Electronic Colloquium on Computational Complexity, Report No. 171 (2015)

# Monotone projection lower bounds from extended formulation lower bounds

Joshua A. Grochow*

October 28, 2015

**Abstract**

In this short note, we show that the permanent is *not* complete for non-negative polynomials in $\mathsf{VNP}_{\mathbb{R}}$ under *monotone* p-projections. In particular, we show that Hamilton Cycle polynomial, $\sum_{n\text{-cycles }\sigma} \prod_{i=1}^{n} x_{i,\sigma(i)}$ and the cut polynomials $\sum_{A\subseteq[n]} \prod_{i\in A, j\notin A} x_{ij}^{q}$ are not monotone p-projections of the permanent. To prove this we introduce a new connection between monotone projections and extended formulations of linear programs that may have further applications.

## 1 Introduction

The permanent $\mathrm{perm}_n(X) = \sum_{\pi\in S_n} x_{1,\pi(1)}x_{2,\pi(2)}\cdots x_{n,\pi(n)}$ has long-fascinated combinatorialists [Min84, vLW01, MM60], more recently physicists [WS10, AA11], and since Valiant's seminal paper [Val79b], 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 #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 $k$ [Val79b], though the proof is more involved. Modulo any other number $n$, the permanent of integer matrices is $\mathsf{Mod}_n\mathsf{P}$-complete.

In contrast, the seemingly similar Hamilton Cycle polynomial,

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

where the sum is only over $n$-cycles rather than over all permutations, does not have these quirks: The Hamilton Cycle polynomial is VNP-complete over any ring $R$ [Val79a] and $\mathsf{Mod}_n\mathsf{P}$-complete for all $n$ (that is, counting Hamilton cycles is complete for these Boolean counting classes).

Jukna [Juk14] observed that if the Hamilton Cycle polynomial were a monotone p-projection of the permanent, then there would be a $2^{n^{\Omega(1)}}$ lower bound on monotone circuits computing the permanent, a lower bound that still remains open. Here we show that no such monotone reduction exists, by connecting monotone p-projections to extended formulations of linear programs.

*Santa Fe Institute, Santa Fe, NM, USA, jgrochow@santafe.edu



ISSN 1433-8092

We use the same technique to show that the cut polynomials $\mathrm{Cut}^q = \sum_{A \subseteq [n]} \prod_{i \in A, j \notin A} x_{ij}^q$ are not monotone p-projections of the permanent. Perhaps the main complexity-theoretic interest in the cut polynomials is that $\mathrm{Cut}^q$ *over the finite field* $\mathbb{F}_q$ is the only known example of a natural polynomial that is neither in $\mathsf{VP}_{\mathbb{F}_q}$ nor $\mathsf{VNP}_{\mathbb{F}_q}$-complete under a standard complexity-theoretic assumption (that $\mathsf{PH}$ doesn't collapse) [Bür99]; there it was also shown that if $\mathsf{VP}_{\mathbb{F}_q} \neq \mathsf{VNP}_{\mathbb{F}_q}$ then such polynomials of intermediate complexity must exist. In that paper, it was asked whether the cut polynomials, considered as polynomials *over the rationals*, were $\mathsf{VNP}_{\mathbb{Q}}$-complete. Although our results don't touch on this question, these previous results motivate the study of these polynomials over $\mathbb{Q}$. In combination with our results, they lead us to the following question:

**Open Question 1.** *Is the $m$-th cut polytope an extension of the $n$-th TSP polytope, for $m \leq poly(n)$?*

A negative answer would show that $\mathrm{Cut}^q$ 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 $\mathsf{VNP}$-complete under general p-projections. Yet even the monotone completeness of the cut polynomials remains open.

Finally, we note that our results shed a little more light on the complicatedness of the known $\mathsf{VNP}$-completeness proofs for the permanent [Val79b, Aar11]. 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, or somewhere requiring that some quantity that is necessarily even be non-zero. This is indeed true both of Valiant's original proof [Val79b] and of Aaronson's independent quantum linear-optics proof [Aar11]. One might hope for a classical analogue of Aaronson's quantum proof, using the characterization of $\mathsf{BPP}$ in terms of stochastic matrices as a replacement for the characterization of $\mathsf{BQP}$ using unitary matrices. However, our result says that any completeness proof for the permanent must use non-monotone reduction, so such a classical analogue is not possible:

**Corollary 1.** *Aaronson's quantum linear optics proof [Aar11] that the permanent is $\#\mathsf{P}$-hard cannot be replaced by one using classical randomized algorithms in place of quantum algorithms.*

In light of these results, Valiant's $4 \times 4$ gadget may perhaps seem less mysterious than the fact that such a gadget exists that is *only* $4 \times 4$!

