A tau-conjecture for Newton polygons

Pascal Koiran, Natacha Portier, Sébastien Tavenas, Stéphan Thomassé

A τ-Conjecture for Newton Polygons

Pascal Koiran, Natacha Portier, Sébastien Tavenas, Stéphan Thomassé
LIP*, École Normale Supérieure de Lyon, Université de Lyon

August 9, 2013

Abstract

One can associate to any bivariate polynomial $P(X, Y)$ its Newton polygon. This is the convex hull of the points (i, j) such that the monomial X^iY^j appears in P with a nonzero coefficient. We conjecture that when P is expressed as a sum of products of sparse polynomials, the number of edges of its Newton polygon is polynomially bounded in the size of such an expression. We show that this "τ-conjecture for Newton polygons," even in a weak form, implies that the permanent polynomial is not computable by polynomial size arithmetic circuits. We make the same observation for a weak version of an earlier "real τ-conjecture." Finally, we make some progress toward the τ-conjecture for Newton polygons using recent results from combinatorial geometry.

1 Introduction

Let $f \in \mathbb{Z}[X]$ be a univariate polynomial computed by an arithmetic circuit (or equivalently, a straight-line program) of size s starting from the variable X and the constant 1. According to Shub and Smale's τ-conjecture [17], the number of integer roots of f should be bounded by a fixed polynomial function of s. It was shown in [17] that the τ-conjecture implies a $\mathsf{P} \neq \mathsf{NP}$ result for the Blum-Shub-Smale model of computation over the complex numbers [4, 3]. A similar result was obtained by Bürgisser [7] for another algebraic version of P versus NP put forward by Valiant [22, 23] at the end of the 1970's. A succinct way of stating this VP versus VNP problem goes as follows: can we compute the permanent of a $n \times n$ matrix with a number of arithmetic operations which is polynomial in n? This question can be formalized using the computation model of arithmetic circuits. The permanent plays a special role here because it is VNP-complete, and it can be replaced by any other VNP-complete family of polynomials. We refer to Bürgisser's book [6] for an introduction to this topic and to two recent surveys on arithmetic circuit complexity by Shpilka and Yehudayoff [16] and by Chen, Kayal and Wigderson [8].

As a natural approach to the τ-conjecture, one can try to bound the number of real roots instead of the number of integer roots. This fails miserably since

*UMR 5668 ENS Lyon, CNRS, UCBL, INRIA. Email: [Pascal.Koiran, Natacha.Portier, Sebastien.Tavenas, Stephan.Thomasse]@ens-lyon.fr

the number of real roots of a univariate polynomial can be exponential in its arithmetic circuit size. Chebyshev polynomials provide such an example [18] (a similar example was provided earlier by Borodin and Cook [5]). A real version of the τ-conjecture was nevertheless proposed in [14]. In order to avoid the aforementioned counterexamples, the attention is restricted to arithmetic circuits of a special form: the sums of products of sparse polynomials. In spite of this restriction, the real τ-conjecture still implies that the permanent is hard to compute for general arithmetic circuits [14].

In this paper, we propose a τ-conjecture for Newton polygons of bivariate polynomials. Like the real τ-conjecture, it deals with sums of products of sparse polynomials and implies that the permanent is hard for general arithmetic circuits. A common idea to these three τ-conjecture is that "simple" arithmetic circuits should compute only "simple" polynomials. In the original τ-conjecture, the simplicity of a polynomial is measured by the number of its integer roots; in the real τ-conjecture it is measured by the number of its real roots; and in our new conjecture by the number of edges of its Newton polygon.

Organization of the paper

In Section 2 we review some basic facts about Newton polygons and formulate the corresponding τ-conjecture. We also state in Theorem 1 the motivating result for this paper: a proof of the conjecture, even in a very weak form, implies a lower bound for the permanent. In Section 3 we give a proof of this result and of a refinement: it suffices to work with sums of *powers* of sparse polynomials rather than with sums of arbitrary products. We also point out that this refinement applies to the real τ-conjecture from [14], and that (like in Theorem 1) a very weak form of this conjecture implies a lower bound for the permanent. These observations improve the results stated in [14]. In Section 4 we use a recent result of convex geometry [9] to provide nontrivial upper bounds on the number of edges of Newton polygons. Our results fall short of establising the new τ-conjecture (even in the weak form required by Theorem 1) but they improve significantly on the naive bound obtained by brute-force expansion. For instance, as a very special case of our results we have that the Newton polygon of $fg + 1$ has $O(t^{4/3})$ edges if the bivariate polynomials f and g have at most t monomials. The straightforward bound obtained by expanding the product fg is only $O(t^2)$. We conclude the paper with a couple of open problems. In particular, we ask whether this $O(t^{4/3})$ upper bound is optimal. In the appendix, we improve on this upper bound by giving a linear upper bound in a special case.

