Discrete & Computational Geometry (2023) 70:268–278
https://doi.org/10.1007/s00454-022-00419-3

On the Extension Complexity of Polytopes Separating Subsets of the Boolean Cube

Pavel Hrubeš[1] · **Navid Talebanfard**[1]

Received: 25 May 2021 / Revised: 19 May 2022 / Accepted: 22 June 2022 /
Published online: 17 August 2022

Abstract
We show that for every $A \subseteq \{0,1\}^n$, there exists a polytope $P \subseteq \mathbb{R}^n$ with $P \cap \{0,1\}^n = A$ and extension complexity $O(2^{n/2})$, and that there exists an $A \subseteq \{0,1\}^n$ such that the extension complexity of any P with $P \cap \{0,1\}^n = A$ must be at least $2^{n(1-o(1))/3}$. We also remark that the extension complexity of any 0/1-polytope in $\mathbb{R}^n$ is at most $O(2^n/n)$ and pose the problem whether the upper bound can be improved to $O(2^{cn})$, for $c < 1$.

Keywords Polytopes · Extension complexity · Boolean cube · Sign patterns

Mathematics Subject Classification 52B05

1 Introduction

A polytope $P \subseteq \mathbb{R}^n$ with many facets can often be expressed as a projection of a higher-dimensional polytope $Q \subseteq \mathbb{R}^m$ with much fewer facets. This is especially significant in the context of linear programming: instead of optimizing a linear function over P, it is more efficient to optimize over Q. *Extension complexity of* P is defined as the smallest k so that P is an affine image of a polytope with k facets. Extension complexity has been studied in the seminal paper of Yannakakis [25], Fiorini et al. [10], Rothvoß [22], and others. In [22], Rothvoß has shown that there exist 0/1-polytopes in $\mathbb{R}^n$ with

Editor in Charge: János Pach

This work was supported by Czech Science Foundation GAČR Grant 19-27871X.

Pavel Hrubeš
pahrubes@gmail.com

Navid Talebanfard
talebanfard@math.cas.cz

[1] Institute of Mathematics of the Czech Academy of Sciences, Prague 1, Czech Republic

extension complexity $2^{n(1-o(1))/2}$; in fact, a random polytope has this property. Our paper originated with the question whether the bound of Rothvoß is tight.

Problem 1.1 Can every 0/1-polytope P be expressed as a projection of a polytope with $O(2^{cn})$ facets, for a constant $c < 1$?

Note that P itself can have many more than 2^n facets [5]. Extension complexity, however, can be bounded by the number of vertices and hence the trivial upper bound is 2^n. In Problem 1.1, we want to know which of the bounds, $2^{n/2}$ vs. 2^n, is closer to the truth. This is reminiscent of a similar problem in $\mathbb{R}^2$. In [10], Fiorini et al. have shown that there exist polygons in $\mathbb{R}^2$ with k vertices and extension complexity $\Omega(\sqrt{k})$. Quite surprisingly, Shitov [23] has shown that every k-vertex polygon has extension complexity $O(k^{2/3})$. Furthermore, there is an $O(k^{1/2})$ upper bound for several natural classes of polygons [19].

Problem 1.1 is related to a similar question about graphs. Given an n-vertex graph, let $P_G \subseteq \mathbb{R}^n$ be the convex hull of characteristic vectors of its edges. An explicit description of P_G in terms of inequalities is known [17, 20], and it is especially simple in the case of bipartite graphs. The trivial upper bound on $\mathrm{xc}(P_G)$ is $O(n^2)$. We point out that any improvement on this trivial bound gives an improvement on extension complexity of 0/1-polytopes. This reduction is similar to the so-called *graph complexity* (see [16, 21]) where an n variate Boolean function is interpreted as defining a graph on exponentially many vertices. Extension complexity of P_G has been investigated by Fiorini et al. in [8], where a non-trivial upper bound $O(n^2/\log n)$ was presented (cf. [3]). This translates to a modest contribution to Problem 1.1: P is a projection of a polytope with $O(2^n/n)$ facets. The latter bound has also been obtained by Averkov et al. in [4].

We mainly focus on a relaxation of Problem 1.1. Given $A \subseteq \{0,1\}^n$, a polytope $P \subseteq \mathbb{R}^n$ will be called *separating* for A if $P \cap \{0,1\}^n = A$. In other words, P separates Boolean points in A from those outside of A. The smallest separating polytope is $\mathsf{conv}(A)$ itself. Extension complexity of separating polytopes has several connections with computational complexity, as extensively discussed in [12]. Here we show that every $A \subseteq \{0,1\}^n$ has a separating polytope with extension complexity $O(2^{n/2})$. This is achieved by the aforementioned reduction to graphs, and by showing that the set of edges of G has a separating polytope of linear size. This quantitatively matches the lower bound of Rothvoß—except that the assumptions are different. There are infinitely many separating polytopes other than $\mathsf{conv}(A)$ itself and so the lower bound is not applicable. In [13], a lower bound of $2^{\Omega(n)}$ on extension complexity of separating polytopes has been given. The constant in the exponent hinges on known bounds on quantifier elimination and it is not hard to see that the proof from [13] gives $2^{n(1-o(1))/5}$. We will improve this bound to $2^{n(1-o(1))/3}$ using a more geometrical argument.

