Electronic Colloquium on Computational Complexity, Report No. 169 (2014)

# Lower Bounds for Monotone Counting Circuits

Stasys Jukna[1,2]

*Institute of Computer Science, Goethe University, Frankfurt am Main, Germany*

## Abstract

A $\{+,\times\}$-circuit *counts* a given multivariate polynomial $f$, if its values on 0-1 inputs are the same as those of $f$; on other inputs the circuit may output arbitrary values. Such a circuit counts the number of monomials of $f$ evaluated to 1 by a given 0-1 input vector (with multiplicities given by their coefficients). A circuit *decides* $f$ if it has the same 0-1 roots as $f$. We first show that some multilinear polynomials can be exponentially easier to count than to compute them, and can be exponentially easier to decide than to count them. Then we give general lower bounds on the size of counting circuits.

*Key words:* Arithmetic circuits, boolean circuits, counting complexity, lower bounds

## 1. Introduction

In this paper we consider computational complexity of multivariate polynomials with nonnegative integer coefficients:

$$f(x_1,\ldots,x_n)=\sum_{e\in\mathbb{N}^n} c_e\prod_{i=1}^{n} x_i^{e_i}\,, \tag{1}$$

where $c_e\in\mathbb{N}=\{0,1,2,\ldots\}$, and $x_i^0=1$. Products $\prod_{i=1}^n x_i^{e_i}$ are *monomials* of $f$; we will often omit monomials whose coefficients $c_e$ are zero. The polynomial is *multilinear*, if $c_e=0$ for all $e\not\in\{0,1\}^n$, and is *homogeneous* of degree $d$, if $e_1+\cdots+e_n=d$ for all $e$ with $c_e\neq 0$.

A standard model of compact representation of such polynomials (with nonnegative coefficients) is that of monotone arithmetic circuits, i.e. of $\{+,\times\}$-circuits. Such a circuit is a directed acyclic graph with three types of nodes: input, addition $(+)$, and multiplication $(\times)$. Input nodes have fanin zero, and correspond to variables $x_1,\ldots,x_n$. All other nodes have fanin two, and are called *gates*. The *size* of a circuit is the number of gates in it.

Every $\{+,\times\}$-circuit syntactically *produces* a unique monotone polynomial $F$ with nonnegative integer coefficients in a natural way: the polynomial produced at an input gate $x_i$ consists of a single monomial $x_i$, and the polynomial produced at a sum (product) gate is the sum (product) of polynomials produced at its inputs; we use distributivity to write a product of polynomials as a sum of monomials. The polynomial $F$ produced by the circuit itself is the polynomial produced at its output gate. Given a polynomial $f(x_1,\ldots,x_n)$, we say that the circuit

*Email addresses:* jukna@thi.informatik.uni-frankfurt.de (Stasys Jukna)
*URL:* http://www.thi.informatik.uni-frankfurt.de/ jukna/ (Stasys Jukna)

[1] Research supported by the DFG grant SCHN 503/6-1.

[2] Affiliated with Institute of Mathematics and Informatics, Vilnius University, Vilnius, Lithuania.

ISSN 1433-8092

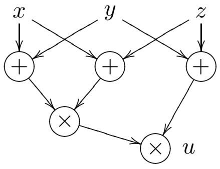

Figure 1: A circuit of size 5 counting the polynomial $f = 2xyz + 2xy + 2xz + 2yz$, and deciding the polynomial $g = xy + xz + yz$. The circuit itself produces the polynomial $F = (x+y)(y+z)(x+z) = 2xyz + x^2y + xy^2 + x^2z + xz^2 + y^2z + yz^2$. Gate $u$ is the output gate.

- *computes* $f$, if $F(a) = f(a)$ holds for all $a \in \mathbb{N}^n$, where $\mathbb{N} = \{0, 1, 2, \dots\}$;
- *counts* $f$, if $F(a) = f(a)$ holds for all $a \in \{0,1\}^n$;
- *decides* $f$, if $F(a) = 0$ exactly when $f(a) = 0$ holds for all $a \in \{0,1\}^n$.

In this paper we are mainly interested in $\{+, \times\}$-circuits *counting* a given polynomial $f$. Such a circuit needs only to correctly compute the restriction $f : \{0,1\}^n \to \mathbb{N}$ of $f$ on 0-1 inputs. Note that, if the polynomial $f$ is monic (has no coefficients $> 1$) then, on every 0-1 input $a \in \{0,1\}^n$, $f(a)$ is the number of monomials of $f$ satisfied by (evaluated to 1 on) $a$. For example, in the case of the permanent polynomial

$$\mathsf{Per}_n(x) = \sum_h \prod_{i=1}^n x_{i,h(i)}$$

with the summation over all permutations $h$ of $[n] = \{1, \dots, n\}$, the value $\mathsf{Per}_n(a)$ is the number of perfect matchings in the bipartite $n \times n$ graph $G_a$ specified by input $a \in \{0,1\}^{n \times n}$; nodes $i$ and $j$ are adjacent in $G_a$ if and only if $a_{ij} = 1$. Thus, a circuit counting $\mathsf{Per}$ outputs the number of perfect matchings in $G_a$, whereas a circuit deciding this polynomial merely tells us whether $G_a$ contains a perfect matching.

