Lexicographical polytopes

Michele Barbato, Roland Grappe *, Mathieu Lacroix, Clément Pira

Université Paris 13, Sorbonne Paris Cité, LIPN, CNRS, (UMR7030), F-93430, Villetaneuse, France

A R T I C L E   I N F O

Article history:
Received 30 March 2015
Received in revised form 4 April 2017
Accepted 19 April 2017
Available online xxxx

Keywords:
Lexicographical polytopes
Polyhedral description
Superdecreasing knapsacks

A B S T R A C T

Within a fixed integer box of $\mathbb{R}^n$, lexicographical polytopes are the convex hulls of the integer points that are lexicographically between two given integer points. We provide their descriptions by means of linear inequalities.

© 2017 Elsevier B.V. All rights reserved.

Throughout, $\ell, u, r, s$ will denote integer points satisfying $\ell \leq r \leq u$ and $\ell \leq s \leq u$, that is $r$ and $s$ are within $[\ell, u]$. A point $x \in \mathbb{Z}^n$ is lexicographically smaller than $y \in \mathbb{Z}^n$, denoted by $x \prec y$, if $x = y$ or the first nonzero coordinate of $y - x$ is positive. We write $x < y$ if $x \prec y$ and $x \neq y$. The lexicographical polytope $P^\ell_s r u$ is the convex hull of the integer points within $[\ell, u]$ that are lexicographically between $r$ and $s$:

$$P^\ell_s r u = \text{conv} \{ x \in \mathbb{Z}^n : \ell \leq x \leq u, r \prec x \leq s \}.$$

The top-lexicographical polytope $P^\ell_s u$ is the special case when $r = \ell$. Similarly, the bottom-lexicographical polytope $P^\ell_s u$ is $\text{conv} \{ x \in \mathbb{Z}^n : \ell \leq x \leq u, r \preceq x \leq s \}$.

Given $a, u \in \mathbb{R}^n_+$ and $b \in \mathbb{R}_+$, the knapsack polytope defined by $K^a_u b = \text{conv} \{ x \in \mathbb{Z}^n : 0 \leq x \leq u, ax \leq b \}$ is superdecreasing if:

$$\sum_{i=k}^n a_i u_i \leq a_k \quad \text{for} \quad k = 1, \ldots, n. \quad (1)$$

Close relations between top-lexicographical and superdecreasing knapsack polytopes appear in the literature. For the 0/1 case, that is when $\ell = 0$ and $u = 1$, Gillmann and Kaibel [2] first noticed that top-lexicographical polytopes are special cases of superdecreasing knapsack ones, and the converse has been later established by Muldoon et al. [5]. Recently, Gupta [3] generalized the latter result by showing that all superdecreasing knapsacks are top-lexicographical polytopes.

To prove this last statement, Gupta [3] observes that a superdecreasing knapsack $K^a_u b$ is the top-lexicographical polytope $P^0_u a$, where $s$ is the lexicographically greatest integer point of $K^a_u b$. The non trivial inclusion actually holds because every integer point $x$ of $P^0_u a$ satisfies $ax \leq as$. Indeed, by definition, if $x < s$, there exists $k \in \{1, \ldots, n\}$ such that $x_k + 1 \leq s_k$ and $x_i = s_i$.
1.1. A flow model for $X^s_{\ell,u}$

for $i < k$. Hence, we have $b - ax \geq as - ax \geq \sum_{i=k} a_i(s_i - x_i) + a_k \geq \sum_{i=k} a_i(s_i - x_i + u_i) \geq 0$, because of (1), $s_i \geq 0$ and $u_i \geq x_i$.

It turns out that top-lexicographical polytopes are superdecreasing knapsack polytopes. Indeed, let $P^s_{\ell,u}$ be a top-lexicographical polytope for some $s$ within $[\ell, u]$. Possibly after translating, we may assume $\ell = 0$. Define $a$ by $a_k = \sum_{i=k} a_i u_i + 1$, for $k = 1, \ldots, n$, and let $b = as$. Since the associated knapsack polytope $K^a_{u,b}$ is superdecreasing, if $x \leq s$ then $ax \leq as = b$, for all $x$ within $[0, u]$. Moreover, the converse holds because, inequalities (1) being all strict, $s < x$ implies $b \geq ax$. Therefore, $P^s_{0,u} = K^a_{u,b}$. These observations are summarized in the following.