Organization of the paper. In Sect. 2 we give basic definitions and state the main result (Theorem 2.1). In Sect. 3 we give examples of bounds on the number of facets of separating polytopes. In Sect. 4 we prove the upper bound (Theorem 4.2) and discuss the connection with graph complexity. Finally, in Sect. 5 we prove the lower bound (Theorem 5.7).

2 The Main Result

A *polytope* $P \subseteq \mathbb{R}^n$ is the convex hull of a finite set of points in $\mathbb{R}^n$. It can also be viewed as a bounded set defined by a finite number of linear constraints. The *extension complexity* of a polytope P, $\mathrm{xc}(P)$, is the smallest k so that there exists a polytope $Q \subseteq \mathbb{R}^m$ with k facets and an affine map $\pi : \mathbb{R}^m \to \mathbb{R}^n$ such that $P = \pi(Q)$. Given $A \subseteq \{0,1\}^n$, its *separation complexity*, $\mathsf{sep}(A)$, is the minimum $\mathrm{xc}(P)$ over all polytopes $P \subseteq \mathbb{R}^n$ with

$$P \cap \{0,1\}^n = A;$$

such a P is called a *separating* polytope for A. We provide non-trivial upper and lower bounds on $\mathsf{sep}(A)$:

Theorem 2.1 (i) *For every* $A \subseteq \{0,1\}^n$, $\mathsf{sep}(A) \leq O(2^{n/2})$.
(ii) *There exists* $A \subseteq \{0,1\}^n$ *with* $\mathsf{sep}(A) \geq 2^{n(1-o(1))/3}$.

Remark 2.2 In [12, 13], separation complexity is defined slightly differently with P allowed to be an *unbounded* polyhedron. This is just a cosmetic detail—we can intersect P with $[0,1]^n$ (or a simplex containing it) which increases its complexity by an additive term of $O(n)$.

As observed in [12, 25], a Boolean circuit of size s which accepts precisely the inputs from A gives a separating polytope for A with extension complexity $O(s+n)$. Hence an upper bound of $O(2^n/n)$ on $\mathsf{sep}(A)$ can be obtained from known upper bounds on Boolean circuit size due to Lupanov (see [15, Sect. 1.4.1]). The upper bound from Theorem 2.1 is more intimately related to a result of Dančík [7] who has obtained an $O(2^{n/2})$ upper bound for depth three circuits with *unbounded fan-in* $\wedge, \vee$-gates. Our proof is virtually the same though it does not seem to follow from Dančík's result in a black box fashion. A lower bound of $2^{\Omega(n)}$ on separation complexity has been obtained in [13]. The estimate presented in Theorem 2.1 is quantitatively stronger.

3 Simple Bounds on the Number of Facets

We first give some elementary bounds on the number of facets of separating polytopes. This is mainly to contrast it both with extension complexity and the number of facets of 0/1-polytopes. These results[1] have been previously obtained by Jeroslow [14], and we include them for completeness.

Proposition 3.1 *Every* $A \subseteq \{0,1\}^n$ *has a separating polytope with at most* 2^n *facets.*

Proof For $x \in \mathbb{R}^n$ and $\sigma \in \{0,1\}^n$, define

$$h_\sigma(x) := \sum_{i=1}^{n} x_i(1-\sigma_i) + (1-x_i)\sigma_i.$$

[1] In fact, Jeroslow obtains the tight estimate 2^{n-1} in Proposition 3.1 while allowing the separating polyhedron to be unbounded.

If x is Boolean, $h_\sigma(x)$ is the Hamming distance between x and σ. Define $P \subseteq \mathbb{R}^n$ by the constraints $h_\sigma(x) \geq 1$ for every $\sigma \in \{0,1\}^n \setminus A$. Then indeed $P \cap \{0,1\}^n = A$. P may be possibly unbounded. This can be remedied by adding the constraints $h_\sigma(x) \geq 0$, $\sigma \in A$. □

Let $\mathsf{ODD}_n \subseteq \{0,1\}^n$ be the set of Boolean strings with odd number of ones.

Proposition 3.2 *If $n \geq 2$, every separating polytope for ODD_n has at least 2^{n-1} facets.*

Proof Let H be a closed half-space $\left\{x \in \mathbb{R}^n : \sum_i a_i x_i \geq b\right\}$. We claim the following: if $\mathsf{ODD}_n \subseteq H$ then $\bar{H} := \mathbb{R}^n \setminus H$ contains at most one even string $\sigma \in \{0,1\}^n \setminus \mathsf{ODD}_n$. To see this, assume an even σ is contained in $\bar{H}$. Without loss of generality, we can assume that σ is the zero vector; otherwise apply an affine map that flips 0 and 1 for the 1-coordinates of σ. Since $\sigma \notin H$, we must have $b > 0$. Since every unit vector is in $\mathsf{ODD}_n \subseteq H$, we have $a_i \geq b$ for every i. This means that $\{0,1\}^n \setminus \{\sigma\} \subseteq H$ and no other even string can be in $\bar{H}$.

