THEORY OF COMPUTING, Volume 13 (18), 2017, pp. 1–15
www.theoryofcomputing.org

Monotone Projection Lower Bounds from Extended Formulation Lower Bounds

Joshua A. Grochow*

Received November 10, 2015; Revised July 27, 2016; Published December 22, 2017

Abstract: In this short note, we reduce lower bounds on monotone projections of polynomials to lower bounds on extended formulations of polytopes. Applying our reduction to the seminal extended formulation lower bounds of Fiorini, Massar, Pokutta, Tiwari, & de Wolf (STOC 2012; J. ACM, 2015) and Rothvoss (STOC 2014; J. ACM, 2017), we obtain the following interesting consequences.

1. The Hamiltonian Cycle polynomial is not a monotone subexponential-size projection of the permanent; this both rules out a natural attempt at a monotone lower bound on the Boolean permanent, and shows that the permanent is *not* complete for non-negative polynomials in $\mathsf{VNP}_{\mathbb{R}}$ under monotone p-projections.
2. The cut polynomials and the perfect matching polynomial (or "unsigned Pfaffian") are not monotone p-projections of the permanent. The latter, over the Boolean and-or semi-ring, rules out monotone reductions in one of the natural approaches to reducing perfect matchings in general graphs to perfect matchings in bipartite graphs.

As the permanent is universal for monotone formulas, these results also imply exponential lower bounds on the monotone formula size and monotone circuit size of these polynomials.

ACM Classification: F.1.3, F.2.1, G.1.6

AMS Classification: 68Q15, 68Q17, 90C05, 15A15, 05C70

Key words and phrases: lower bounds, algebraic circuit complexity, extended formulations of polytopes, Newton polytope, monotone formula, monotone circuit, projection, permanent, VNP, matching

*The author was supported during this work by an Omidyar Fellowship from the Santa Fe Institute.

DOI: 10.4086/toc.2017.v013a018

1 Introduction

The permanent

$$\mathrm{perm}_n(X) = \sum_{\pi \in S_n} x_{1,\pi(1)} x_{2,\pi(2)} \cdots x_{n,\pi(n)}$$

(where S_n denotes the symmetric group of all permutations of $\{1,\ldots,n\}$) has long fascinated combinatorists [17, 14, 18], more recently physicists [33, 2], and, since Valiant's seminal paper [29], has also been a key object of study in computational complexity. Despite its beauty, the permanent has some computational quirks: in particular, although the permanent of integer matrices is $\#\mathsf{P}$-complete and the permanent is VNP-complete in characteristic zero, the permanent *mod 2* is the same as the determinant, and hence can easily be computed. In fact, computing the permanent mod 2^k is easy for any k [29], though the proof is more involved. Modulo any odd number n, the permanent of integer matrices is $\mathsf{Mod}_n\mathsf{P}$-complete [29].

In contrast, the seemingly similar Hamiltonian Cycle polynomial,

$$\mathrm{HC}_n(X) = \sum_{n\text{-cycles } \sigma} x_{1,\sigma(1)} x_{2,\sigma(2)} \cdots x_{n,\sigma(n)}\,,$$

where the sum is only over n-cycles rather than over all permutations, does not have these quirks: the Hamiltonian Cycle polynomial is VNP-complete over any ring R [28] and $\mathsf{Mod}_n\mathsf{P}$-complete for all n (that is, counting Hamiltonian cycles is complete for these Boolean counting classes).

Jukna [12] observed that, over the Boolean semi-ring, if the Hamiltonian Cycle polynomial were a monotone p-projection of the permanent, there would be a $2^{n^{\Omega(1)}}$ lower bound on monotone circuits computing the permanent, a lower bound that still remains open. (The current record is still Razborov's $n^{\Omega(\log n)}$ [20].) Even over the real numbers, such a monotone p-projection would give an alternative proof of a $2^{n^{\Omega(1)}}$ lower bound on the permanent. (Jerrum and Snir [11] already showed the permanent requires monotone circuits of size $2^{\Omega(n)}$ over $\mathbb{R}$ and over the tropical $(\min,+)$ semi-ring.) Here, by building on Fiorini *et al.*'s [8] and Rothvoss's [22] extended formulation lower bound for the TSP polytope, we show that no such monotone reduction exists—over $\mathbb{R}$, nor over the tropical semi-ring, nor over the Boolean semi-ring—by connecting monotone p-projections to extended formulations of polytopes.

In the past five years, there has been exciting progress on extended formulations of polytopes, which we leverage by using our new connection. Indeed, with this connection in hand, one immediately gets a monotone projection lower bound from essentially *any* lower bound on extended formulations. An *extended formulation* of a polytope P is another polytope in a higher-dimensional space that projects down onto P by an affine linear map. Since linear programming can be solved in polynomial time, and optima of linear programs are preserved by affine linear projections, solving the LP on the extended formulation allows one to solve the LP on the original polytope. Thus, if a polytope P has an extended formulation that is in some sense "small," one can solve LP optimization problems over P by instead solving them over its smaller extended formulation; if the extended formulation is small enough, this would yield a polynomial-time algorithm. To show that such an extended formulation is not small, it suffices to prove a lower bound on its number of facets. In 1988, Yannakakis [34] ruled out a large and natural class of extended formulations of the TSP polytope—so-called *symmetric* extended formulations—thus showing that a certain natural class of algorithms for an NP-complete problem indeed did not solve it in polynomial time, and ruling out several attempted proofs that $\mathsf{P} = \mathsf{NP}$. But for more than 20 years, it was an open question of how to remove the condition of symmetry from Yannakakis's result. In a landmark result, Fiorini, Massar, Pokutta, Tiwary, and de Wolf [8] achieved this, by showing an exponential lower bound on *arbitrary* extended formulations of several different polytopes. We will use their lower bound on the cut polytope below. Rothvoss [22] then showed such lower bounds on several other polytopes; we use his lower bound on the TSP polytope, improving that of Fiorini *et al.* [8], to get the result above.

