

## A tau-conjecture for Newton polygons

Pascal Koiran, Natacha Portier, Sébastien Tavenas, Stéphan Thomassé

► **To cite this version:**

Pascal Koiran, Natacha Portier, Sébastien Tavenas, Stéphan Thomassé. A tau-conjecture for Newton polygons. 2014, pp.14. <ensl-00850791v2>

**HAL Id: ensl-00850791**

**<https://hal-ens-lyon.archives-ouvertes.fr/ensl-00850791v2>**

Submitted on 12 May 2014

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# A $\tau$ -Conjecture for Newton Polygons

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

May 12, 2014

## 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  $X^i Y^j$  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 “ $\tau$ -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  $\tau$ -conjecture.” Finally, we make some progress toward the  $\tau$ -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  $\tau$ -conjecture [21], the number of integer roots of  $f$  should be bounded by a fixed polynomial function of  $s$ . It was shown in [21] that the  $\tau$ -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  $\mathsf{P}$  versus  $\mathsf{NP}$  put forward by Valiant [27, 28] at the end of the 1970’s. A succinct way of stating this  $\mathsf{VP}$  versus  $\mathsf{VNP}$  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  $\mathsf{VNP}$ -complete, and it can be replaced by any other  $\mathsf{VNP}$ -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 [20] and by Chen, Kayal and Wigderson [8].

---

\*UMR 5668 ENS Lyon, CNRS, UCBL, INRIA. Email: [Pascal.Koiran, Natacha.Portier, Sebastien.Tavenas, Stephan.Thomasse]@ens-lyon.fr. The authors are supported by ANR project CompA.

As a natural approach to the  $\tau$ -conjecture, one can try to bound the number of real roots instead of the number of integer roots. This fails miserably since the number of real roots of a univariate polynomial can be exponential in its arithmetic circuit size. Chebyshev polynomials provide such an example [22] (a similar example was provided earlier by Borodin and Cook [5]). A real version of the  $\tau$ -conjecture was nevertheless proposed in [17]. 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  $\tau$ -conjecture still implies that the permanent is hard to compute for general arithmetic circuits [17].

In this paper, we propose a  $\tau$ -conjecture for Newton polygons of bivariate polynomials. Like the real  $\tau$ -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  $\tau$ -conjecture is that “simple” arithmetic circuits should compute only “simple” polynomials. In the original  $\tau$ -conjecture, the simplicity of a polynomial is measured by the number of its integer roots; in the real  $\tau$ -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. These conjectures are independent in the sense that we know of no implication between two of them.

## Organization of the paper

In Section 2 we review some basic facts about Newton polygons and formulate the corresponding  $\tau$ -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  $\tau$ -conjecture from [17], 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 [17]. 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 establishing the new  $\tau$ -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

In the following we will consider a field  $\mathbb{K}$  of characteristic 0. In fact, most of the results of this paper are valid for a general field.

We first recall some standard background on Newton polygons. Much more can be found in the survey [23]. Consider a bivariate polynomial  $f \in \mathbb{K}[X, Y]$ . 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  $\text{Mon}(f)$  this finite set of points. If  $A$  is a set of points in the plane, we denote by  $\text{conv}(A)$  the convex hull of  $A$ . By definition the Newton polygon of  $f$ , denoted  $\text{Newt}(f)$ , is the convex hull of  $\text{Mon}(f)$  (In particular,  $\text{Newt}(f) = \text{conv}(\text{Mon}(f))$ ). Note that  $\text{Newt}(f)$  has at most  $t$  edges if  $f$  has  $t$  monomials. It is well known [19] that the Newton polygon of a product of polynomials is the Minkowski sum of their Newton polygons, i.e.,

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

A short proof of this fact can be found in [11]. As a result, if  $f$  has  $s$  monomials and  $g$  has  $t$  monomials then  $\text{Newt}(fg)$  has at most  $s + t$  edges. More generally, for a product  $f = g_1 g_2 \cdots g_m$ ,  $\text{Newt}(f)$  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** ( $\tau$ -conjecture for Newton polygons). *There is a polynomial  $p$  such that the following property holds.*

*Consider any bivariate polynomial  $f \in \mathbb{K}[X, Y]$  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.*

Note that the bound only depends on  $k$ ,  $m$  and  $t$ , and so does not depend on the degrees and coefficients of the polynomials  $f_{i,j}$ .