If $n = 2$, the statement of the proposition is clear. Let $n \geq 3$ and assume that P is a separating polytope for ODD_n with r facets. Then $P = \bigcap_{i=1}^r H_i$ where H_i are closed half-spaces. (This is because P is full-dimensional for $n \geq 3$). We have $\mathsf{ODD}_n \subseteq H_i$ for every i, and every even σ is contained in at least one $\bar{H}_i$. Since $|\{0,1\}^n \setminus \mathsf{ODD}_n| = 2^{n-1}$, this gives $r \geq 2^{n-1}$. □

By the result of Bárány [5], A can have $2^{\Omega(n \log n)}$ facets—hence Proposition 3.1 shows that a separating polytope for A can have much fewer facets than $\mathsf{conv}(A)$. The convex hull of ODD_n, also known as the parity polytope, has extension complexity $O(n)$ (see [6]), and it is trivially a separating polytope for ODD_n—hence Proposition 3.2 shows that taking extensions into a higher dimension can be exponentially powerful. It also shows that the $O(2^{n/2})$ upper bound from Theorem 2.1 cannot be achieved simply by counting the facets of the separating polytope.

4 The Upper Bound

We now prove the upper bound from Theorem 2.1. Let $B_2^n \subseteq \{0,1\}^n$ be the set of Boolean vectors of Hamming weight two (i.e., with exactly two ones). For a natural number n, $[n]$ will denote the set $\{1, \ldots, n\}$.

Lemma 4.1 *Let $H \subseteq B_2^n$. Then there exists a polytope $R_H \subseteq [0,1]^n \subseteq \mathbb{R}^n$ with at most $2n$ facets such that $R_H \cap \{0,1\}^n = H$.*

Proof It is convenient to view H as representing edges of a graph with vertex set $[n]$. Namely, $i \neq j$ are adjacent iff $e_i + e_j \in H$, where e_i is the i-th unit vector. Given $i \in [n]$, let $N(i)$ be the set of vertices adjacent with i. Let R_H be defined by the following constraints: $0 \leq x_i$ for $i \in [n]$ and

$$\sum_{i \in [n]} x_i = 2, \tag{1}$$

$$\sum_{j \in N(i)} x_j \geq x_i, \qquad i \in [n]. \tag{2}$$

There are $2n$ inequalities. It is easy to see they imply $x_i \leq 1$ for every $i \in [n]$ and so $R_H \subseteq [0,1]^n$. Given $e_i + e_j \in H$, the constraints defining R_H are satisfied and so $H \subseteq R_H$. If $\sigma \in \{0,1\}^n \setminus R_H$ then either $\sigma \notin B_2^n$, and then σ falsifies (1), or $\sigma = e_i + e_j$ with $j \notin N(i)$, and then σ falsifies $x_i \leq \sum_{k \in N(i)} x_k$. Hence $R_H \cap \{0,1\}^n = H$. □

Theorem 4.2 *Let $A \subseteq \{0,1\}^n$. Then there exists a polytope $P \subseteq [0,1]^n$ with $\mathrm{xc}(P) = O(2^{n/2})$ and $P \cap \{0,1\}^n = A$.*

Proof Without loss of generality, assume that n is even and $N := 2^{n/2}$. Assume $A \subseteq \{0,1\}^{[n]}$ and partition $[n]$ into two equal parts X_1 and X_2. Let $F_1 := \{0,1\}^{X_1}$ and $F_2 := \{0,1\}^{X_2}$. Hence every $\sigma \in \{0,1\}^{[n]}$ can be uniquely written as $\sigma = \sigma_1 \cup \sigma_2$ with $\sigma_1 \in F_1, \sigma_2 \in F_2$. We identify $\mathbb{R}^{2N}$ with $\mathbb{R}^{F_1 \cup F_2}$, so that the coordinates are indexed by elements of $F_1 \cup F_2$. The standard unit vectors are $e_{\sigma_1}, e_{\sigma_2}, \sigma_1 \in F_1, \sigma_2 \in F_2$. Let $H \subseteq B_2^{2N}$ be defined as

$$H := \{e_{\sigma_1} + e_{\sigma_2} : \sigma_1 \cup \sigma_2 \in A\}.$$

Let R_H be the polytope from the previous lemma. We want to express P in terms of R_H. Let $T \subseteq \mathbb{R}^{2N}$ be the intersection of $[0,1]^{2N}$ with the hyperplanes

$$\sum_{\sigma_1 \in F_1} x_{\sigma_1} = 1, \qquad \sum_{\sigma_2 \in F_2} x_{\sigma_2} = 1. \tag{3}$$

Let $\pi : \mathbb{R}^{2N} \to \mathbb{R}^n$ be the linear map so that for every $\sigma_1 \in F_1, \sigma_2 \in F_2$, $\pi(e_{\sigma_1}) = \sigma_1 \cup 0$ and $\pi(e_{\sigma_2}) = 0 \cup \sigma_2$ (where 0 is the zero vector in F_2 and F_1, respectively). This guarantees

$$\pi(e_{\sigma_1} + e_{\sigma_2}) = \sigma_1 \cup \sigma_2.$$

Moreover, for every $\sigma \in \{0,1\}^n$ with $\sigma = \sigma_1 \cup \sigma_2$, $e_{\sigma_1} + e_{\sigma_2}$ is the *unique* vector $x \in T$ with $\pi(x) = \sigma$. For if $\pi(x) = \sigma$, we have $\sum_{\beta \in F_1} x_\beta \beta = \sigma_1$ and $\sum_{\beta \in F_1} x_\beta = 1$, $0 \leq x_\beta \leq 1$, by (3). In other words, x gives a convex combination of σ_1 in terms of the Boolean vectors in F_1 which is easily seen to be unique. (Similarly for σ_2). Finally, let $P := \pi(R_H \cap T)$. Then $\mathrm{xc}(P) \leq 2N$. Given $\sigma \in \{0,1\}^n$, we have $\sigma \in P$ iff $e_{\sigma_1} + e_{\sigma_2} \in R_H$. By the definition of H, this is equivalent to $\sigma \in A$. Hence indeed $P \cap \{0,1\}^n = A$. □