**Observation 1.** Superdecreasing knapsacks are top-lexicographical polytopes, and conversely (up to translations).

Motivated by a wide range of applications, such as knapsack cryptosystems [6] or binary expansion of bounded integer variables (e.g., [8, p. 477]), several papers are devoted to the polyhedral description of these families of polytopes. For the 0/1 case, the description appeared in [4] from the knapsack point of view. It was later rediscovered from the lexicographical point of view in [2,5]. Moreover, Muldoon et al. [5] and Angulo et al. [1] independently showed that intersecting a 0/1 top-with a 0/1 bottom-lexicographical polytope yields the description of the corresponding lexicographical polytope. Recently, these results were generalized for the bounded case by Gupta [3].

In this paper, we provide the description of the lexicographical polytopes using extended formulations. Our approach provides alternative proofs of the aforementioned results of Gupta [3].

The outline of the paper is as follows. In Section 1, we provide a flow based extended formulation of the convex hull of the componentwise maximal points of a top-lexicographical polytope. Projecting this formulation is surprisingly straightforward, and thus we get the description in the original space. In Section 2, using the fact that a top-lexicographical polytope is, up to translation, the submision of the above convex hull, we derive the description of top-lexicographical polytopes. We then show that a lexicographical polytope is the intersection of its top- and bottom-lexicographical polytopes.

1. Convex hull of componentwise maximal points

From now on, $X^s_{\ell,u}$ will denote the set of the points $p^i = (s_1, \ldots, s_{i-1}, s_i - 1, u_{i+1}, \ldots, u_n)$, for $i = 1, \ldots, n+1$ such that $s_i > \ell_i$, where $p^{n+1} = s$ by definition. Note that $X^s_{\ell,u}$ consists of the componentwise maximal integer points of $P^s_{\ell,u}$, to which we added, for later convenience, the point $p^n = (s_1, \ldots, s_{n-1}, s_n - 1)$ if $s_n > \ell_n$.

1.1. A flow model for $X^s_{\ell,u}$

We first model the points of $X^s_{\ell,u}$ as paths from 1 to $n + 1$ in the digraph given in Fig. 1.

Our digraph is composed of $n + 1$ layers, each containing two nodes except the first and the last ones. There are three arcs connecting the layer $k$ to the layer $k + 1$, an upper arc $y_k$, a diagonal arc $t_k$ and a lower arc $z_k$. The only exception concerns the first level, which does not have the upper arc.

The arcs connecting two successive layers correspond to a coordinate of $x \in X^s_{\ell,u}$. More precisely, given a directed path $P$ from 1 to $n + 1$, we define the point $x$ by setting, for $k = 1, \ldots, n$,

$$x_k = \begin{cases} u_k & \text{if } y_k \in P, \\ s_k - 1 & \text{if } t_k \in P, \\ s_k & \text{if } z_k \in P. \end{cases}$$

As shown in Observation 2, the set of $(x, y, z, t)$ satisfying the following set of inequalities is an extended formulation of $conv(X^s_{\ell,u})$:

$$x_i = u_i y_i + (s_i - 1) t_i + s_i z_i \quad \text{for } i = 1, \ldots, n,$$

$$y_1 = 0$$

$$y_i = y_{i-1} + t_{i-1} \quad \text{for } i = 2, \ldots, n,$$

$$z_i = z_{i+1} + t_{i+1} \quad \text{for } i = 1, \ldots, n - 1,$$

$$t_i = 0$$

whenever $s_i = \ell_i,$

$$y_n + t_n + z_n = 1$$

$$y_i, t_i, z_i \geq 0 \quad \text{for } i = 1, \ldots, n.$$
Observation 2. \( \text{conv}(X_{t,u}^{\text{es}}) = \text{proj}_k(x, y, z, t) \) satisfying \( (2)-(8) \).

