in \mathbb{R}^{n\times n}$ and a point $s \in \mathbb{R}^n$ define an n-dimensional *ellipse*

$$\mathcal{E}(E,s) := \{x : (x-s)^{\mathrm{T}}E^{-1}(x-s) \leqslant 1\} = \{E^{1/2}(x-s) : \|x\| \leqslant 1\}.$$

In particular, the image of $\mathcal{E}(E,0)$ under the mapping $\xi \mapsto E^{-1/2}\xi$ is the unit ball $\mathcal{E}(I,0)$.

Instead of *vol*$(\mathcal{E}(E,s))$ we write *vol*(E) only (as the volume does not depend on s). Recall that in every dimension *vol*(E) is proportional to $\sqrt{\det E}$. More precisely, for every dimension n there is a constant τ_n such that

$$\mathit{vol}(E) = \tau_n \cdot \sqrt{\det E}. \tag{2}$$

Given a polyhedron $\mathcal{P} = \{x : Ax \leqslant b\}$, the tuple (A,b) is called *facet description* of the polyhedron $\mathcal{P}$. If A and b are rational, then we define the *size of the facet description* as *size*(A,b).

1.2. The Löwner–John Theorem

The following theorem is a fundamental result in convex geometry; see [7] (Sect. 3.1), [9] and [11] (Sect. 15.4).

Theorem and Definition 1.1. For every full-dimensional bounded convex set $C \subseteq \mathbb{R}^n$ there is an ellipse $\mathcal{E}(E,s)$ such that

$$\mathcal{E}(\tfrac{1}{n^2}\cdot E, s) \subseteq C \subseteq \mathcal{E}(E,s).$$

That ellipse is called **Löwner–John ellipse** for C.

Observe that the factor n^{-2} is tight: the extremal example is the n-dimensional simplex.

Theorem 1.1 shows that convex sets can be tightly approximated with ellipses. In our context, it is interesting in particular if the approximated set C is a polyhedron. Then we can roughly say that a polyhedron — a convex object which might be complex from the combinatorial point of view — is tightly approximated with a reasonably simple convex object such as an ellipse. This is also the reason why the procedure or replacement of the approximated polyhedron by its approximating ellipse is sometimes referred to as "rounding" of the polyhedron.

The rounding procedure has interesting applications: for example, if the object C itself is too complex to optimize over it, then we can optimize approximately over the simple rounded object. Moreover, as Theorem 1.1 says, we can round both "downwards" and "upwards" and hence (with reasonable objective functions) get both lower and upper bounds on the optimal value.

In general, the Löwner–John ellipse cannot be found algorithmically: for example, it may happen that the matrix E is not rational. Whenever we think of algorithmic methods, we want to find a tight rational approximation. The following definition formalizes the notion of an approximate Löwner–John ellipse; it roughly says that an approximate Löwner–John ellipse is a Löwner–John ellipse up to "a small blowup".

Definition 1.2. Let $\varepsilon > 0$. The ellipse $\mathcal{E}(E, s)$ is called **ε-approximate Löwner–John ellipse** for a convex set C if

$$\mathcal{E}(\tfrac{1}{n^2} \cdot E, s) \subseteq C \subseteq \mathcal{E}((1+\varepsilon) \cdot E, s)$$

holds.

Theorem 1.1 is nonconstructive: it does not offer an algorithm for finding the Löwner–John ellipse (or an approximate Löwner–John ellipse) given (a description of) the set C. Goffin's algorithm [6, 7, 11] is such a method for the case when C is a full-dimensional bounded polyhedron given by a facet description. Goffin's algorithm is of great theoretical importance as it finds the approximate Löwner–John ellipse in polynomial time (i. e., in time polynomial in the size of the facet description of the polyhedron). Therefore, Goffin's algorithm is sometimes called as an effective version of the Löwner–John Theorem for polyhedra.

1.3. Zonotopes

Let $A \subseteq \mathbb{R}^n$ be a set and $x \in \mathbb{R}^n$. We define

$$A \oplus x := \mathit{convexhull}(A \cup (A + x)),$$

where $A + x = \{a + x : a \in A\}$. The operation $\oplus$ is also called (a special case of) the *Minkowski sum*. Instead of $(\cdots((A \oplus x_1) \oplus x_2) \oplus \cdots) \oplus x_n$ we will write $A \oplus x_1 \oplus x_2 \oplus \cdots \oplus x_n$ only.

Definition 1.3. A **zonotope** $\mathcal{Z} := \mathcal{Z}(s; g_1, \ldots, g_m)$ is the set

$$\{s\} \oplus g_1 \oplus \cdots \oplus g_m.$$

The vectors $g_1, \ldots, g_m \in \mathbb{R}^n$ are called **generators** and the vector $s \in \mathbb{R}^n$ is called **shift**. The $(m+1)$-tuple $(s, g_1, \ldots, g_m)$ is called **generator description** of $\mathcal{Z}$.

If the vectors $s, g_1, \ldots, g_m$ are rational, we define the **size** of (the generator description of) the zonotope $\mathcal{Z}$ as

$$\mathit{size}(\mathcal{Z}) := \mathit{size}(s) + \sum_{i=1}^{m} \mathit{size}(g_i).$$

The sequence of zonotopes $\{s\}$, $\{s\} \oplus g_1$, $\{s\} \oplus g_1 \oplus g_2, \ldots$ is called *evolution* of a zonotope. The evolution gives a good geometric insight how a zonotope originates. It follows that a zonotope is indeed a bounded polyhedron.

Observe that $\mathit{dim}(\mathcal{Z})$, the dimension of the zonotope $\mathcal{Z}$, equals to the dimension of the linear space spanned by $g_1, \ldots, g_m$. We say that the zonotope is *full-dimensional* (in $\mathbb{R}^n$) if its dimension is n. Thus:

$$\mathcal{Z} \text{ is full-dimensional iff the generators } g_1, \ldots, g_m \text{ span } \mathbb{R}^n. \tag{3}$$

Zonotopes, given by generator descriptions, are objects of its own interest in polyhedral geometry [1, 8, 14]. They have also interesting applications in combinatorial optimization [5] and in data analysis [4, 10].