4.1 Graphs and Problem 1.1

Given a (simple undirected) graph G with vertex set $[n]$, let $P_G \subseteq \mathbb{R}^n$ be the convex hull of characteristic vectors of edges in G:

$$P_G = \mathsf{conv}(\{e_i + e_j : i \neq j \text{ are adjacent in } G\}).$$

Note that P_G has at most $\binom{n}{2}$ vertices and so $\mathrm{xc}(P_G)$ is at most quadratic. Fiorini et al. in [8] have given an improved bound $\mathrm{xc}(P_G) \leq O(n^2/\log n)$ for any graph. It is however

not known whether $\mathrm{xc}(P_G) \leq O(n^c)$ for some constant $c < 2$. We summarize the connection between this problem and Problem 1.1 as follows[2]:

Proposition 4.3 *Let $A \subseteq \{0,1\}^n$. Then $\mathrm{xc}(\mathsf{conv}(A)) \leq O(2^n/n)$. Moreover, assume that for every bipartite graph G on $2m$ vertices (with the parts of equal size), $\mathrm{xc}(P_G) \leq O(m^c)$, where $c \leq 2$ is an absolute constant. Then $\mathrm{xc}(A) \leq O(2^{cn/2})$*

Proof This is analogous to the proof of Theorem 4.2. The set H corresponds to a bipartite graph G on $2N$ vertices with $N = 2^{n/2}$. The projection π maps vertices of $P_G \subseteq T$ to Boolean vectors in $\mathbb{R}^n$. Hence $\pi(P_G) = \mathsf{conv}(A)$ and $\mathrm{xc}(\mathsf{conv}(A)) \leq \mathrm{xc}(P_G)$. From [8, Lem. 3.4] we know $\mathrm{xc}(P_G) \leq O(N^2/\log N)$ which gives $\mathrm{xc}(\mathsf{conv}(A)) \leq O(2^n/n)$; the "moreover" part is similar. □

An explicit description of P_G in terms of linear inequalities can be found in [17, 20]. Apart from the general constraints $\sum x_i = 2$, $0 \leq x_i$, every inequality $\sum_{i \in S} x_i \leq 1$ is valid whenever S is an independent set. In the case of *bipartite* G, this indeed gives a complete description of P_G. This also means that P_G can have exponentially many facets—in particular, the polytope from Lemma 4.1 must be strictly larger than P_G for some G.

The lemma can be somewhat strengthened when considering independent sets of size 2. Let Q_G be the polyhedron defined by the constraints $x_i + x_j \leq 1$ for every $i \neq j$ not adjacent in G. Clearly, $P_G \subseteq Q_G$ and they contain the same set of Boolean vectors of Hamming weight two (i.e., the edges of G).

Remark 4.4 Let G be a bipartite n-vertex graph. Then there exists a polytope R'_G with $O(n)$ facets with $P_G \subseteq R'_G \subseteq Q_G$.

Proof Let L and R be the parts of G with $L \cup R = [n]$. Then R'_G defined by the following constraints has the desired properties: $0 \leq x_i$ for $i \in [n]$,

$$\sum_{i \in L} x_i = 1, \quad \sum_{i \in R} x_i = 1, \quad \text{and} \quad x_i + \sum_{j \in R \setminus N(i)} x_j \leq 1, \quad i \in L. \qquad \square$$

Using the machinery of non-negative rank factorizations of slack matrices (see, e.g., [9, 22, 25]), the quantity $\mathrm{xc}(P_G)$ can be captured by the nonnegative rank of an explicit matrix EIS_G: its rows are indexed by edges e of G, columns by independent sets S. The entry corresponding to e and S equals 1, if e and S are disjoint, and 0 otherwise. This matrix is intimately related to the famous Clique vs Independent Set problem of Yannakakis [25]; see also [11]. If G is bipartite, $\mathrm{xc}(P_G)$ corresponds to the non-negative rank of EIS_G. An interesting submatrix of EIS_G is the ENE_G matrix obtained by restricting the columns to independent sets of size two (i.e., non-edges). A similar matrix has been considered in [18] from the point of view of communication complexity. Since ENE_G can have size $O(n^2) \times O(n^2)$, one may perhaps hope to obtain quadratic lower bounds on $\mathrm{xc}(P_G)$ using the non-negative rank of ENE_G. We note that this is impossible.[3]

[2] The first part of the statement can also be found in [4].

[3] This could also be concluded from Remark 4.4.

