A Short Proof that the Extension Complexity of the Correlation Polytope Grows Exponentially

Volker Kaibel, Stefan Weltge[1]

Otto-von-Guericke-Universität Magdeburg, Germany

Abstract

We establish that the extension complexity of the $n \times n$ correlation polytope is at least 1.5^n by a short proof that is self-contained except for using the fact that every face of a polyhedron is the intersection of all facets it is contained in. The main innovative aspect of the proof is a simple combinatorial argument showing that the rectangle covering number of the unique-disjointness matrix is at least 1.5^n, and thus the nondeterministic communication complexity of the unique-disjointness predicate is at least $.58n$. We thereby slightly improve on the previously best known lower bounds 1.24^n and $.31n$, respectively.

Keywords: correlation polytope, extended formulations, unique disjointness, communication complexity
2010 MSC: 52Bxx, 90C57, 94Axx

1. Introduction

The concept of extended formulations aims at writing polytopes as affine images of polyhedra of lower complexity. In particular, for a polytope P, one is interested in its *extension complexity*, i.e., the smallest number of facets of any polyhedron whose affine image is P. As the first explicit example of a $0/1$-polytope whose extension complexity is not bounded by a polynomial in its dimension, Fiorini et al. [1] showed that the extension complexity of the *correlation polytope*

$$\mathrm{CORR}(n) := \operatorname{conv}\left\{ y \in \{0,1\}^{n \times n} : y_{ij} = x_i x_j \ \forall\, i, j \in [n],\ x \in \{0,1\}^n \right\}$$

grows exponentially in n. Since $\mathrm{CORR}(n)$ can be found as an affine image of a face of many other combinatorial polytopes of similar dimension, this result has been used to show that the extension complexities of polytopes such as traveling salesman polytopes [1], certain stable set polytopes [1], certain knapsack polytopes [2, 3], and other polytopes associated with NP-hard optimization problems [2] are also not bounded polynomially. Independently of the correlation polytope, Rothvoß [4] recently even established an exponential lower bound on the extension complexity of the perfect matching polytope.

Email addresses: kaibel@ovgu.de (Volker Kaibel), weltge@ovgu.de (Stefan Weltge)

[1] Partially funded by the German Research Foundation (DFG): “Extended Formulations in Combinatorial Optimization” (KA 1616/4-1)

The proof of the statement on CORR(n) given in [1] follows a strategy developed in [5] and uses a lower bound on the rectangle covering number of the unique-disjointness matrix obtained in [6], which essentially is due to [7]. This amounts to a rather involved proof in total, leaving it unclear how “deep” the result actually is (while its great relevance is out of discussion, of course).

The aim of this paper is to provide a short combinatorial, self-contained (except for using the fact that every face of a polyhedron is the intersection of all facets containing it) proof showing that the extension complexity of CORR(n) is at least 1.5^n. The main new contribution of the proof is a simple combinatorial argument (see the half-a-page proof of Thm. 1) instead of using [6, 7]. Furthermore, the lower bound 1.5^n improves slightly upon the previously best known one 1.24^n following from [8].

2. The Main Proof

For a nonnegative integer n we set $[n] := \{1, \ldots, n\}$ and define $2^{[n]}$ as the set of all subsets of $[n]$. The Euclidian scalar product of two vectors v, w is denoted by $\langle v, w\rangle = \sum_i v_i w_i$. Further, for a set $a \subseteq [n]$ let $\chi(a) \in \{0,1\}^n$ be its characteristic vector, i.e., $\chi(a)_i = 1$ if and only if $i \in a$. For a set $b \subseteq [n] := \{1, \ldots, n\}$ let $y^b \in \{0,1\}^{n\times n}$ be the 0/1-matrix with $y^b_{ij} = 1$ if and only if $i \in b$ and $j \in b$ hold. With this notation, we have that $\mathrm{CORR}(n) = \mathrm{conv}\{y^b : b \subseteq [n]\}$.

We first extract the single combinatorial property of CORR(n) that is relevant for the proof and then, by a few polyhedral arguments, establish a general lower bound on the extension complexity of CORR(n) in terms of sizes of so-called coverings. This part is basically a compact reformulation of known arguments.

Lemma 1. *For every $a \subseteq [n]$ there is a face F_a of* CORR(n) *such that*

$$y^b \in F_a \iff |a \cap b| = 1$$

holds for all $b \subseteq [n]$.