1.4. The main theorem and organization of the paper

Goffin's method will be sketched in Section 2. The main aim of this text is to adopt the method for zonotopes. As we have seen, a zonotope $\mathcal{Z}$ is a special kind of a polyhedron. Hence, the basic Goffin's method may be applied to $\mathcal{Z}$ *provided that the facet description of $\mathcal{Z}$ is available.* If we want to apply Goffin's method to a zonotope given by a generator description, we would first need to construct the facet description from the generator description. The problem is that the construction may generally take superpolynomial time. The reason is quite interesting: by [3, 13] (see also [14]) it holds that the sizes of the facet description and the generator description are not polynomially related — there are zonotopes with a superpolynomial number of facets compared to the number of generators. Said otherwise, *generator description may be extremely short* compared to the facet description. Of course, we want to preserve polynomiality (i. e., polynomiality *in the size of the short generator description*); so this obstacle has to be overcome (and not only this one). We will take the advantage of the fact that a polyhedron with a short description can be expected to be, in some sense, "regular" (though the polyhedron may be complex from the combinatorial point of view, e. g. with respect to dimension, the number of facets and vertices). The regularity properties are studied in Section 3. Finally, the adaptation of Goffin's method for zonotopes given by generator descriptions is presented in Section 4.

Our aim is to prove:

Theorem 1.4. For each $\varepsilon > 0$ there is a polynomial-time algorithm that computes the ε-approximate Löwner–John ellipse for a given full-dimensional zonotope represented by a rational generator description.

2. GOFFIN'S ALGORITHM

In this section we sketch the main idea of Goffin's algorithm. All the propositions stated here without proofs can be found in [7, 11]. Let the following data be available:

(i) the facet description (A, b) of a bounded full-dimensional polyhedron $\mathcal{P} = \{x : Ax \leqslant b\} \subseteq \mathbb{R}^n$;

(ii) an ellipse $\mathcal{E}(E_0, s_0)$ such that $\mathcal{P} \subseteq \mathcal{E}(E_0, s_0)$;

(iii) a number μ satisfying $0 < \mu \leqslant vol(\mathcal{P})$.

The item (iii) is not important for description of the algorithm but it is important for the analysis of its convergence; see the inequality (9).

Goffin's algorithm is a form of Khachiyan's Ellipsoid Method with shallow cuts. It constructs a finite sequence of ellipses $\mathcal{E}(E_0, s_0), \mathcal{E}(E_1, s_1), \ldots$ of shrinking volume satisfying

$$\text{if } \mathcal{P} \subseteq \mathcal{E}(E_j, s_j), \text{ then } \mathcal{P} \subseteq \mathcal{E}(E_{j+1}, s_{j+1}). \tag{4}$$

The property (4) together with (ii) implies that every ellipse $\mathcal{E}(E_j, s_j)$ circumscribes $\mathcal{P}$.

Let us describe the work in one iteration. The ellipse $\mathcal{E}(E_j, s_j) \supseteq \mathcal{P}$ is available; we either terminate or construct $\mathcal{E}(E_{j+1}, s_{j+1})$.

By shift we can assume that $s_j = 0$. We apply the transformation $\Phi : \xi \mapsto E_j^{-1/2}\xi$; under this transformation, the ellipse $\mathcal{E}(E_j, s_j = 0)$ is mapped to the unit ball $B = \mathcal{E}(I, 0)$ and the polyhedron $\mathcal{P} = \{x : Ax \leqslant b\}$ is mapped to the polyhedron $\mathcal{P}' = \{x : A'x \leqslant b\}$ with $A' = AE_j^{1/2}$. The situation is depicted in Figure 1.

Now we shrink the unit ball B slightly more than by a factor n, say by a factor $n \cdot \sqrt{1+\varepsilon}$, where $\varepsilon > 0$ is a small number: we set $B' := \mathcal{E}(\frac{1}{n^2(1+\varepsilon)} I, 0)$. Now we test whether

$$B' \subseteq \mathcal{P}'. \tag{5}$$

If the answer is positive, then we terminate — we have found an approximate Löwner–John ellipse. (Indeed, $B' \subseteq \mathcal{P}' \subseteq B$ implies $\mathcal{E}(\frac{1}{n^2(1+\varepsilon)} E_j, 0) = \Phi^{-1}(B') \subseteq \mathcal{P} \subseteq \Phi^{-1}(B) = \mathcal{E}(E_j, 0)$ and we are done: setting $E^* := \frac{1}{1+\varepsilon} E_j$ we have $\mathcal{E}(\frac{1}{n^2} E^*, 0) \subseteq \mathcal{P} \subseteq \mathcal{E}((1+\varepsilon)E^*, 0)$.)

How the test (5) can be performed? We know the facet description (A', b); say that $a_1^{\mathrm{T}} x \leqslant b_1, \ldots, a_k^{\mathrm{T}} x \leqslant b_k$ are the inequalities of the system $A'x \leqslant b$. Assume further that they are normalized in the way that $\|a_1\| = \cdots = \|a_k\| = 1$. Now the situation is easy. We test whether the following condition holds:

$$b_i \geqslant \frac{1}{n \cdot \sqrt{1+\varepsilon}} \quad \text{for all } i = 1, \ldots, k. \tag{6}$$

- If (6) holds, then the test (5) is successful.

  (Proof. Let $x \in B'$. Then $\|x\| \leqslant \frac{1}{n \cdot \sqrt{1+\varepsilon}}$. Using Cauchy–Schwarz inequality $\alpha^{\mathrm{T}}\beta \leqslant \|\alpha\| \cdot \|\beta\|$, for every $i = 1, \ldots k$ we can write $a_i^{\mathrm{T}} x \leqslant \|a_i\| \cdot \|x\| \leqslant 1 \cdot \frac{1}{n \cdot \sqrt{1+\varepsilon}} \leqslant b_i$, which implies that $x \in \mathcal{P}'$.)

- If (6) does not hold, there is an index i_0 such that $b_{i_0} < \frac{1}{n \cdot \sqrt{1+\varepsilon}}$. Then we have found a violated inequality (say, a facet) $a_{i_0}^{\mathrm{T}} x \leqslant b_{i_0}$ of $\mathcal{P}'$ which proves that the test (5) fails. (Indeed, the point $x := \frac{a_{i_0}}{n \cdot \sqrt{1+\varepsilon}}$ satisfies $x \in B'$, but $a_{i_0}^{\mathrm{T}} x = \frac{1}{n \cdot \sqrt{1+\varepsilon}} a_{i_0}^{\mathrm{T}} a_{i_0} = \frac{1}{n \cdot \sqrt{1+\varepsilon}} > b_{i_0}$; the i_0th inequality is violated by some point in B'.)

If the test (5) fails we use the vector a_{i_0} for a cut, called a_{i_0}-*cut*: we construct the smallest-volume ellipse $\mathcal{E}' = \mathcal{E}(E', s')$ containing the set $C := B \cap \{x : a_{i_0}^{\mathrm{T}} x \leqslant \frac{1}{n \cdot \sqrt{1+\varepsilon}}\}$. By the above discussion, it is guaranteed that $\mathcal{P}' \subseteq C \subseteq \mathcal{E}'$. We set $\mathcal{E}(E_{j+1}, s_{j+1}) = \Phi^{-1}(\mathcal{E}')$ and the iteration is finished.