We use the same connection to extended formulations, now in combination with Rothvoss's lower bound on extended formulations of the perfect matching polytope [22], to show that the perfect matching polynomial or "unsigned Pfaffian"

$$\frac{1}{2^n n!}\sum_{\pi\in S_{2n}}\prod_{i=1}^{n} x_{\pi(2i-1),\pi(2i)} = \sum_{\substack{\pi\in S_{2n}\\ \pi(1)<\pi(3)<\cdots<\pi(2n-1)\\ \pi(2k-1)<\pi(2k)\ \forall k}}\prod_{i=1}^{n} x_{\pi(2i-1),\pi(2i)}$$

is not a monotone p-projection of the permanent. As the perfect matching polynomial counts perfect matchings in a general graph, and the permanent counts perfect matchings in a bipartite graph, it is interesting to consider this result in the context of the difference in complication between algorithms for finding perfect matchings in bipartite graphs (e. g., [19, 7]) and those for finding perfect matchings in general graphs (e. g., [6, 16, 32, 27]).

Remark 1.1 (On the Boolean semi-ring)**.** Our results also hold for *formal polynomials* over the Boolean semi-ring $\mathbb{B} = (\{0,1\},\vee,\wedge)$. Over the Boolean semi-ring, the permanent is the indicator function of the existence of a perfect matching in a bipartite graph, and the unsigned Pfaffian is the indicator function of a perfect matching in a general graph. However, over $\mathbb{B}$, each function is represented by more than one formal polynomial, and we do not know how to extend our results to the setting of *functions* over $\mathbb{B}$. See Section 5 for details and specific questions.

We also use the same technique, this time in combination with the lower bound of Fiorini *et al.* on extended formulations of the cut polytope [8], to show that the cut polynomials

$$\mathrm{Cut}^q = \sum_{A\subseteq[n]}\prod_{i\in A, j\notin A} x_{ij}^{q-1}$$

are not monotone p-projections of the permanent. Perhaps the main complexity-theoretic interest in the cut polynomials is that Cut^q *over the finite field* $\mathbb{F}_q$ was (until recently [15]) the only known example of a natural polynomial that is neither expected to be in $\mathsf{VP}_{\mathbb{F}_q}$ nor to be $\mathsf{VNP}_{\mathbb{F}_q}$-complete. (Indeed, either its membership in $\mathsf{VP}_{\mathbb{F}_q}$ *or* its $\mathsf{VNP}_{\mathbb{F}_q}$-completeness would imply the collapse of the polynomial-time hierarchy [4], contradicting a standard complexity-theoretic hypothesis.) There Bürgisser also showed that if $\mathsf{VP}_{\mathbb{F}_q} \neq \mathsf{VNP}_{\mathbb{F}_q}$ then such polynomials of intermediate complexity must exist. In that paper, Bürgisser asked whether the cut polynomials, considered as polynomials *over the rationals*, were $\mathsf{VNP}_{\mathbb{Q}}$-complete.[1] Although our results don't touch on this question, these previous results motivate the study of these polynomials over $\mathbb{Q}$.

[1] Cut^2 was subsequently shown to be $\mathsf{VNP}_{\mathbb{Q}}$-complete under circuit reductions [23]; its completeness under projections remains open.

Because the permanent is universal for monotone formulas, our lower bounds also imply exponential lower bounds on the monotone algebraic formula size—and, by balancing algebraic circuits, monotone algebraic circuit size—of these polynomials; see Section 4.2.

Finally, we note that our results shed a little more light on the intricacy of the known VNP-completeness proofs for the permanent [29, 3, 1]. Namely, prior to our result, the fact that the permanent is not hard modulo 2 already implied that any completeness result must use 2 in a "bad" way: for example, dividing by 2 somewhere. This is indeed true of Valiant's original proof [29], Ben-Dor & Halevi's proof [3], and Aaronson's quantum linear-optics proof [1].

Remark 1.2. One might hope for a classical analogue of Aaronson's quantum proof, using the characterization of BPP in terms of stochastic matrices as a replacement for the characterization of BQP using unitary matrices. However, our result indicates that the most straightforward adaptation of Aaronson's proof from the BQP setting to the BPP setting cannot work, as the use of stochastic matrices in this manner would produce a monotone reduction.

Our results also imply the necessity of the use of negative numbers in Valiant's 4×4 gadget [29, p. 195] and Ben-Dor and Halevi's 7×7 gadget [3, App. A]. In light of these results, Valiant's 4×4 gadget may perhaps seem less mysterious than the fact that such a gadget exists that is *only* 4×4!

To prove these results, we show that a monotone projection between non-negative polynomials essentially implies that the Newton polytope of one polynomial is an extension of the Newton polytope of the other (Lemma 3.1), and then apply known lower bounds on the extension complexity of certain polytopes. We hope that the connection between Newton polytopes, monotone projections, and extended formulations finds further use.

2 Preliminaries

A polynomial $f(x_1,\ldots,x_n)$ is a *(simple) projection* of a polynomial $g(y_1,\ldots,y_m)$ if f can be constructed from g by replacing each y_i with a constant or with some x_j. The polynomial f is an *affine projection* of g if f can be constructed from g by replacing each y_i with an affine linear function $\pi_i(\vec{x})$. When we say "projection" we mean simple projection. Given two families of polynomials, (f_n) and (g_n), if there is a function $p(n)$ such that f_n is a projection of $g_{p(n)}$ for all sufficiently large n, then we say that (f_n) is a projection of (g_n) with *blow-up* $p(n)$. If (f_n) is a projection of (g_n) with polynomial blow-up, we say that (f_n) is a *p-projection* of (g_n).

Over any subring of $\mathbb{R}$—or more generally any totally ordered semi-ring (see below)—a *monotone projection* is a projection in which all constants appearing in the projection are non-negative. Monotone p-projection is defined analogously.

To each monomial $x_1^{e_1}\cdots x_n^{e_n}$ we associate its exponent vector $(e_1,\ldots,e_n)$, as a point in $\mathbb{N}^n \subseteq \mathbb{R}^n$. These vectors determine the Newton polytope, defined as follows.

Definition 2.1. The *Newton polytope* of a polynomial $f(x_1,\ldots,x_n)$, denoted $\mathrm{Newt}(f)$, is the convex hull in $\mathbb{R}^n$ of the exponent vectors of all monomials appearing in f with non-zero coefficient.

