Lexicographical polytopes[☆]

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

Université Paris 13, Sorbonne Paris Cité, LIPN, CNRS, (UMR 7030), F-93430, Villetaneuse, France.

Abstract

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.

Keywords: Lexicographical polytopes, polyhedral description, superdecreasing knapsacks.

Throughout, ℓ, 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 $x \preccurlyeq y$, if $x = y$ or the first nonzero coordinate of $y - x$ is positive. We write $x \prec y$ if $x \preccurlyeq y$ and $x \neq y$. The *lexicographical polytope* $P_{\ell,u}^{r \preccurlyeq s}$ is the convex hull of the integer points within $[\ell, u]$ that are lexicographically between r and s:

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

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

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

$$\sum_{i>k} a_i u_i \leq a_k \qquad \text{for } k = 1, \ldots, n. \tag{1}$$

Close relations between top-lexicographical and superdecreasing knapsack polytopes appear in the literature. For the 0/1 case, that is when $\ell = \mathbf{0}$ and $u = \mathbf{1}$, 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, Gupte [3] generalized the latter result by showing that all superdecreasing knapsacks are top-lexicographical polytopes.

To prove this last statement, Gupte [3] observes that a superdecreasing knapsack $K_u^{a,b}$ is the top-lexicographical polytope $P_{\mathbf{0},u}^{\preccurlyeq s}$, where s the lexicographically greatest integer point of $K_u^{a,b}$. The non trivial inclusion actually holds because every integer point x of $P_{\mathbf{0},u}^{\preccurlyeq s}$ satisfies $ax \leq as$. Indeed, by definition, if $x \prec s$, there exists $k \in \{1, \ldots, n\}$ such that $x_k + 1 \leq s_k$ and $x_i = s_i$ 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 $P_{\ell,u}^{\preccurlyeq s}$ be a top-lexicographical polytope for some s within $[\ell, u]$. Possibly after translating, we may assume $\ell = \mathbf{0}$. 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 $K_u^{a,b}$

[*] Corresponding author

Email address: Michele.Barbato@lipn.univ-paris13.fr, Roland.Grappe@lipn.univ-paris13.fr, Mathieu.Lacroix@lipn.univ-paris13.fr, Clement.Pira@lipn.univ-paris13.fr (Michele Barbato, Roland Grappe[*], Mathieu Lacroix, Clément Pira)

is superdecreasing, if $x \preccurlyeq s$ then $ax \leq as = b$, for all x within $[\mathbf{0}, u]$. Moreover, the converse holds because, inequalities (1) being all strict, $s \prec x$ implies $b = as < ax$. Therefore, $P^{\preccurlyeq s}_{\mathbf{0},u} = K^{a,b}_u$. 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 Gupte [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 Gupte [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 submissive 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, $X^{\preccurlyeq s}_{\ell,u}$ 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 $X^{\preccurlyeq s}_{\ell,u}$ consists of the componentwise maximal integer points of $P^{\preccurlyeq s}_{\ell,u}$, 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 $X^{\preccurlyeq s}_{\ell,u}$

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

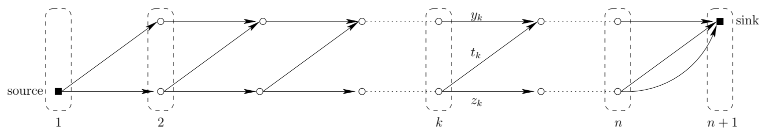

Figure 1: Path representation of the points of $X^{\preccurlyeq s}_{\ell,u}$.