*Remark* 1. Let us stress that we only consider *monotone* arithmetic circuits. The reason is that counting $\{+, -, \times\}$-circuits are already omnipotent: they are as powerful as boolean $\{\vee, \wedge, \neg\}$-circuits. This is because each boolean operation can be simulated over $\{0,1\}$: $x \wedge y$ by $xy$, $\neg x$ by $1 - x$, and $x \vee y$ by $x + y - xy$.

If a $\{+, \times\}$-circuit computes, counts or only decides a given polynomial $f$, what can then be said about the structure of the produced by the circuit polynomial $F$?

If the circuit *computes* $f$, then $F = f$ must hold, that is, then the produced polynomial $F$ and the target polynomial $f$ must coincide as formal expressions, i.e. as sums of monomials (see, e.g. Claim 10 below for simple a proof). In particular, then $\mathrm{mon}(F) = \mathrm{mon}(f)$ must also hold, where

- $\mathrm{mon}(f)$ is the set of monomials appearing in $f$ with nonzero coefficients.

This ensures that no "invalid" monomials can be formed during the computation, and severely limits the power of such circuits. In particular, if the target polynomial $f$ is *multilinear* (no variable has degree larger than 1, then the circuit itself must be multilinear: the polynomials produced at inputs of each product gate must depend on *disjoint* sets of variables. This limitation is essentially exploited in all lower bounds for monotone arithmetic circuits, including [17, 19, 10, 27, 22, 6, 24, 7].

In counting circuits, $\mathrm{mon}(F) = \mathrm{mon}(f)$ needs not to hold, due to the multiplicative idempotence axiom $x^2 = x$ valid on 0-1 inputs. That is, here exponents (and hence, degrees of monomials) do not mater (see Fig. 1). Still, it can be shown (see Lemma 5 below) that here we have a weaker, but still strong enough property $\sup(F) = \sup(f)$, where

- $\sup(f)$ is the *support* of $f$, that is, the family of sets of variables of monomials in $\mathrm{mon}(f)$.

In deciding circuits, even $\sup(F) = \sup(f)$ needs not to hold, due to the additional absorption axiom $x + xy = x$. In such circuits, we only have a weak property $\min(F) = \min(f)$, where

- $\min(f) \subseteq \sup(f)$ is the family of all members of $\sup(f)$ which are minimal in the sense than they do not contain any other members of $\sup(f)$; hence, $\min(f)$ forms an antichain.

Deciding $\{+, \times\}$-circuits are actually monotone *boolean* circuits, and we have the following relations concerning the minimum circuit size for every given polynomial (we will prove that both gaps can be exponential):

$$\text{Deciding} \leqslant \text{Counting} \leqslant \text{Computing}.$$

To prove lower bounds for deciding, and hence, also for counting $\{+, \times\}$-circuits, one can use lower-bounds arguments for monotone boolean circuits (see, e.g. [12, Chapt. 9] and the literature cited herein), but these are not easy to apply. The reason here lies in a "dual character" of these arguments: in order to obtain a large lower bound on the decision complexity of a given polynomial $f$, not only the set of monomials of the polynomial $f$ itself but also that of the "dual" polynomial $f^*$ must have some good structural properties (see the discussion before Theorem 8 below).

On the other hand, due to the limitations we mentioned above, lower bounds for $\{+, \times\}$-circuits *computing* a given polynomial are relatively easy to obtain, because here we have a full knowledge about the polynomial which a circuit must produce. In particular, there is then no need to consider dual polynomials. *Counting* $\{+, \times\}$-circuits allow more freedom, because they can use $x^2 = x$. In this case we only know the structure of the support of the produced polynomial, but not about its monomials. So, it is natural to ask whether known lower bounds for exactly computing $\{+, \times\}$-circuits can be extended to counting circuits?

That they sometimes *can* be extended was demonstrated by Sengupta and Venkateswaran in [18], where they show that an exponential lower bound of Jerrum and Snir [10] for $\{+, \times\}$-circuits computing the permanent polynomial $\mathsf{Per}$ can be adopted to yield the same lower bound for circuits only counting this polynomial. Still, at least three questions remained open:

1. Can counting circuits be substantially smaller than computing circuits?
2. Can deciding circuits be substantially smaller than counting circuits?
3. Can lower-bounds *arguments* for computing $\{+, \times\}$-circuits, not just bounds for specific polynomials (like the permanent polynomial), be extended to $\{+, \times\}$-counting circuits?

In this paper, we answer these questions affirmatively.

## 2. Results

For a polynomial $f$, let $\mathrm{C}(f)$ denote the minimum size of a $\{+, \times\}$-circuit *computing* $f$, $\mathrm{C}_{0/1}(f)$ the minimum size of such a circuit *counting* $f$, and $\mathrm{D}(f)$ the minimum size of a $\{+, \times\}$-circuit *deciding* $f$. Note that, for every polynomial $f$, we have that

$$\mathrm{D}(f) \leqslant \mathrm{C}_{0/1}(f) \leqslant \mathrm{C}(f)\,.$$

We first show that the gaps $\mathrm{C}(f)/\mathrm{C}_{0/1}(f)$ as well as $\mathrm{C}_{0/1}(f)/\mathrm{D}(f)$ can be exponential. When doing this, we will use known lower bound for the permanent polynomial.