The ellipse $\mathcal{E}'$ can be computed directly: it is of the form

$$s' = -\frac{1 - \frac{1}{\sqrt{1+\varepsilon}}}{n+1} a_{i_0}, \quad E' = \frac{(1+\varepsilon)n^2 - 1}{(1+\varepsilon)(n^2-1)} \cdot \left(I - \frac{2n}{n+1} \cdot \frac{\sqrt{1+\varepsilon} - 1}{n \cdot \sqrt{1+\varepsilon} - 1} a_{i_0} a_{i_0}^{\mathrm{T}} \right). \tag{7}$$

It remains to show how to choose the initial ellipse $\mathcal{E}(E_0, s_0)$, how to choose the lower bound μ on volume, to show that the algorithm terminates and that it terminates in time polynomial in L, where $L := \mathit{size}(A, b)$. We sketch these issues only briefly.

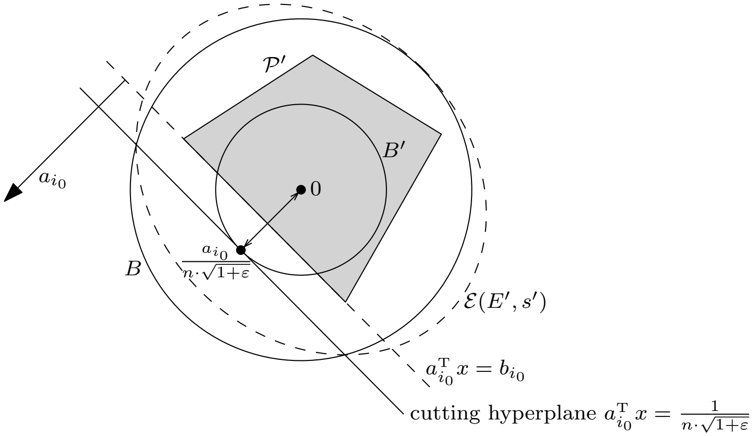
$\mathcal{P}'$
B'
0
a_{i_0}
$\frac{a_{i_0}}{n\cdot\sqrt{1+\varepsilon}}$
B
$\mathcal{E}(E', s')$
$a_{i_0}^{\mathrm{T}} x = b_{i_0}$
cutting hyperplane $a_{i_0}^{\mathrm{T}} x = \frac{1}{n\cdot\sqrt{1+\varepsilon}}$

Fig. 1. The balls B and B', the polyhedron $\mathcal{P}'$, a violated inequality $a_{i_0}^{\mathrm{T}} x \leqslant b_{i_0}$ and the ellipse $\mathcal{E}(E', s')$ resulting from the a_{i_0}-cut.

Choice of the initial ellipse. In the theory of linear programming, there is an important theorem: *there exists a polynomial p_1 such that for every polyhedron $\mathcal{Q}$ with facet description of size L_0, every vertex of $\mathcal{Q}$ has size at most $p_1(L_0)$.* As the polyhedron $\mathcal{P}$ is bounded, it is the convex hull of its vertices, each of which has size at most $p_1(L)$. By (1), a number of size at most $p_1(L)$ can be at most $2^{p_1(L)}$ in absolute value. It follows that $\mathcal{P}$ is contained in the ball $\mathcal{E}(E_0 := n \cdot 2^{2p_1(L)} \cdot I, 0)$.

We can write $\mathit{vol}(E_0) \leqslant (2\sqrt{n} \cdot 2^{p_1(L)})^n \leqslant 2^{n(1+n+p_1(L))}$ (we have used $\sqrt{n} \leqslant 2^n$ in the second inequality).

Choice of the lower bound μ on the volume of $\mathcal{P}$. For the lower bound, a theorem of similar nature holds: *there exists a polynomial p_2 such that for every full-dimensional polyhedron $\mathcal{Q}$ with facet description of size L_0 it holds $\mathit{vol}(\mathcal{Q}) \geqslant 2^{-p_2(L_0)}$.* Hence we can choose $\mu := 2^{-p_2(L)}$.

Convergence. By inspection of the ellipse (7) it can be shown that

$$\textit{for every } \varepsilon > 0 \textit{ there is a constant } \kappa_\varepsilon > 0 \textit{ such that } \frac{\mathit{vol}(E_{j+1})}{\mathrm{vol}(E_j)} \leqslant 2^{-\kappa_\varepsilon/n}. \qquad (8)$$

Remark. This theorem does not hold for $\varepsilon = 0$, which can be easily seen from the equation (7) with $\varepsilon = 0$. This is one of the crucial points why some tolerance ε, though arbitrarily small, is necessary.

We claim that the algorithm terminates after no more than

$$N := \frac{n}{\kappa_\varepsilon} \cdot [n \cdot (1 + n + p_1(L)) + p_2(L) + 1]$$

iterations. (This is, for every fixed $\varepsilon > 0$, a number polynomially bounded in L as $n \leqslant L$.) Suppose otherwise: then we have

$$\begin{aligned} vol(E_N) &\leqslant vol(E_0) \cdot (2^{-\kappa_\varepsilon/n})^N \leqslant 2^{n\cdot(1+n+p_1(L))} \cdot (2^{-\kappa_\varepsilon/n})^N = 2^{n\cdot(1+n+p_1(L))-N\kappa_\varepsilon/n} \\ &= 2^{n\cdot(1+n+p_1(L))-[n\cdot(1+n+p_1(L))+p_2(L)+1]} = \tfrac{1}{2} \cdot 2^{-p_2(L)} = \tfrac{1}{2}\mu < \mu. \end{aligned} \tag{9}$$

But the polyhedron $\mathcal{P}$ of volume $\geqslant \mu$ is contained in $\mathcal{E}(E_N, s_N)$ and hence $vol(E_N) \geqslant \mu$ — contradiction.

Implementation issues. Throughout the presentation of the algorithm, we have freely performed operations which cannot be computed with a Turing machine exactly: in particular, it is the computation of the square root of a positive definite matrix (which is necessary for computation of A', for evaluation of Φ^{-1}) and for the replacement of a vector a by its normalized form $\frac{a}{\|a\|}$. It is a tedious (but achievable) task to show that all necessary matrices, vectors and numbers can be approximated with sufficient precision such that polynomial computation time is preserved and the errors of approximations remain "hidden" within a certain tolerance ε. (This is another crucial point why some tolerance ε must be introduced.)

3. PROPERTIES OF ZONOTOPES

Whenever we say that a zonotope $\mathcal{Z}$ is *given*, we understand that a rational generator description of $\mathcal{Z}$ is given. When we speak about a polynomial-time algorithm, we mean an algorithm working in time polynomial in the size of the given generator description of $\mathcal{Z}$.

