Goffin’s Algorithm for Zonotopes

Michal Černý

Abstract. The Löwner-John ellipse of a full-dimensional bounded convex set is a circumscribed ellipse with the property that if we shrink it by a 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).

AMS Classification. 90C57, 52B12, 52B55, 68U05.

Keywords. Löwner-John ellipse; zonotope; Goffin’s algorithm; ellipsoid method

1 Introduction

1.1 Basic definitions and notation

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

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

For a natural number $k$, let $\text{size}(k)$ denote the length of its binary representation; clearly it holds $\text{size}(k) \approx \log_2 k$. For a rational number $r = \pm \frac{p}{q}$, where $p$ and $q$ are natural numbers (with $p$ possibly zero), we define $\text{size}(r) = 1 + \text{size}(p) + \text{size}(q)$. For a rational matrix $A$, the symbol $\text{size}(A)$ denotes the sum of $\text{size}$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 $\text{size}(a_1, \ldots, a_\ell) = \sum_{i=1}^\ell \text{size}(a_i)$. 

1Department of Econometrics, University of Economics, Prague; Náměstí Winstona Churchilla 4, CZ13067 Prague 3, Czech Republic. cernym@vse.cz.
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 \( \text{size}(r) \leq L \) we have
\[
2^{-L} \leq r \leq 2^L. \tag{1}
\]

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
\[
\mathcal{E}(E, s) := \{ x : (x - s)^T E^{-1} (x - s) \leq 1 \} = \{ E^{1/2} (x - s) : \|x\| \leq 1 \}.
\]
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 \( \text{vol}(\mathcal{E}(E, s)) \) we write \( \text{vol}(E) \) only (as the volume does not depend on \( s \)). Recall that in every dimension \( \text{vol}(E) \) is proportional to \( \sqrt{\det E} \). More precisely, for every dimension \( n \) there is a constant \( \tau_n \) such that
\[
\text{vol}(E) = \tau_n \cdot \sqrt{\det E}. \tag{2}
\]

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

### 1.2 The Löwner-John Theorem

The following theorem is a fundamental result in convex geometry.

**Theorem and Definition 1.** For each full-dimensional bounded convex set \( C \subseteq \mathbb{R}^n \) there is an ellipse \( \mathcal{E}(E, s) \) such that
\[
\mathcal{E}(\frac{1}{n^2} \cdot E, s) \subseteq C \subseteq \mathcal{E}(E, s).
\]
That ellipse is called \textbf{Löwner-John ellipse} for \( C \). \( \square \)

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

Theorem 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 combinatorially complex convex object—a polyhedron—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 referred to as “rounding” of the polyhedron.

The rounding procedure has important 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 the Theorem 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 2.** Let $\varepsilon > 0$. The ellipse $\mathcal{E}(E, s)$ is called $\varepsilon$-approximate Löwner-John ellipse for a convex set $C$ if

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

holds.

Theorem 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 $C$. The Goffin’s algorithm [6] is such a method for the case when $C$ is a full-dimensional bounded polyhedron given by a facet description. The 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, the 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

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

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

**Definition 3.** A **zonotope** $Z := Z(s; g_1, \ldots, g_m)$ is the set

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

The vectors $g_1, \ldots, g_m$ are called **generators** and the vector $s$ is called **shift**. The $(m+1)$-tuple $(s, g_1, \ldots, g_m)$ is called **generator description** of $Z$.

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

$$\text{size}(Z) := \text{size}(s) + \sum_{i=1}^{m} \text{size}(g_i).$$
The sequence of zonotopes \( \{s\}, \{s\} \oplus g_1, \{s\} \oplus g_1 \oplus g_2, \ldots \) is called \textit{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 \( \dim(Z) \), the dimension of the zonotope \( Z \), equals to the dimension of the linear space spanned by \( g_1, \ldots, g_m \). We say that the zonotope is \textit{full-dimensional} (in \( \mathbb{R}^n \)) if its dimension is \( n \). Thus:

\[ Z \text{ is full-dimensional iff the generators } g_1, \ldots, g_m \text{ span } \mathbb{R}^n. \] (3)

Zonotopes, given by generator descriptions, are objects of its own interest in polyhedral geometry \([1, 8, 12]\). They have also important applications in combinatorial optimization \([5]\) and in statistics \([4, 9]\).