**Theorem 1** ([10, 18])**.** *If $f = \mathsf{Per}_n$, then $\mathrm{C}_{0/1}(f) \geqslant n2^{n-1}$.*

This lower bound on $\mathrm{C}(f)$ was proved by Jerrum and Snir [10], and was extended to $\mathrm{C}_{0/1}(f)$ by Sengupta and Venkateswaran [18] (see also Corollary 1 below for a short proof of a weaker $2^{\Omega(n)}$ lower bound).

We will also use the (simple) fact that it is not harder to compute the so-called "lower" and "higher" envelopes of polynomial than to compute the polynomial itself. The *lower envelope* of a polynomial $f$ is a homogeneous polynomial $f_{\mathrm{le}}$ consisting of the monomials of $f$ of smallest degree. The *higher envelope* $f_{\mathrm{he}}$ is defined by taking monomials of largest degree. (As usually, the degree of a monomial is the sum of exponents of its variables, and a polynomial is *homogeneous*, if all its monomials have the same degree.) As observed already by Jerrum and Snir [10], every $\{+,\times\}$-circuit producing a polynomial $f$ can be easily transformed into a circuit producing $f_{\mathrm{le}}$ or $f_{\mathrm{he}}$ by just discarding (if necessary) some of the sum-gates. Hence, we always have

$$\mathrm{C}(f) \geqslant \max\{\mathrm{C}(f_{\mathrm{he}}), \mathrm{C}(f_{\mathrm{le}}\}\ . \tag{2}$$

### *2.1. Gaps*

To show that the gap $\mathrm{C}(f)/\mathrm{C}_{0/1}(f)$ can be exponential, we will show a stronger fact that both gaps $\mathrm{C}_{0/1}(f_{\mathrm{he}})/\mathrm{C}_{0/1}(f)$ and $\mathrm{C}_{0/1}(f_{\mathrm{le}})/\mathrm{C}_{0/1}(f)$ can be exponential. Recall that, by (2), no such gap is possible for *computing* $\{+,\times\}$-circuits.

**Theorem 2.** *There are multilinear polynomials $f$ and $g$ of $n$ variables such that $\mathrm{C}_{0/1}(f) = O(n)$ and $\mathrm{C}_{0/1}(g) = O(n^{3/2})$, but both $\mathrm{C}_{0/1}(f_{\mathrm{he}})$ and $\mathrm{C}_{0/1}(g_{\mathrm{le}})$ are $2^{\Omega(\sqrt{n})}$.*

*Remark* 2. Together with (2), the theorem implies that the gap $\mathrm{C}(f)/\mathrm{C}_{0/1}(f)$ between the sizes of $\{+,\times\}$-circuits computing and counting $f$ can be exponential. Important in this result is that the gap is obtained for *multilinear* polynomials: this shows that, under the presence of multiplicative idempotence $x^2 = x$, non-multilinear circuits counting multilinear polynomials can be much more efficient. In this connection, let us mention that without this restriction (to multilinear polynomials) a non-trivial gap follows from the classical lower bound $\Omega(n \log d)$ of Strassen [23], and Baur and Strassen [2] on the size of arithmetic (not necessarily monotone) circuits computing the polynomial $f = x_1^d + x_2^d + \cdots + x_n^d$, which can be trivially counted by a $\{+,\times\}$-circuit $F = x_1 + x_2 + \cdots + x_n$ of size only $n-1$. But this example merely says that, under the presence of multiplicative idempotence $x^2 = x$, rising to powers is redundant.

To show that the gap $\mathrm{C}_{0/1}(f)/\mathrm{D}(f)$ can also be exponential, it is enough to take any polynomial $g(x_1,\ldots,x_n)$ such that $\mathrm{C}_{0/1}(g)$ is exponential, and consider the polynomial $f = g + h$ where $h = \sum_{i=1}^n x_i$. If $g(0,\ldots,0) = 0$ then, on every 0-1 input $a$, we have that $f(a) = 0$ if and only if $h(a) = 0$. So, $f$ has a small decision complexity: $\mathrm{D}(f) \leqslant \mathrm{D}(h) \leqslant n$. So, if the counting complexity $\mathrm{C}_{0/1}(f)$ of the extended polynomial $f$ remains exponential, then the gap $\mathrm{C}_{0/1}(f)/\mathrm{D}(f)$ is exponential. In particular, one can establish such a gap by using the permanent polynomial $g = \mathsf{Per}$ (the only small "technicality" here is to show that the counting complexity of $f$ remains large).