2 Newton Polygons

We first recall some standard background on Newton polygons. Much more can be found in the survey [19]. Consider a bivariate polynomial $f \in \mathbb{C}[X, Y]$. To each monomial $X^i Y^j$ appearing in f with a nonzero coefficient we associate the point with coordinates (i, j) in the Euclidean plane. We denote by $\mathrm{Mon}(f)$ this finite set of points. By definition the Newton polygon of f, denoted $\mathrm{Newt}(f)$,

is the convex hull of $\mathrm{Mon}(f)$. Note that $\mathrm{Newt}(f)$ has at most t edges if f has t monomials. It is well known that the Newton polygon of a product of polynomials is the Minkowski sum of their Newton polygons, i.e.,

$$\mathrm{Newt}(fg) = \mathrm{Newt}(f) + \mathrm{Newt}(g) = \{p + q;\ p \in \mathrm{Newt}(f),\ q \in \mathrm{Newt}(g)\}.$$

As a result, if f has s monomials and g has t monomials then $\mathrm{Newt}(fg)$ has at most $s + t$ edges. More generally, for a product $f = g_1 g_2 \cdots g_m$, $\mathrm{Newt}(f)$ has at most $\sum_{i=1}^{m} t_i$ edges where t_i is the number of monomials of g_i; but f can of course have up to $\prod_{i=1}^{m} t_i$ monomials. The number of edges of a Newton polygon is therefore easy to control for a product of polynomials. In contrast, the situation is not at all clear for a sum of products. We propose the following conjecture.

Conjecture 1 (τ-conjecture for Newton polygons)**.** *There is a polynomial p such that the following property holds.*

Consider any bivariate polynomial $f \in \mathbb{C}[X, Y]$ of the form

$$f(X, Y) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X, Y) \tag{1}$$

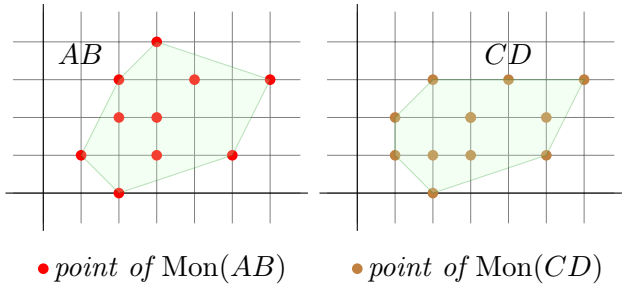
where the f_{ij} have at most t monomials. Then the Newton polygon of f has at most $p(kmt)$ edges.

The "real τ-conjecture" [14] is a similar conjecture for real roots of sums of products of sparse[1] univariate polynomials, and it implies that the permanent does not have polynomial-size arithmetic circuit. As we shall see shortly, the same lower bound would follow from Conjecture 1.

By expanding the products in (1) we see that f has at most $k.t^m$ monomials, and this is an upper bound on the number of edges of its Newton polygon. In order to improve this very coarse bound, the main difficulty we have to face is that the k-fold summation in the definition of f may lead to cancellations of monomials. As a result, some of the vertices of $\mathrm{Newt}(f)$ might not be vertices of the Newton polygons of any of the k products $\prod_{j=1}^{m} f_{ij}(X, Y)$. We give two examples of such cancellations below. If there are no cancellations (for instance, if the f_{ij} only have positive coefficients) then we indeed have a polynomial upper bound. In this case, $\mathrm{Newt}(f)$ is the convex hull of the union of the Newton polygons of the k products. Each of these k Newton polygons has at most mt vertices, so $\mathrm{Newt}(f)$ has at most kmt vertices and as many edges.

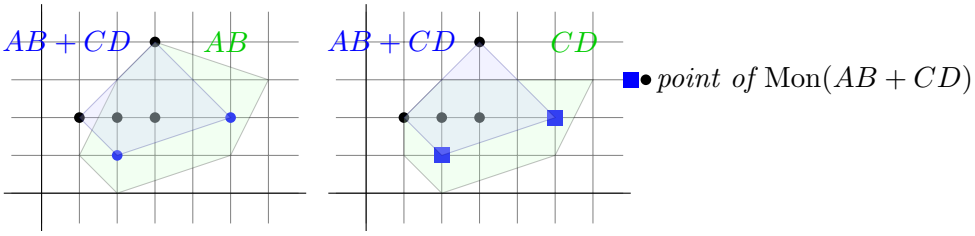
Example 1. *We define $A(X, Y) = XY + X^2 + X^2Y^2 + X^3Y + X^5Y$, $B(X, Y) = 1 + XY^2$, $C(X, Y) = -X - XY - X^2Y^2$ and $D(X, Y) = Y + X + X^2Y + X^4Y$.*

[1] Here and in [14], the term "sparse" refers to the fact that we measure the size of a polynomial f_{ij} by the number of its monomials.