In this section we sketch some important properties of zonotopes, which will be useful later, give several definitions and prove several lemmas.

Let a full-dimensional zonotope $\mathcal{Z} = \mathcal{Z}(s; g_1, \dots, g_m)$ be given. The boundary of $\mathcal{Z}$ is denoted $\partial\mathcal{Z}$.

The zonotope $\mathcal{Z}$ is a centrally symmetric set; its center is $\mathcal{Z}_{\text{center}} := s + \frac{1}{2}\sum_{i=1}^m g_i$. (This statement follows from the fact that the operation $\oplus$ preserves central symmetry.)

From now on we shall assume that

$$\mathcal{Z}_{\text{center}} = 0 \tag{10}$$

and

$$\text{if } g \text{ is a generator, then also } -g \text{ is a generator.} \tag{11}$$

These are purely technical, "normalization" requirements.

Comment of (10). Changing the shift s, a zonotope can easily be centered at 0 (which is of no loss of generality for construction of the Löwner–John ellipse).

Comment of (11). If $g_1, \dots, g_M$ is the set of generators, we can replace them with the set of $m := 2M$ generators $\frac{1}{2}g_1, \dots, \frac{1}{2}g_M, -\frac{1}{2}g_1, \dots, -\frac{1}{2}g_M$. Clearly, both generator sets generate (up to a shift) the same zonotope.

Lemma 3.1. There is a matrix $G \in \mathbb{R}^{n\times(m/2)}$ such that $\mathcal{Z} = \{G\alpha : -1 \leqslant \alpha \leqslant 1, \alpha \in \mathbb{R}^{m/2}\}$.

Proof. It is easily seen that for a convex set A it holds

$$A \oplus x = \{a + \alpha x : a \in A, \alpha \in [0,1]\}. \tag{12}$$

Using (11) we can assume that the generators $g_1, \dots, g_m$ are arranged in the list

$$g_1, \quad \dots, \quad g_{m/2}, \quad g_{(m/2)+1} = -g_1, \quad g_{(m/2)+2} = -g_2, \quad \dots, \quad g_m = -g_{m/2}. \tag{13}$$

Let

$$G := (g_1, \dots, g_{m/2}). \tag{14}$$

Now we can write

$$\begin{aligned}
\mathcal{Z} &= \{0\} \oplus g_1 \oplus \dots \oplus g_m \\
&= \left\{ \sum_{i=1}^{m} \alpha_i g_i : \alpha_1 \in [0,1], \cdots, \alpha_m \in [0,1] \right\} \qquad \text{[using (12)]} \\
&= \left\{ \sum_{i=1}^{m/2} \alpha_i g_i - \sum_{i=(m/2)+1}^{m} \alpha_i g_{i-m/2} : \alpha_1 \in [0,1], \cdots, \alpha_m \in [0,1] \right\} \text{[using (13)]} \\
&= \left\{ \sum_{i=1}^{m/2} \alpha_i g_i : \alpha_1 \in [-1,1], \cdots, \alpha_{m/2} \in [-1,1] \right\} \\
&= \left\{ G\alpha : \alpha \in [-1,1]^{m/2} \right\}.
\end{aligned} \tag{15}$$

□

Lemma 3.1 shows that a zonotope can be understood as an image of a high-dimensional cube in a low-dimensional space under a linear mapping.

Lemma 3.2. Let (13) be the set of generators of $\mathcal{Z}$. For every $x \in \mathcal{Z}$ there is a choice of signs $\sigma_1, \dots, \sigma_{m/2} \in \{-1, 1\}$ such that whenever t is a vector fulfilling $t_i \in \{0, \sigma_i\}$ for all $i = 1, \dots, m/2$, then $x + \sum_{i=1}^{m/2} t_i g_i \in \mathcal{Z}$. In particular, for every $x \in \mathcal{Z}$ and every generator g, it holds $x + g \in \mathcal{Z}$ or $x - g \in \mathcal{Z}$.

Proof. Let G be the matrix (14). Then we have $x = Gy$ for some y satisfying $-1 \leqslant y \leqslant 1$. Clearly there is a ±1-vector σ such that $-1 \leqslant y + \sigma \leqslant 1$, and hence also $-1 \leqslant y + t \leqslant 1$. Therefore $x + \sum_{i=1}^{m/2} t_i g_i \in \mathcal{Z}$. □

Zonotopes have also the following interesting structural property: if $\mathcal{Z}$ is a zonotope generated by a set Γ of generators and F is a face of $\mathcal{Z}$, then F is a zonotope generated by some set of generators $\Gamma' \subseteq \Gamma$.

Let F be a k-dimensional face of $\mathcal{Z}$ and let A be its affine hull. A set of linearly independent generators $g'_1, \dots, g'_k$ which form a basis of A is called *basis* of the face F. We write

$$bas(F) = \{g'_1, \dots, g'_k\}.$$

In particular, if F is a vertex then $bas(F) = \emptyset$.

Remark. The basis need not be unique. Whenever we write the expressions like "$\Xi := bas(F)$", we mean that Ξ is *some* basis of F, if more bases exist. (It will be apparent that it is not important which particular basis is chosen, if more bases exist.)

Given a point $x \in \mathcal{Z}$, we define the *degree* of x as

$$deg(x) := \min\{dim(F) : F \text{ is a face of } \mathcal{Z} \text{ containing } x\}.$$

The face F, for which the minimum is attained, is denoted as

$$\mathcal{F}(x).$$

In particular, a point x in the interior of a facet has degree $n-1$, and $\mathcal{F}(x)$ is that facet.

In the proof of the following theorem we use that fact that linear programming is a polynomial-time solvable problem.

Theorem 3.3. Let $\mathcal{Z}$ be a symbol for a zonotope given by rational generators and let x be a symbol for a rational vector.

(a) The relation $x \in \mathcal{Z}$ is polynomial-time decidable.

(b) The relation $x \in \partial\mathcal{Z}$ is polynomial-time decidable.

(c) The number $deg(x)$ is polynomial-time computable.

(d) The set $bas(\mathcal{F}(x))$ is polynomial-time computable.

Proof. Let G be the matrix from Lemma 3.1.

(a) By Lemma 3.1 we have $x \in \mathcal{Z}$ iff the linear system

$$x = G\alpha, \quad -1 \leqslant \alpha \leqslant 1$$

is feasible. This is a linear programming problem.

(b) By (10) we know that $\mathcal{Z}$ is centered at 0. Now we have that $x \in \partial\mathcal{Z}$ iff

$$\max\{\delta : \delta x = G\alpha,\ -1 \leqslant \alpha \leqslant 1\} = 1,$$

which is a linear programming problem.