1.4 The main theorem and organization of the paper

The 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 \( Z \) is a special kind of a polyhedron. Hence, the basic Goffin’s method may be applied to \( Z \) provided that the facet description of \( Z \) is available. If we want to apply the 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 \([3, 11]\) (see also \([12]\)) 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, \textit{generator description may be extremely short} compared to the facet description. Of course, we want to preserve polynomiality (i.e., polynomiality \textit{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 the Goffin’s method for zonotopes given by generator descriptions is presented in Section 4.

Our aim is to prove:

\begin{theorem}
For each \( \varepsilon > 0 \) there is a polynomial-time algorithm that computes the \( \varepsilon \)-approximate Löwner-John ellipse for a given full-dimensional zonotope represented by a rational generator description.
\end{theorem}

\[ \square \]

2 The Goffin’s algorithm

In this section we sketch the main idea of the Goffin’s algorithm. All the propositions stated here without proofs can be found in \([7, 10]\). Let the following data be available:
(i) the facet description $(A, b)$ of a bounded full-dimensional polyhedron $P = \{ x : Ax \leq b \}$;

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

(iii) a number $\mu$ satisfying $0 < \mu < vol(P)$.

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

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

$$\text{if } P \subseteq E(E_i, s_i), \text{ then } P \subseteq E(E_{i+1}, s_{i+1}). \quad (4)$$

The property (4) together with (ii) implies that every ellipse $E(E_i, s_i)$ circumscribes $P$.

Let us describe the work in one iteration. The ellipse $E(E_i, s_i) \supseteq P$ is available; we either terminate or construct $E(P_{i+1}, s_{i+1})$.

By shift we can assume that $s_i = 0$. We apply the transformation $\Phi : \xi \mapsto B_i^{-1/2} \xi$; under this transformation, the ellipse $E(E_i, s_i = 0)$ is mapped to the unit ball $B = E(I, 0)$ and the polyhedron $P = \{ x : Ax \leq b \}$ is mapped to the polyhedron $P' = \{ x : A'x \leq b' \}$ with $A' = AE_i^{1/2}$. 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 $n \cdot \sqrt{1 + \epsilon}$, where $\epsilon > 0$ is a small number: we set $B' := E(\frac{1}{n^{2(1+\epsilon)}} I, 0)$. Now we test whether

$$B' \subseteq P'. \quad (5)$$

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

How the test (5) can be performed? We know the facet description $(A', b)$; say that $a_i^T x \leq b_1, \ldots, a_k^T x \leq b_k$ are the inequalities of the system $A'x \leq b$. Assume further that they are normalized in a way that $\|a_1\| = \cdots = \|a_k\| = 1$.

Now the situation is easy. We test whether the following condition holds:

$$b_i \geq \frac{1}{n \cdot \sqrt{1 + \epsilon}} \text{ for all } i = 1, \ldots, k. \quad (6)$$

- If (6) holds, then the test (5) is successful. (Proof. Let $x \in B'$. Then $\|x\| \leq \frac{1}{n \cdot \sqrt{1 + \epsilon}}$. Using the Cauchy-Schwarz inequality $a_i^T \beta \leq \|a_i\| \cdot \|\beta\|$, for every $i = 1, \ldots, k$ we can write $a_i^T x \leq \|a_i\| \cdot \|x\| \leq 1 \cdot \frac{1}{n \cdot \sqrt{1 + \epsilon}} \leq b_i$, which implies that $x \in P'$.)

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

If the test (5) fails we use the vector \( a_i \) for a cut, called \( a_i \)-cut: we construct the smallest-volume ellipse \( E' = E(E', s') \) containing the set \( C := B \cap \{ x : a_i^T x \leq \frac{1}{n \sqrt{1 + \varepsilon}} \} \). By the above discussion, it is guaranteed that \( P' \subseteq C \subseteq E' \).