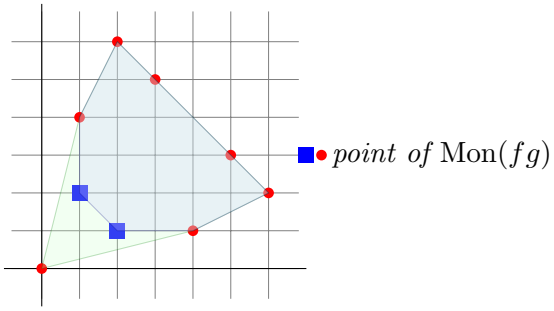
Then,

$$\begin{aligned} AB + CD =& (XY + X^2 + X^2Y^2 + X^3Y + X^5Y + X^2Y^3 + X^3Y^2 + X^3Y^4 \\ &+ X^4Y^3 + X^6Y^3) - (XY + X^2 + X^3Y + X^5Y + XY^2 \\ &+ X^2Y + 2X^3Y^2 + X^5Y^2 + X^2Y^3 + X^4Y^3 + X^6Y^3) \\ =& X^2Y^2 + X^3Y^4 - XY^2 - X^2Y - X^3Y^2 - X^5Y^2 \end{aligned}$$



The two rectangle points lie on the convex hull of $\mathrm{Mon}(AB + CD)$*, but do not lie on the convex hulls of* $\mathrm{Mon}(AB)$ *or* $\mathrm{Mon}(CD)$*.*

Example 2. *We define* $f(X,Y) = 1+X^2Y+Y^2X$*,* $g(X,Y) = 1+X^4Y+XY^4$ *and we consider* $\mathrm{Mon}(fg-1)$*.*



The two rectangle points lie on the convex hull of $\mathrm{Mon}(fg-1)$*, but do not lie on the convex hull of* $\mathrm{Mon}(fg)$*.*

Conjecture 1 implies that the permanent is hard for arithmetic circuits. In fact, a significantly weaker bound on the number of edges would be sufficient:

Theorem 1. *Assume that for some universal constant* $c < 2$*, the upper bound* $2^{(m+\log kt)^c}$ *on the number of edges of* $\mathrm{Newt}(f)$ *holds true for polynomials of the form (1) whenever the product* kmt *is sufficiently large. Then the permanent is not computable by polynomial size, constant-free arithmetic circuits.*

For instance, an upper bound of the form $2^{O(m)}(kt)^{O(1)}$ would be sufficient. Note that the parameter m plays a very different role than the parameters k and t. By "constant-free arithmetic circuit" we mean that -1 is the only constant allowed as input to the circuit (if subtraction gates are allowed in adition to $+$ and $\times$ gates, one can of course replace -1 by 1). It is possible to give a similar result for circuits using arbitrary complex constants, but this seems to require the use of the Generalized Riemann Hypothesis (to learn more on complex constants and the role of GRH one may consult [7, 6, 13]).

3 Proof of Theorem 1, and a Refinement

Consider the polynomial

$$f_n(X,Y) = \prod_{i=1}^{2^n}(X + Y^i). \tag{2}$$

The Newton polygon of f_n has exactly 2^{n+1} edges: each factor $X + Y^i$ contributes an edge of horizontal length 1 and slope $-i$. Each edge appears twice on the boundary of $\mathrm{Newt}(f_n)$, once on the lower hull and once on the upper hull.

Our proof of Theorem 1 is by contradiction. Assuming that the permanent is computable by polynomial size, constant-free arithmetic circuits we will show that f_n can be put under form (1) with $k = n^{O(\sqrt{n}\log n)}$, $t = n^{O(\sqrt{n}\log n)}$ and $m = O(\sqrt{n})$. Note that the upper bound on m is much smaller than those on k and t. Then, from the assumption in Theorem 1 we conclude that $\mathrm{Newt}(f_n)$ has at most $2^{(m+\log kt)^c}$ edges. This is a contradiction since for large enough n, this upper bound is smaller than the actual number of edges of $\mathrm{Newt}(f_n)$, namely, 2^{n+1} (here, we use the fact that the constant c in Theorem 1 is smaller than 2).

Reduction of arithmetic circuits to depth 4 is an important ingredient in the proof of Theorem 1. This phenomenon was discovered by Agrawal and Vinay [1]. We will use it under the following form [15] (recall that a depth 4 circuit is a sum of products of sums of products of inputs; sum and product gates may have arbitrary fan-in).

Theorem 2. *Let C be an arithmetic circuit of size t computing a polynomial of degree d. There is an equivalent depth four circuit Γ of size $t^{O(\sqrt{d}\log d)}$ with multiplication gates of fan-in $O(\sqrt{d})$.*

Note that Theorem 3 of [15] provides this bound for the case where d is the so-called "formal degree" of C rather than the degree of the polynomial computed by C. Theorem 2 as stated above can then be derived by an application of the standard homogenization trick (see e.g. Proposition 5 and Theorem 5 in [15]). It was recently shown [21] that the size bound for Γ can be reduced from $t^{O(\sqrt{d}\log d)}$ to $t^{O(\sqrt{d})}$ when d is polynomially bounded in t; this improvement preserves the $O(\sqrt{d})$ bound on the fan-in of multiplication gates.