**Theorem 3.** *If $f = \mathsf{Per}_n + \sum_{i,j=1}^n x_{ij}$, then $\mathrm{D}(f) \leqslant n^2$ but $\mathrm{C}_{0/1}(f) = 2^{\Omega(n)}$.*

The polynomial used in this theorem is somewhat artificial. Actually, one can establish an exponential gap using a more natural (and important) $s$-$t$ path polynomial $\mathsf{Path}_n$. This polynomial has one variable $x_{i,j}$ for each edge of a complete undirected graph on $n+2$ nodes $\{s,1,2,\ldots,n,t\}$. Each monomial of $f$ corresponds to a simple directed path from node $s$ to node $t$:

$$\mathsf{Path}_n(x) = x_{s,t} + \sum_{l=1}^{n} \sum_{\substack{i_1,\ldots,i_l\\ \text{distinct}}} x_{s,i_1} x_{i_1,i_2} \cdots x_{i_{l-1},i_l} x_{i_l,t}\ .$$

On a 0-1 input $a$, $\mathsf{Path}_n(a)$ gives the number of $s$-$t$ paths in the graph specified by $a$. Jerrum and Snir [10] have shown that every $\{+,\times\}$-circuit *computing* $f = \mathsf{Path}_n$ must have exponential size, i.e. that $\mathrm{C}(f) = 2^{\Omega(n)}$. We show that even $\{+,\times\}$-circuits *counting* $\mathsf{Path}$ must have exponential size.

**Theorem 4.** *If $f = \mathsf{Path}_n$, then $\mathrm{D}(f) = O(n^3)$, but $\mathrm{C}_{0/1}(f) \geqslant 2^{n^{\Omega(1)}}$.*

### *2.2. Lower bounds*

Recall that, if a $\{+,\times\}$-circuit *computes* a given polynomial $f$, then the produced by the circuit polynomial $F$ must just coincide with $f$ (as formal expressions). In counting and deciding circuits we only have weaker conditions on $F$.

By the *linearization* of a polynomial $f$ we will mean a multilinear polynomial $\overline{f}$ obtained from $f$ by removing all (nonzero) exponents from all monomials of $f$. For example, the linearization of $f = 2xy^2 + 3x^4y^2 + 6y^2z$ is $\overline{f} = 5xy + 6yz$. It is clear that $\overline{f}(a) = f(a)$ holds for all $a \in \{0,1\}^n$.

**Lemma 5.** *If a $\{+,\times\}$-circuit producing a polynomial $F$ counts $f$, then $\overline{F} = \overline{f}$, and hence, also $\sup(F) = \sup(f)$. A $\{+,\times\}$-circuit decides $f$ if and only if $\min(F) = \min(f)$.*

Our next structural result is the following lemma. The *support* of a monomial is the set of variables appearing in it with nonzero degree; the size of this set is the *length* of the monomial. A product $gh$ of two polynomials is *$m$-balanced*, if the minimum length $l$ of one these polynomials satisfies $m/3 < l \leqslant 2m/3$. A monomial $p$ *appears $m$-balanced* in a product $gh$ of two polynomials, if there are monomials $r \in \mathrm{mon}(g)$ and $s \in \mathrm{mon}(h)$ such that $rs$ and $p$ have the same support, and the length $l$ of $r$ satisfies $m/3 < l \leqslant 2m/3$. Note that here the order of polynomials in their product $gh$ is important: the condition is only on parts of monomials appearing in the first polynomial. In particular, if several monomials appear $m$-balanced in $gh$, then we know the bounds on the lengths of their parts in *one and the same* of the two polynomials.

**Lemma 6.** *Let $m \geqslant 2$, and let $f$ a polynomial of counting complexity $\mathrm{C}_{0/1}(f) = s$.*

(i) *If every monomial of $f$ has length at least $m$, then $\sup(f)$ is a union of at most $s$ supports of $m$-balanced products of polynomials.*

(ii) *There are $s$ products $gh$ of polynomials such that $\sup(gh) \subseteq \sup(f)$, and every monomial of $f$ of length at least $m$ appears $m$-balanced in at least one of these products.*

Various versions of claim (i) (with degree of or the total number of variables in polynomials used instead of their length) were observed by several authors including Hyafil [9], Jerrum and Snir [10], Valiant [27], and Raz and Yehudayoff [16]. The advantage of claim (ii) is its wider applicability: the polynomial $f$ itself is allowed to have also short monomials, shorter than $m$.

Our next results are more *explicit* lower bounds for counting circuits. The *$r$-th degree*, $\#_r(A)$, of a family of sets $A$ is the maximum number of sets in $A$ containing a fixed $r$-element set:

$$\#_r(A) = \max_{|b|=r} |\{a \in A \colon a \supseteq b\}|\,.$$

In other words, the intersection of any $\#_r(A)$ sets in $A$ can have at most $r$ elements. Note that

$$|A| = \#_0(A) \geqslant \#_1(A) \geqslant \ldots \geqslant \#_r(A) = 1 > 0 = \#_{r+1}(A)\,.$$

where $r = \max\{|a|\colon a \in A\}$. Also, $A \subseteq B$ implies $\#_r(A) \leqslant \#_r(B)$. If $A$ is a graph (viewed as a set of edges), then $\#_1(A)$ is the maximum degree of $A$. In general, $\#_r(A)$ is related with $|A|$ as follows: if $A$ is a family of $m$-element subsets on $[n]$, then for every $r \leqslant m$ we have that

$$|A|\binom{m}{r} \leqslant \#_r(A) \cdot \binom{n}{r}.$$

This can be shown by counting in two ways the number $M$ of pairs $(a, b)$, where $a \in A$, $|b| = r$ and $a \supseteq b$ holds. By first fixing sets $a \in A$, we get that $M$ is equal to the left-hand side. By fixing sets $b$, and taking all possible $m$-element sets $a$ containing $b$, we get that $M$ is at most the right-hand size.