A polytope is *integral* if all its vertices have integer coordinates; note that Newton polytopes are always integral. A *face* of a polytope P is the intersection of P with a linear space L such that none of the interior points of P lie in L.

For a polytope P, let $\mathrm{c}(P)$ denote the "complexity" of P, as measured by the minimal number of linear inequalities needed to define P (equivalently, the number of faces of P of dimension $\dim P - 1$). A polytope $Q \subseteq \mathbb{R}^m$ is an *extension* or *extended formulation* of $P \subseteq \mathbb{R}^n$ if there is an affine linear map $\ell \colon \mathbb{R}^m \to \mathbb{R}^n$ such that $\ell(Q) = P$. The *extension complexity* of P, denoted $\mathrm{xc}(P)$, is the minimum complexity of any extension of P (of any dimension): $\mathrm{xc}(P) = \min\{\mathrm{c}(Q) \mid Q \text{ is an extension of } P\}$.

The m-th *cycle cover polytope* (also known as the bipartite perfect matching polytope) is the convex hull in $\mathbb{R}^{m^2}$ of the $\{0,1\}$-indicator functions of the directed cycle covers of the complete directed graph with self-loops on m vertices. The cycle cover polytope is the Newton polytope of the permanent, as each monomial in the permanent corresponds to such a cycle cover.

A totally ordered semi-ring (we only consider commutative ones here) is a totally ordered set together with two operations, denoted $(R, \leq, \times, +, 1, 0)$ such that $(R, \times, 1)$ and $(R, +, 0)$ are both commutative monoids, $\times$ distributes over $+$, $0 \times a = 0$ for all a, $a + c \leq b + c$ whenever $a \leq b$, and $ac \leq bc$ whenever $a \leq b$ and $0 \leq c$. An element c of a totally ordered semi-ring is non-negative if $0 \leq c$, and is positive if furthermore $c \neq 0$. We will restrict our attention to *non-zero* totally ordered semi-rings; equivalently, we assume $1 \neq 0$. Note that in a totally ordered semiring, $1 + \cdots + 1$ is never zero.

The following totally ordered semi-rings are of particular interest.

- The real numbers with its usual ordering and arithmetic operations, $(\mathbb{R}, \leq, \times, +)$.
- The so-called "tropical semi-ring" $(\mathbb{R}, \leq, +, \min)$, which is the real numbers with its usual ordering, where the product is taken to be real addition and the addition operation is taken to be the minimum.
- The Boolean and-or semi-ring $\mathbb{B} = (\{0,1\}, \leq, \wedge, \vee)$, where $0 \leq 1$.

To get a feel for the latter two semi-rings, note that polynomials over the tropical semi-ring generally compute some optimization problem, and over $\mathbb{B}$ generally compute a decision problem. For example, the Hamiltonian Cycle polynomial over the tropical semi-ring computes the Traveling Salesperson Problem, and over $\mathbb{B}$, the indicator function of the existence of a Hamiltonian cycle. Note that over $\mathbb{R}$, if two formal polynomials compute the same function then they must be identical, but this is not true over the tropical or Boolean semi-rings.

3 Main lemma

Lemma 3.1. *Let R be a totally ordered semi-ring, and let $f(x_1, \ldots, x_n)$ and $g(y_1, \ldots, y_m)$ be polynomials over R with non-negative coefficients. If f is a monotone projection of g, then some face of* $\mathrm{Newt}(g)$ *is an extension of* $\mathrm{Newt}(f)$. *In particular,* $\mathrm{xc}(\mathrm{Newt}(f)) \leq \mathrm{c}(\mathrm{Newt}(g))$.

Proof. Under simple projections, a monomial in the y_i maps to some scalar multiple of a monomial in the x_j (possibly the empty monomial, resulting in a constant term, or possibly the zero multiple, resulting in zero). Let π be a monotone projection map, defined on the variables y_i, and extended naturally to monomials and terms in the y_i. (Recall that a *term* of a polynomial is a monomial together with its coefficient.) Since each term t of g is a monomial multiplied by a positive coefficient, and since π is non-negative, $\pi(t)$ is either zero or a single monomial in the x_j with nonzero coefficient. The former situation can happen only if t contains some variable y_i such that $\pi(y_i) = 0$. Let $\ker(\pi)$ denote the set $\{y_i \mid \pi(y_i) = 0\}$. Thus, for every term t of g that is disjoint from $\ker(\pi)$, $\pi(t)$ actually appears in f—possibly with a different coefficient, but still non-zero—since no terms can cancel under projection by π.

Let $e_1, \dots, e_m$ be the coordinate functions on $\mathbb{R}^m$, the ambient space of $\mathrm{Newt}(g)$; that is, $e_i \colon \mathbb{R}^m \to \mathbb{R}$ is projection onto the i-th coordinate. Let K denote the subspace of $\mathbb{R}^m$ defined by the equations $e_i = 0$ for each i such that $y_i \in \ker(\pi)$. Let P be the intersection of $\mathrm{Newt}(g)$ with K, considered as a polytope in K; since all vertices of $\mathrm{Newt}(g)$ are non-negative, intersecting $\mathrm{Newt}(g)$ with a coordinate hyperplane, $e_i = 0$, results in a face of $\mathrm{Newt}(g)$, and thus P is a face of $\mathrm{Newt}(g)$. Note that P is exactly the convex hull of the exponent vectors of monomials in g that are disjoint from $\ker(\pi)$. In particular, since π is multiplicative on monomials, it induces a *linear* map ℓ_π from K to $\mathbb{R}^n$ (the ambient space of $\mathrm{Newt}(f)$). By the previous paragraph, the exponent vectors of f are exactly ℓ_π applied to the exponent vectors of monomials in g that are disjoint from $\ker(\pi)$. By the linearity of ℓ_π and the convexity of P and $\mathrm{Newt}(f)$, we have that $\mathrm{Newt}(f) = \ell_\pi(P)$, so P is an extension of $\mathrm{Newt}(f)$. Since P is defined by intersecting $\mathrm{Newt}(g)$ with additional linear equations, the lemma follows. $\square$

Several partial converses to our Main Lemma also hold. Perhaps the most natural and interesting of these is the following.