We can now complete the proof of Theorem 1. We will be brief because the details are almost exactly the same as in [14], see especially Section 5 of that

paper (here we have to deal with bivariate instead of univariate polynomials, but this does lead to any significant complication). First, we expand the polynomial f_n in (2) as an (exponential-size) sum of monomials:

$$f_n(X,Y) = \sum_{\alpha,\beta} a(n,\alpha,\beta) X^\alpha Y^\beta.$$

Then we expand the integers coefficients $a(n,\alpha,\beta)$ in base 2:

$$a(n,\alpha,\beta) = \sum_i a_i(n,\alpha,\beta) 2^i$$

where $a_i(n,\alpha,\beta) \in \{0,1\}$. Putting these two expansions together, we obtain

$$f_n(X,Y) = \sum_{i,\alpha,\beta} a_i(n,\alpha,\beta) 2^i X^\alpha Y^\beta.$$

We now expand the exponents i, α and β in base 2. This leads to the equality

$$f_n(X,Y) = h_n(X^{2^0}, X^{2^1}, X^{2^2}, \ldots, Y^{2^0}, Y^{2^1}, Y^{2^2}, \ldots, 2^{2^0}, 2^{2^1}, 2^{2^2}, \ldots) \qquad (3)$$

where $h_n(x_0, x_1, x_2, \ldots, y_0, y_1, y_2, \ldots, z_0, z_1, z_2, \ldots)$ is the multilinear polynomial

$$\sum_{i,\alpha,\beta} a_i(n,\alpha,\beta) x_0^{\alpha_0} x_1^{\alpha_1} x_2^{\alpha_2} \cdots y_0^{\beta_0} y_1^{\beta_1} y_2^{\beta_2} \cdots z_0^{i_0} z_1^{i_1} z_2^{i_2} \cdots$$

Here the exponents i_j, α_j, β_j denote the binary digits of the integers i, α, β. Note that h_n is a polynomial in $O(n)$ variables since those integers have $O(n)$ bits. Next, we use our hypothesis that the permanent is computable by polynomial size, constant-free arithmetic circuits. This implies that the coefficients $a_i(n,\alpha,\beta)$ can be computed non-uniformly in time polynomial in n (a detailed argument for the case of univariate polynomials is provided in Lemma 3 and Theorem 6 of [14]; it hinges on the fact that these coefficients lie unconditionally in the couting hiearchy, and this hierarchy collapses if the permanent is easy to compute). By Valiant's criterion [6], this implies that the polynomial family (h_n) belongs to the complexity class VNP. Since the permanent is VNP-complete and is assumed to have polynomial-size circuits, (h_n) also has polynomial-size circuits. By Theorem 2, it follows that the polynomials h_n are computable by depth 4 circuits of size $n^{O(\sqrt{n}\log n)}$ with multiplication gates of fan-in $O(\sqrt{n})$. Using (3), we can plug in powers of X, Y and powers of 2 into those circuits to express f_n as a sum of products like in (1). The resulting parameters k and t are of order $n^{O(\sqrt{n}\log n)}$, and $m = O(\sqrt{n})$. As explained at the beginning of this section, this leads to a contradiction with the assumption in Theorem 1. □

In the remainder of this section we give a refinement of Theorem 1. We show that it suffices to bound the number of edges of the Newton polygons of sums of *powers* of sparse polynomials in order to obtain a lower bound for the permanent.

Theorem 3. *Fix a universal constant $c < 2$, and assume that we have the upper bound $2^{(m+\log kt)^c}$ on the number of edges of* $\mathrm{Newt}(f)$ *for polynomials of the form*

$$f(X,Y) = \sum_{i=1}^{k} a_i f_i(X,Y)^m \tag{4}$$

where $a_i \in \mathbb{C}$ and the f_i have at most t monomials (as in Theorem 1, we require this upper bound to hold only if kmt is sufficiently large). Then the permanent is not computable by polynomial size, constant-free arithmetic circuits.

Clearly, we can assume that all the coefficients a_i are equal to 1 (multiply f_i by a m-th root of a_i if necessary).

Theorem 3 is an easy consequence of Theorem 1 and Fischer's formula [10]. This formula shows that any monomial $z_1 z_2 \cdots z_m$ can be expressed as a linear combination of 2^{m-1} powers of linears forms.