The “real  $\tau$ -conjecture” [17] is a similar conjecture for real roots of sums of products of sparse<sup>1</sup> univariate polynomials, and it implies that the permanent does not have polynomial-size arithmetic circuits. We are not able to compare these two conjectures. However, as we shall see shortly, Conjecture 1 also implies that the permanent does not have polynomial-size arithmetic circuits.

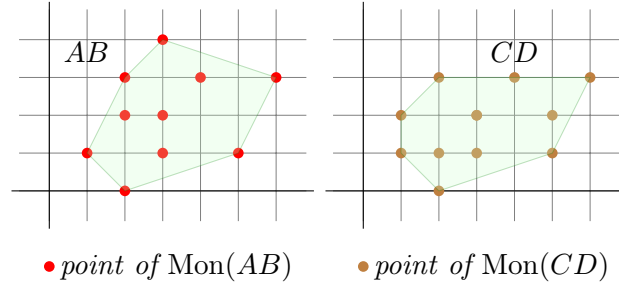
One can also formulate a  $\tau$ -conjecture for the multiplicities of (complex) nonzero roots of univariate polynomials (see Corollary 2.4.1 in [14]). This conjecture again implies that the permanent is hard for arithmetic circuits.

---

<sup>1</sup>Here and in [17], the term “sparse” refers to the fact that we measure the size of a polynomial  $f_{ij}$  by the number of its monomials.

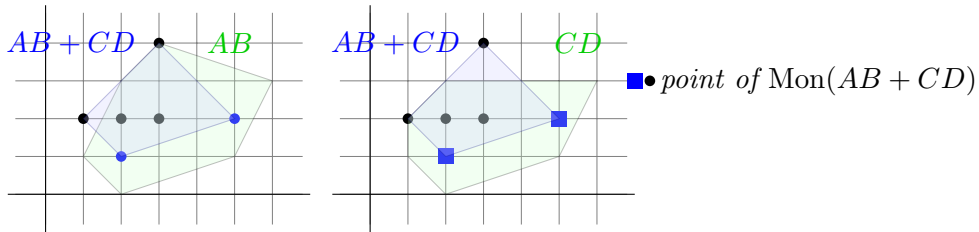
By expanding the products in (1) we see that  $f$  has at most  $k \cdot t^m$  monomials, and this is an upper bound on the number of edges of its Newton polygon. In order to improve this very coarse bound, the main difficulty we have to face is that the  $k$ -fold summation in the definition of  $f$  may lead to cancellations of monomials. As a result, some of the vertices of  $\text{Newt}(f)$  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,  $\text{Newt}(f)$  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  $\text{Newt}(f)$  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  $D(X, Y) = Y + X + X^2Y + X^4Y$ .



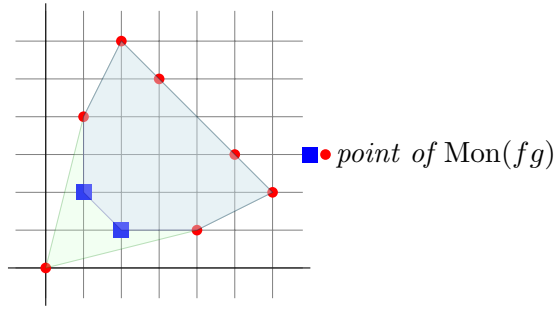
Then,

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



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

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



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

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  $\text{Newt}(f)$  holds true for polynomials of the form (1) whenever the product  $kmt$  is sufficiently large. Then the permanent is not computable by polynomial size 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  $t$ .