Observation 3.2. *Let R be a totally ordered semi-ring. Given any sequence of non-negative integral polytopes $P_n \subseteq \mathbb{R}^n$ such that the* $\mathrm{poly}(n)$*-th cycle cover polytope is an extension of P_n along an affine linear map $\ell_n \colon \mathbb{R}^{\mathrm{poly}(n)} \to \mathbb{R}^n$ with integer coefficients of polynomial bit-length, there is a sequence of polynomials $(f_n) \in \mathsf{VNP}_R$ such that* $\mathrm{Newt}(f_n) = P_n$ *and f is a monotone p-projection of the permanent.*

Proof. Let C_m denote the m-th cycle cover polytope, let $m(n)$ be a polynomial such that $C_{m(n)}$ is an extended formulation of P_n, and let $b(n)$ be a polynomial upper bound on the bit-length of the coefficients of ℓ_n. Let V_m denote the vertex set of the cycle cover polytope, i. e., the incidence vectors of cycle covers. Define f_n as

$$\sum_{\vec{e} \in V_m} \vec{y}^{\ell_n(\vec{e})},$$

where $\vec{y} = (y_1, \dots, y_n)$, and the vector notation $\vec{y}^{\vec{e}'}$ is defined as $y_1^{e'_1} y_2^{e'_2} \cdots y_n^{e'_n}$. Note that ℓ_n has only integer coefficients by assumption, and each $\vec{e} \in V_m$ is integral, so the vector $\ell_n(\vec{e})$ is integral, and the above expression is a well-defined Laurent polynomial. To see that all the exponents are non-negative, note that by assumption each $\ell_n(\vec{e})$ lies in P_n, which is itself a non-negative polytope, so the above expression is in fact a well-defined *polynomial*. By construction, every exponent vector of f_n is in $\ell_n(C_{m(n)}) = P_n$. Conversely, every vertex of P_n is an exponent vector of f_n, since its coefficient is simply $1 + 1 + \cdots + 1$, which is never zero in a totally ordered semi-ring. (Without noting this, it would be possible that k distinct vertices in V_m would get mapped to the same point under ℓ_n, and then the corresponding monomials $\vec{y}^{\ell_n(\vec{e})}$ might add up to 0 in f_n.) Thus $\mathrm{Newt}(f_n) = P_n$. Furthermore, f_n is a monotone *nonlinear* projection of the permanent using the map $x_{ij} \mapsto \vec{y}^{\ell((0,0,\dots,1,\dots,0))}$, where the 1 is in the (i, j) position. Using the universality of the permanent and repeated squaring, this can easily be turned into a monotone *simple* projection of the permanent of size $\mathrm{poly}(m(n), b(n))$. $\square$

This can be generalized from the cycle cover polytopes and the permanent to arbitrary integral polytopes and the natural associated polynomial (the sum over all monomials whose exponent vectors are vertices of the polytope), but at the price of using "monomial projections"—in which each variable is replaced by a monomial—rather than simple projections. There ought to be a version of this observation over sufficiently large fields and allowing rational coefficients in ℓ, using Strassen's division trick [26], but the only such versions the author could come up with had so many hypotheses as to seem uninteresting.

4 Applications

4.1 Projection lower bounds

Remark 4.1. The following theorems hold over any totally ordered semi-ring, including the Boolean and-or semi-ring, the non-negative real numbers under multiplication and addition, and the tropical semi-ring of real numbers under addition and min. To see that this introduces no additional difficulty, note that over any totally ordered semi-ring R, the Newton polytope of a polynomial over R is still a polytope in a vector space over the real numbers, so standard results on polytopes and the cited results on extension complexity still apply.

Theorem 4.2 (Main Lemma + Rothvoss's TSP polytope lower bound)**.** *Over any totally ordered semi-ring, the Hamiltonian Cycle polynomial is not a monotone affine p-projection of the permanent; in fact, any monotone affine projection from the permanent to the Hamiltonian Cycle polynomial has blow-up at least* $2^{\Omega(n)}$.

We will need the following folklore lemma; as we could not find a proof in the literature, we a sketch its well-known proof here for completeness, and so that it can be verified that the standard proof preserves monotonicity.

Lemma 4.3 (Folklore)**.** *If an n-variable polynomial is an affine projection of the $m \times m$ permanent, then it is a simple projection of the $N \times N$ permanent for $N = m + (n+1)m^2$. The same holds with "affine projection" replaced by "monotone affine projection" in both places.*

Proof sketch. Let $\pi_{ij}(\vec{x})$ be the affine linear function corresponding to the variable y_{ij} of the $m \times m$ permanent, and write $\pi_{ij} = a_0 + a_1x_1 + \cdots + a_nx_n$. Let G be the complete directed graph with loops on m vertices and edge weights y_{ij}. Replace the edge (i, j) by $n+1$ parallel edges with weights $a_0, a_1x_1, \cdots, a_nx_n$. Add a new vertex on each of these parallel edges, splitting each parallel edge into two. For the edge weighted a_0, the two edges have weights $1, a_0$, and for the remaining edges the new edges get weights a_i, x_i. On each of the added vertices, add a self-loop of weight 1. Now consider the permanent of the weighted adjacency matrix of this edge-weighted directed graph. It is a simple exercise to see that this has the desired effect. Note also that if the original affine projection π was monotone, then so is the constructed simple projection. □

Proof of Theorem 4.2. By Lemma 4.3, it suffices to show the result for simple projections. If the Hamiltonian Cycle polynomial were a monotone projection of the permanent, then by the Main Lemma, some face of Newt(perm) would be an extension of Newt(HC).

The Newton polytope of the permanent is the cycle cover polytope (see Section 2). The cycle cover polytope can easily be described by the m^2 inequalities asserting that all variables $x_{i,j}$ are non-negative, together with the equalities asserting that each vertex has in-degree and out-degree exactly 1, namely $\sum_i x_{i,j} = 1$ for all j and $\sum_j x_{i,j} = 1$ for all i. (It is easy to see that these are necessary; for sufficiency, see, e. g., [25, Theorem 18.1].) Since equalities do not count towards the complexity of a polytope, we have $\mathrm{c}(\mathrm{Newt}(\mathrm{perm}_m)) \leq m^2$.