We set \( E(E_i + 1, s_i + 1) = \Phi^{-1}(E') \) and the iteration is finished.

The ellipse \( E' \) can be computed directly: it is of the form

\[
s' = -\frac{1}{n + 1} a_i, \quad E' = \frac{(1 + \varepsilon)n^2 - 1}{(1 + \varepsilon)(n^2 - 1)} \left( I - \frac{2n}{n + 1} \cdot \frac{\sqrt{1 + \varepsilon} - 1}{n \cdot \sqrt{1 + \varepsilon} - 1} a a^T \right).
\]

(7)

![Figure 1: The balls \( B \) and \( B' \), the polyhedron \( P' \), a violated inequality \( a_i^T x \leq b_i \) and the ellipse \( E(E', s') \) resulting from the \( a_i \)-cut.](image)

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

**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 \( Q \) with facet description of size \( L_0 \), every vertex of \( Q \) has size at most \( p_1(L_0) \). By (1), a number of size at most \( p_1(L_0) \) can be at most \( 2^{p_1(L_0)} \) in absolute value. As the polyhedron \( \mathcal{P} \) is bounded, it is the convex hull of its vertices, each of which has size at most \( p_1(L) \). It follows that \( \mathcal{P} \) is contained in the ball \( E(E_0 := n \cdot 2^{2p_1(L)} \cdot I, 0) \).

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

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

**Convergence.** By inspection of the ellipse (7) it can be shown that for every \(\varepsilon > 0\) there is a constant \(\kappa_\varepsilon \in (0, 1)\) such that \(\frac{\text{vol}(E_{i+1})}{\text{vol}(E_i)} \leq \kappa_\varepsilon\). (8)

This shows that, indeed, the ellipsoids are shrinking exponentially fast. (Moreover, 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 \(\varepsilon\), though arbitrarily small, is necessary.)

We claim that the algorithm terminates after no more than

\[ N := -\frac{1}{\log_2 \kappa_\varepsilon} \cdot \left[ n \cdot \left(1 + n + p_1(L)\right) + p_2(L) + 1 \right] \]

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

\[ \text{vol}(E_N) \leq \text{vol}(E_0) \cdot \kappa_\varepsilon^N \leq 2^{n \cdot (1 + n + p_1(L)) + p_2(L) + 1} \cdot \kappa_\varepsilon = 2^{n \cdot (1 + n + p_1(L)) + N \log_2 \kappa_\varepsilon} \]

\[ = \frac{n}{2} \cdot 2^{-p_2(L)} = \frac{1}{2} \mu < \mu. \]

But the polyhedron \(P\) of volume \(\geq \mu\) is contained in \(E(E_N, s_N)\) and hence \(\text{vol}(E_N) \geq \mu\) — 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 a square root of a positive definite matrix (which is necessary for computation of \(A'\) and for evaluation of \(\Phi^{-1}\)) and 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 \(\varepsilon\). (This is another crucial point why some tolerance \(\varepsilon\) must be introduced.)

3 Properties of zonotopes

Whenever we say that a zonotope \(Z\) is *given*, we understand that a rational generator description of \(Z\) 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 \(Z\).

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 \(Z = Z(s; g_1, \ldots, g_m)\) be given. The boundary of \(Z\) is denoted \(\tilde{Z}\).
The zonotope $Z$ is a centrally symmetric set; its center is $Z^c := s + \frac{1}{2} \sum_{i=1}^m g_i$. (This statement follows from the fact that the operation $\oplus$ preserves central symmetry.)

From now on we shall assume that

\[ Z^c = 0 \]  \hspace{1cm} (10)

and

\[ \text{if } g \text{ is a generator, then also } -g \text{ is a generator.} \]  \hspace{1cm} (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 $g_1, \ldots, g_m$ is the set of generators, we can replace them with the set of $2m$ generators $\frac{1}{2} g_1, \ldots, \frac{1}{2} g_m, -\frac{1}{2} g_1, \ldots, -\frac{1}{2} g_m$. Clearly, both generator sets generate (up to a shift) the same zonotope.