**Remark 1.** *Theorem 1 holds true even in the case of a field of positive characteristic different from two. In characteristic two, the permanent is equal to the determinant and is therefore easy for arithmetic circuits. However, the conclusion of Theorem 1 remains true in characteristic two if we replace the permanent by the Hamiltonian polynomial (or any other polynomial family which is VNP-complete in characteristic two).*

### 3 Proof of Theorem 1, and a Refinement

Consider the polynomial

$$f_n(X, Y) = \sum_{i=0}^{2^n-1} X^i Y^{i^2}. \quad (2)$$

The Newton polygon of  $f_n$  has exactly  $2^n$  edges.

Our proof of Theorem 1 is by contradiction. Assuming that the permanent is computable by polynomial size 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  $\text{Newt}(f_n)$  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  $\text{Newt}(f_n)$ , namely,  $2^n$  (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 [18] (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  $\Gamma$  of size  $t^{O(\sqrt{d}\log d)}$  with multiplication gates of fan-in  $O(\sqrt{d})$ .*

Note that Theorem 3 of [18] 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 [18]). It was recently shown [25] that the size bound for  $\Gamma$  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. The idea of this proof is based on the one of Proposition 2 in [17], but is simpler since it doesn’t use the counting hierarchy. A similar simplification can be done for the real  $\tau$ -conjecture [26].

We can expand the exponents  $i$  and  $i^2$  of (2) in base 2. This leads to the equality

$$f_n(X, Y) = h_n(X^{2^0}, X^{2^1}, \dots, X^{2^{n-1}}, Y^{2^0}, \dots, Y^{2^{2n-1}}) \quad (3)$$

where  $h_n(x_0, x_1, \dots, x_{n-1}, y_0, \dots, y_{2n-1})$  is the multilinear polynomial

$$\sum_{\alpha \in \{0,1\}^n, \beta \in \{0,1\}^{2n}} a(n, \alpha, \beta) x_0^{\alpha_0} x_1^{\alpha_1} \dots x_{n-1}^{\alpha_{n-1}} y_0^{\beta_0} \dots y_{2n-1}^{\beta_{2n-1}}.$$

Here the exponents  $\alpha_j, \beta_j$  denote the coordinates of the vectors  $\alpha, \beta$ . The coefficient  $a(n, \alpha, \beta)$  equals 1 if the vector  $\beta$  corresponds to the square of the vector  $\alpha$  and 0 otherwise. Note that  $h_n$  is a polynomial in  $3n$  variables. The coefficients  $a(n, \alpha, \beta)$  can be computed in time polynomial in  $n$ . 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.  $\square$

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  $\text{Newt}(f)$  for polynomials of the form

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

where  $a_i \in \mathbb{K}$  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 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 linear forms.

**Lemma 1.** For any  $m$ , we have

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

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  $m = O(\sqrt{n})$ . The idea of using Fischer's formula to turn a product into sums of powers comes from [12, 15].

*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  $a_i \in \mathbb{K}$ , the  $f_i$  have at most  $mt$  monomials, and  $k' = 2^{m-1}k$ . We are now in position to apply Theorem 1:  $\text{Newt}(f)$  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 conclude that the permanent is hard for arithmetic circuits.  $\square$

**Remark 2.** For Theorem 3, the fact that  $\mathbb{K}$  has characteristic 0 is important. Indeed, in positive characteristic Lemma 1 does not allow to rewrite a monomial  $z_1 z_2 \cdots z_m$  as a linear combination of powers of linear forms.

**Remark 3.** As pointed out in the introduction, we gave in [17] 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 [17] and the remarks following it). In fact, the same proof shows that 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). These results apply to fields of arbitrary characteristic. 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 [24]). A linear upper bound is known [13] for the case where  $P$  and  $Q$  are convexly independent.

We first consider sums of products of two polynomials.