As we mentioned in the introduction, lower bounds for deciding, and hence, also for counting $\{+, \times\}$-circuits, can be obtained using lower-bounds arguments for monotone boolean circuits (see, e.g. [12, Chapt. 9] and the literature cited herein), but these are not easy to apply. The reason here lies in a "dual character" of these arguments: in order to obtain a large lower bound of the decision complexity of a polynomial $f$ given by (1), not only the set of monomials of $f$ itself but also that of its "dual" $f^*$ must have some good structural properties. The *dual* $f^*$ of a polynomial

$$f = \sum_{u \subseteq [n]} c_u \prod_{i \in u} x_i \quad \text{is} \quad f^* = \prod_{u : c_u > 0} \sum_{i \in u} x_i \,.$$

Note that, for every 0-1 input $a = (a_1, \ldots, a_n)$, $f(a) = 0$ if and only if $f^*(\bar{a}) \neq 0$, where $\bar{a} = (1 - a_1, \ldots, 1 - a_n)$. This holds, because every set in $\sup(f^*)$ intersects every set in $\sup(f)$. More precisely, a general lower bound for deciding $\{+, \times\}$-circuits is the following.

**Theorem 7** ([11]). *Let $f(x_1, \ldots, x_n)$ be a polynomial, and $2 \leqslant r, s \leqslant n$ be integers. Then for every $A \subseteq \sup(f)$ and $B \subseteq \sup(f^*)$ such that $\#_1(A) \leqslant |A|/2(s-1)$, we have*

$$\mathrm{D}(f) \geqslant \min\left\{ \frac{|A|}{2(s-1)^r \cdot \#_r(A)}, \frac{|B|}{(r-1)^s \cdot \#_s(B)} \right\}.$$

As shown in [11] (see also [12, Chapt. 9]), this criterion allows to obtain strong (super-polynomial) lower bounds on $\mathrm{D}(f)$, and hence, also on $\mathrm{C}_{0/1}(f)$ and $\mathrm{C}(f)$, for some explicit polynomials. The strength of this criterion lies in the possibility to arbitrarily chose both the parameters $r, s$ as well as sub-families $A$ and $B$. The weakness, however, lies in its "dual nature" making it not easy to apply: *both* $|A|/\#_r(A)$ *and* $|B|/\#_s(B)$ must be large. It is usually easy to ensure that $|A|/\#_r(A)$ is large. The problem, however, is with the dual set $B$, because the set of monomials of the dual polynomial $f^*$ may be rather "messy", even though the polynomial $f$ itself has a "nice" structure. Say, if $f = \mathsf{Per}_n$, then $|A|/\#_r(A) = n!/(n-r)!$ is large enough already for $A = \sup(f)$. But monomials of $f^*$ correspond then to complements of graphs without perfect matchings, and it is difficult to ensure that $|B|/\#_s(B)$ is also large for some family $B$ of such graphs.

For counting $\{+, \times\}$-circuits, we have a much more handy lower-bounds criterion, avoiding the need of dual polynomials. By the $r$-th degree, $\#_r(f)$, of a polynomial $f$ we will mean the $r$-th degree $\#_r(A)$ of its support $A = \sup(f)$. Thus, if $f$ is multilinear, then $\#_r(f)$ is the maximum number of monomials of $f$ containing a common factor of degree $r$.

**Theorem 8.** *Let $f = g + h$ be a polynomial such that every monomial of $g$ has at least $m \geqslant 2$ variables, and every monomial of $h$ has fewer than $m/3$ variables. Then there is an integer $r$ between $m/3$ and $2m/3$ such that*

$$\mathrm{C}_{0/1}(f) \geqslant \frac{|\sup(g)|}{\#_r(g) \cdot \#_{m-r}(g)}\,. \tag{3}$$

There is yet another general lower-bounds criterion for monotone arithmetic circuits, due to Gashkov [6], and Gashkov and Sergeev [7]. They call a polynomial $f$ $(k,l)$-*sparse*, if

$$\mathrm{mon}(gh) \subseteq \mathrm{mon}(f) \text{ implies } |\mathrm{mon}(g)| \leqslant k \text{ or } |\mathrm{mon}(h)| \leqslant l.$$

They proved that $\mathrm{C}(f)+1 \geqslant |\mathrm{mon}(f)|/\max\{k^3,l^2\}$ holds for every such polynomial. Note that the bound is not trivial, because the fact that $|\mathrm{mon}(g)| \leqslant k$ or $|\mathrm{mon}(h)| \leqslant l$ holds does not imply that $|\mathrm{mon}(gh)| \leqslant kl$ must also hold (because we have an "or", not "and" here). To obtain a similar lower bound for counting circuits, we will modify their notion of "sparsity".