(c) Given a generator g, set

$$\begin{aligned}\delta_1 &= \max\{\delta : x + \delta g = G\alpha,\ -1 \leqslant \alpha \leqslant 1\},\\ \delta_2 &= \max\{\delta : x - \delta g = G\alpha,\ -1 \leqslant \alpha \leqslant 1\},\\ \delta &= \min\{\delta_1, \delta_2\}.\end{aligned}$$

If $\delta > 0$ we say that the generator g *can move x in both directions.*

Let H be the set of generators which can move x in both directions. Using linear programming, H can be computed in polynomial time. The dimension of $\mathit{linearhull}(H)$ is equal to $\mathit{deg}(x)$.

(d) Let H be as above. Any basis (i. e., maximal linearly independent subset) of H is a basis of $\mathcal{F}(x)$. □

Finally, the following observation will be useful.

Lemma 3.4. Let $x \in \mathcal{Z}$ and $\mathit{deg}(x) < n-1$. Then there is a number γ and a generator g, which can be found in polynomial time, such that $x^* := x + \gamma g$ and x are in the same facet of $\mathcal{Z}$ and $\mathit{deg}(x) < \mathit{deg}(x^*) \leqslant n - 1$.

Proof. By assumption the point x is in some k-dimensional face F, where $n - 1 > k := \mathit{deg}(x)$. There is a facet $F' \supseteq F$. As F' has higher dimension than F, there is a generator g of F' which is linearly independent of $\mathit{bas}(F)$. Denote $\gamma^* = \max\{\gamma' : x + \gamma' g = G\alpha, -1 \leqslant \alpha \leqslant 1\}$, where G is the matrix from Lemma 3.1. We can assume that $\gamma^* > 0$ (otherwise we set $g := -g$ using (11)). Then g and $\gamma = \frac{1}{2}\gamma^*$ fulfill the requirements of the Lemma. We have shown existence.

It remains to show a method to find some g and γ. Let $\gamma > 0$ be a small number. To find g it suffices to find a generator g such that

(i) $g \notin \mathit{linearhull}(\mathit{bas}(\mathcal{F}(x)))$ and

(ii) $x + \gamma g \in \partial\mathcal{Z}$.

By Theorem 3.3, both conditions can be efficiently tested. With γ sufficiently small it is guaranteed by (ii) that x and $x^* := x + \gamma g$ are in the same facet. Moreover, by (11), even the choice $\gamma = 1$ works. As $x^* \in \partial\mathcal{Z}$, we have $\deg(x^*) \leqslant n - 1$. □

The usage of Lemma 3.4 is illustrated in Figure 2. Iterating Lemma 3.4 for at most $n - 1$ times we get the following corollary.

Corollary 3.5. Let $x \in \mathcal{Z}$ be a point of degree $\leqslant n - 1$. Then, a point x^* with the following property can be found in polynomial time: there is a facet F such that $\{x, x^*\} \subseteq F$ and x^* is in the interior of F.

4. ADAPTATION OF GOFFIN'S METHOD FOR ZONOTOPES

First we reformulate the important ingredients of Goffin's method sketched in Section 2 for the case of zonotopes given by generator descriptions. Then, in Section 4.6, we finally summarize the algorithm.

Given a zonotope $\mathcal{Z}$, we use the symbol L for the *size* its generator description.

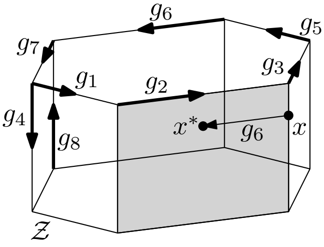

Fig. 2. Illustration of Lemma 3.4. A zonotope $\mathcal{Z} \subseteq \mathbb{R}^3$ with generators $\Gamma := \{g_1, \dots, g_8\}$. The point x can be moved in both directions by g_4 and g_8. By (i), only generators $\Gamma \setminus \{g_4, g_8\}$ are admissible. By (ii), only generators g_3 and g_6 are admissible. The picture shows an example where $x^* = x + g_6$ (which is a point in the interior of the shaded facet).

4.1. Initial ellipse

Let us construct an initial ellipse $\mathcal{E}(E_0, 0) \supseteq \mathcal{Z}$. By Lemma 3.1 the zonotope $\mathcal{Z}$ is the image of the $(m/2)$-dimensional cube $[-1,1]^{m/2}$ under the mapping $\Gamma : \xi \mapsto G\xi$. Consider the ball $K := \mathcal{E}(\frac{m}{2} \cdot I, 0)$ in $\mathbb{R}^{m/2}$; it is the smallest ball circumscribing the cube $[-1,1]^{m/2}$. Then, $\Gamma(K)$ is an ellipse in $\mathbb{R}^n$ circumscribing $\Gamma([-1,1]^{m/2}) = \mathcal{Z}$. We set

$$\mathcal{E}(E_0, 0) := \Gamma(K) = \mathcal{E}(\tfrac{m}{2} \cdot GG^{\mathrm{T}}, 0).$$

The last expression shows that the matrix E_0 can be computed in time polynomial in L.

In the proof of convergence of the algorithm we will also need an estimate on $\mathit{vol}(E_0)$. We have

$$\mathit{vol}(E_0) \leqslant 2^n \cdot \sqrt{\det E_0} \leqslant 2^n \cdot \det E_0$$

assuming, without loss of generality, that $\det E_0 \geqslant 1$. The number $\det E_0$ can be computed with a polynomial time algorithm; it follows that $\mathit{size}(\det E_0) \leqslant p_0(L)$ for some polynomial p_0, and hence $\det E_0 \leqslant 2^{p_0(L)}$ by (1). Setting $p_1(L) := n + p_0(L)$ we have

$$\mathit{vol}(E_0) \leqslant 2^n \cdot \det E_0 \leqslant 2^{n+p_0(L)} = 2^{p_1(L)}.$$

We have shown the following lemma.

Lemma 4.1. There exists a polynomial p_1 such that $\mathit{vol}(E_0) \leqslant 2^{p_1(L)}$.

Remark. This is not the only possible choice of the initial ellipse. As the computation time depends on the volume of the initial ellipse, it might be also reasonable to try other choices.

We know that $\mathcal{Z} = \left\{G\alpha : \alpha \in [-1,1]^{m/2}\right\}$, where $G = (g_1, \dots, g_{m/2})$. Let G_{ij} be the (i,j)th entry of the matrix G. We can write

$$\mathcal{E}_0 := \mathcal{E}(n \cdot \mathit{diag}(\beta_1^2, \dots, \beta_n^2), 0) \supseteq B \supseteq \mathcal{Z},$$

where $\beta_i = \sum_{j=1}^{m/2} |G_{ij}|$ and B is the "rectangle" $[-\beta_1, \beta_1] \times \cdots \times [-\beta_n, \beta_n]$. Hence $\mathcal{E}_0$ can be used as the initial ellipse as well.