But the Newton polytope of the n-th Hamiltonian Cycle polynomial is exactly the TSP polytope, which, by a recent result by Rothvoss [22, Corollary 2], requires extension complexity $2^{\Omega(n)}$. □

Theorem 4.4 (Main Lemma + Rothvoss's perfect matching polytope lower bound)**.** *Over any totally ordered semi-ring, the perfect matching polynomial (or "unsigned Pfaffian") is not a monotone affine p-projection of the permanent; in fact, any monotone affine projection from the permanent to the perfect matching polynomial has blow-up at least* $2^{\Omega(n)}$.

Proof. The proof is the same as for the Hamiltonian Cycle polynomial, using [22, Theorem 1] by Rothvoss, which gives a lower bound of $2^{\Omega(n)}$ on the extension complexity of the perfect matching polytope, which is the Newton polytope of the perfect matching polynomial. □

Theorem 4.5 (Main Lemma + Fiorini *et al.*'s cut polytope lower bound)**.** *Over any totally ordered semi-ring, for any q, the q-th cut polynomial is not a monotone affine p-projection of the permanent; in fact, any monotone affine projection from the permanent to the q-th cut polynomial has blow-up at least* $2^{\Omega(n)}$.

Proof. Use [8, Theorem 7] by Fiorini *et al.* which says that $\mathrm{xc}(\mathrm{Newt}(\mathrm{Cut}^2)) \geq 2^{\Omega(n)}$, as $\mathrm{Newt}(\mathrm{Cut}^2)$ is the cut polytope. The one additional observation we need is that $\mathrm{Newt}(\mathrm{Cut}^q)$ is just the $(q-1)$-scaled version of $\mathrm{Newt}(\mathrm{Cut}^2)$, and this rescaling does not affect the extension complexity. □

4.2 Monotone formula and circuit lower bounds

As pointed out by an anonymous reviewer, the universality of the permanent for formula size also holds in the monotone setting, so lower bounds on monotone projections from the permanent imply the same lower bounds on monotone formula size, and therefore quasi-polynomially related lower bounds on monotone circuit size. We assume circuits only have gates of bounded fan-in; with unbounded fan-in, rather than losing a factor of a half in the exponent of the exponent, we lose a factor of a third.

Proposition 4.6. *Any polynomial computable by a monotone formula of size s is a monotone projection of* perm_{s+1}.

Proof. The proof of the universality of the permanent given in [5, Proposition 2.16] works *mutatis mutandis* in the monotone setting. □

As a consequence of this, Theorems 4.2–4.5 are nearly tight, since every monotone polynomial in n variables of $\mathrm{poly}(n)$ degree can be written as a monotone formula of size $2^{O(n\log n)}$ (write it as a sum of monomials).

Corollary 4.7. *Over any totally ordered semi-ring, any monotone formula computing the Hamiltonian Cycle polynomial, the perfect matching polynomial, or the q-th cut polynomial has size at least* $2^{\Omega(n)}$*. Consequently, any monotone circuit computing these polynomials has size at least* $2^{\Omega(\sqrt{n})}$.

For the cut polynomials, we believe this result to be new. For the other polynomials, this provides a new proof of (slightly weaker versions of) previously known lower bounds. Namely, Jerrum and Snir gave a lower bound of $(n-1)((n-2)2^{n-3}+1) = 2^{n+\Omega(\log n)}$ on the monotone circuit size of HC [11, Section 4.4], and a lower bound of $n(2^{n-1}-1)$ on the monotone circuit size of the permanent [11, Section 4.3]. As the permanent is a monotone projection of the perfect matching polynomial—namely, restrict the perfect matching polynomial to a bipartite graph, e. g., by setting $x_{ij}=0$ whenever i and j have the same parity—the same lower bound holds for the perfect matching polynomial.

Proof. The first part follows by combining Proposition 4.6 with Theorems 4.2–4.5. The second part follows from the fact that monotone circuits of size s can be balanced to have size $\mathrm{poly}(s)$ and depth $O(\log^2 s)$ (the proof in [31] works *mutatis mutandis* in the monotone setting), which can then be converted to monotone formulas of size $s^{O(\log s)} = 2^{O(\log^2 s)}$ by the usual conversion from bounded fan-in circuits to formulas. If there is a monotone circuit of size s computing any of these polynomials, there is thus a monotone formula of size $2^{O(\log^2 s)}$, which must be at least $2^{\Omega(n)}$, so $s \geq 2^{\Omega(n^{1/2})}$. □

5 Open questions

Despite the common feeling that Razborov's super-polynomial lower bound [20] on monotone Boolean circuits for CLIQUE "finished off" monotone Boolean circuit lower bounds, several natural and interesting question remain. For example, does Directed *s*-*t* Connectivity require monotone Boolean circuits of size $\Omega(n^3)$? (A matching upper bound is given by the Bellman–Ford algorithm.) Is there a monotone Boolean reduction from general perfect matching to bipartite perfect matching? A positive answer to the following question would rule out such monotone (projection) reductions.

Open Question 5.1. *Extend Theorem 4.4 from formal polynomials over the Boolean semi-ring to Boolean functions.*

However, there are even easier questions, intermediate between the Boolean function case and the algebraic case considered in this paper; Jukna [13] discusses the notion of one polynomial "counting" another, which means that they agree on all $\{0,1\}$ inputs.