Lemma 1. *For any m, we have*

$$2^{m-1} m! z_1 z_2 \cdots z_m = \sum_{r=(r_2,\ldots,r_m)\in\{-1,1\}^{m-1}} (\prod_{i=2}^{m} r_i)(x_1 + \sum_{i=2}^{m} r_i x_i)^m.$$

Note that the exponential blowup entailed by Fischer's formula is acceptable because we will apply it with a value of m which is small compared to the main complexity parameter n, i.e., with $m = O(\sqrt{n})$. Other recent applications of this formula to arithmetic circuit complexity can be found in [11, 12].

Proof of Theorem 3. We show that the assumption in Theorem 3 implies that of Theorem 1. Consider therefore a polynomial f of the form (1). We rewrite it as a sum of powers by applying Lemma 1 to each of the k products in (1). This yields an identity of the form

$$f(X,Y) = \sum_{i=1}^{k'} a_i f_i(X,Y)^m$$

where $a_i \in \mathbb{C}$, the f_i have at most mt monomials, and $k' = 2^{m-1}k$. We are now in position to apply Theorem 3: $\mathrm{Newt}(f)$ has at most $2^{(m+\log k't')^c}$ edges. For any constant $c' > c$, this is less than $2^{(m+\log kt)^{c'}}$ if kmt is sufficiently large. We have therefore derived the hypothesis of Theorem 1 from that of Theorem 3, and we can conlude that the permanent is hard for arithmetic circuits. □

Remark 1. *As pointed out in the introduction, we gave in [14] similar results for real roots of univariate polynomials rather than for Newton polygons of bivariate polynomials. More precisely, let us measure the size of a sum of products of sparse polynomials by $s = kmt$. This definition of "size" applies to bivariate polynomials of the form (1) as well as to their univariate analogues. We showed that for any constant $c < 2$, a $2^{(\log s)^c}$ upper bound on the number of real roots implies that the permanent is hard for arithmetic circuit (see Conjecture 3 in [14] and the remarks following it). In fact, the same proof shows*

than an upper bound of the form $2^{(m+\log kt)^c}$ as in Theorem 1 is sufficient. This is clearly a better way of stating our result since it allows for a much worse dependency of the number of real roots with respect to m. Moreover, as in Theorem 3 it is sufficient to establish this bound for sums of powers. As in the proof of Theorem 3, this follows from a straightforward application of Fischer's formula.

4 Upper Bounds from Convexity Arguments

In this section we improve the coarse upper bound $k.t^m$ upper bound on the number of edges of Newton polygons of polynomials of the form (1). Our main tool is a result of convex geometry [9].

Theorem 4. *Let P and Q be two planar point sets with $|P| = s$ and $|Q| = t$. Let S be a subset of the Minkowski sum $P+Q$. If S is convexly independent (i.e., its elements are the vertices of a convex polygon) we have $|S| = O(s^{2/3}t^{2/3} + s + t)$.*

It is known that this upper bound is optimal up to constant factors [2] (a non-optimal lower bound was also given in [20]).

We first consider sums of products of two polynomials.

Theorem 5. *Consider a bivariate polynomial $f \in \mathbb{C}[X, Y]$ of the form*

$$f(X, Y) = \sum_{i=1}^{k} f_i g_i(X, Y) \tag{5}$$

where the f_i have at most r monomials and the g_i have at most s monomials. The Newton polygon of f has $O(k(r^{2/3}s^{2/3} + r + s))$ edges.

Proof. Let S_i be the set of monomials of $f_i g_i$ which appear in f with a nonzero coefficient. Since $\mathrm{Newt}(f)$ is the convex hull of $\bigcup_{i=1}^{k} \mathrm{conv}(S_i)$, it is enough to bound the number of vertices of $\mathrm{conv}(S_i)$. Those vertices form a convexly independent subset of the Minkowski sum $\mathrm{Mon}(f_i)+\mathrm{Mon}(g_i)$. By Theorem 4, it follows that $\mathrm{conv}(S_i)$ has $O(r^{2/3}s^{2/3} + r + s)$ vertices. Multiplying this estimate by k yields an upper bound on the number of vertices and edges of $\mathrm{Newt}(f)$. □

From this result it is easy to derive an upper bound for the general case, where we have products of $m \geq 2$ polynomials. We just divide the m factors into two groups of approximately $m/2$ factors, and in each group we expand the product by brute force.

Theorem 6. *Consider any bivariate polynomial $f \in \mathbb{C}[X, Y]$ of the form*

$$f(X, Y) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X, Y) \tag{6}$$

where $m \geq 2$ and the f_{ij} have at most t monomials. The Newton polygon of f has $O(k.t^{2m/3})$ edges.