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

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

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 points in the plane corresponding to the monomials of  $f_i g_i$  which appear in  $f$  with a nonzero coefficient. Since  $\text{Newt}(f)$  is the convex hull of  $\bigcup_{i=1}^k \text{conv}(S_i)$ , it is enough to bound the number of vertices of  $\text{conv}(S_i)$ . Those vertices form a convexly independent subset of the Minkowski sum  $\text{Mon}(f_i) + \text{Mon}(g_i)$ . By Theorem 4, it follows that  $\text{conv}(S_i)$  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  $\text{Newt}(f)$ .  $\square$

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  $f \in \mathbb{K}[X, Y]$  of the form

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

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

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  $\text{Mon}(f_{i1}), \dots, \text{Mon}(f_{im})$ . 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  $P_0, \dots, P_{m-1}$  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  $b^2 \times b$  grid made of the integer points  $(x, y)$  such that:

- all the digits in base  $b^2$  of  $x$  are equal to zero, except possibly the digit of weight  $b^{2k}$ ;
- all the digits in base  $b$  of  $y$  are equal to zero, except possibly the digit of weight  $b^k$ .

More explicitly,

$$P_k = \{(b^{2k} \cdot i, b^k \cdot j); 0 \leq i \leq b^2 - 1 \text{ and } 0 \leq j \leq b - 1\}.$$

Clearly, the Minkowski sum  $P_0 + \dots + P_{m-1}$  is the grid  $\{0, \dots, b^{2m} - 1\} \times \{0, \dots, b^m - 1\}$  of size  $b^{2m} \times b^m$ .

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  $n(n-1)/2 < M$  and  $n < N$  it is possible to find  $n$  convexly independent points in the grid  $M \times N$ .

*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  $n(n-1)/2 < M$  and  $n < N$ . Altogether, the  $n-1$  segments have  $n$  endpoints and they are convexly independent.  $\square$

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

$$M_m(t) \geq t^{m/3} - 1.$$

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

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  $P_0, P_1, \dots, P_{m-1}$  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 Minkowski sum  $P + P + \dots + P$  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  $M'_m(t) \geq \lfloor t/m \rfloor^{m/3} - 1$ .

## 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  $f, g \in \mathbb{K}[X, Y]$  with at most  $t$  monomials each. What is the maximum number of edges on the Newton polygon of  $fg + 1$ ? The difficult case appears when the constant term of  $fg$  equals  $-1$ . 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.,  $\text{Mon}(f) = \text{Mon}(g)$ ) and that the square of any nonconstant monomial appearing in  $f$  and  $g$  does not appear in  $fg$ .
2. More generally, what is the maximum number of edges on the Newton polygon of  $f_1 \dots f_m + 1$ , 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 and an improvement was suggested by an anonymous referee. We thank the three referees for suggesting several improvements in the presentation of the paper.

## 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 Břilka, 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 “ $P \neq NP$ ?”. 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] S. Gao. Absolute irreducibility of polynomials via Newton polytopes. *Journal of Algebra*, 237(2):501–520, 2001.
- [12] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Arithmetic circuits: A chasm at depth three. *Electronic Colloquium on Computational Complexity (ECCC)*, 20, 2013.
- [13] N. Halman, S. Onn, and U. Rothblum. The convex dimension of a graph. *Discrete Applied Mathematics*, 155:1373–1383, 2007.
- [14] P. Hrubeš. On the Real  $\tau$ -Conjecture and the Distribution of Complex Roots. *Theory of Computing*, 9(10):403–411, 2013.
- [15] N. Kayal. An exponential lower bound for the sum of powers of bounded degree polynomials. *Electronic Colloquium on Computational Complexity (ECCC)*, 19, 2012.
- [16] P. Koiran. Hilbert’s Nullstellensatz is in the polynomial hierarchy. *Journal of Complexity*, 12(4):273–286, 1996. Long version: DIMACS report 96-27.
- [17] 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](http://arxiv.org/abs/1004.4960).