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 $\ell_i(\vec{x})$. When we say "projection" we mean simple projection. Given two families of polynomials $(f_n)$, $(g_n)$, 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 a subring of $\mathbb{R}$ (or more generally, over a totally ordered ring), 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 $\mathbb{N}^n \subseteq \mathbb{R}^n$. We then have:

**Definition.** *The* Newton polytope *of a polynomial $f(x_1, \ldots, x_n)$, denoted* $\mathrm{New}(f)$*, 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.

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

The $n$-th TSP polytope is the convex hull of all points in $\{0,1\}^{\binom{n}{2}}$ corresponding to a Hamilton cycle in the complete graph $K_n$. The $n$-th cut polytope is the convex hull of all points in $\{0,1\}^{\binom{n}{2}}$ corresponding to cuts in the complete graph—that is, edge sets whose removal results in a disonnected graph.

## 3 Main Lemma

**Lemma 1.** *Let $f(x_1, \ldots, x_n)$ and $g(y_1, \ldots, y_m)$ be polynomials over $\mathbb{R}$ with non-negative coefficients. If $f$ is a monotone projection of $g$, then the intersection of* $\mathrm{New}(g)$ *with some linear subspace is an extension of* $\mathrm{New}(f)$*. In particular, $xc(\mathrm{New}(f)) \leq m + c(\mathrm{New}(g))$.*

Recall that a *term* of a polynomial is a monomial together with its coefficient.

*Proof.* Under simple projections, a monomial in the $y$'s maps to some scalar multiple of a monomial in the $x$'s (possibly the empty monomial, resulting in a constant term, or possibly the zero multiple, resulting in zero). Let $\pi$ be a monotone projection map, defined on the variables $y_i$, and extended naturally to monomials and terms in the $y$'s. Since each term $t$ of $g$ is a monomial multiplied by a positive coefficient, and since $\pi$ is non-negative, $\pi(t)$ is either zero or a single monomial in the $x$'s 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 $\{y_i | \pi(y_i) = 0\}$. Thus, for every term $t$ of $g$ that is disjoint from $\ker(\pi)$, $\pi(t)$ actually appears (possibly with a different coefficient, but still non-zero) in $f$, since no two terms can cancel under projection by $\pi$.

Let $e_1, \ldots, e_m$ be the coordinates on $\mathbb{R}^m$, the ambient space of $\mathrm{New}(g)$. 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 $\mathrm{New}(g)$ with $K$, considered as a polytope in $K$; note that $P$ is exactly the convex hull of the exponent vectors of monomials in $g$ that are disjoint from $\ker(\pi)$. Since $\pi$ is multiplicative on monomials, it induces a *linear* map $\ell_\pi$ from $K$ to $\mathbb{R}^n$ (the ambient space of $\mathrm{New}(f)$). By the previous paragraph, the exponent vectors of $f$ are exactly $\ell_\pi$ applied to the exponent vectors of monomials in $g$ that are disjoint from $\ker(\pi)$. By the linearity of $\ell_\pi$ and the convexity of $P$ and $\mathrm{New}(f)$, we have that $\mathrm{New}(f) = \ell_\pi(P)$, so

$P$ is an extension of $\mathrm{New}(f)$. Since $P$ is defined by intersecting $\mathrm{New}(g)$ with $\leq m$ additional linear equations, the lemma follows. □

Several partial converses to our main lemma also hold. Perhaps the most natural and interesting of these is:

**Observation 1.** *Given any sequence of integral polytopes $(P_n \subseteq \mathbb{R}^n)$ such that the poly$(n)$-th cycle cover polytope is an extension of $P_n$ along a projection $\pi_n \colon \mathbb{R}^{poly(n)} \to \mathbb{R}^n$ with integer coefficients of polynomial bit-length, there is a sequence of polynomials $(f_n) \in \mathsf{VNP}$ such that $\mathrm{New}(f_n) = P_n$ 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 $\pi_n$. Let $V_m$ denote the vertex set of the cycle cover polytope, i.e. the incidence vectors of cycle covers. Define $f_n$ as $\sum_{\vec{e} \in V_m} \vec{y}^{\pi(\vec{e})}$, where $\vec{y} = (y_1, \ldots, y_n)$. As every exponent vector of $f_n$ is in $\pi_n(C_{m(n)}) = P_n$, and conversely every vertex of $P_n$ is an exponent vector of $f_n$, we have $\mathrm{New}(f_n) = P_n$. Furthermore, $f_n$ is a monotone *nonlinear* projection of the permanent using the map $x_{ij} \mapsto \vec{y}^{\pi((0,0,\ldots,1,\ldots,0))}$, 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 $\mathrm{poly}(m(n), b(n))$. □

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 allowing rational coefficients in $\pi$ and using Strassen's division trick [Str73], but the only such versions the author could come up with had so many hypotheses as to seem uninteresting.