**Proof.** First, note that there is a one-to-one correspondence between the points of \( X_{t,u}^{\text{es}} \) and the paths from layer 1 to layer \( n + 1 \) of the digraph. This implies that \( X_{t,u}^{\text{es}} \) is the projection onto the \( x \) variables of the integer points of \( Q = \{ (x, y, z, t) \) satisfying \( (2)-(8) \}. \) The digraph being acyclic, the set of \( (y, z, t) \) satisfying \( (3)-(8) \) is an integral polytope [7, Theorem 13.10]. The integrality of \( u \) and \( s \) implies that \( Q \) is integer, hence so is its projection onto the \( x \) variables, which concludes the proof. \( \square \)

1.2. Description of \( \text{conv}(X_{t,u}^{\text{es}}) \)

In the following result, we use Observation 2 to provide a linear description of \( \text{conv}(X_{t,u}^{\text{es}}) \).

**Lemma 3.** \( \text{conv}(X_{t,u}^{\text{es}}) \) is described by the inequalities:

\[
\sum_{i=1, s_i > \ell_i}^n A_i(x) \geq -1 \\
A_k(x) \leq 0 \quad \text{for } k = 1, \ldots, n, \\
A_k(x) \geq 0 \quad \text{when } s_k = \ell_k,
\]

where, for \( k = 1, \ldots, n, \)

\[
A_k(x) := (x_k - s_k) + (u_k - s_k) \sum_{i=1, s_i > \ell_i}^{k-1} \left( \prod_{j=i+1, s_j > \ell_j}^{k-1} (u_j - s_j + 1) \right) (x_i - s_i).
\]

**Proof.** By Observation 2, it suffices to project onto the \( x \) variables of the set of \( x, y, t, z \) satisfying \( (2)-(8) \).

For \( k = 1, \ldots, n \), we get \( y_k = \sum_{i=1}^{k-1} t_i \) by (3) and (4). This, combined with (5) and (7), yields \( z_k = 1 - \sum_{i=1}^k t_i \). Using those two equations in (2), and \( t_k = 0 \) whenever \( s_k = \ell_k \), we obtain

\[
t_k = s_k - x_k + (u_k - s_k) \sum_{i=1, s_i > \ell_i}^{k-1} t_i, \quad \text{for } k = 1, \ldots, n.
\]

We now show by induction on \( k \) that, for all \( k = 1, \ldots, n, \)

\[
\sum_{i=1, s_i > \ell_i}^k t_i = \sum_{i=1, s_i > \ell_i}^k (s_i - x_i) \prod_{j=i+1, s_j > \ell_j}^k (u_j - s_j + 1).
\]

By definition of \( t_k \), (13) holds for \( k = 1 \). Let us suppose that (13) holds for \( k < n \) and show that it holds for \( k + 1 \). The result is immediate if \( s_{k+1} = \ell_{k+1} \), hence assume that \( s_{k+1} > \ell_{k+1} \). We have

\[
\sum_{i=1, s_i > \ell_i}^{k+1} t_i = (s_{k+1} - x_{k+1}) + (u_{k+1} - s_{k+1}) \sum_{i=1, s_i > \ell_i}^k t_i + \sum_{i=1, s_i > \ell_i}^k t_i
\]

\[
= (s_{k+1} - x_{k+1}) + (u_{k+1} - s_{k+1} + 1) \sum_{i=1, s_i > \ell_i}^k (s_i - x_i) \prod_{j=i+1, s_j > \ell_j}^k (u_j - s_j + 1)
\]

\[
= \sum_{i=1, s_i > \ell_i}^{k+1} (s_i - x_i) \prod_{j=i+1, s_j > \ell_j}^{k+1} (u_j - s_j + 1).
\]

Above, equality (14) follows from (12) applied to \( t_{k+1} \) and equality (15) follows using (13).