Remark 4.5 If G is a bipartite n-vertex graph, ENE_G can be written as a sum of $O(n)$ 0/1-matrices. For a non-bipartite G, the bound is $O(n \log n)$.

Proof Let G be a bipartite graph on vertices $L \cup R$. Let E be the set of edges of G and $\bar{E}$ the set of non-edges. Given $\ell \in L, r \in R$, define the following sets A_ℓ, B_r, $C_\ell \subseteq E \times \bar{E}$ of edge/non-edge pairs.

- A_ℓ consists of pairs with $e = \{\ell_1, r_1\}$, $\bar{e} = \{\ell, r_2\}$ with $\ell \neq \ell_1 \in L$, $r_1, r_2 \in R$, and $r_1 \in N(\ell)$.
- B_r consists of pairs $e = \{\ell_1, r\}$, $\bar{e} = \{v_1, v_2\}$, where either $v_1 \neq v_2 \in R \setminus \{r\}$, or $v_1 \in L$, $v_2 \in R \setminus \{r\}$, and $v_1 \notin N(r)$.
- C_ℓ are the pairs $\{\ell, r_1\}, \{\ell_1, \ell_2\}$ with $\ell_1 \neq \ell_2 \in L \setminus \{\ell\}$.

It is easy to see that the sets form a partition of the set of disjoint edge/non-edge pairs. Moreover, each of the sets is a product set (of the form $C \times C'$ with $C \subseteq E$, $C' \subseteq \bar{E}$). Identifying a subset of $E \times \bar{E}$ with the 0/1-matrix representing its characteristic function, we can thus write

$$\mathsf{ENE}_G = \sum_\ell A_\ell + \sum_r B_r + \sum_\ell C_\ell,$$

where the summands are 0/1-matrices of rank one. A general n-vertex graph can be expressed as an edge-disjoint union of a bipartite graph and two graphs with $\lceil n/2 \rceil$ vertices, and we can proceed by induction. □

5 The Lower Bound

Our proof of the lower bound from Theorem 2.1 uses Warren's estimate on the number of sign patterns of a polynomial map, and Alon's bound on the number of combinatorial types of polytopes. We overview these results first.

For $b \in \mathbb{R}$ define

$$\operatorname{sgn}(b) = \begin{cases} 1, & b > 0, \\ 0, & b = 0, \\ -1, & b < 0. \end{cases}$$

For a sequence $f = \langle f_1(y_1, \ldots, y_p), \ldots, f_s(y_1, \ldots, y_p) \rangle$ of real functions, $b \in \mathbb{R}^p$, let $\operatorname{sgn}(f(b)) := \langle \operatorname{sgn}(f_1(b)), \ldots, \operatorname{sgn}(f_s(b)) \rangle \in \{-1, 0, +1\}^s$, which we call the *sign-pattern of f at b*. A result of Warren and its extension by Alon gives a bound on the number of sign patterns when f_i are polynomials of degree at most d.

Theorem 5.1 (Warren [24], Alon [2]) *Let f be a sequence of s polynomials of degree at most $d \geq 1$ in the same set of p variables with $2s \geq p$. Then $|\{\operatorname{sgn}(f(b)) : b \in \mathbb{R}^p\}| \leq (8eds/p)^p$.*

Given a polytope P, the *face lattice* of P, $L(P)$, is the poset of the faces of P ordered by inclusion (including $\emptyset$ and P itself). It is naturally equipped with join and meet

operations, hence it is a lattice. See, e.g., [26] for details. The lattice-isomorphism equivalence class of $L(P)$ captures the *combinatorial type* of P.

Theorem 5.2 (Alon [1]) *The number of non-isomorphic face lattices arising from polytopes with r vertices is at most $2^{r^3(1+o(1))}$.*

By duality, this implies:

Corollary 5.3 *The number of non-isomorphic face lattices arising from polytopes with r facets is at most $2^{r^3(1+o(1))}$.*

We now proceed to prove the lower bound from Theorem 2.1. We call a set $S \subseteq \mathbb{R}^n$ *full-dimensional* if no hyperplane in $\mathbb{R}^n$ contains S. Note that if A is full-dimensional then so is any separating P for A.

Lemma 5.4 *There are at least $2^{2^n(1-o(1))}$ full-dimensional subsets of $\{0,1\}^n$.*

Proof If A contains 0 and the n unit vectors, it is full-dimensional. There are 2^{2^n-n-1} such A's. □

Lemma 5.5 *For every $m \geq n$ there are polynomials $f_1, \ldots, f_s$ in mn variables such that*

- *$s = O(m^{n+1})$, each f_i has degree at most n and has at most $2^{O(n \log n)}$ non-zero coefficients,*
- *for every $V \in \mathbb{R}^{m \times n}$ viewed as m points in $\mathbb{R}^n$, if $\mathsf{conv}(V)$ is full-dimensional then the set $\mathsf{conv}(V) \cap \{0,1\}^n$ is uniquely determined by $\langle \mathrm{sgn}(f_1(V)), \ldots, \mathrm{sgn}(f_s(V)) \rangle$.*

Proof We will construct a set of polynomials such that for any $V = \{v_1, \ldots, v_m\}$, we can determine $\mathsf{conv}(V) \cap \{0,1\}^n$ by evaluating the signs of these polynomials on V. The idea is as follows. For every set V' of n points from V, we can compute the unique hyperplane H passing through V' (if such a *unique* hyperplane exists). If all points in V lie in the same closed half-space determined by H, then $\mathsf{conv}(V) \cap H$ is a facet of $\mathsf{conv}(V)$. Let us call such closed half-space *good*. Then, given $\sigma \in \{0,1\}^n$, we can determine whether $\sigma \in \mathsf{conv}(V)$ by checking whether it appears in all good half-spaces.