# 4 Applications

**Theorem 2.** *The Hamilton Cycle polynomial is not a monotone affine p-projection of the permanent; in fact, any monotone affine projection from the permanent to the Hamilton Cycle polynomial has blow-up at least $2^{\Omega(n^{1/4})}$.*

*Proof.* First, recall that if an $n$-variable polynomial is an affine projection of the $m \times m$ permanent, then it is a simple projection of the $(n+1)m \times (n+1)m$ permanent. For completeness we recall the brief proof: Let $\ell_{ij}(\vec{x})$ be the affine linear function corresponding to the variable $y_{ij}$ of the $m \times m$ permanent, and write $\ell_{ij} = a_0 + a_1 x_1 + \cdots + a_n x_n$. 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 $a_0, a_1 x_1, \cdots, a_n x_n$. 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 $a_i, x_i$. It is a simple and instructive exerise to see that this has the desired effect.

Now we show the result for simple projections. If the Hamilton Cycle polynomial were a monotone projection of the permanent, then by the Main Lemma, New(perm) (intersected with a linear subspace) would be an extension of New($HC$).

The Newton polytope of the permanent is the convex hull of all vectors in $\{0,1\}^{n^2}$ corresponding to directed cycle covers of a graph, as each monomial in the permanent

corresponds to such a cycle cover. The cycle cover polytope can easily be described by the $n$ equations saying that each vertex has in-degree and out-degree exactly 1. Thus $c(\mathrm{New}(\mathrm{perm}_n)) \leq n$.

But the Newton polytope of the Hamilton Cycle polynomial is exactly the TSP polytope, which by [FMP$^+$12, Theorem 11] requires extension complexity $2^{\Omega(n^{1/4})}$. □

**Theorem 3.** *For any $q$, the $q$-th cut polynomial is not a monotone $p$-projection of the permanent; in fact, any monotone projection from the permanent to the $q$-th cut polynomial has blow-up at least $2^{\Omega(n)}$.*

*Proof.* The proof is the same as for the Hamilton Cycle polynomial, using [FMP$^+$12, Theorem 7] which gives a lower bound of $2^{\Omega(n)}$ on the extension complexity of $\mathrm{New}(\mathrm{Cut}^1)$, the cut polytope. The one additional observation we need is that $\mathrm{New}(\mathrm{Cut}^q)$ is just the $q$-scaled version of $\mathrm{New}(\mathrm{Cut}^1)$, and this rescaling does not affect the extension complexity. □

**Acknowledgment.** We would like to thank Stasys Jukna for the question that motivated this paper [Juk14], and `cstheory.stackexchange.com` for providing a forum for the question. We thank Ketan Mulmuley and Youming Qiao for collaborating on [GMQ15], which is why the author had Newton polytopes on the mind.

## References

[AA11] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing*, STOC '11, pages 333–342, New York, NY, USA, 2011. ACM.

[Aar11] Scott Aaronson. A linear-optical proof that the permanent is #p-hard. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 467(2136):3393–3405, 2011.

[Bür99] Peter Bürgisser. On the structure of Valiant's complexity classes. *Discrete Math. Theor. Comput. Sci.*, 3(3):73–94, 1999.

[FMP$^+$12] Samuel Fiorini, Serge Massar, Sebastian Pokutta, Hans Raj Tiwary, and Ronald de Wolf. Linear vs. semidefinite extended formulations: Exponential separation and strong lower bounds. In *Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing*, STOC '12, pages 95–106, New York, NY, USA, 2012. ACM.

[GMQ15] Joshua A. Grochow, Ketan D. Mulmuley, and Youming Qiao. Degenerations of VP and VNP. In preparation, 2015.

[Juk14] Stasys Jukna. "Why is Hamilton Cycle so different from permanent?". `http://cstheory.stackexchange.com/q/27496/129`, 2014.

[Min84] Henryk Minc. *Permanents*. Cambridge University Press, 1984.

[MM60] Thomas Muir and William H. Metzler. *A treatise on the theory of determinants*. Dover, New York, 1960.

[Str73] Volker Strassen. Vermeidung von Divisionen. *J. Reine Angew. Math.*, 264:184–202, 1973.

[Val79a] Leslie G. Valiant. Completeness classes in algebra. In *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing*, STOC '79, pages 249–261, New York, NY, USA, 1979. ACM.

[Val79b] Leslie G. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8(2):189–201, 1979.

[vLW01] J. H. van Lint and R. M. Wilson. *A course in combinatorics*. Cambridge University Press, 2001.

[WS10] Tzu-Chieh Wei and Simone Severini. Matrix permanent and quantum entanglement of permutation invariant states. *Journal of Mathematical Physics*, 51(9), 2010.



ECCC ISSN 1433-8092

http://eccc.hpi-web.de