Injecting (13) in (12) yields

\[
t_k = s_k - x_k + (u_k - s_k) \sum_{i=1, s_i > \ell_i}^{k-1} (s_i - x_i) \prod_{j=i+1, s_j > \ell_j}^{k-1} (u_j - s_j + 1) \quad \text{for } k = 1, \ldots, n.
\]

Up to now, we only used linear transformations, thus projecting out the variables \( y, z \) gives us (16), \( \sum_{i=1, s_i > \ell_i}^n t_i \leq 1, t_k = 0 \) whenever \( s_k = \ell_k \) and \( t_k \geq 0 \) otherwise. Then, projecting onto the \( x \) variable gives the desired result. \( \square \)
Note that the following derives from the above proof by combining (12) and the fact that, by (16), we have $t_k = -A_k$:

$$A_k(x) = (x_k - s_k) + (u_k - s_k) \sum_{i=1, i \neq \ell_i} A_i(x), \quad \text{for } k = 1, \ldots, n. \quad (17)$$

2. Lexicographical polytopes

In this section, we first provide the description of top-lexicographical polytopes. We then show that a lexicographical polytope is the intersection of its top- and bottom-lexicographical polytopes.

2.1. Description of top-lexicographical polytopes

The following observation unveils the polyhedral relation between a top-lexicographical polytope and the convex hull of its componentwise maximal points.

**Observation 4.** $P^{\text{ts}}_{\ell,u} = (\text{conv}(X^{\text{qs}}_{\ell,u}) + \mathbb{R}^n) \cap \{x \geq \ell\}.$

**Proof.** Since conv$(X^{\text{qs}}_{\ell,u})$ is integer and contained in $\{x \geq \ell\}$, the polyhedron on the right is integer. Seen the definitions, the observation follows. □

Remark that, when $\ell = 0$, $P^{\text{ts}}_{\ell,u}$ is precisely the submissive of conv$(X^{\text{qs}}_{\ell,u})$. Now, we derive from Lemma 3 and Observation 4 the linear description of top-lexicographical polytopes.

**Theorem 5.** $P^{\text{ts}}_{\ell,u} = \{x \in \mathbb{R}^n : \ell \leq x \leq u, A_k(x) \leq 0, \quad \text{for } k = 1, \ldots, n\}.$

**Proof.** Theorem 5 immediately follows from Observation 4 and the following description of conv$(X^{\text{qs}}_{\ell,u}) + \mathbb{R}^n$.

$$\text{conv}(X^{\text{qs}}_{\ell,u}) + \mathbb{R}^n = \{x \in \mathbb{R}^n : \ell \leq x \leq u, A_k(x) \leq 0, \quad \text{for } k = 1, \ldots, n\}. \quad (18)$$

To prove (18), denote by $Q$ its right hand side. By Lemma 3, the above inequalities are valid for conv$(X^{\text{qs}}_{\ell,u})$. Since their coefficients for $x$ are nonnegative, they also hold for conv$(X^{\text{qs}}_{\ell,u}) + \mathbb{R}^n$. Note that the latter and $Q$ have the same recession cone, thus it remains to show that the vertices of $Q$ are vertices of conv$(X^{\text{qs}}_{\ell,u})$. Let us prove it by induction on the dimension, the base case being immediate. We may assume that $u_n > s_n$, as otherwise $A_n(x) = x_n - s_n$ and the induction concludes. Let $\bar{x}$ be a vertex of $Q$.

**Claim 6.** $\sum_{i=1, i \neq \ell_i} A_i(\bar{x}) \geq -1.$

**Proof.** The indices $i$ of $A_i(x)$ involved in sums throughout this proof satisfy $s_i > \ell_i$, yet to ease the reading, we will omit the subscripts “$s_i > \ell_i$”. By contradiction, assume that $\sum_{i=1}^n A_i(\bar{x}) < -1$. Since $\bar{x}$ is a vertex, and $x_n$ appears only in $x_n \leq u_n$ and $A_n(x) \leq 0$, at least one of them holds with equality. If the latter does, then by (17) and $u_n > s_n$, we get the contradiction $0 = A_n(\bar{x}) \leq (u_n - s_n)(1 + A_1(\bar{x}) + \cdots + A_{n-1}(\bar{x})) < (u_n - s_n)(1 - 1) = 0$. Therefore $A_n(\bar{x}) < 0$ and $\bar{x}_n = u_n$. For $x \in \mathbb{R}^n$, we denote $\bar{x}' := (x_1, \ldots, x_{n-1})$. Necessarily, $\bar{x}'$ satisfies to equality $n - 1$ linearly independent of the remaining inequalities, and hence $\bar{x}'$ is a vertex of $\{x \in \mathbb{R}^{n-1} : \ell \leq x \leq u, A_k(x) \leq 0, \quad \text{for } k = 1, \ldots, n-1\}$. By the induction hypothesis, $\bar{x}'$ is a vertex of conv$(X^{\text{qs}}_{\ell,u'}) + \mathbb{R}^{n-1}$, hence $\sum_{i=1}^{n-1} A_i(\bar{x}') \geq -1$. But now $A_n(\bar{x}') < 0, \bar{x}_n = u_n$ and (17) imply $A_1(\bar{x}') + \cdots + A_{n-1}(\bar{x}') < -1$, a contradiction. ■