Let, as before, $\min(f) \subseteq \sup(f)$ denote the family of all members of $\sup(f)$ which are minimal in the sense than they do not contain any other members of $\sup(f)$. Call a polynomial $f$ $(k,l)$-*free* if, for every two polynomials $g$ and $h$,

$$\sup(gh) \subseteq \sup(f) \text{ implies } |\min(g)| \leqslant k \text{ or } |\min(h)| \leqslant l.$$

The reason to only require $|\min(g)| \leqslant k$ instead of $|\sup(g)| \leqslant k$ is that then it is (potentially) easier to show that a given polynomial is $(k,l)$-free: $|\min(g)|$ can be much smaller than $|\sup(g)|$.

**Theorem 9.** *Let $1 \leqslant k \leqslant l$ be integers. For every $(k,l)$-free polynomial $f$, its support $\sup(f)$ is a union of at most $2\mathrm{C}_{0/1}(f)$ supports $\sup(gh)$ of products $gh$ of polynomials such that $|\min(gh)| \leqslant kl^2$. In particular,*

$$\mathrm{C}_{0/1}(f) \geqslant \frac{|\min(f)|}{2kl^2}\,.$$

*Remark* 3. The proofs of Theorems 8 and 9 extend to $\mathrm{C}_{0/1}(f)$ the arguments used in [6, 7, 13] to lower-bound $\mathrm{C}(f)$. The main difficulty with the extension (stipulated by the idempotence axiom $x^2 = x$) is that, unlike the measure $\mu(f) = |\mathrm{mon}(f)|$ (used to lower-bound $\mathrm{C}(f)$), the measures $|\sup(f)|$ and $|\min(f)|$ are no more "monotone " in the sense that $\mu(f) \leqslant \mu(fg)$. To see this, take, for example, $f = x_1 + x_2 + \cdots + x_n$ and $g = x_1x_2\cdots x_n$. Then $|\sup(f)| = n$ but $|\sup(fg)| = 1$.

*Remark* 4. The proofs of Theorems 8 and 9 are based on the fact (Lemma 5) that, if a $\{+,\times\}$-circuit counts a polynomial $f$, then the produced by the circuit polynomial $F$ must satisfy $\sup(F) = \sup(f)$. Thus, these bounds do not extend to monotone *boolean* circuits, where we only have a much weaker property $\min(F) = \min(f)$.

## 3. Some Applications

Theorem 8 allows us to easily obtain strong lower bounds on $\mathrm{C}_{0/1}(f)$ for many polynomials. Let us demonstrate this on some of them. First, associate with very set $H$ of permutations $h : [n] \to [n]$ the polynomial in $n^2$ variables $x_{i,j}$:

$$f_H(x) = \sum_{h\in H} \prod_{i=1}^{n} x_{i,h(i)}\,.$$

For example, if $H$ consists of all permutations, then $f_H$ is the permanent polynomial $\mathsf{Per}_n$. If $H$ consists of al *cyclic* permutations, then the monomial of $f_H$ correspond to Hamiltonian cycles in $K_n$.

**Corollary 1.** *For every set $H$ of permutations of $[n]$, there is an $r$ such that $n/3 < r \leqslant 2n/3$ and*

$$\mathrm{C}_{0/1}(f) \geqslant \frac{|H|\binom{n}{r}}{n!}\,.$$

In particular, $\mathrm{C}_{0/1}(\mathsf{Per}_n) \geqslant \binom{n}{r} = 2^{\Omega(n)}$.

*Proof.* The polynomial $f_H$ has $|H|$ monomials, each specified by a permutation $h \in H$ of $[n]$. If some $r$ variables are fixed, this fixes $r$ values of $h$. Hence, at most $(n-r)!$ of the permutations can take $r$ pre-described values, implying that $\#_r(f) \leqslant (n-r)!$. Thus, Theorem 8 gives that $\mathrm{C}_{0/1}(f)$ is at least $|H|$ divided by the maximum of $r!(n-r)!$ over all $n/3 < r \leqslant 2n/3$. □

In some cases, Theorem 8 allows to even obtain almost optimal bounds. A *partial* $t$*–*$(n, m, \lambda)$ *design* is a family $A$ of $k$-element subsets of $\{1, \ldots, n\}$ such that any $t$-element set is contained in at most $\lambda$ of its members. We can associate with each such design $A$ a multilinear polynomial

$$f_A(x) = \sum_{a\in A}\prod_{i\in a} x_i\,.$$

**Corollary 2.** *For every partial $t$–$(n, m, \lambda)$ design $A$ with $m/3 \leqslant t \leqslant 2m/3$, we have $\mathrm{C}_{0/1}(f_A) \geqslant |A|/\lambda^2$.*

*Proof.* For all $m/3 \leqslant r \leqslant 2m/3$, we have that both $r$ and $m-r$ are at least $m/3$. Thus, the design property implies that both $\#_r(A)$ and $\#_{m-r}(A)$ are at most $\lambda$, and the desired lower bound follows directly from Theorem 8. □