**Lemma 5.** There is a matrix $G$ such that $Z = \{ G\alpha : -1 \leq \alpha \leq 1 \}$.

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

\[ A \oplus x = \{ a + \alpha x : a \in A, \alpha \in [0,1] \}. \]  \hspace{1cm} (12)

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

\[ g_1, \ldots, \frac{m}{2}, g_{(m/2)+1} = -g_1, g_{(m/2)+2} = -g_2, \ldots, g_m = -g_{m/2}. \]  \hspace{1cm} (13)

Let

\[ G := (g_1, \ldots, g_{m/2}). \]  \hspace{1cm} (14)

Now we can write

\[ Z = \{ 0 \} \oplus g_1 \oplus \cdots \oplus g_m \]

\[ \overset{(12)}{=} \left\{ \sum_{i=1}^m \alpha_i g_i : \alpha_1 \in [0,1], \ldots, \alpha_m \in [0,1] \right\} \]

\[ \overset{(13)}{=} \left\{ \sum_{i=1}^{m/2} \alpha_i g_i - \sum_{i=(m/2)+1}^m \alpha_i g_{i-m/2} : \alpha_1 \in [0,1], \ldots, \alpha_m \in [0,1] \right\} \]

\[ \overset{(15)}{=} \left\{ \sum_{i=1}^{m/2} \alpha_i g_i : \alpha_1 \in [-1,1], \ldots, \alpha_{m/2} \in [-1,1] \right\} \]

\[ = \left\{ G\alpha : \alpha \in [-1,1]^{m/2} \right\}. \]

Lemma 5 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 6. Let (13) be the set of generators of $Z$. For every $x \in Z$ there is a choice of signs $s_1, \ldots, s_{m/2} \in \{-1, 1\}$ such that whenever $t$ is a vector fulfilling $t_i \in \{0, s_i\}$ for all $i = 1, \ldots, m/2$, then $x + \sum_{i=1}^{m/2} t_i g_i \in Z$. In particular, for every $x \in Z$ and every generator $g$, it holds $x + g \in Z$ or $x - g \in Z$.

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

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

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

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

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

Given a point $x \in Z$, we define the degree of $x$ as

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

The face $F$, for which the minimum is attained, is denoted as $F(x)$.

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

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

**Theorem 7.** Let $Z$ be given and let $x$ be a symbol for a rational vector.

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

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

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

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

**Proof.** Let $G$ be the matrix from Lemma 5.

(a) By Lemma 5 we have $x \in Z$ if the linear system

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

is feasible. This is a linear programming problem.
(b) By (10) we know that $Z$ is centered at 0. Now we have that $x \in Z$ iff
\[
\max \{ \delta : \delta x = G\alpha, \ -1 \leq \alpha \leq 1 \} = 1,
\]
which is a linear programming problem.

(c) Given a generator $g$, set
\[
\delta_1 = \max \{ \delta : x + \delta g = G\alpha, \ -1 \leq \alpha \leq 1 \},
\]
\[
\delta_2 = \max \{ \delta : x - \delta g = G\alpha, \ -1 \leq \alpha \leq 1 \},
\]
\[
\delta = \min \{ \delta_1, \delta_2 \}.
\]
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 $\text{linearhull}(H)$ is equal to $\deg(x)$.

(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 8.** Let $x \in Z$ and $\deg(x) < n - 1$. Then there is a number $\gamma$ 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 $Z$ and $\deg(x) < \deg(x^*) \leq n - 1$.

**Proof.** By assumption the point $x$ is in some $k$-dimensional face $F$, where $n - 1 > k := \deg(x)$. 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 $\text{bas}(F)$. Denote $\gamma^* = \max \{ \gamma' : x + \gamma' g = G\alpha, \ -1 \leq \alpha \leq 1 \}$, where $G$ is the matrix from Lemma 5. 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 $\gamma$. Let $\gamma > 0$ be a small number. To find $g$ it suffices to find a generator $g$ such that

(i) $g \not\in \text{linearhull}(\text{bas}(\mathcal{F}(x)))$ and

(ii) $x + \gamma g \in Z$.