Open Question 5.2. *Prove that no monotone polynomial-size projection of the permanent agrees with the perfect matching polynomial on all $\{0,1\}$ inputs ("counts the perfect matching polynomial"). Similarly, prove that no monotone polynomial-size projection of the permanent counts the Hamiltonian cycle polynomial.*

S. Jukna points out (personal communication) that projections of the *s*-*t* connectivity polynomial correspond, even in the Boolean setting, to switching-and-rectifier networks, so the known lower bounds on monotone switching-and-rectifier networks (see, e. g., the survey [21]) imply that the Hamiltonian path polynomial and the permanent are not monotone p-projections of the *s*-*t* connectivity polynomial, even over the Boolean semi-ring. This helps explain why the only known monotone lower bound on the *s*-*t* connectivity polynomial that we are aware of [13] goes by a somewhat roundabout proof: Razborov's lower bound on CLIQUE [20], followed by Valiant's reduction from the clique polynomial to the Hamiltonian path polynomial [28], followed by a standard reduction from Hamiltonian path to counting *s*-*t* paths. In the course of discussing this, we were led to the following question; although the motivation for the question has since disappeared, it still seems like an interesting question about polytopes, whose answer may require new methods.

Open Question 5.3 (S. Jukna, personal communication)**.** *Is the m-th s-t path polytope an extension of the n-th TSP polytope (or n-th cycle cover polytope) with* $m \leq \mathrm{poly}(n)$*?*

Since the separation problem for the *s*-*t* path polytope is NP-hard (see, e. g., [25, §13.1])—and the cycle cover polytope has low (extension) complexity—answering this question negatively seems to require more subtle understanding of these polytopes than "simply" an extended formulation lower bound.

Another example of a natural polytope question with a similar flavor comes from the cut polynomials. In combination with Bürgisser's results and questions on the cut polynomials [4] (discussed in Section 1), we are led to the following question.

Open Question 5.4. *Is the m-th cut polytope an extension of the n-th TSP polytope, for* $m \leq \mathrm{poly}(n)$*?*

A negative answer would show that Cut^q is not complete for non-negative polynomials in $\mathsf{VNP}_{\mathbb{Q}}$ under monotone p-projections, though as with the example of the permanent, this is not necessarily an obstacle to being VNP-complete under general p-projections. Yet even the monotone completeness of the cut polynomials remains open. In fact, even more basic questions remain open:

Open Question 5.5. *Is every non-negative polynomial in* VNP *a monotone projection of the Hamiltonian Cycle polynomial? Is there any polynomial that is "positive* VNP*-complete" in this sense?*

To relate this to the current proofs of VNP-completeness of HC_n, we need to draw a distinction. Let $\mathsf{VP}_{\mathbb{R}}^{\geq 0}$ denote the polynomial families in $\mathsf{VP}_{\mathbb{R}}$ all of whose coefficients are non-negative, and let $\mathsf{mVP}_{\mathbb{R}}$ ("monotone VP") denote the class of families of polynomials with polynomially many variables, of polynomial degree, and computable by polynomial-size *monotone* circuits over $\mathbb{R}$. Similarly, define $\mathsf{VNP}_{\mathbb{R}}^{\geq 0}$ to be the non-negative polynomials in $\mathsf{VNP}_{\mathbb{R}}$, and $\mathsf{mVNP}_{\mathbb{R}}$ to be the function families of the form

$$f_n = \sum_{\vec{e} \in \{0,1\}}^{\mathrm{poly}(n)} g_m(\vec{e}, \vec{x}) \, ,$$

where $m \leq \mathrm{poly}(n)$ and $(g_m) \in \mathsf{mVP}_{\mathbb{R}}$.

Valiant's original completeness proof for the Hamiltonian Cycle polynomial [28] is "mostly" monotone: it uses polynomial-size formulas for the coefficients of the monomials (coming from the definition of VNP), but otherwise is entirely monotone. In other words, the proof shows that HC is mVNP-hard under monotone projections. However, we note that it is not clear whether HC is even *in* mVNP! Question 5.5 asks whether HC, or indeed any polynomial, is $\mathsf{VNP}^{\geq 0}$-complete under monotone projections; the question of whether there exist polynomials that are mVNP-complete under monotone projections also seems potentially interesting.

Finally, we ask about stronger notions of monotone reduction, which seem to require a different kind of proof technique. Recall that a *c-reduction* from f to g is a family of polynomial-size algebraic circuits for f with oracle gates for g.

Open Question 5.6. *Do the analogues of Theorems 4.2–4.5 hold for monotone bounded-depth c-reductions in place of affine p-projections? What about weakly-skew or even general monotone c-reductions?*

6 Subsequent developments

Since the appearance of the preliminary version of this paper [9], our Main Lemma 3.1 has been used by Mahajan and Saurabh [15] to prove that several other polynomials of combinatorial and complexity-theoretic interest are not subexponential-size projections of the permanent.

1. The n-th *satisfiability polynomial* over $\mathbb{F}_q$ is a polynomial in $n+8\binom{n}{3}$ variables denoted $X_1,\ldots,X_n$ and $\{Y_c : c \in C_n\}$ where C_n denote the set of clauses on 3 literals in n variables. It is defined as

$$\mathrm{Sat}_n^q(X,Y) = \sum_{a\in\{0,1\}^n} \left(\prod_{i\in[n]} X_i^{q-1}\right)\left(\prod_{c\in C_n:c(a)=1} Y_c^{q-1}\right).$$

2. A *clow* in an n-vertex graph is a closed walk of length exactly n, in which the minimum-numbered vertex appears exactly once. The n-th *clow polynomial* over $\mathbb{F}_q$ is a polynomial in $\binom{n}{2}+n$ variables X_e for each edge e in the complete undirected graph K_n on n vertices and Y_v for each $v \in [n]$. It is defined as

$$\mathrm{Clow}_n^q(X,Y) = \sum_{w\text{:clow of length } n} \left(\prod_{e\text{:edges in } w} X_e^{q-1}\right)\left(\prod_{v\text{:distinct vertices in } w} Y_v^{q-1}\right),$$

or more precisely,

$$\mathrm{Clow}_n^q(X,Y) = \sum_{w=[v_0,\ldots,v_{n-1}]} \left(\prod_{i\in[n]} X_{(v_{i-1},v_{i \bmod n})}^{q-1}\right)\left(\prod_{v\in\{v_0,\ldots,v_{n-1}\}} Y_v^{q-1}\right),$$

where the sum is over clows w and v_0 denotes the minimum-numbered vertex in w.