Let us show that $A_k(\bar{x}) = 0$ whenever $s_k = \ell_k$. Indeed, in this case, $\bar{x}_k$ only appears in $A_k(\bar{x}) \leq 0$ and $\bar{x}_k \leq u_k$, and one is satisfied with equality since $\bar{x}$ is a vertex. If $\bar{x}_k = u_k$, then by (17), Claim 6 and $A_i(\bar{x}) \leq 0$, for $i = 1, \ldots, n$, we get $0 \geq A_k(\bar{x}) = (u_k - s_k)(1 + \sum_{i=1, i \neq \ell_i} A_i(\bar{x})) \geq 0$. Consequently, $\bar{x}$ belongs to conv$(X^{\text{qs}}_{\ell,u})$ and this proves (18). □

Symmetrically, bottom-lexicographical polytopes are described as follows.

**Corollary 7.** $P^{\text{bs}}_{\ell,u} = \{x \in \mathbb{R}^n : \ell \leq x \leq u, B_k(x) \leq 0, \quad \text{for } k = 1, \ldots, n\},$ where, for $k = 1, \ldots, n$,

$$B_k(x) = (r_k - x_k) + (r_k - \ell_k) \sum_{i=1, i \neq \ell_i} B_i(x) \left( \sum_{j=i+1, j \neq \ell_j}^{k-1} (r_j - \ell_j + 1) \right) (r_j - x_j).$$
2.2. Lexicographical polytopes

By definition, we have $P_{t,u}^{rs} \subseteq P_{t,u}^{ss} \cap P_{t,u}^{ns}$. It turns out that the converse holds, see Theorem 8. In particular, $P_{t,u}^{ss} \cap P_{t,u}^{ns}$ is an integer polytope.

Theorem 8. A lexicographical polytope is the intersection of its top- and bottom-lexicographical polytopes.

Proof. It remains to prove that $P_{t,u}^{ss} \subseteq Q$, where $Q = P_{t,u}^{ss} \cap P_{t,u}^{ns}$. Let us prove it by induction on the dimension, the one-dimensional case being immediate.

If $r_1 = s_1$, then the problem reduces to the $(n-1)$-dimensional case, and using induction concludes.

If $r_1 + 1 \leq s_1 - 1$ for some integer $\pi$, then let $\ell'$ be obtained from $\ell$ by replacing $\ell_1$ by $\pi$. By $s_1 > \ell'_1$ and the definition of $A(t,x)$, applying Theorem 5 gives $P_{t,u}^{ss} \cap \{x_1 \geq \pi\} = P_{t,u}^{ss}$. Moreover, since $s_1 > r_1$, the latter is contained in $P_{t,u}^{ss}$. Therefore $Q \cap \{x_1 \geq \pi\} = P_{t,u}^{ss}$ is integer. Similarly, $Q \cap \{x_1 \leq \pi\}$ is integer, hence so is $Q$, and we are done.

The remaining case is when $r_1 = s_1 - 1$. Let $\bar{x} \in P_{t,u}^{ss} \cap P_{t,u}^{ns}$. If $\bar{x}_1 = s_1$, then $\bar{x}$ is written as a convex combination of integer points of $P_{t,u}^{ss}$, all of them have their first coordinate equal to $s_1$, and hence belong to $P_{t,u}^{ss}$. By convexity, so does $\bar{x}$ and we are done. A similar argument may be applied if $\bar{x}_1 = r_1$. Therefore, we may assume that $r_1 < \bar{x}_1 < s_1$.