Proof. For a set $a \subseteq [n]$, let $\pi_a(x) \in \mathbb{R}[x_i : i \in [n]]$ be the quadratic polynomial $(\langle\chi(a), x\rangle - 1)^2$ with variable vector $x = (x_1, \ldots, x_n)$. Denote by $\Pi_a(y) \in \mathbb{R}[y_{ij} : i, j \in [n]]$ the linear polynomial arising from $\pi_a(x)$ by substituting each monomial $x_i x_j$ by y_{ij} and each monomial x_i by y_{ii}. Due to $y^b_{ij} = \chi(b)_i\chi(b)_j$ and $y^b_{ii} = \chi(b)_i$ we have $\Pi_a(y^b) = \pi_a(\chi(b)) \geq 0$ for each $b \subseteq [n]$. This implies that the linear inequality $\Pi_a(y) \geq 0$ is valid for CORR(n) and hence defines a face F_a of CORR(n). Note that a point y^b is contained in F_a if and only if $\langle\chi(a), \chi(b)\rangle = 1$, i.e., $|a \cap b| = 1$ holds. □

Let us define the set $\mathcal{D}(n) := \{(a, b) \in 2^{[n]} \times 2^{[n]} : a \cap b = \emptyset\}$ of pairs of disjoint subsets of $[n]$. A set $R \subseteq \mathcal{D}(n)$ is called *valid* if it satisfies

$$\forall\ (a, b),\ (a', b') \in R : \quad |a \cap b'| \neq 1. \tag{1}$$

Further, we say that a set $R_1, \ldots, R_k$ of valid sets for $\mathcal{D}(n)$ is a *covering* of $\mathcal{D}(n)$ of size k if

$$\mathcal{D}(n) \subseteq \bigcup_{i=1}^{k} R_i$$

holds.

Lemma 2. *Let Q be a polyhedron having f facets such that* $\mathrm{CORR}(n)$ *is an affine image of Q. Then there exists a covering of $\mathcal{D}(n)$ of size f.*

Proof. Let p be an affine map such that $p(Q) = \mathrm{CORR}(n)$. For every facet G of Q let us define the set

$$R_G := \left\{(a,b) \in \mathcal{D}(n) : p^{-1}(F_a) \subseteq G, y^b \notin p(G)\right\}.$$

First, note that R_G is valid: For (a,b), $(a',b') \in R_G$ we observe that $|a \cap b'| = 1$ is equivalent to $y^{b'} \in F_a$, which, in case of $p^{-1}(F_a) \subseteq G$ implies $y^{b'} \in F_a \subseteq p(G)$.

Second, we claim that $\{R_G : G \text{ facet of } Q\}$ is a covering of $\mathcal{D}(n)$. Towards this end, let $(a,b) \in \mathcal{D}(n)$. Observe that $p^{-1}(F_a)$ is a face of Q and let $G_1, \ldots, G_k$ be the facets of Q containing $p^{-1}(F_a)$. Since $p^{-1}(F_a) = \bigcap_{i=1}^k G_i$ holds, we have

$$y^b \notin F_a = p(\bigcap_{i \in [k]} G_i) \subseteq \bigcap_{i \in [k]} p(G_i).$$

Hence there is some $i \in [k]$ with $y^b \notin p(G_i)$, thus we obtain $(a,b) \in R_{G_i}$ (due to $p^{-1}(F_a) \subseteq G_i$). □

We are now ready to prove our main result:

Theorem 1. *The extension complexity of* $\mathrm{CORR}(n)$ *is at least* 1.5^n.

Proof. By Lemma 2, it suffices to show that any covering of $\mathcal{D}(n)$ has size of at least 1.5^n. Therefore, let $\varrho(n)$ be the largest cardinality of any valid subset of $\mathcal{D}(n)$. By the fact that any covering of $\mathcal{D}(n)$ must have size of at least $\frac{|\mathcal{D}(n)|}{\varrho(n)}$ and the fact that $|\mathcal{D}(n)| = 3^n$, it remains to show that $\varrho(n) \leq 2^n$, which we will establish by showing that $\varrho(n) \leq 2\varrho(n-1)$ holds for all $n \geq 1$. (Note that $\varrho(0) = 1$ since the only valid subset of $\mathcal{D}(n)$ is $\{(\emptyset, \emptyset)\}$.)