By Theorem 7, both conditions can be efficiently tested. With $\gamma$ 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 $x^* \in Z$, we have $\deg(x^*) \leq n - 1$.

The usage of Lemma 8 is illustrated in Figure 2. Iterating Lemma 8 for at most $n - 1$ times we get the following corollary.

**Corollary 9.** Let $x \in Z$ be a point of degree $\leq n - 1$. Then, a point $x^*$ in the interior of a facet containing both $x$ and $x^*$ can be found in polynomial time.
Figure 2: Illustration of Lemma 8. A zonotope $Z \subseteq \mathbb{R}^3$ with generators $\Gamma := \{g_1, \ldots, g_8\}$. The point $x$ can be moved in both directions by $g_1$ and $g_5$. By (i), only generators $\Gamma \setminus \{g_1, g_5\}$ 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 Adaptation of the Goffin’s method for zonotopes

First we reformulate the important ingredients of the 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 $Z$, we use the symbol $L$ for the size of its generator description.

4.1 The initial ellipse

Let us construct an initial ellipse $\mathcal{E}(E_0, 0) \supseteq Z$. By Lemma 5 the zonotope $Z$ 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 $\Gamma([-1, 1]^{m/2}) = Z$. We set

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

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 $\text{vol}(E_0)$. We have

$$\text{vol}(E_0) \leq 2^n \cdot \sqrt{\det E_0} \leq 2^n \cdot \det E_0$$

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

$$\text{vol}(E_0) \leq 2^n \cdot \det E_0 \leq 2^{n+p_0(L)} = 2^{p_1(L)}.$$
Lemma 10. There exists a polynomial $p_1$ such that $\text{vol}(E_0) \leq 2^{p_1(L)}$. 

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

$$E_0 := E(n \cdot \text{diag}(\beta_1^2, \ldots, \beta_n^2), 0) \supseteq B \supseteq Z,$$

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 $E_0$ can be used as the initial ellipse as well.

4.2 The lower bound on volume

As the zonotope $Z$ 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 $\text{vol}(Z) \geq |\det G| > 0$. As the positive number $|\det G|$ can be computed by a polynomial time algorithm, we have $\text{size}(|\det G|) \leq p_2(L)$ with some polynomial $p_2$. Hence

$$\text{vol}(Z) \geq |\det G| \geq 2^{-p_2(L)}$$

using (1).

Lemma 11. There exists a polynomial $p_2$ such that $\text{vol}(Z) \geq 2^{-p_2(L)}$. 

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 $Z \subseteq \{x : c^T x \leq \gamma\}$, then also $Z \subseteq \{x : c^T x \geq -\gamma\}$. 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 12. Let $c$ be a vector satisfying $\|c\| = 1$, let $B = E(I, 0)$ be an $n$-dimensional unit ball and let $\gamma \in (0, \frac{1}{\sqrt{n}})$. The smallest-volume $n$-dimensional ellipse containing the set $B \cap \{x : -\gamma \leq c^T x \leq \gamma\}$ is the ellipse $E(E, 0)$ with

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

(16)

We say that $E$ results from $B$ with a cut $(c, \gamma)$. 

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

Lemma 13. Let $\varepsilon > 0$. Then there exists a constant $\kappa_\varepsilon \in (0, 1)$, depending only on $\varepsilon$, such that the following holds: whenever a vector $c$ satisfying $\|c\| = 1$
is given and the ellipse $E(E, 0)$ results from the unit ball $B$ with a cut $(e, \gamma := \frac{1}{\sqrt{n(1+\varepsilon)}})$, then $\text{vol}(E) \leq \kappa_{\varepsilon} \cdot \text{vol}(B)$.