Let $\bar{\lambda} = \bar{x}_1 - r_1$, and define $y$ by $y_1 = s_1$ and $y_1 = u_1 + \frac{\bar{x}_1 - u_1}{\lambda_1} = 0$ for $k = 2, \ldots, n$. Similarly, define $z$ by $z_1 = r_1$ and $z_1 = \ell_1 + \frac{\bar{x}_1 - r_1}{\lambda_1}$, for $i = 2, \ldots, n$. The following claim finishes the proof, where, given two points $v$ and $w$ of $\mathbb{R}^n$, max$(v, w)$ (resp. min$(v, w)$) will denote the point of $\mathbb{R}^n$ whose ith coordinate is max$(v_i, w_i)$ (resp. min$(v_i, w_i)$) for $i = 1, \ldots, n$.

Claim 9. $\bar{x}$ is a convex combination of $\bar{y} = \max(y, \ell)$ and $\bar{z} = \min(z, u)$ which both belong to $P_{t,u}^{ss}$.

Proof. First, let us show that $y \in \text{conv}(X_{t,u}^{ss}) + \mathbb{R}^n$. As $\bar{x}_1 \leq u$, we have $y_1 \leq u$. Moreover, $A_1(y) = y_1 - s_1 = 0$. Now, we prove by induction that $A_k(y) = \frac{1}{\lambda_k} A_k(\bar{x})$ for $k = 2, \ldots, n$. Using (17), $A_1(y) = 0$, the definition of $y_k$, and the induction hypothesis, we have $A_k(y) = \frac{1}{\lambda_k} [\bar{x}_k - s_k + (\lambda_1 - 1)(u_k - s_k) + (u_k - s_k) \sum_{i=2}^{n} \lambda_i A_i(\bar{x})]$. Since $\lambda_1 - 1 = \bar{x}_1 - s_1 = A_1(\bar{x})$ and $s_1 = r_1 + 1 > \ell_1$, we get by (17) that $A_k(y) = \frac{1}{\lambda_k} A_k(\bar{x})$, for $k = 2, \ldots, n$. Since $A_k(\bar{x}) \leq 0$, we have $A_k(y) \leq 0$. Hence, $y \in \text{conv}(X_{t,u}^{ss}) + \mathbb{R}^n$. Therefore, there exists $y^+$ of $\text{conv}(X_{t,u}^{ss})$ with $y^+ \geq y$. Clearly, $y^+ \geq \ell$ hence $y^+ \geq \max(y, \ell)$. Thus, $\max(y, \ell)$ belongs to $\text{conv}(X_{t,u}^{ss}) + \mathbb{R}^n$ and, by Observation 4, to $P_{t,u}^{ss}$. Moreover, as its first coordinate equals $\ell$, max$(y, \ell)$ belongs to $P_{t,u}^{ss}$. Similarly, min$(z, u)$ also belongs to $P_{t,u}^{ss}$.

Finally, we have $(1 - \lambda) \bar{z}_1 + \lambda \bar{y}_1 = (1 - \lambda) (s_1 - 1) + \lambda s_1 = s_1 - 1 + \lambda = \bar{x}_1$. For $i \in \{2, \ldots, n\}$, we have $(1 - \lambda) \bar{z}_i + \lambda \bar{y}_i = \min(\bar{x}_i - \lambda \ell_i, (1 - \lambda) u_i + \bar{x}_i, \lambda(1 - \lambda) u_i + \bar{x}_i) = \bar{x}_i - \max(\lambda \ell_i, (1 - \lambda) u_i + \bar{x}_i, \lambda \ell_i) = \bar{x}_i$. Therefore, $\bar{x} = (1 - \lambda) \bar{z} + \lambda \bar{y}$ and we are done.

Note that the above result implies that the family of lexicographical polytopes defined on a fixed box $[\ell, u]$ is closed by intersection. Beside, combined with Theorem 5 and Corollary 7, it provides the description of lexicographical polytopes.

Corollary 10. The lexicographical polytope $P_{t,u}^{ss}$ is described as follows:

$$P_{t,u}^{ss} = \{ x \in \mathbb{R}^n : \begin{align*}
A_k(x) &\leq 0 &\text{for } k = 1, \ldots, n, \\
B_k(x) &\leq 0 &\text{for } k = 1, \ldots, n, \\
\ell &\leq x \leq u
\end{align*} \}.$$