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 $x \in X^{\preccurlyeq s}_{\ell,u}$. 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 $\text{conv}(X_{\ell,u}^{\preccurlyeq s})$:

$$\begin{aligned}
&x_i = u_i y_i + (s_i - 1)t_i + s_i z_i && \text{for } i = 1, \dots, n, && (2)\\
&y_1 = 0 && && (3)\\
&y_i = y_{i-1} + t_{i-1} && \text{for } i = 2, \dots, n, && (4)\\
&z_i = z_{i+1} + t_{i+1} && \text{for } i = 1, \dots, n-1, && (5)\\
&t_i = 0 && \text{whenever } s_i = \ell_i, && (6)\\
&y_n + t_n + z_n = 1 && && (7)\\
&y_i, t_i, z_i \geq 0 && \text{for } i = 1, \dots, n. && (8)
\end{aligned}$$

Observation 2. $\text{conv}(X_{\ell,u}^{\preccurlyeq s}) = \text{proj}_x\{(x, y, z, t)$ *satisfying* (2)-(8)$\}$.

Proof. First, note that there is a one-to-one correspondence between the points of $X_{\ell,u}^{\preccurlyeq s}$ and the paths from layer 1 to layer $n+1$ of the digraph. This implies that $X_{\ell,u}^{\preccurlyeq s}$ 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 a path polytope and thus 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. □

1.2. Description of $\text{conv}(X_{\ell,u}^{\preccurlyeq s})$

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

Lemma 3. $\text{conv}(X_{\ell,u}^{\preccurlyeq s})$ *is described by the inequalities:*

$$\begin{aligned}
\sum_{i=1, s_i > \ell_i}^{n} A_i(x) &\geq -1 && && (9)\\
A_k(x) &\leq 0 && \textit{for } k = 1, \dots, n, && (10)\\
A_k(x) &\geq 0 && \textit{when } s_k = \ell_k, && (11)
\end{aligned}$$

where, for $k = 1, \dots, n$,

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

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

For $k = 1, \dots, n$, we get $y_k = \sum_{i=1}^{k-1} t_i$ by (3) and (4). This, combined with (5), (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

$$t_k = s_k - x_k + (u_k - s_k) \sum_{i=1, s_i > \ell_i}^{k-1} t_i, \quad \text{for } k = 1, \dots, n. \tag{12}$$

We now show by induction on k that, for all $k = 1, \dots, n$,

$$\sum_{i=1, s_i > \ell_i}^{k} t_i = \sum_{i=1, s_i > \ell_i}^{k} (s_i - x_i) \prod_{j=i+1, s_j > \ell_j}^{k} (u_j - s_j + 1). \tag{13}$$

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

$$\sum_{i=1, s_i>\ell_i}^{k+1} t_i = (s_{k+1} - x_{k+1}) + (u_{k+1} - s_{k+1}) \sum_{i=1, s_i>\ell_i}^{k} t_i + \sum_{i=1, s_i>\ell_i}^{k} t_i \tag{14}$$

$$= (s_{k+1} - x_{k+1}) + (u_{k+1} - s_{k+1} + 1) \sum_{i=1, s_i>\ell_i}^{k} (s_i - x_i) \prod_{j=i+1, s_j>\ell_j}^{k} (u_j - s_j + 1) \tag{15}$$

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

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

Injecting (13) in (12) yields

$$t_k = s_k - x_k + (u_k - s_k) \sum_{i=1, s_i>\ell_i}^{k-1} (s_i - x_i) \prod_{j=i+1, s_j>\ell_j}^{k-1} (u_j - s_j + 1) \qquad \text{for } k = 1, \dots, n. \tag{16}$$

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. □

Note that the following derives from the above proof by combining (12) and the fact that, by (16), we have $t_k = -A_k$:

$$A_k(x) = (x_k - s_k) + (u_k - s_k) \sum_{i=1, s_i>\ell_i}^{k-1} A_i(x), \text{ for } k = 1, \dots, n. \tag{17}$$

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. $P_{\ell,u}^{\preccurlyeq s} = (\text{conv}(X_{\ell,u}^{\preccurlyeq s}) + \mathbb{R}_-^n) \cap \{x \geq \ell\}$.