There are many explicit partial designs $A$ with $\lambda << \sqrt{|A|}$. For every of them, the counting complexity of the polynomial $f_A$ is almost the same as the number of monomials. To give an example, let $n$ be a prime power, and let $A$ consist of all subsets $a = \{(i, h(i) \colon i \in \mathrm{GF}(n)\}$ of the grid $\mathrm{GF}(n) \times \mathrm{GF}(n)$ corresponding to polynomials $h(z)$ of degree at most $d-1$ over $\mathrm{GF}(n)$. Since no two distinct polynomials of degree $< d$ can coincide on $d$ points, we have that no two monomials of $f$ can share $d$ variables in common, $A$ is a partial 1-$(n^2, n, 1)$ design, and we obtain $n^d = |A| \leqslant \mathrm{C}_{0/1}(f_A) \leqslant n^{d+1}$.

Theorem 9 is more difficult to apply than Theorem 8, but it may help for polynomials, on which the latter theorem fails. To demonstrate this, let $A$ be a set of edges of a bipartite point-line incidence graph of a projective plane $PG(2, q)$, introduced by Singer [20]. The nodes on the left-side correspond to $n = q^2 + q + 1$ points $x$, and those on the left-side to $n$ lines $L$, and $x$ and $L$ are adjacent if $x \in L$. Since every line $L$ has $|L| = q + 1$ points, and every point lies in $q + 1$ lines, this is a $d$-regular graph of degree $d = q + 1 > \sqrt{n}$. Moreover, the graph is $K_{2,2}$-free (i.e. contains no complete $2 \times 2$ subgraphs), because every two point lie in only one line, and every two lines share only one point. For the polynomial

$$f_A(x) = \sum_{uv\in A} x_u x_v\,,$$

Theorem 8 can only give a trivial lower bound $\mathrm{C}_{0/1}(f_A) \geqslant |A|/d^2 = \Omega(\sqrt{n})$. Indeed, in this case we have $m = 2$, and hence, $r = 1$. But then both $\#_r(f_A)$ and $\#_{m-r}(f_A)$ are equal $d > \sqrt{n}$. On the other hand, it is not difficult to verify that the $K_{2,2}$-freeness of $A$ implies that the polynomial $f_A$ is $(k,l)$-free for $k=l=1$. Thus, Theorem 9 yields an almost optimal lower bound

$$\mathrm{C}_{0/1}(f_A) = \Theta(n^{3/2})\,.$$

As a second example, let us consider the structurally much simpler *triangle polynomial* of $n=3m^2$ variables with $m^3=\Theta(n^{3/2})$ monomials:

$$\Delta_n(x,y,z) = \sum_{i,j,k\in[m]} x_{ik}y_{kj}z_{ij}\,.$$

Schnorr [17] has shown that $\mathrm{C}(\Delta_n)=\Theta(n^{3/2})$; this also follows from the lower bound of Gashkov and Sergeev [7] mentioned above, because the polynomial is $(1,1)$-sparse: any triangle is uniquely determined by any two of its edges.

Concerning *counting* circuit complexity of $f=\Delta_n$, Theorem 8 can only yield a trivial lower bound $\mathrm{C}_{0/1}(f)\geqslant m^3/m = m^2 = n/3$, because up to $m$ triangles can share a common edge. Still, Theorem 9 (with some more effort) allows us to obtain an almost optimal lower bound.

**Corollary 3.** *If $f=\Delta_n$, then $\mathrm{C}_{0/1}(f)=\Theta(n^{3/2})$.*

*Proof.* The upper bound $\mathrm{C}_{0/1}(f)=O(m^3)=O(n^{3/2})$ is trivial. To prove the lower bound $\mathrm{C}_{0/1}(f)=\Omega(m^3)$, we will use Theorem 9. Since $|\mathrm{sup}(f)|=m^3$, it is enough to show that $f$ is $(1,1)$-free. To show this, assume that $\mathrm{sup}(gh)\subseteq\mathrm{sup}(f)$ for some polynomials $g$ and $h$ such that $|\min(g)|\geqslant 2$ and $|\min(h)|\geqslant 2$. Take any two sets $a_1,a_2\in\min(g)$, and two sets $b_1,b_2\in\min(h)$. Then all four unions $a_i\cup b_j$ must be triangles (not just contain a triangle). Moreover, $a_1$ and $a_2$, as well as $b_1$ and $b_2$ must be incomparable under inclusion.

Case 1: Some of the sets $a_1,a_2,b_1,b_2$ forms a triangle $T$, say $a_1=T$. Hence, $b_1$ and $b_2$ lie in $T$, and $a_2\not\subseteq T$ since $a_1$ and $a_2$ must be incomparable. Consider the triangles $T_1=a_2\cup b_1$ and $T_2=a_2\cup b_2$. If $|b_i|\geqslant 2$ for some $i\in\{1,2\}$, then $|T_i\cap T|\geqslant|b_i|\geqslant 2$, implying that $T_i=T$, and hence, also $a_2\subseteq T$, a contradiction. So, $b_1=\{e_1\}$ and $b_2=\{e_2\}$ for some edges $e_1\neq e_2$. Since then $|a_2|\geqslant 2$, the triangles $T_1$ and $T_2$ are uniquely determined by $a_2$, implying that $T_1=T_2$ must be the same triangle. But this triangle shares two distinct edges $e_1$ and $e_2$ with $T$, implying that $T_1=T$, and hence also $a_2\subseteq T$, a contradiction.