4.2. Lower bound on volume

As the zonotope $\mathcal{Z}$ is full-dimensional, we can choose $j_1, \ldots, j_n$ such that the generators $g_{j_1}, \ldots, g_{j_n}$ are linearly independent. Setting $G := (g_{j_1}, \ldots, g_{j_n})$ we have $\mathit{vol}(\mathcal{Z}) \geqslant |\det G| > 0$. As the positive number $|\det G|$ can be computed by a polynomial time algorithm, we have $\mathit{size}(|\det G|) \leqslant p_2(L)$ with some polynomial p_2. Hence

$$\mathit{vol}(\mathcal{Z}) \geqslant |\det G| \geqslant 2^{-p_2(L)}$$

using (1).

Lemma 4.2. There exists a polynomial p_2 such that $\mathit{vol}(\mathcal{Z}) \geqslant 2^{-p_2(L)}$.

4.3. Parallel cuts

We take the advantage of the fact that a zonotope is a centrally symmetric body centered at zero. Central symmetry implies that whenever we know that $\mathcal{Z} \subseteq \{x : c^{\mathrm{T}}x \leqslant \gamma\}$, then also $\mathcal{Z} \subseteq \{x : c^{\mathrm{T}}x \geqslant -\gamma\}$. It follows that instead of (7) we can use the following type of cuts, called *parallel cuts*. The lemma comes from [2] (and can be easily proved by geometry); see also [7], where it has been used for a more general class of centrally symmetric polyhedra.

Lemma and Definition 4.3. Let c be a vector satisfying $\|c\| = 1$, let $B = \mathcal{E}(I, 0)$ be the n-dimensional unit ball and let $\gamma \in (0, \frac{1}{\sqrt{n}})$. The smallest-volume n-dimensional ellipse containing the set $B \cap \{x : -\gamma \leqslant c^{\mathrm{T}}x \leqslant \gamma\}$ is the ellipse $\mathcal{E}(E, 0)$ with

$$E = \frac{n(1-\gamma^2)}{n-1}\left(I - \frac{1-n\gamma^2}{1-\gamma^2} \cdot cc^{\mathrm{T}}\right). \tag{16}$$

We say that E **results from** B **with a cut** (c, γ).

We will also need an analogy of the property (8).

Lemma 4.4. Let $\varepsilon > 0$. Then there exists a constant $\kappa_\varepsilon \in (0,1)$, depending only on ε, such that the following holds: whenever a vector c satisfying $\|c\| = 1$ is given and the ellipse $\mathcal{E}(E, 0)$ results from the unit ball B with a cut $(c, \gamma := \frac{1}{\sqrt{n(1+\varepsilon)}})$, then $\mathit{vol}(E) \leqslant \kappa_\varepsilon \cdot \mathit{vol}(B)$.

Proof. By rotation, which does not change volume, we can assume $c = e_1$. Then the formula (16) is in the simple form

$$E = \frac{n}{n-1}\left(1 - \frac{1}{n(1+\varepsilon)}\right)\left(I - \frac{1-\frac{1}{1+\varepsilon}}{1-\frac{1}{n(1+\varepsilon)}} e_1 e_1^{\mathrm{T}}\right)$$
$$= \begin{pmatrix} \frac{1}{1+\varepsilon} & 0 & \cdots & 0 \\ 0 & 1 + \frac{\varepsilon}{1+\varepsilon} \cdot \frac{1}{n-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 + \frac{\varepsilon}{1+\varepsilon} \cdot \frac{1}{n-1} \end{pmatrix}.$$

We have used equalities $\frac{n}{n-1}(1-\frac{1}{n(1+\varepsilon)})\left(1-\frac{1-\frac{1}{1+\varepsilon}}{1-\frac{1}{n(1+\varepsilon)}}\right)=\frac{1}{1+\varepsilon}$ and $\frac{n}{n-1}(1-\frac{1}{n(1+\varepsilon)})=1+\frac{\varepsilon}{1+\varepsilon}\cdot\frac{1}{n-1}$, which are verified easily using elementary algebra.

By (2) we have $\frac{vol(E)}{vol(B)}=\sqrt{\frac{\det E}{\det I}}=\sqrt{\det E}$. It remains to show that $\sqrt{\det E}$ can be bounded by a constant $\kappa_\varepsilon<1$. As the matrix E is diagonal, we have

$$\begin{aligned}\sqrt{\det E}&=\frac{1}{\sqrt{1+\varepsilon}}\cdot\left(1+\frac{\varepsilon}{1+\varepsilon}\cdot\frac{1}{n-1}\right)^{(n-1)/2}\\ &=\left(1+\frac{1}{\sqrt{1+\varepsilon}}-1\right)\cdot\left(1+\frac{\varepsilon}{1+\varepsilon}\cdot\frac{1}{n-1}\right)^{(n-1)/2}\\ &\overset{(\star)}{\leqslant}\exp\left(\frac{1}{\sqrt{1+\varepsilon}}-1+\frac{n-1}{2}\cdot\frac{\varepsilon}{1+\varepsilon}\cdot\frac{1}{n-1}\right)\\ &=\exp\left(\frac{1}{\sqrt{1+\varepsilon}}+\frac{1}{2}\cdot\frac{\varepsilon}{1+\varepsilon}-1\right)=:\kappa_\varepsilon.\end{aligned}$$

In the inequality $(\star)$ we have used $1+\xi\leqslant e^\xi$ with $\xi=\frac{1}{\sqrt{1+\varepsilon}}-1$ and with $\xi=\frac{\varepsilon}{1+\varepsilon}\cdot\frac{1}{n-1}$.

It remains to show that $\kappa_\varepsilon<1$. By elementary algebraic manipulations we observe that $\frac{1}{\sqrt{1+\varepsilon}}+\frac{1}{2}\cdot\frac{\varepsilon}{1+\varepsilon}<1$ iff $2\sqrt{1+\varepsilon}+\varepsilon<2+2\varepsilon$ iff $2\sqrt{1+\varepsilon}<2+\varepsilon$ iff $4(1+\varepsilon)<4+4\varepsilon+\varepsilon^2$ iff $\varepsilon^2>0$. □

4.4. Testing whether $\mathcal{Z}$ contains a ball

The next crucial step is the test (5). In Section 2 we could perform the test easily using the fact that the facet description of the polyhedron under consideration was available. However, now we cannot lean on that description.

