A SHORT PROOF THAT THE EXTENSION COMPLEXITY OF THE CORRELATION POLYTOPE GROWS EXPONENTIALLY

VOLKER KAIBEL AND STEFAN WELTGE

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 $.58n$.

For $b \subseteq [n] := \{1, \ldots, n\}$, 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. The *correlation polytope* is $\mathrm{CORR}(n) := \mathrm{conv}\{y^b : b \subseteq [n]\}$. In [4] it was shown that the *extension complexity* of $\mathrm{CORR}(n)$, i.e., the minimum number of facets of some polyhedron of which $\mathrm{CORR}(n)$ is the image under a linear map, grows exponentially with n. From this result, it has then been deduced that also the extension complexities of polytopes such as traveling salesman polytopes [4], certain stable set polytopes [4], certain knapsack polytopes [1, 7], and other polytopes associated with NP-hard optimization problems [1] are not bounded polynomially.

The proof of the statement on $\mathrm{CORR}(n)$ given in [4] follows a strategy developed in [9] and uses a lower bound on the rectangle covering number of the unique-disjointness matrix obtained in [3], which essentially is due to [8]. In this note, we provide a self-contained (except for using that every face of a polyhedron is the intersection of all facets containing it) proof showing that the extension complexity of $\mathrm{CORR}(n)$ is at least 1.5^n. The main new contribution of the proof is a simple combinatorial argument instead of using [3, 8]. Furthermore, the lower bound 1.5^n improves slightly upon the previously best known one 1.4548^n following from [2].

Theorem. *Each polyhedron $Q \subseteq \mathbb{R}^q$ for which there is a linear map $p \colon \mathbb{R}^q \to \mathbb{R}^{n \times n}$ with $p(Q) = \mathrm{CORR}(n)$ has at least 1.5^n facets.*

Proof. For $a \subseteq [n]$ 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 $x = (x_1, \ldots, x_n)$, where we use $\langle v, w\rangle = \sum_i v_i w_i$, and $\chi(a) \in \{0,1\}^n$ is the characteristic vector of $a \subseteq [n]$ with $\chi(a)_i = 1$ if and only if $i \in a$. 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 $\mathrm{CORR}(n)$ and hence defines a face F_a of $\mathrm{CORR}(n)$ with $y^b \in F_a$ for $b \subseteq [n]$ if and only if $\langle \chi(a), \chi(b)\rangle = 1$, i.e., $|a \cap b| = 1$ holds.

Denoting by $2^{[n]}$ the set of all subsets of $[n]$, we define $\mathcal{P}_0(n)$, $\mathcal{P}_1(n)$, and $\mathcal{P}_\star(n)$ to be the sets of all ordered pairs $(a,b) \in 2^{[n]} \times 2^{[n]}$ with $|a \cap b| = 0$, $|a \cap b| = 1$, and $|a \cap b| > 1$, respectively. Defining, for every facet G of Q,

$$A_G := \{a \subseteq [n] : p^{-1}(F_a) \subseteq G\} \qquad \text{and} \qquad B_G := \{b \subseteq [n] : y^b \notin p(G)\},$$

we are going to establish the equation

$$\mathcal{P}_0(n) \cup \mathcal{P}_\star(n) = \bigcup_{G \text{ facet of } Q} A_G \times B_G\,. \tag{1}$$

Towards this end, we first observe that $(A_G \times B_G) \cap \mathcal{P}_1(n) = \varnothing$ holds for every facet G of Q (since $(a,b) \in \mathcal{P}_1(n)$ is equivalent to $y^b \in F_a$, which, in case of $a \in A_G$, implies $y^b \in F_a \subseteq p(G)$). Thus, in order to prove (1), it suffices to show that for all $a, b \subseteq [n]$ with $y^b \notin F_a$ there is some facet G of Q with $(a,b) \in A_G \times B_G$. To

Date: September 10, 2013.

show this, observe that $p^{-1}(F_a)$ is a face of Q and let $G_1, \ldots, G_k$ be the facets of Q containing $p^{-1}(F_a)$. In particular, $a \in A_{G_i}$ holds for all $i \in [k]$. Since $p^{-1}(F_a) = \bigcap_{i=1}^k G_i$ holds, we have

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

Hence there is some $i \in [k]$ with $y^b \notin p(G_i)$, thus $(a,b) \in A_{G_i} \times B_{G_i}$.