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

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

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

By (2) we have $\text{vol}(E) \cdot \text{vol}(B) = \sqrt{\det E \cdot \det I} = \sqrt{\det E}$. 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

$$\sqrt{\det E} = \frac{1}{\sqrt{1+\varepsilon}} \cdot \left( 1 + \frac{\varepsilon}{1+\varepsilon} \cdot \frac{1}{n-1} \right)^{(n-1)/2}$$

$$\leq \exp \left( \frac{1}{\sqrt{1+\varepsilon}} \cdot \left( 1 + \frac{\varepsilon}{1+\varepsilon} \cdot \frac{1}{n-1} \right) \right)^{(n-1)/2}$$

$$\leq \exp \left( \frac{1}{\sqrt{1+\varepsilon}} + \frac{\varepsilon}{2} \cdot \frac{1}{1+\varepsilon} - 1 \right) =: \kappa_{\varepsilon} .$$

In the inequality $(\ast)$ we have used $1 + \xi \leq e^{\xi}$ with $\xi = \frac{1}{\sqrt{1+\varepsilon}} - 1$ and with $\xi = \frac{\varepsilon}{2} \cdot \frac{1}{1+\varepsilon}$. It remains to show that $\kappa_{\varepsilon} < 1$. By elementary algebraic manipulations we observe that $\sqrt{1+\varepsilon} + \frac{\varepsilon}{2} \cdot \frac{1}{1+\varepsilon} < 1$ if $2\sqrt{1+\varepsilon} + \varepsilon < 2 + 2\varepsilon$ if $2\sqrt{1+\varepsilon} < 2 + \varepsilon$ if $4(1+\varepsilon) < 4 + 4\varepsilon + \varepsilon^2$ if $\varepsilon^2 > 0$.

**4.4 Testing whether $Z$ contains a large 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 $Z$, centered at zero, satisfies $K_\gamma \subseteq Z$, where $K_\gamma = E(\gamma^2 \cdot I, 0)$ is a ball with radius $\gamma$. 

13
Research problem. Let $T$ be the problem “given a rational generator description of a full-dimensional zonotope $Z$ centered at zero, does $K_1 \subseteq Z$ hold?”. We conjecture that the problem $T$ is co-NP-complete. The complement of $T$ seems to be in NP: the fact $K_1 \not\subseteq Z$ can be witnessed by a point $x$ satisfying $\|x\|^2 \leq 1$ and $x \not\in Z$. The former fact is verified in polynomial time easily; the latter fact can be verified in polynomial time by Theorem 7(a).

If the conjecture is right, 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 7(a) we can use essentially the same simple trick as in [7]: instead of testing $K_\gamma \subseteq Z$ we test whether \[ \gamma e_i \in Z \quad \text{for all } i = 1, \ldots, n. \] (17)

If the test is successful (for all $i = 1, \ldots, n$), by central symmetry we know that all the points $\pm \gamma e_1, \ldots, \pm \gamma e_n$ are in $Z$; then also \[ Z \supseteq \text{convexhull}\{\pm \gamma e_i : i = 1, \ldots, n\} \supseteq \mathcal{E}(\frac{\gamma^2}{n}, 0). \] (18)

(Observe that convexhull(\{\pm \gamma e_i : i = 1, \ldots, n\} is the dual of an $n$-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 $\mathcal{E}(\frac{1}{n(1+\varepsilon)} I, 0) \subseteq Z$;

(b) if the test (17) is unsuccessful, we know an index $i_0$ such that $\frac{1}{\sqrt{n(1+\varepsilon)}} e_{i_0} \not\in Z$.

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 $B' := \mathcal{E}(\frac{1}{\sqrt{n(1+\varepsilon)}} I, 0)$ satisfying $x_0 \not\in Z$. 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 $Z$ is not available.

We will construct a single inequality $a^T x \leq b$ such that $Z \subseteq \{x : a^T x \leq b\}$ and $x_0 \not\in \{x : a^T x \leq b\}$. Moreover, we will construct $a$ and $b$ such that $\{x : a^T x = b\} \cap Z$ is a facet of $Z$.