We now formally define our set of polynomials. Given $S \in \binom{[m]}{n}$ and $V \in \mathbb{R}^{m \times n}$, let V_S be the set of vectors $\{v_i : i \in S\}$. We start by constructing the following polynomials/sets of polynomials. They take V_S as input, but we hide the dependence.

(i) $a_{S,1}, \ldots a_{S,n}$ are polynomials of degree $n-1$ such that V_S is affinely independent iff some $a_{S,i}$ is non-zero,

(ii) b_S is a polynomial of degree n such that whenever V_S is affinely independent then $H_S(V) := \left\{x \in \mathbb{R}^n : \sum_i a_{S,i} x_i = b_S\right\}$ is the unique hyperplane passing through V_S,

(iii) F_S is a set of $m-n$ polynomials of degree n such that if V_S is affinely independent, then $\mathsf{conv}(V) \cap H_S(V)$ is a facet of $\mathsf{conv}(V)$ iff all polynomials in F_S are all non-positive or all non-negative.

Parts (i) and (ii) are an exercise in linear algebra. F_S is obtained by evaluating the hyperplane equation from (ii) on all points from $V \setminus V_S$—the hyperplane defines a

facet if all points in V lie on the same side. Let F be the set of polynomials containing $F_S, a_{S,1}, \ldots, a_{S,n}$ and

$$\sum_i a_{S,i}\sigma_i - b_S,$$

for every $S \in \binom{[m]}{n}$ and $\sigma \in \{0,1\}^n$. Then $\mathsf{conv}(V) \cap \{0,1\}^n$ is uniquely determined by the signs of polynomials in F. The number of polynomials is $(2^n+n+1+(m-n))\binom{m}{n} \leq (2^n+m+1)m^n/n! \leq O(m^{n+1})$ and their degrees are at most n. The bound on the number of non-zero coefficients follows by noting that each polynomial depends on $O(n^2)$ variables. □

Before proceeding to the next lemma, let us make some comments about rational functions. Given a p-variate rational function $f = g/h$ with g, h coprime polynomials and $h \neq 0$, define its degree as the maximum of the degrees of g and h. Thus f defines a partial function : $\mathbb{R}^p \to \mathbb{R}$. Warren's estimate can be extended to rational functions as follows. Given a rational map $f = \langle f_1, \ldots, f_s \rangle$ from $\mathbb{R}^p$ to $\mathbb{R}^s$ with each f_i of degree at most $d \geq 1$, we have

$$|\{\mathrm{sgn}(f(b)) : b \in \mathbb{R}^p, f(b) \text{ is defined}\}| \leq (cds)^p, \tag{4}$$

where $c > 0$ is an absolute constant. This follows from Theorem 5.1 by considering signs of numerators and denominators separately.[4]

Furthermore, we need the following estimate on the degree of composition. Suppose that $f(x_1, \ldots, x_m)$ is a polynomial of degree d_1 with k non-zero coefficients and $g_1, \ldots, g_m$ are rational functions of degree at most d_2. Then it is easy to see that the degree of $f(g_1, \ldots, g_m)$ is at most kd_1d_2.

Lemma 5.6 *Let L be a face lattice of a d-dimensional polytope with $r \geq d$ facets. Assume $d \geq n$ and let S_L be the set of $A \subseteq \{0,1\}^n$ such that A is full-dimensional and there exists a polytope Q in $\mathbb{R}^d$ with combinatorial type L such that the projection of Q on the first n coordinates is separating for A. Then $|S_L| \leq 2^{O(nr^3)}$.*

Proof Consider a polytope Q in $\mathbb{R}^d$ with face lattice L. Since Q is full-dimensional, we can write it as $\{y \in \mathbb{R}^d : By \leq b\}$ where $b \in \mathbb{R}^r$, $B \in \mathbb{R}^{r \times d}$. Hence Q can be described using $p := (r+1)d \leq O(r^2)$ constants $z = \langle B, b \rangle$. Let U be the vertices of Q. Then $|U| \leq 2^r$. Every vertex is the unique intersection of d hyperplanes defining facets of the polytope. Furthermore, the lattice L specifies for each vertex, which facets it is contained in and, moreover, which d of them have the desired unique intersection (see, e.g., [26]). For each vertex $u \in U$, canonically pick d such facets. Then u is the unique solution to a system of d linear equations, and its coordinates can be seen as rational functions of z. More exactly, using Cramer's rule, we can write $u(z) = u_0(z)^{-1}\langle u_1(z), \ldots, u_d(z) \rangle$, where $u_0, \ldots, u_d$ have degree d. Note that $u_0(z)$ is non-zero whenever the polytope described by z is indeed of type L.

[4] We also have no assumption on p since the number of sign patterns can be trivially bounded by 3^p.