Towards this end, let $R \subseteq \mathcal{D}(n)$ be valid (with $n \geq 1$) and let us define the following two sets:

$$R_1 := (\{(a,b) \in R : n \in a\} \cup \{(a,b) \in R : (a \cup \{n\}, b) \notin R\}) \cap ([n] \times [n-1])$$
$$R_2 := (\{(a,b) \in R : n \in b\} \cup \{(a,b) \in R : (a, b \cup \{n\}) \notin R\}) \cap ([n-1] \times [n])$$

Further, let us define the function $f\colon R \to \mathcal{D}(n-1)$ with $f(a,b) := (a \setminus \{n\}, b \setminus \{n\})$. Since $R_1 \subseteq R$ is valid and since $R_1 \subseteq [n] \times [n-1]$, $f(R_1)$ is valid. Similarly, $f(R_2)$ is also valid. Further, by the definition of R_i, f is injective on R_i for $i = 1, 2$. By induction, we hence obtained that

$$|R_1| + |R_2| = |f(R_1)| + |f(R_2)| \leq 2\varrho(n-1) = 2^n.$$

Thus, it suffices to show that $R \subseteq R_1 \cup R_2$: Let $(a,b) \in R$. Since $a \cap b = \emptyset$, we have that $(a,b) \subseteq ([n] \times [n-1]) \cup ([n-1] \times [n])$. Thus, if $n \in a \cup b$, we clearly have that $(a,b) \in R_1 \cup R_2$. It remains to show that for any $(a,b) \in R$ with $n \notin a \cup b$, we cannot have that $(a \cup \{n\}, b) \in R$ and $(a, b \cup \{n\}) \in R$. Indeed, this is true since, otherwise, the validity of R would imply

$$1 \neq |(a \cup \{n\}) \cap (b \cup \{n\})| = |\{n\}| = 1,$$

a contradiction. □

3. Remarks on Related Results

From the Perspective of Communication Complexity
Using the terminology from the theory of communication complexity, the proof of Theorem 1 shows that the *rectangle covering number* of the *unique-disjointness matrix* UDISJ(n) (see, e.g., [9]) is at least 1.5^n. To see that, observe that our notion of valid sets corresponds to sets of 1-entries in UDISJ(n) that can be covered simultaneously by one rectangle. In particular, this implies that the *nondeterministic communication complexity* of the *unique-disjointness* predicate is at least $\log_2(1.5^n) \geq .58n$. For the background of these remarks, we refer to [10] or [9].

Applicability to the Matching Polytope
Most superpolynomial lower bounds on the extension complexities of combinatorial polytopes are a direct consequence of the fact that the extension complexity of the correlation polytope grows exponentially and hence can also be derived from our argumentation. In contrast to this, Rothvoß' [4] result on an exponential lower bound on the extension complexity of the (perfect) matching polytope of the complete graph seems to be of a considerably more complicated nature. It follows already from [5] that this result cannot be deduced from the results on the correlation polytope in a similar manner as it is possible for, say, the TSP polytope. In fact, Rothvoß' approach exploits more than the mere combinatorial structure of the matching polytopes. The ideas underlying the proof presented in this paper seem to be of little use in that context, leaving wide open the question for a similarly simple proof of the fact that the extension complexity of the perfect matching polytope cannot be bounded polynomially.

Acknowledgements. We thank Yuri Faenza and Kanstantsin Pashkovich for their helpful remarks on an earlier version of this paper.

References

[1] S. Fiorini, S. Massar, S. Pokutta, H. R. Tiwary, R. de Wolf, Linear vs. semidefinite extended formulations: exponential separation and strong lower bounds, in: STOC, 2012, pp. 95–106.

[2] D. Avis, H. R. Tiwary, On the extension complexity of combinatorial polytopes, in: F. V. Fomin, R. Freivalds, M. Z. Kwiatkowska, D. Peleg (Eds.), Automata, Languages, and Programming, Vol. 7965 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2013, pp. 57–68. doi:10.1007/978-3-642-39206-1_6.
URL http://dx.doi.org/10.1007/978-3-642-39206-1_6

[3] S. Pokutta, M. V. Vyve, A note on the extension complexity of the knapsack polytope, Oper. Res. Lett. 41 (4) (2013) 347–350. doi:http://dx.doi.org/10.1016/j.orl.2013.03.010.
URL http://www.sciencedirect.com/science/article/pii/S0167637713000394

[4] T. Rothvoß, The matching polytope has exponential extension complexity, arXiv:1311.2369 (2013).
URL http://arxiv.org/abs/1311.2369

[5] M. Yannakakis, Expressing combinatorial optimization problems by linear programs, J. Comput. Syst. Sci. 43 (3) (1991) 441–466.

[6] R. de Wolf, Nondeterministic quantum query and communication complexities, SIAM J. Comput. 32 (3) (2003) 681–699.

[7] A. A. Razborov, On the distributional complexity of disjointness, Theoretical Computer Science 106 (2) (1992) 385–390.

[8] G. Braun, S. Pokutta, Common information and unique disjointness, in: FOCS (to appear), 2013.

[9] S. Jukna, Boolean function complexity: advances and frontiers, Springer, 2012.

[10] E. Kushilevitz, N. Nisan, Communication complexity, Cambridge University Press, 2006.