Proof. As suggested above, we write each of the k products as a product of two polynomials $F_i = \prod_{i=1}^{\lfloor m/2 \rfloor} f_i$ and $G_i = \prod_{i=1}^{\lceil m/2 \rceil} f_i$. We can now apply Theorem 5 to $f = \sum_{i=1}^{k} F_i G_i$, with $r = t^{\lfloor m/2 \rfloor}$ and $s = t^{\lceil m/2 \rceil}$. In the resulting $O(k(r^{2/3}s^{2/3} + r + s))$ upper bound the term $kr^{2/3}s^{2/3}$ dominates since $r^{2/3}s^{2/3} = t^{2(\lfloor m/2 \rfloor + \lceil m/2 \rceil)/3} = t^{2m/3}$ and $m \geq 2$. □

In order to avoid the brute force expansion in the proof of this theorem it is natural to consider for each i a convexly independent subset S_i of the Minkowski sum of the m sets $\mathrm{Mon}(f_{i1}), \ldots, \mathrm{Mon}(f_{im})$. This is exactly the open problem at the end of [2]: determine the maximal cardinality $M_m(t)$ of a convexly independent subset of the Minkowski sum of m sets $P_0, \ldots, P_{m-1}$ of t points in the Euclidean plane. For instance, the lower bound of [2] combined with the upper bound of [9] shows that $M_2(t) = \Theta(t^{4/3})$. Unfortunately, we shall see that $M_m(t) = t^{\Omega(m)}$, so that brute force expansion is not very far from the optimum.

Example 3. *Fix an integer $b \geq 2$. Let P_k be the $b \times b$ grid made of the integer points whose coordinates have all their base b digits equal to zero, except possibly the digit of weight b^k. More explicitly,*

$$P_k = \{(b^k.i, b^k.j;\ 0 \leq i, j \leq b-1\}.$$

Clearly, the Minkowksi sum $P_0 + \ldots + P_{m-1}$ is the $b^m \times b^m$ grid $\{0, \ldots, b^m - 1\}^2$.

The next lemma (which is certainly not optimal) shows how to find a fairly large set of convexly independent points in a grid.

Lemma 2. *If $n(n-1)/2 < N$ it is possible to find n convexly independent points in the grid $[N]^2$.*

Proof. We start from the origin and build a sequence of $n-1$ line segments. The i-th segment has horizontal length i and slope $1/i$. We can keep going as long as we do not go out of the grid, i.e., as long as $n(n-1)/2 < N$. Altogether, the $n-1$ segments have n endpoints and they are convexly independent. □

Proposition 1. *For all m and infinitely many values of t we have:*

$$M_m(t) \geq \sqrt{2} t^{m/4}.$$

Proof. From Example 3 and Lemma 2 we have $M_m(b^2) \geq n$ if $n(n-1) < 2b^m$. Hence $M_m(b^2) \geq \sqrt{2b^m}$. The result follows by setting $t = b^2$. □

This result shows that other ingredients than Theorem 4 will be needed to answer Conjecture 1 positively. A similar argument can be made for the case where the sets $P_0, P_1, \ldots, P_{m-1}$ in the Minkowski sum are all equal (this is a natural case to look at in light of Theorem 3, which shows that it suffices to deal with sums of powers in order to obtain a lower bound for the permanent). More precisely, let $M'_m(t)$ be the maximal cardinality of a convexly independent subset of an m-fold Minkoski sum $P + P + \cdots + P$ where P is a set of at most m points. By definition we have $M'_m(t) \leq M_m(t)$. In the other direction we have $M'_m(t) \geq M_m(\lfloor t/m \rfloor)$: just replace the m sets of size $\lfloor t/m \rfloor$ by their union. Hence we have $M'_m(t) \geq \sqrt{2} \lfloor t/m \rfloor^{m/4}$.

5 Final Remarks

In this paper we have proposed a conjecture on the number of edges of the Newton polygon of a sum of products of sparse polynomials; and we have shown in Theorem 1 that even a weak version of this conjecture implies a lower bound for the permanent. We conclude with a couple of additional open problems.

1. Consider two polynomials $f, g \in \mathbb{C}[X, Y]$ with at most t monomials each. What is the maximum number of edges on the Newton polygon of $fg+1$? Theorem 5 provides a $O(t^{4/3})$ upper bound, but as far as we know the "true" bound could be linear in t. In the appendix we prove a linear upper bound under the assumption that f and g have the same supports (i.e., $\mathrm{Mon}(f) = \mathrm{Mon}(g)$) and that the square of any nonconstant monomial appearing in f and g does not appear.

2. More generally, what is the maximum number of edges on the Newton polygon of $f_1 \ldots ... f_m + 1$, where the f_i again have at most t monomials? Theorem 6 provides a $O(t^{2m/3})$ upper bound, but the true bound could be of the form $2^{O(m)}t^{O(1)}$; it could even be polynomial in m and t, as implied by Conjecture 1.

Acknowledgments

Proposition 1 arose from a discussion with Mark Braverman.

References

[1] M. Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. In *Proc. 49th IEEE Symposium on Foundations of Computer Science*, pages 67–75, 2008.

[2] Ondrej Bílka, Kevin Buchin, Radoslav Fulek, Masashi Kiyomi, Yoshio Okamoto, Shin–ichi Tanigawa, and Csaba D. Tóth. A tight lower bound for convexly independent subsets of the Minkowski sums of planar point sets. *Electr. J. Comb.*, 17(1), 2010.