Project Q on the first n coordinates to obtain $P \subseteq \mathbb{R}^n$. We want to specify which elements of the Boolean cube are contained in P. Let V be the projection of the vertices of Q so that $P = \mathsf{conv}(V)$. Assume that P is full-dimensional (otherwise it cannot contain a full-dimensional A). Lemma 5.5 gives us a set of polynomials $f_1(V), \ldots, f_s(V)$ whose sign pattern determines $P \cap \{0,1\}^n$. We also have $s \leq O(|U|^{n+1}) \leq 2^{O(rn)}$, and each f_i has degree at most n and it has $2^{O(n \log n)}$ non-zero coefficients. The coordinates of vertices of V are degree d rational functions of z, hence $f_i(V(z))$ is a rational function of z of degree at most $d' \leq dn2^{O(n \log n)} \leq r2^{O(n \log n)}$. By (4), the number of sign patterns of $\langle f_1(V(z)), \ldots, f_s(V(z))\rangle$ can be bounded by $(c'sd')^p$. Since $s \leq 2^{O(rn)}$, $p \leq O(r^2)$, $d' \leq r2^{O(n \log n)}$, and $n \leq r$, the bound can be written as $2^{O(r^3 n)}$. This gives the desired estimate on $|S_L|$. □

Theorem 5.7 *There exists* $A \in \{0,1\}^n$ *such that* $\mathsf{sep}(A) \geq 2^{n(1-o(1))/3}$.

Proof Let $\mathcal{A}$ be the set of full-dimensional subsets $A \subseteq \{0,1\}^n$. Let $r \geq n$ be such that every $A \in \mathcal{A}$ has separation complexity at most r. Without loss of generality, assume that this is exhibited by a full-dimensional polytope $Q \subseteq \mathbb{R}^d$ with r facets such that the projection of Q on the first n coordinates is a separating polytope for A, and $n \leq d \leq r$. We then have

$$|\mathcal{A}| \leq |\mathcal{L}| \cdot \max_{L \in \mathcal{L}} |S_L|,$$

where $\mathcal{L}$ is the set of combinatorial types of polytopes with r facets. By Lemma 5.6, $|S_L| \leq 2^{O(nr^3)}$. By Corollary 5.3, we have $|\mathcal{L}| \leq 2^{r^3(1+o(1))}$. Therefore $|\mathcal{A}| \leq 2^{cnr^3}$ (for some constant c and n sufficiently large). By Lemma 5.4, we must have $2^{cnr^3} \geq 2^{2^n(1-o(1))}$ and thus $r \geq 2^{n(1-o(1))/3}$. □

Acknowledgements We are grateful to Fedor Part for discussions, Gennadiy Averkov and Emil Jeřábek for useful references. This work was done while Talebanfard was participating in the program *Satisfiability: Theory, Practice, and Beyond* at the Simons Institute for the Theory of Computing.

Data Availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

1. Alon, N.: The number of polytopes, configurations and real matroids. Mathematika **33**(1), 62–71 (1986)
2. Alon, N.: Tools from higher algebra. In: Handbook of Combinatorics, vol. 2, pp. 1749–1783. North Holland, Amsterdam (1995)
3. Aprile, M., Faenza, Yu., Fiorini, S., Huynh, T., Macchia, M.: Extension complexity of stable set polytopes of bipartite graphs. In: Graph-Theoretic Concepts in Computer Science (Eindhoven 2017). Lecture Notes in Computer Science, vol. 10520, pp. 75–87. Springer, Cham (2017)
4. Averkov, G., Kaibel, V., Weltge, S.: Maximum semidefinite and linear extension complexity of families of polytopes. Math. Program. Ser. A **167**(2), 381–394 (2018)
5. Bárány, I., Pór, A.: On 0-1 polytopes with many facets. Adv. Math. **161**(2), 209–228 (2001)
6. Carr, R.D., Konjevod, G.: Polyhedral combinatorics. In: Tutorials on Emerging Methodologies and Applications in Operations Research (Denver 2004). International Series in Operations Research & Management Science, vol. 76, pp. 2-1–2-46. Springer, New York (2005)