The inequality $a^T x \leq b$ is called a separator (of $x_0$ from $Z$). We can use the separator $a$ 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 5. Recall that we assume that the zonotope $Z$ is centered at zero.
Step 1. We set $\beta^* := \max\{\beta \in \mathbb{R} : \beta x_0 = Ga, \ -1 \leq \alpha \leq 1\}$ (using linear programming). It follows that $x^* := \beta^* x_0 \in \mathbb{Z}$; hence, $\deg(x^*) \leq n - 1$. Now our aim is to find (some) facet of $Z$ containing $x^*$.

Step 2. If $\deg(x^*) < n - 1$, we replace $x^*$ by a point of degree $n - 1$ using Corollary 9.

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

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

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 $Z$ be given. (Observe that by (3), an incorrect input — a zonotope which is not full-dimensional — can be easily detected.)

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

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

We set
$$
\gamma := \frac{1}{\sqrt{n(1 + \varepsilon)}}
$$
and we perform the test (17) with $\gamma$ and $Z'$. If the test passes, we can finish — by (18) we know that
$$
\mathcal{E}(\frac{1}{n(1 + \varepsilon)}I, 0) \subseteq Z' \subseteq \mathcal{E}(I, 0),
$$
and hence
$$
\mathcal{E}(\frac{1}{n(1 + \varepsilon)}E_i, 0) \subseteq Z \subseteq \mathcal{E}(E_i, 0).
$$
It follows that $\mathcal{E}(\frac{1}{n(1 + \varepsilon)}E_i, 0)$ is the $\varepsilon$-approximate Löwner-John ellipse for $Z$.

If the test (17) with $\gamma$ and $Z'$ fails, we determine the vector $a$ using the separation algorithm of Section 4.5 and perform a cut $(a, \gamma)$ using Lemma 12. We get a matrix $E$ from that Lemma. We set $E_{i+1} := \Phi^{-1}(E)$ and the iteration is done. We know that $Z \subseteq \mathcal{E}(E_{i+1}, 0)$.
The mapping $\Phi$ does not change ratios of volumes of ellipses; hence we have
\[ \frac{\text{vol}(E_{i+1})}{\text{vol}(E_i)} = \frac{\text{vol}(E)}{\text{vol}(I)} \leq \kappa_\varepsilon < 1, \quad (19) \]
where $\kappa_\varepsilon$ is the constant of Lemma 13.

Recall that $L$ be the size of the generator description of $Z$. 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 10 and $p_2$ is the polynomial of Lemma 11. Assume that we have reached $N$-th iteration. Then, using (19),
\[ \text{vol}(E_N) \leq \text{vol}(E_0) \cdot \kappa_\varepsilon^N \leq 2^{p_1(L)} \cdot \kappa_\varepsilon^N = 2^{p_1(L)+N \log_2 \kappa_\varepsilon^2} = 2^{\frac{1}{2} (p_1(L)+p_2(L)+1) \log_2 \kappa_\varepsilon} \leq \frac{1}{2} \cdot 2^{-p_2(L)} < 2^{-p_2(L)}. \]

But the zonotope $Z$ of volume $\geq 2^{-p_2(L)}$ (using Lemma 11) is contained in $E(E_N, 0)$ and hence $\text{vol}(E_N) \geq 2^{-p_2(L)}$ — contradiction.

5 Conclusion

The basic question is whether the statement of Theorem 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 large ball. If that test could be implemented, then we could strengthen the theorem and find an ellipse satisfying $E(\frac{1}{n} E_1, 0) \subseteq Z \subseteq E((1 + \varepsilon) E_1, 0)$. This does not contradict Theorem 1: Theorem 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 conjecture of Section 4.4 is important to understand whether we could reach 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 4 for any fixed $\varepsilon > 0$. Clearly, the degree of the polynomial bounding the running time of the algorithm depends on $\varepsilon$. It is worth considering whether some adaptive strategy of changing $\varepsilon$ inside the work of the algorithm could bring some (say, at least practical) improvement. Of course, the problem is that $\kappa_\varepsilon \to 1$ 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 supported by the Internal Grant Agency of University of Economics, Prague.
References