[3] L. Blum, F. Cucker, M. Shub, and S. Smale. Algebraic settings for the problem "P≠NP?". In J. Renegar, M. Shub, and S. Smale, editors, *The Mathematics of Numerical Analysis*, volume 32 of *Lectures in Applied Mathematics*, pages 125–144. American Mathematical Society, 1996.

[4] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bulletin of the American Mathematical Society*, 21(1):1–46, July 1989.

[5] A. Borodin and S. Cook. On the number additions to compute specific polynomials. *SIAM Journal on Computing*, 5(1):146–157, 1976.

[6] P. Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*. Number 7 in Algorithms and Computation in Mathematics. Springer, 2000.

[7] P. Bürgisser. On defining integers and proving arithmetic circuit lower bounds. *Computational Complexity*, 18:81–103, 2009. Conference version in STACS 2007.

[8] Xi Chen, Neeraj Kayal, and Avi Wigderson. Partial derivatives in arithmetic complexity and beyond. *Foundations and Trends in Theoretical Computer Science*, 6(1):1–138, 2011.

[9] Friedrich Eisenbrand, János Pach, Thomas Rothvoß, and Nir B. Sopher. Convexly independent subsets of the Minkowski sum of planar point sets. *Electr. J. Comb.*, 15(1), 2008.

[10] Ismor Fischer. Sums of like powers of multivariate linear forms. *Mathematics Magazine*, 67(1):59–61, 1994.

[11] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Arithmetic circuits: A chasm at depth three. *Electronic Colloquium on Computational Complexity (ECCC)*, 20, 2013.

[12] N. Kayal. An exponential lower bound for the sum of powers of bounded degree polynomials. *Electronic Colloquium on Computational Complexity (ECCC)*, 19, 2012.

[13] P. Koiran. Hilbert's Nullstellensatz is in the polynomial hierarchy. *Journal of Complexity*, 12(4):273–286, 1996. Long version: DIMACS report 96-27.

[14] P. Koiran. Shallow circuits with high-powered inputs. In *Proc. Second Symposium on Innovations in Computer Science (ICS 2011)*, 2011. arxiv.org/abs/1004.4960.

[15] P. Koiran. Arithmetic circuits: the chasm at depth four gets wider. *Theoretical Computer Science*, (448):56–65, 2012.

[16] Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5(3-4), 2010.

[17] M. Shub and S. Smale. On the intractability of Hilbert's Nullstellensatz and an algebraic version of "P=NP". *Duke Mathematical Journal*, 81(1):47–54, 1995.

[18] S. Smale. Mathematical problems for the next century. *Mathematical Intelligencer*, 20(2):7–15, 1998.

[19] Bernd Sturmfels. Polynomial equations and convex polytopes. *The American Mathematical Monthly*, 105(10):907–922, 1998.

[20] Konrad J. Swanepoel and Pavel Valtr. Large convexly independent subsets of Minkowski sums. *Electr. J. Comb.*, 17(1), 2010.

[21] S. Tavenas. Improved bounds for reduction to depth 4 and depth 3. In *Proc. 38th International Symposium on Mathematical Foundations of Computer Science (MFCS)*, 2013.

[22] L. G. Valiant. Completeness classes in algebra. In *Proc. 11th ACM Symposium on Theory of Computing*, pages 249–261, 1979.

[23] L. G. Valiant. Reducibility by algebraic projections. In *Logic and Algorithmic (an International Symposium held in honour of Ernst Specker)*, pages 365–380. Monographie n^o 30 de L'Enseignement Mathématique, 1982.

Appendix: the Newton polygon of $fg+1$

We give here (in Theorem 7) a linear upper bound assuming the following two properties:

(i) The polynomials f and g have the same support, i.e., $\mathrm{Mon}(f) = \mathrm{Mon}(g)$. We denote by $\{p_0, \ldots, p_{t-1}\}$ this common support.

(ii) If f and g have a constant term we assume without loss of generality that $p_0 = 0$ and we add the following requirement: if p_j is an extremal point of $\mathrm{conv}(p_1, p_2, \ldots, p_{t-1})$ then $2p_j$ is not in the support of f and g.

We do not know how to prove a linear upper bound assuming only (i). Condition (ii) is satisfied in particular when the points in $\mathrm{Mon}(f) = \mathrm{Mon}(g)$ are convexly independent.

The interesting case, which we consider first, is when f and g have a constant term but $fg+1$ has no constant term. As explained above we assume that p_0 corresponds to the constant terms of f and g, i.e., $p_0 = 0$. Under these hypotheses we have the following result.