- [18] P. Koiran. Arithmetic circuits: the chasm at depth four gets wider. *Theoretical Computer Science*, (448):56–65, 2012.
- [19] A.M. Ostrowski. ber die Bedeutung der Theorie der konvexen Polyeder fr die formale Algebra. *Jahresberichte Deutsche Math. Verein*, 20:98–99, 1921.
- [20] 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.
- [21] 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.
- [22] S. Smale. Mathematical problems for the next century. *Mathematical Intelligencer*, 20(2):7–15, 1998.
- [23] Bernd Sturmfels. Polynomial equations and convex polytopes. *The American Mathematical Monthly*, 105(10):907–922, 1998.
- [24] Konrad J. Swanepoel and Pavel Valtr. Large convexly independent subsets of Minkowski sums. *Electr. J. Comb.*, 17(1), 2010.
- [25] 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.
- [26] S. Tavenas. Bornes inférieures et supérieures pour les circuits arithmétiques. PhD thesis, 2014.
- [27] L. G. Valiant. Completeness classes in algebra. In *Proc. 11th ACM Symposium on Theory of Computing*, pages 249–261, 1979.
- [28] 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° 30 de L’Enseignement Mathématique, 1982.

## Appendix: the Newton polygon of $fg + 1$

In this section we denote by  $0$  the point in the plane with coordinates  $(0, 0)$ .

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.,  $\text{Mon}(f) = \text{Mon}(g)$ . We denote by  $\{p_0, \dots, p_{t-1}\}$  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  $\text{conv}(p_1, p_2, \dots, p_{t-1})$  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  $\text{Mon}(f) = \text{Mon}(g)$  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.** *Under assumptions (i) and (ii),*

$$\text{Newt}(fg + 1) = \text{conv}(2p_1, \dots, 2p_{t-1}, (p_i)_{i \in I})$$

where  $(p_i)_{i \in I}$  is the subset of those monomials in  $\text{Mon}(f)$  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

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

The left-hand side can be written as  $\text{conv}((2p_j)_{j \in J})$  where the  $(p_j)_{j \in J}$  form a convexly independent subset of  $\{p_1, \dots, p_{t-1}\}$ . 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  $i \neq k$ . 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  $\text{conv}((2p_j)_{j \in J}) \subseteq \text{Newt}(fg + 1)$ , and the proof is complete.  $\square$

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  $\text{Newt}(fg + 1)$  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,  $\text{Newt}(fg + 1)$  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  $\{p_0, \dots, p_{t-1}\}$ . If  $0$  does not belong to this support then  $\text{Newt}(fg + 1)$  is the convex hull of  $\{0\}$  and  $\text{Newt}(fg)$ . Moreover,  $\text{Newt}(fg) = \text{Newt}(f) + \text{Newt}(g) = \text{conv}(2p_0, \dots, 2p_{t-1})$ .

If  $0$  is in the support and  $fg + 1$  has a constant term then  $\text{Newt}(fg + 1) = \text{Newt}(fg)$  has at most  $t$  edges ( $t$  and not  $2t$  since  $f$  and  $g$  have the same support).

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  $\text{Newt}(fg + 1)$  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  $\text{conv}(2p_1, \dots, 2p_{t-1}, (p_i)_{i \in I}) = \text{conv}((2p_j)_{j \in J}, (p_k)_{k \in K})$  where  $J \subseteq \{1, \dots, t - 1\}$  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  $|J| + |K| = |J \cup K| + |J \cap K| \leq (t - 1) + 2 = t + 1$ .  $\square$

**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  $0prq$ . Then the line  $pq$  separates  $0$  from  $r$ . As a result,  $r \in \text{conv}(p, q, 2r)$ .
2. If the 4 points are not convexly independent, assume for instance that  $r \in \text{conv}(0, p, q)$ . In this case,  $2r \in \text{conv}(2p, 2q, r)$ .  $\square$