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

Remark that, when $\ell = \mathbf{0}$, $P_{\ell,u}^{\preccurlyeq s}$ is precisely the submissive of $\text{conv}(X_{\ell,u}^{\preccurlyeq s})$. Now, we derive from Lemma 3 and Observation 4 the linear description of top-lexicographical polytopes.

Theorem 5. $P_{\ell,u}^{\preccurlyeq s} = \{x \in \mathbb{R}^n : \ell \leq x \leq u, A_k(x) \leq 0, \textit{for } k = 1, \dots, n\}$.

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

$$\text{conv}(X_{\ell,u}^{\preccurlyeq s}) + \mathbb{R}_-^n = \{x \in \mathbb{R}^n : x \leq u \text{ and } A_k(x) \leq 0, \text{ for } k = 1, \dots, n\}. \tag{18}$$

To prove (18), denote by Q its right hand side. By Lemma 3, the above inequalities are valid for $\text{conv}(X_{\ell,u}^{\preccurlyeq s})$. Since their coefficients for x are nonnegative, they also hold for $\text{conv}(X_{\ell,u}^{\preccurlyeq s}) + \mathbb{R}_-^n$. Note that the latter and Q

have the same recession cone, thus it remains to show that the vertices of Q are vertices of $\mathrm{conv}(X_{\ell,u}^{\preccurlyeq s})$. 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. $\displaystyle\sum_{i=1, s_i > \ell_i}^{n} A_i(\bar{x}) \geq -1.$

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 $x' := (x_1, \ldots, x_{n-1})$. Necessarily, $\bar{x}'$ satisfies to equality $n-1$ linearly independent of the remaining inequalities, and hence $\bar{x}'$ is a vertex of $\{x \in \mathbb{R}^{n-1} : x_k \leq u_k, A_k(x) \leq 0, \text{ for } k = 1, \ldots, n-1\}$. By the induction hypothesis, $\bar{x}'$ is a vertex of $\mathrm{conv}(X_{\ell',u'}^{\preccurlyeq s'}) + \mathbb{R}_-^{n-1}$, 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 $0 \geq A_k(\bar{x}) = (u_k - s_k)(1 + \sum_{i=1, s_i > \ell_i}^{k-1} A_i(\bar{x})) \geq 0$. Consequently, $\bar{x}$ belongs to $\mathrm{conv}(X_{\ell,u}^{\preccurlyeq s})$ and this proves (18). □

Symmetrically, bottom-lexicographical polytopes are described as follows.

Corollary 7. $P_{\ell,u}^{r\preccurlyeq} = \{x \in \mathbb{R}^n : \ell \leq x \leq u, B_k(x) \leq 0, \textit{for } k = 1, \ldots, n\}$*, where, for* $k = 1, \ldots, n$*,*

$$B_k(x) = (r_k - x_k) + (r_k - \ell_k) \sum_{i=1, r_i < u_i}^{k-1} \left(\prod_{j=i+1, r_j < u_j}^{k-1} (r_j - \ell_j + 1) \right) (r_i - x_i).$$