3. The *clique polynomial* is a polynomial in $\binom{n}{2}$ variables X_e:

$$\mathrm{Clique}_n(X) = \sum_{\substack{T\subseteq\binom{[n]}{2} \\ T \text{ is a clique in } K_n}} \prod_{e\in T} X_e .$$

Theorem (Mahajan and Saurabh [15, Theorems 2 and 6])**.** *Over any totally ordered semi-ring, any monotone affine projection from the permanent to* Sat_n^q *or to the clique polynomial requires blow-up at least* $2^{\Omega(\sqrt{n})}$. *Any monotone affine projection from the permanent to* Clow_n^q *requires blow-up at least* $2^{\Omega(n)}$.

As in Section 4.2, we get the following corollary. Again, we note that the lower bound on the clique polynomial over the Boolean semi-ring only works for the formal clique polynomial (in contrast to Razborov's result [20], which works for any monotone Boolean circuit computing the CLIQUE *function*).

Corollary 6.1. *Over any totally ordered semi-ring, any monotone formula computing* Clow_n^q *has size at least* $2^{\Omega(n)}$ *and any monotone circuit computing* Clow_n^q *has size at least* $2^{\Omega(\sqrt{n})}$*. Any monotone formula computing* Sat_n^q *or* Clique_n *has size at least* $2^{\Omega(\sqrt{n})}$ *and any monotone circuit computing these polynomials has size at least* $2^{\Omega(n^{1/4})}$.

For the clow and satisfiability polynomials, we believe this result to be new. For the clique polynomials, this provides a new proof of a weaker version of the exponential monotone circuit lower bound due to Schnorr [24].[2]

Acknowledgment. We would like to thank Stasys Jukna for the question that motivated this paper [12], and `cstheory.stackexchange.com` for providing a forum for the question. We also thank Stasys for comments on a draft, pointing out the paper by Schnorr [24], and interesting discussions leading to Questions 5.2 and 5.3. We thank Leslie Valiant for an interesting conversation that led to Question 5.5. We thank Ketan Mulmuley and Youming Qiao for collaborating on [10], which is why the author had Newton polytopes on the mind. We thank an anonymous reviewer for pointing out the monotone universality of the permanent and therefore the implications for monotone formula and circuit size (Section 4.2 and Corollary 6.1). We thank Laci Babai for detailed comments on the journal submission.

References

[1] SCOTT AARONSON: A linear-optical proof that the permanent is #P-hard. *Proc. Royal Soc. London A*, 467(2136):3393–3405, 2011. [doi:10.1098/rspa.2011.0232, arXiv:1109.1674] 4

[2] SCOTT AARONSON AND ALEX ARKHIPOV: The computational complexity of linear optics. *Theory of Computing*, 9(4):143–252, 2013. Preliminary version in STOC'11. [doi:10.4086/toc.2013.v009a004, arXiv:1011.3245] 2

[3] AMIR BEN-DOR AND SHAI HALEVI: Zero-one permanent is #P-complete, a simpler proof. In *Proc. 2nd Israeli Symp. on Theory and Computing Systems*. IEEE Comp. Soc. Press, 1993. [doi:10.1109/ISTCS.1993.253457] 4

[4] PETER BÜRGISSER: On the structure of Valiant's complexity classes. *Discr. Math. & Theoret. Comput. Sci.*, 3(3):73–94, 1999. HAL. Preliminary version in STACS'98. 3, 10

[5] PETER BÜRGISSER: *Completeness and Reduction in Algebraic Complexity Theory*. Volume 7 of *Algorithms and Computation in Mathematics*. Springer, 2000. [doi:10.1007/978-3-662-04179-6] 8

[6] JACK EDMONDS: Paths, trees, and flowers. *Canad. J. Math.*, 17:449–467, 1965. [doi:10.4153/CJM-1965-045-4] 3

[2]Schnorr showed a $\binom{n}{k}-1$ lower bound on the monotone circuit size of the the k-th clique polynomial Clique_n^k, the sum over all cliques of size k, rather than all cliques. For $k = n/2$, this lower bound is asymptotically equal to $2^n/\sqrt{\pi n/2}$. The k-th clique polynomial Clique_n^k is the degree k homogeneous component of the clique polynomial Clique_n; by homogenization (implicit in Strassen's work, explicit in Valiant [30, Lemma 2]), any monotone circuit of size s for Clique_n can be converted into a monotone circuit of size $s(n/2+1)^2$ computing $\mathrm{Clique}_n^{n/2}$. Thus Schnorr's result implies a lower bound of $\Omega(2^n/n^{5/2})$ on the monotone circuit complexity of Clique_n.

[7] STEPHEN A. FENNER, ROHIT GURJAR, AND THOMAS THIERAUF: Bipartite perfect matching is in quasi-NC. In *Proc. 48th STOC*, pp. 754–763. ACM Press, 2016. [doi:10.1145/2897518.2897564, arXiv:1601.06319] 3

[8] SAMUEL FIORINI, SERGE MASSAR, SEBASTIAN POKUTTA, HANS RAJ TIWARY, AND RONALD DE WOLF: Exponential lower bounds for polytopes in combinatorial optimization. *J. ACM*, 62(2):17:1–23, 2015. Preliminary version in STOC'12. [doi:10.1145/2716307, arXiv:1111.0837] 2, 3, 8

[9] JOSHUA A. GROCHOW: Monotone projection lower bounds from extended formulation lower bounds, 2015. ECCC TR15-171. [arXiv:1510.08417] 11

[10] JOSHUA A. GROCHOW, KETAN D. MULMULEY, AND YOUMING QIAO: Boundaries of VP and VNP. In *Proc. 43rd Internat. Colloq. on Automata, Languages and Programming (ICALP'16)*, pp. 34:1–34:14. Springer, 2016. [doi:10.4230/LIPIcs.ICALP.2016.34, arXiv:1605.02815] 12

[11] MARK JERRUM AND MARC SNIR: Some exact complexity results for straight-line computations over semirings. *J. ACM*, 29(3):874–897, 1982. [doi:10.1145/322326.322341] 2, 9

[12] STASYS JUKNA: Why is Hamilton cycle so different from permanent? StackExchange, 2014. 2, 12