Proposition 2. $\mathrm{Newt}(fg+1) = \mathrm{conv}(2p_1, \ldots, 2p_{t-1}, (p_i)_{i\in I})$ *where* $(p_i)_{i\in I}$ *is the subset of those monomials in* $\mathrm{Mon}(f)$ *which appear in* $fg+1$ *with a nonzero coefficient.*

Proof. We first prove the inclusion from left to right. Since $fg+1$ has no constant term, all monomials of $fg+1$ are of the form $p_i + p_j$ where $i \geq 1$ or $j \geq 1$. Consider first the case where i and j are both nonzero. If $i = j$ this monomial appears in the right-hand side, and if $i \neq j$ it is the middle point of two points (namely, $2p_i$ and $2p_j$) appearing in the right-hand side. The remaining case is when $i = 0$ or $j = 0$. If e.g. $j = 0$ we have $p_i + p_j = p_i$ and we see from the definition of I that this monomial also appears in the right-hand side.

Now we prove the inclusion from right to left. Again by definition of I, all the p_i with $i \in I$ are monomials of $fg+1$. Hence it remains to show that

$$\mathrm{conv}(2p_1, \ldots, 2p_{t-1}) \subseteq \mathrm{Newt}(fg+1).$$

The left-hand side can be written as $\mathrm{conv}((2p_j)_{j\in J})$ where the p_j form a convexly independent subset of $\{p_1, \ldots, p_{t-1}\}$. Any monomial of the form $2p_j$ with $j \in J$ appears in $fg+1$ with a nonzero coefficient because it can be obtained in a unique way by expansion of the product fg. Assume indeed that $2p_j = p_i + p_k$ with $i, k \neq j$. Then p_j is the middle point of p_i and p_k. If $i \geq 1$ and $k \geq 1$, this is impossible by construction of J. If $i = 0$ or $k = 0$, this is also impossible by hypothesis (ii). We thus have $\mathrm{conv}((2p_j)_{j\in J}) \subseteq \mathrm{Newt}(fg+1)$, and the proof is complete. □

We note that this proposition does not hold without assumption (ii), as shown by the following example: take $f = 1 + X^2Y + XY^2 + (1/2)X^2Y^4 + (1/2)X^4Y^2$ and $g = -1 + X^2Y + XY^2 - (1/2)X^2Y^4 - (1/2)X^4Y^2$. Then $fg+1 = 2X^3Y^3 - (1/2)X^6Y^6 - (1/4)X^4Y^8 - (1/4)X^8Y^4$. The monomial X^3Y^3 is a vertex of $\mathrm{Newt}(fg+1)$ but is not of the form p_i or $2p_j$ prescribed by Proposition 2.

Theorem 7. *Under the same assumptions (i) and (ii) as above,* $\mathrm{Newt}(fg+1)$ *has at most* $t+1$ *edges where* t *denotes the number of monomials of* f *and* g.

Proof. We continue to denote the common support of f and g by $\{p_0, \ldots, p_{t-1}\}$. If 0 does not belong to this support then $\mathrm{Newt}(fg+1)$ is the disjoint union of $\{0\}$ and $\mathrm{Newt}(fg)$. Moreover, $\mathrm{Newt}(fg) = \mathrm{Newt}(f) + \mathrm{Newt}(g) = \mathrm{conv}(2p_0, \ldots, 2p_{t-1})$.

If 0 is in the support and $fg+1$ has a constant term then $\mathrm{Newt}(fg+1) = \mathrm{Newt}(fg)$ has at most t edges.

In the remaining case (0 is in the support but $fg+1$ has no constant term) we need to use hypothesis (ii). This case is treated in Proposition 2. At first sight it seems that $\mathrm{Newt}(fg+1)$ can have up to $2(t-1)$ vertices, but the list of possible vertices can be shortened by picking a convexly independent subsequence. More precisely, write $\mathrm{conv}(2p_1, \ldots, 2p_{t-1}, (p_i)_{i\in I}) = \mathrm{conv}((2p_j)_{j\in J}, (p_k)_{k\in K})$ where $J \subseteq \{1, \ldots, t-1\}$ and $K \subseteq I$ are chosen so that the points in this sequence are convexly independent. By the lemma below, $|J \cap K| \leq 2$. As a result, the number of points in the sequence is $|J| + |K| = |J \cup K| + |J \cap K| \leq (t-1) + 2 = t+1$. □

Lemma 3. *If p, q, r are 3 distinct nonzero points in the plane then the 6 points p, q, r, $2p$, $2q$, $2r$ are not convexly independent.*

This is clear from a picture and can be proved for instance by considering the 4 points 0, p, q, r. There are two cases.

1. If these 4 points are convexly independent, assume for instance that pq is a diagonal of the quadrangle $0pqr$. Then the line pq separates 0 from r. As a result, $r \in \mathrm{conv}(p, q, 2r)$.
2. If the 4 points are not convexly independent, assume for instance that $r \in \mathrm{conv}(0, p, q)$. In this case, $2r \in \mathrm{conv}(2p, 2q, r)$. □