2.2. Lexicographical polytopes

By definition, we have $P_{\ell,u}^{r\preccurlyeq s} \subseteq P_{\ell,u}^{r\preccurlyeq} \cap P_{\ell,u}^{\preccurlyeq s}$. It turns out that the converse holds, see Theorem 8. In particular, $P_{\ell,u}^{r\preccurlyeq} \cap P_{\ell,u}^{\preccurlyeq s}$ 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 $P_{\ell,u}^{r\preccurlyeq s} \supseteq Q$, where $Q = P_{\ell,u}^{r\preccurlyeq} \cap P_{\ell,u}^{\preccurlyeq s}$. 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 $r_1 + 1 \leq \pi \leq s_1 - 1$ for some integer π, then let ℓ' be obtained from ℓ by replacing ℓ_1 by π. By $s_1 > \ell_1'$ and the definition of $A_k(x)$, applying Theorem 5 gives $P_{\ell,u}^{\preccurlyeq s} \cap \{x_1 \geq \pi\} = P_{\ell',u}^{\preccurlyeq s}$. Moreover, since $\pi > r_1$, the latter is contained in $P_{\ell,u}^{r\preccurlyeq}$. Therefore $Q \cap \{x_1 \geq \pi\} = P_{\ell',u}^{\preccurlyeq s}$ 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 $\bar{x} \in P_{\ell,u}^{r\preccurlyeq} \cap P_{\ell,u}^{\preccurlyeq s}$. If $\bar{x}_1 = s_1$, when $\bar{x}$ is written as a convex combination of integer points of $P_{\ell,u}^{\preccurlyeq s}$, all of them have their first coordinate equal to s_1, and hence belong to $P_{\ell,u}^{r\preccurlyeq s}$. 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 $\lambda = \bar{x}_1 - r_1$, and define y by $y_1 = s_1$ and $y_k = u_k + \frac{\bar{x}_k - u_k}{\lambda}$ for $k = 2, \ldots, n$. Similarly, define z by $z_1 = r_1$ and $z_i = \ell_i + \frac{\bar{x}_i - \ell_i}{1 - \lambda}$, 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 i^{th} 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 $P_{\ell,u}^{r\preccurlyeq s}$.

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

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 $(1 - \lambda)\bar{z}_i + \lambda \bar{y}_i = \min(\bar{x}_i - \lambda \ell_i, (1 - \lambda)u_i) + \max((\lambda - 1)u_i + \bar{x}_i, \lambda \ell_i) = \bar{x}_i - \max(\lambda \ell_i, (\lambda - 1)u_i + \bar{x}_i) + \max((\lambda - 1)u_i + \bar{x}_i, \lambda \ell_i) = \bar{x}_i$. 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 $P^{r \preccurlyeq s}_{\ell,u}$ is described as follows:*

$$P^{r \preccurlyeq s}_{\ell,u} = \left\{ \begin{array}{lll} x \in \mathbb{R}^n : & A_k(x) \leq 0 & \textit{for } k = 1, \ldots, n \\ & B_k(x) \leq 0 & \textit{for } k = 1, \ldots, n \\ & \ell \leq x \leq u & \end{array} \right\}.$$

References

[1] G. Angulo, S. Ahmed, and S.S. Dey. Forbidding extreme points from the 0-1 hypercube. *Optimization Online*, May 2012.

[2] R. Gillmann and V. Kaibel. Revlex-initial 0/1-polytopes. *Journal of Combinatorial Theory, Series A*, 113(5):799–821, 2006.

[3] A. Gupte. Convex hulls of superincreasing knapsacks and lexicographic orderings. *Discrete Applied Mathematics*, 201:150–163, 2016.

[4] M. Laurent and A. Sassano. A characterization of knapsacks with the max-flow–min-cut property. *Oper. Res. Lett.*, 11(2):105–110, 1992.

[5] F.M. Muldoon, W.P. Adams, and H.D. Sherali. Ideal representations of lexicographic orderings and base-2 expansion of integer variables. *Operations Research Letters*, 41:32–39, 2013.

[6] A.M. Odlyzko. The rise and fall of knapsack cryptosystems. In *Cryptology and Computational Number Theory*, pages 75–88. A.M.S, 1990.

[7] A. Schrijver. *Combinatorial optimization: polyhedra and efficiency.* Springer-Verlag, Berlin, Heidelberg, New York, 2003.

[8] F. Vanderbeck and L.A. Wolsey. Reformulation and decomposition of integer programs. In Michael Jünger, Thomas M. Liebling, Denis Naddef, George L. Nemhauser, William R. Pulleyblank, Gerhard Reinelt, Giovanni Rinaldi, and Laurence A. Wolsey, editors, *50 Years of Integer Programming 1958-2008*, pages 431–502. Springer Berlin Heidelberg, 2010.