[13] STASYS JUKNA: Lower bounds for monotone counting circuits. *Discr. Appl. Math.*, 213:139–152, 2016. Preliminary version in ECCC TR14-169. [doi:10.1016/j.dam.2016.04.024, arXiv:1502.01865] 9

[14] JACOBUS H. VAN LINT AND RICHARD M. WILSON: *A Course in Combinatorics*. Cambridge Univ. Press, 2001. 2

[15] MEENA MAHAJAN AND NITIN SAURABH: Some complete and intermediate polynomials in algebraic complexity theory. In *Proc. 11th Comput. Sci. Symp. in Russia (CSR'16)*, pp. 251–265. Springer, 2016. Full version available at ECCC TR16-038. [doi:10.1007/978-3-319-34171-2_18, arXiv:1603.04606] 3, 11

[16] SILVIO MICALI AND VIJAY V. VAZIRANI: An O(sqrt(|V|) |E|) algorithm for finding maximum matching in general graphs. In *Proc. 12th STOC*, pp. 17–27. ACM Press, 1980. [doi:10.1109/SFCS.1980.12] 3

[17] HENRYK MINC: *Permanents*. Cambridge Univ. Press, 1984. 2

[18] THOMAS MUIR AND WILLIAM H. METZLER: *A Treatise on the Theory of Determinants*. Dover, 1960. 2

[19] KETAN MULMULEY, UMESH V. VAZIRANI, AND VIJAY V. VAZIRANI: Matching is as easy as matrix inversion. *Combinatorica*, 7(1):105–113, 1987. Preliminary version in STOC'87. [doi:10.1007/BF02579206] 3

[20] ALEXANDER A. RAZBOROV: Lower bounds on monotone complexity of the logical permanent function. *Math. Notes*, 37(6):485–493, 1985. [doi:10.1007/BF01157687] 2, 9, 11

[21] ALEXANDER A. RAZBOROV: Lower bounds for deterministic and nondeterministic branching programs. In *Fundamentals of Computation Theory (FCT'91)*, volume 529 of *LNCS*, pp. 47–60. Springer, 1991. [doi:10.1007/3-540-54458-5_49] 9

[22] THOMAS ROTHVOSS: The matching polytope has exponential extension complexity. *J. ACM*, 64(6):41:1–19, 2017. Preliminary version in STOC'14. [doi:10.1145/3127497, arXiv:1311.2369] 2, 3, 8

[23] NICOLAS DE RUGY-ALTHERRE: A dichotomy theorem for homomorphism polynomials. In *Proc. 37th Internat. Symp. Math. Found. Comput. Sci. (MFCS'12)*, pp. 308–322. Springer, 2012. [doi:10.1007/978-3-642-32589-2_29, arXiv:1210.7641] 3

[24] CLAUS-PETER SCHNORR: A lower bound on the number of additions in monotone computations. *Theoret. Comput. Sci.*, 2(3):305–315, 1976. [doi:10.1016/0304-3975(76)90083-9] 12

[25] ALEXANDER SCHRIJVER: *Combinatorial optimization. Polyhedra and efficiency. Vol. A*. Volume 24 of *Algorithms and Combinatorics*. Springer, 2003. Chapters 1–38. 8, 10

[26] VOLKER STRASSEN: Vermeidung von Divisionen. *J. Reine Angew. Math.*, 1973(264):184–202, 1973. [doi:10.1515/crll.1973.264.184] 7

[27] OLA SVENSSON AND JAKUB TARNAWSKI: The matching problem in general graphs is in quasi-NC. In *Proc. 58th FOCS*, pp. 696–707. IEEE Comp. Soc. Press, 2017. [doi:10.1109/FOCS.2017.70, arXiv:1704.01929] 3

[28] LESLIE G. VALIANT: Completeness classes in algebra. In *Proc. 11th STOC*, pp. 249–261. ACM Press, 1979. [doi:10.1145/800135.804419] 2, 9, 10

[29] LESLIE G. VALIANT: The complexity of computing the permanent. *Theoret. Comput. Sci.*, 8(2):189–201, 1979. [doi:10.1016/0304-3975(79)90044-6] 2, 4

[30] LESLIE G. VALIANT: Negation can be exponentially powerful. *Theoret. Comput. Sci.*, 12(3):303–314, 1980. Preliminary version in STOC'79. [doi:10.1016/0304-3975(80)90060-2] 12

[31] LESLIE G. VALIANT, SVEN SKYUM, STUART BERKOWITZ, AND CHARLES RACKOFF: Fast parallel computation of polynomials using few processors. *SIAM J. Comput.*, 12(4):641–644, 1983. Preliminary version in MFCS'81. [doi:10.1137/0212043] 9

[32] VIJAY V. VAZIRANI: A simplification of the MV matching algorithm and its proof, 2013. [arXiv:1210.4594] 3

[33] TZU-CHIEH WEI AND SIMONE SEVERINI: Matrix permanent and quantum entanglement of permutation invariant states. *J. Math. Phys.*, 51(9), 2010. [doi:10.1063/1.3464263, arXiv:0905.0012] 2

[34] MIHALIS YANNAKAKIS: Expressing combinatorial optimization problems by linear programs. *J. Comput. System Sci.*, 43(3):441–466, 1991. Preliminary version in STOC'88. [doi:10.1016/0022-0000(91)90024-Y] 2

AUTHOR

Joshua A. Grochow
Assistant professor
Departments of Computer Science and Mathematics
University of Colorado, Boulder, CO, USA
jgrochow@colorado.edu
http://www.cs.colorado.edu/~jgrochow

ABOUT THE AUTHOR

JOSHUA A. GROCHOW is an Assistant Professor in the Departments of Computer Science and Mathematics and the University of Colorado, Boulder. Prior to that he was an Omidyar Postdoctoral Fellow at the Santa Fe Institute, and a postdoc in the theory group at University of Toronto. He graduated from The University of Chicago in 2012; his advisors were Lance Fortnow and Ketan Mulmuley. In addition to his interests in algebraic and geometric complexity theory, he is also interested in broader issues in complex networks and complex adaptive systems, sometimes referred to in our community as “the other” complexity theory.