Equation (1) implies $\mathcal{P}_0(n) \subseteq \bigcup_{G \text{ facet of } Q}(A_G \times B_G)$ and

$$(A_G, B_G) \;\in\; \mathcal{R}(n) := \{(A,B) \,:\, A, B \subseteq 2^{[n]}, (A \times B) \cap \mathcal{P}_1(n) = \varnothing\}$$

for all facets G of Q. Due to $|\mathcal{P}_0(n)| = 3^n$, we conclude that Q has at least $3^n/\varrho(n)$ facets, where

$$\varrho(n) := \max\{|(A \times B) \cap \mathcal{P}_0(n)| \,:\, (A,B) \in \mathcal{R}(n)\}\,.$$

Therefore, in order to finally prove the theorem, it suffices to show $\varrho(n) \leq 2^n$, which we will do by establishing $\varrho(n) \leq 2\varrho(n-1)$ for all $n \geq 1$ (note that $\varrho(0) = 1$ holds due to $\mathcal{R}(0) = \{(\varnothing, \varnothing)\}$). Towards this end, let $(A,B) \in \mathcal{R}(n)$ (with $n \geq 1$), and define the following sets:

$$\begin{aligned} A^1 &:= \{a \subseteq [n-1] \,:\, a \in A\} & A^2 &:= \{a \subseteq [n-1] \,:\, a \cup \{n\} \in A\} \\ B^1 &:= \{b \subseteq [n-1] \,:\, b \in B\} & B^2 &:= \{b \subseteq [n-1] \,:\, b \cup \{n\} \in B\} \end{aligned}$$

Denote $C_n := \{c \cup \{n\} \,:\, c \in C\}$ for all $C \subseteq [n-1]$. We first observe

$$(A^1 \times B^1) \cap \mathcal{P}_0(n-1) \;\subseteq\; ((A^1 \setminus A^2) \times B^1) \cup (A^1 \times (B^1 \setminus B^2))\,, \tag{2}$$

which holds since we have $(A^2 \times B^2) \cap \mathcal{P}_0(n) = \varnothing$ (due to $A^2_n \times B^2_n \subseteq A \times B$ and $(A \times B) \cap \mathcal{P}_1(n) = \varnothing$). We further find $(A^2_n \times B^2_n) \cap \mathcal{P}_0(n) = \varnothing$ and thus

$$\begin{aligned} |(A \times B) \cap \mathcal{P}_n(0)| &= |(A^1 \times B^1) \cap \mathcal{P}_n(0)| + |(A^2_n \times B^1) \cap \mathcal{P}_n(0)| + |(A^1 \times B^2_n) \cap \mathcal{P}_n(0)| \\ &= |(A^1 \times B^1) \cap \mathcal{P}_{n-1}(0)| + |(A^2 \times B^1) \cap \mathcal{P}_{n-1}(0)| + |(A^1 \times B^2) \cap \mathcal{P}_{n-1}(0)| \\ &\overset{(2)}{\leq} |\underbrace{((A^1 \cup A^2) \times B^1)}_{\in \mathcal{R}(n-1)} \cap \mathcal{P}_{n-1}(0)| + |\underbrace{(A^1 \times (B^1 \cup B^2))}_{\in \mathcal{R}(n-1)} \cap \mathcal{P}_{n-1}(0)| \\ &\leq 2\varrho(n-1). \end{aligned}$$

□

The matrix $M(n) \in \{0,1,\star\}^{2^n \times 2^n}$ whose rows and columns are indexed by the subsets of $[n]$, and whose entries are defined according to the sets $\mathcal{P}_n(0)$, $\mathcal{P}_n(1)$, and $\mathcal{P}_n(\star)$, is known as the *unique-disjointness matrix* [6]. Our proof shows that the *rectangle covering number* of $M(n)$ is at least $1.5^{\,n}$, and hence the *nondeterministic communication complexity* of the *unique-disjointness predicate* is at least $\log_2(1.5^{\,n}) \geq .58n$ (see, e.g., [5] for the background of these remarks).

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

References

1. David Avis and Hans Tiwary, *On the extension complexity of combinatorial polytopes*, ICALP (to appear), 2013.
2. Gabor Braun and Sebastian Pokutta, *Common information and unique disjointness*, FOCS (to appear), 2013.
3. Ronald de Wolf, *Nondeterministic quantum query and communication complexities*, SIAM J. Computing **32** (2003), no. 3, 681–699.
4. Samuel Fiorini, Serge Massar, Sebastian Pokutta, Hans Raj Tiwary, and Ronald de Wolf, *Linear vs. semidefinite extended formulations: exponential separation and strong lower bounds*, STOC, 2012, pp. 95–106.
5. Stasys Jukna, *Boolean function complexity: Advances and frontiers*, Springer, 2012.
6. Eyal Kushilevitz and Noam Nisan, *Communication complexity*, Cambridge University Press, 2006.
7. Sebastian Pokutta and Mathieu van Vywe, *A note on the extension complexity of the knapsack polytope*, Oper. Res. Let. (to appear).
8. A. A. Razborov, *On the distributional complexity of disjointness*, Theoret. Comput. Sci. **106** (1992), no. 2, 385–390.
9. Mihalis Yannakakis, *Expressing combinatorial optimization problems by linear programs*, J. Comput. Syst. Sci. **43** (1991), no. 3, 441–466.

Institut für Mathematische Optimierung, Otto-von-Guericke Universität Magdeburg, Germany
E-mail address: {kaibel,weltge}@ovgu.de