7. Dančík, V.: Complexity of Boolean functions over bases with unbounded fan-in gates. Inf. Process. Lett. **57**(1), 31–34 (1996)
8. Fiorini, S., Kaibel, V., Pashkovich, K., Theis, D.O.: Combinatorial bounds on nonnegative rank and extended formulations. Discrete Math. **313**(1), 67–83 (2013)
9. Fiorini, S., Massar, S., Pokutta, S., Tiwary, H.R., de Wolf, R.: Exponential lower bounds for polytopes in combinatorial optimization. J. ACM **62**(2), # 17 (2015)
10. Fiorini, S., Rothvoß, Th., Tiwary, H.R.: Extended formulations for polygons. Discrete Comput. Geom. **48**(3), 658–668 (2012)
11. Göös, M.: Lower bounds for clique vs. independent set. In: 56th Annual Symposium on Foundations of Computer Science (Berkeley 2015), pp. 1066–1076. IEEE, Los Alamitos (2015)
12. Hrubeš, P.: On ϵ-sensitive monotone computations. Comput. Complexity **29**(2), # 6 (2020)
13. Hrubeš, P.: On the complexity of computing a random Boolean function over the reals. Theory Comput. **16**, # 9 (2020)
14. Jeroslow, R.G.: On defining sets of vertices of the hypercube by linear inequalities. Discrete Math. **11**, 119–124 (1975)
15. Jukna, S.: Boolean Function Complexity. Algorithms and Combinatorics, vol. 27. Springer, Heidelberg (2012)
16. Jukna, S.: Computational complexity of graphs. In: Advances in Network Complexity. Quantitative and Network Biology, vol. 4, pp. 99–153. Wiley-Blackwell, Weinheim (2013)
17. Kaibel, V., Loos, A.: Finding descriptions of polytopes via extended formulations and liftings. In: Progress in Combinatorial Optimization, pp. 151–169. ISTE, London (2012)
18. Kushilevitz, E., Weinreb, E.: On the complexity of communication complexity. In: ACM International Symposium on Theory of Computing (Bethesda 2009), pp. 465–473. ACM, New York (2009)
19. Kwan, M., Sauermann, L., Zhao, Y.: Extension complexity of low-dimensional polytopes. Trans. Am. Math. Soc. **375**(6), 4209–4250 (2022)
20. Maurras, J.-F.: Convex hull of the edges of a graph and near bipartite graphs. Discrete Math. **46**(3), 257–265 (1983)
21. Pudlák, P., Rödl, V., Savický, P.: Graph complexity. Acta Inform. **25**(5), 515–535 (1988)
22. Rothvoß, Th.: Some 0/1 polytopes need exponential size extended formulations. Math. Program. Ser. A **142**(1–2), 255–268 (2013)
23. Shitov, Y.: Sublinear extension of polygons (2014). arXiv:1412.0728
24. Warren, H.E.: Lower bounds for approximation by nonlinear manifolds. Trans. Am. Math. Soc. **133**, 167–178 (1968)
25. Yannakakis, M.: Expressing combinatorial optimization problems by linear programs. J. Comput. Syst. Sci. **43**(3), 441–466 (1991)
26. Ziegler, G.M.: Lectures on Polytopes. Graduate Texts in Mathematics, vol. 152. Springer, New York (1995)

Terms and Conditions

Springer Nature journal content, brought to you courtesy of Springer Nature Customer Service Center GmbH ("Springer Nature").

Springer Nature supports a reasonable amount of sharing of research papers by authors, subscribers and authorised users ("Users"), for small-scale personal, non-commercial use provided that all copyright, trade and service marks and other proprietary notices are maintained. By accessing, sharing, receiving or otherwise using the Springer Nature journal content you agree to these terms of use ("Terms"). For these purposes, Springer Nature considers academic use (by researchers and students) to be non-commercial.

These Terms are supplementary and will apply in addition to any applicable website terms and conditions, a relevant site licence or a personal subscription. These Terms will prevail over any conflict or ambiguity with regards to the relevant terms, a site licence or a personal subscription (to the extent of the conflict or ambiguity only). For Creative Commons-licensed articles, the terms of the Creative Commons license used will apply.

We collect and use personal data to provide access to the Springer Nature journal content. We may also use these personal data internally within ResearchGate and Springer Nature and as agreed share it, in an anonymised way, for purposes of tracking, analysis and reporting. We will not otherwise disclose your personal data outside the ResearchGate or the Springer Nature group of companies unless we have your permission as detailed in the Privacy Policy.

While Users may use the Springer Nature journal content for small scale, personal non-commercial use, it is important to note that Users may not:

1. use such content for the purpose of providing other users with access on a regular or large scale basis or as a means to circumvent access control;
2. use such content where to do so would be considered a criminal or statutory offence in any jurisdiction, or gives rise to civil liability, or is otherwise unlawful;
3. falsely or misleadingly imply or suggest endorsement, approval , sponsorship, or association unless explicitly agreed to by Springer Nature in writing;
4. use bots or other automated methods to access the content or redirect messages
5. override any security feature or exclusionary protocol; or
6. share the content in order to create substitute for Springer Nature products or services or a systematic database of Springer Nature journal content.

In line with the restriction against commercial use, Springer Nature does not permit the creation of a product or service that creates revenue, royalties, rent or income from our content or its inclusion as part of a paid for service or for other commercial gain. Springer Nature journal content cannot be used for inter-library loans and librarians may not upload Springer Nature journal content on a large scale into their, or any other, institutional repository.

These terms of use are reviewed regularly and may be amended at any time. Springer Nature is not obligated to publish any information or content on this website and may remove it or features or functionality at our sole discretion, at any time with or without notice. Springer Nature may revoke this licence to you at any time and remove access to any copies of the Springer Nature journal content which have been saved.

To the fullest extent permitted by law, Springer Nature makes no warranties, representations or guarantees to Users, either express or implied with respect to the Springer nature journal content and all parties disclaim and waive any implied warranties or warranties imposed by law, including merchantability or fitness for any particular purpose.

Please note that these rights do not automatically extend to content, data or other material published by Springer Nature that may be licensed from third parties.

If you would like to use or distribute our Springer Nature journal content to a wider audience or on a regular basis or in any other manner not expressly permitted by these Terms, please contact Springer Nature at

onlineservice@springernature.com