At the moment we cannot design a polynomial-time algorithm for testing whether a given zonotope $\mathcal{Z}$, centered at zero, satisfies $K_\gamma\subseteq\mathcal{Z}$, where $K_\gamma=\mathcal{E}(\gamma^2\cdot I,0)$ is a ball with radius γ.

Problem. Let T be the problem "given a rational generator description of a full-dimensional zonotope $\mathcal{Z}$ centered at zero and a rational number $\gamma>0$, does $K_\gamma\subseteq\mathcal{Z}$ hold?". The problem is in *co-**NP***, but we do not have a conjecture whether or not it is *co-**NP***-complete. (To see $T\in$ *co-**NP***, consider the case $K_\gamma\not\subseteq\mathcal{Z}$. Then there is a facet F of $\mathcal{Z}$ intersecting the interior of K_γ. The set *bas*(F) can be taken as the witness of the fact $K_\gamma\not\subseteq\mathcal{Z}$.)

If the problem T is *co-**NP***-complete, it seems to be a serious obstacle. We overcome it for a certain price: we construct a smaller inscribed ellipse (see (18)). This "loss" will be discussed in detail in Section 5.

With Theorem 3.3(a) we can use essentially the same trick as in [7]: instead of testing $K_\gamma\subseteq\mathcal{Z}$ we test whether

$$\gamma e_i\in\mathcal{Z}\quad\text{for all } i=1,\dots,n. \tag{17}$$

If the test is successful (for all $i=1,\dots,n$), by central symmetry we know that all the points $\pm\gamma e_1,\dots,\pm\gamma e_n$ are in $\mathcal{Z}$; then also

$$\mathcal{Z}\supseteq \mathit{convexhull}\{\pm\gamma e_i: i=1,\dots,n\}\supseteq\mathcal{E}(\tfrac{\gamma^2}{n},0). \tag{18}$$

(Observe that *convexhull*$\{\pm\gamma e_i : i = 1, \ldots, n\}$ is the dual of the n-dimensional cube.) We will perform the test with $\gamma = \frac{1}{\sqrt{n(1+\varepsilon)}}$. Then:

(a) if the test (17) is successful, we have $\mathcal{E}(\frac{1}{n^2(1+\varepsilon)} I, 0) \subseteq \mathcal{Z}$;

(b) if the test (17) is unsuccessful, we know an index i_0 such that $\frac{1}{\sqrt{n(1+\varepsilon)}} \cdot e_{i_0} \notin \mathcal{Z}$.

4.5. The separation algorithm

If the test (17) is unsuccessful, by statement (b) of the previous section we know a point $x_0 = \frac{1}{\sqrt{n(1+\varepsilon)}} \cdot e_{i_0}$ on the boundary of the ball $B' := \mathcal{E}(\frac{1}{\sqrt{n(1+\varepsilon)}} \cdot I, 0)$ satisfying $x_0 \notin \mathcal{Z}$. Then we would like to perform a parallel a-cut of the unit ball $B = \mathcal{E}(I, 0)$ with some suitable a. In Section 2 we selected a as the normal vector of the found violated inequality — but this is not possible here because the facet description of $\mathcal{Z}$ is not available.

We will construct a single inequality $a^{\mathrm{T}}x \leqslant b$ such that $\mathcal{Z} \subseteq \{x : a^{\mathrm{T}}x \leqslant b\}$ and $x_0 \notin \{x : a^{\mathrm{T}}x \leqslant b\}$. Moreover, we will construct a and b such that $\{x : a^{\mathrm{T}}x = b\} \cap \mathcal{Z}$ is a facet of $\mathcal{Z}$.

The inequality $a^{\mathrm{T}}x \leqslant b$ is called a *separator* (of x_0 from $\mathcal{Z}$). We can use the vector a for the (parallel) a-cut.

In general, an algorithm for construction of a is called *separation algorithm*, or, in the terminology of [7], a *separation oracle.*

Let G be the matrix from Lemma 3.1. Recall that we assume that the zonotope $\mathcal{Z}$ is centered at zero.

Step 1. We set $\beta^* := \max\{\beta \in \mathbb{R} : \ \beta x_0 = G\alpha, \ -1 \leqslant \alpha \leqslant 1\}$ (using linear programming). It follows that $x^* := \beta^* x_0 \in \partial\mathcal{Z}$; hence, $\mathit{deg}(x^*) \leqslant n - 1$. Now our aim is to find (some) facet of $\mathcal{Z}$ containing x^*.

Step 2. If $\mathit{deg}(x^*) < n - 1$, we replace x^* by a point of degree $n - 1$ using Corollary 3.5.

Step 3. We compute $\{h_1, \ldots, h_{n-1}\} = \mathit{bas}(\mathcal{F}(x^*))$. Clearly, the affine hull of the facet $\mathcal{F}(x^*)$ is the separator of x_0 from $\mathcal{Z}$.

Step 4. We find a vector orthogonal to $h_1, \ldots, h_{n-1}$: set $H := (h_1, \ldots, h_{n-1})$ and define $a := (I - H(H^{\mathrm{T}}H)^{-1}H^{\mathrm{T}})x_0$. The vector a is the output of the algorithm.

By the theory of Section 3, all tests and operations can be performed in polynomial time.

Remark. Observe that we constructed the separator without using the Yudin-Nemirovski Theorem [12], see also Sect. 4.3 of [7].

4.6. The algorithm

All the necessary ingredients have been prepared. Let $\varepsilon > 0$ be fixed. Let a generator description of a full-dimensional zonotope $\mathcal{Z}$ be given.

Remark. Observe that by (3), an incorrect input — a zonotope which is not full-dimensional — can be easily detected. If a zonotope is not full-dimensional, it is easy to apply a projection of the zonotope into a lower-dimensional space, where the zonotope is full-dimensional. Then we can run the algorithm in that space.

At the beginning of the algorithm we choose the initial ellipse $\mathcal{E}(E_0, 0) \supseteq \mathcal{Z}$ as described in Section 4.1.

Let us describe the work in one iteration. We have $\mathcal{E}(E_j, 0) \supseteq \mathcal{Z}$ from the previous iteration; we either terminate or construct E_{j+1}. We apply the mapping $\Phi : \xi \mapsto E_j^{-1/2}\xi$ under which the ellipse $\mathcal{E}(E_j, 0)$ is projected to the unit ball $\mathcal{E}(I, 0)$ and the zonotope $\mathcal{Z}$ generated by $g_1, \dots, g_m$ is projected to a zonotope $\mathcal{Z}'$ generated by $\Phi(g_1), \dots, \Phi(g_m)$.

We set

$$\gamma := \frac{1}{\sqrt{n(1+\varepsilon)}}$$

and we perform the test (17) with γ and $\mathcal{Z}'$. If the test passes, we can terminate — by (18) we know that

$$\mathcal{E}(\tfrac{1}{n^2(1+\varepsilon)} I, 0) \subseteq \mathcal{Z}' \subseteq \mathcal{E}(I, 0),$$

and hence

$$\mathcal{E}(\tfrac{1}{n^2(1+\varepsilon)} E_j, 0) \subseteq \mathcal{Z} \subseteq \mathcal{E}(E_j, 0).$$

It follows that $\mathcal{E}(\frac{1}{1+\varepsilon} E_j, 0)$ is the ε-approximate Löwner–John ellipse for $\mathcal{Z}$.

If the test (17) with γ and $\mathcal{Z}'$ fails, we determine the vector a using the separation algorithm of Section 4.5 and perform a cut ($c := \frac{a}{\|a\|}, \gamma$) using Lemma 4.3. We get a matrix E from that Lemma. We set $E_{j+1} := \Phi^{-1}(E)$ and the iteration is finished.

The mapping Φ does not change ratios of volumes of ellipses; hence we have

$$\frac{vol(E_{j+1})}{vol(E_j)} = \frac{vol(E)}{vol(I)} \leqslant \kappa_\varepsilon < 1, \tag{19}$$

where κ_ε is the constant of Lemma 4.4.

Recall that L is the size of the generator description of $\mathcal{Z}$. We claim that the algorithm terminates after no more than

$$N := -\frac{1}{\log_2 \kappa_\varepsilon}(1 + p_1(L) + p_2(L))$$

iterations, where p_1 is the polynomial of Lemma 4.1 and p_2 is the polynomial of Lemma 4.2. Assume that we have reached Nth iteration. Then, using (19),

$$\begin{aligned} vol(E_N) &\leqslant vol(E_0) \cdot \kappa_\varepsilon^N \leqslant 2^{p_1(L)} \cdot \kappa_\varepsilon^N = 2^{p_1(L) + N \log_2 \kappa_\varepsilon} \\ &= 2^{p_1(L) - \frac{1}{\log_2 \kappa_\varepsilon} \cdot (p_1(L) + p_2(L) + 1) \log_2 \kappa_\varepsilon} = \tfrac{1}{2} \cdot 2^{-p_2(L)} < 2^{-p_2(L)}. \end{aligned}$$

But the zonotope $\mathcal{Z}$ of volume $\geqslant 2^{-p_2(L)}$ (using Lemma 4.2) is contained in $\mathcal{E}(E_N, 0)$ and hence $vol(E_N) \geqslant 2^{-p_2(L)}$ — contradiction.

5. CONCLUSION

The basic question is whether the statement of Theorem 1.4 can be improved. In Section 4.4 we have lost a factor of n (or, in terms of lengths of semiaxes, a factor $\sqrt{n}$) not being able to test whether a given zonotope contains a ball. If that test could be implemented, then we could strengthen the result and find an approximation of the form $\mathcal{E}(\frac{1}{n}E, 0) \subseteq \mathcal{Z} \subseteq \mathcal{E}((1+\varepsilon)E, 0)$. This does not contradict Theorem 1.1: Theorem 1.1 talks about a general convex set C, where the factor n^{-2} is necessary, but there exists a result — known as Jordan's Theorem — that for a centrally symmetric set (not only a zonotope) that factor can be improved to n^{-1}. The problem of Section 4.4 is important to understand whether we could achieve a better factor than n^{-2} with a Goffin-like method or not. Also the test (17) could be possibly improved to get a larger inscribed ball than the ball in (18).

We formulated Theorem 1.4 for any *fixed* $\varepsilon > 0$. Clearly, the degree of the polynomial bounding the running time of the algorithm depends on ε. It is worth considering whether some adaptive strategy of changing ε inside the work of the algorithm could bring some (say, at least practical) improvement. Of course, the problem is that $\kappa_\varepsilon \to 1$ very fast with $\varepsilon \to 0$.

Also deeper parallel cuts can improve the performance of the algorithm (at least practically). And finally, a good choice of the initial ellipse is also an important factor.

ACKNOWLEDGMENT

The author's work was partially supported by Grant No. P403/12/1947 of the Czech Science Foundation. The author was also partially supported by Project No. F4/18/2011 of I.G.A. of University of Economics, Prague.

(Received September 4, 2011)

REFERENCES

[1] D. Avis and K. Fukuda: Reverse search for enumeration. Disc. Appl. Math. *65* (1996), 21–46.

[2] R. G. Bland, D. Goldfarb, and M. J. Todd: The ellipsoid method: a survey. Oper. Res. *29* (1981), 1039–1091.

[3] R. C. Buck: Partion of space. Amer. Math. Monthly *50* (1943), 541–544.

[4] M. Černý, J. Antoch, and M. Hladík: On the Possibilistic Approach to Linear Regression Models Involving Uncertain, Indeterminate or Interval Data. Technical Report, Department of Econometrics, University of Economics, Prague 2011. `http://nb.vse.cz/~cernym/plr.pdf`.

[5] J.-A. Ferrez, K. Fukuda, and T. Liebling: Solving the fixed rank convex quadratic maximization in binary variables by a parallel zonotope construction algorithm. Europ. J. Oper. Res. *166* (2005), 35–50.

[6] J.-L. Goffin: Variable metric relaxation methods. Part II: The ellipsoid method. Math. Programming *30* (1984), 147–162.

[7] M. Grötschel, L. Lovász, and A. Schrijver: Geometric Algorithms and Combinatorial Optimization. Springer Verlag, Berlin 1993.

[8] L. J. Guibas, A. Nguyen, and L. Zhang: Zonotopes as bounding volumes. In: Proc. Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms, SIAM, Pennsylvania 2003, pp. 803–812.

[9] F. John: Extremum problems with inequalities as subsidiary conditions. In: Fritz John, Collected Papers (J. Moser, ed.), Volume 2. Birkhäuser, Boston 1985, pp. 543–560.

[10] S. Schön and H. Kutterer: Using zonotopes for overestimation-free interval least-squares — some geodetic applications. Reliable Computing *11* (2005), 137–155.

[11] A. Schrijver: Theory of Linear and Integer Programming. Wiley, New York 2000.

[12] D. B. Yudin and A. S. Nemirovski: Informational complexity and efficient methods for the solution of convex extremal problems. Matekon *13 (3)* (1977), 25–45.

[13] T. Zaslavsky: Facing up to arrangements: face-count formulas for partitions of space by hyperplanes. Mem. Amer. Math. Soc. *154* (1975), 102 pp.

[14] G. Ziegler: Lectures on Polytopes. Springer Verlag, Berlin 2004.

Michal Černý, Department of Econometrics, University of Economics, Prague, Winston Churchill Square 4, 130 67 Praha 3. Czech Republic.
e-mail: cernym@vse.cz