Case 2: None of the sets $a_1,a_2,b_1,b_2$ forms a triangle. In this case, some of the sets must have exactly two edges, say $a_1=\{e_1,e_2\}$. Since a triangle is uniquely determined by any two of its edges, we have that both unions $a_1\cup b_1$ and $a_1\cup b_2$ must form the same triangle $T=\{e_1,e_2,e_3\}$. The sets $b_1$ and $b_2$ must be incomparable, and both of them must contain the "missing" edge $e_3$. Since none of these two sets can be a triangle, this implies that $b_1=\{e_1,e_3\}$ and $b_2=\{e_2,e_3\}$. These two sets also uniquely determine the same triangle $T$, implying that $a_2\cup b_1=a_2\cup b_2=T$. Thus, $a_2$ must contain both missing edges $e_1$ and $e_2$ of $T$. But this means that $a_2$ contains the set $a_1$, a contradiction with $a_1$ and $a_2$ being incomparable. □

We now turn to the proofs of our main results.

## 4. Proof of Theorem 2

To show that the gap $\mathrm{C}(f_{\mathrm{he}})/\mathrm{C}(f)$ can be exponential, consider the following polynomial in $n=m^2+m$ variables:

$$\mathsf{Per}^*(x,y) = \prod_{i=1}^{m}\sum_{j=1}^{m} x_{ij}y_j\,. \tag{4}$$

The relation to the permanent polynomial $\mathsf{Per}$ is that the coefficient of the monomial $y_1y_2\cdots y_m$ in $\mathsf{Per}^*(x,y)$ is exactly $\mathsf{Per}_m(x)$.

Now, let $f(x,y)$ be the linearization of $\mathsf{Per}^*(x,y)$. That is, $f(x,y)$ is a multilinear polynomial obtained from $\mathsf{Per}^*(x,y)$ by removing all nonzero exponents from all monomials. Every monomial of $f$ has degree (sum of exponents) between $m+1$ and $2m$, and the monomials

$$x_{1,j_1}x_{2,j_2}\cdots x_{m,j_m}y_1y_2\cdots y_m$$

of degree $2m$ with all $j_1,\ldots,j_m$ distinct are exactly the monomials of the polynomial

$$h(x,y)=\mathsf{Per}_m(x)\cdot y_1y_2\cdots y_m\,.$$

Thus, $h=f_{\mathrm{he}}$ is the higher envelope of $f$. Since $h(x,1,\ldots,1)=\mathsf{Per}_m(x)$, Theorem 1 yields

$$\mathrm{C}_{0/1}(f_{\mathrm{he}})\geqslant\mathrm{C}_{0/1}(\mathsf{Per}_m)=2^{\Omega(m)}=2^{\Omega(\sqrt{n})}\,.$$

On the other hand, since exponents play no role on 0-1 inputs, we have that $\mathsf{Per}^*(a)=f(a)$ holds for all 0-1 inputs $a$. Thus, the polynomial $f$ can be counted by the circuit given by the definition (4) of $\mathsf{Per}^*$. This gives the desired upper bound $\mathrm{C}_{0/1}(f)=O(m^2)=O(n)$.

To show that the gap $\mathrm{C}(g_{\mathrm{le}})/\mathrm{C}(g)$ can also be exponential, consider the following polynomial in $n=m^2$ variables $x_{ij}$ given by the formula:

$$\mathsf{Isol}_n(x)=\prod_{i=1}^{m}\prod_{j=m+1}^{2m}\Bigg(\sum_{k=m+1}^{2m}x_{ik}\Bigg)\Bigg(\sum_{l=1}^{m}x_{lj}\Bigg)\,. \tag{5}$$

The monomials of this polynomial are obtained as follows. We interpret the variables $x_{ij}$ as edges of a complete bipartite $m\times m$ graph $I\times J$ with parts $I=\{1,\ldots,m\}$ and $J=\{m+1,\ldots,2m\}$. To get a monomial of $\mathsf{Isol}$, we take, for each node $i\in I$ exactly one edge $x_{ik}$ incident with $i$, and take, for each node $j\in J$ exactly one edge $x_{lj}$ incident with $j$. So, every variable has degree at most 2. Note that on every 0-1 input $a\in\{0,1\}^n$, $\mathsf{Isol}(a)=0$ if and only if the graph specified by $a$ has an isolated node.

Let $g$ be the linearization of $\mathsf{Isol}_n$. Every monomial of $g$ has degree between $m$ and $2m$, and the monomials of degree $m$ correspond to perfect matchings. Thus, the lower envelope $g_{\mathrm{le}}$ of $g$ is just the permanent polynomial, i.e. $g_{\mathrm{le}}=\mathsf{Per}_m$. By Theorem 1, $\mathrm{C}(g_{\mathrm{le}})=2^{\Omega(m)}$.

On the other hand, since exponents play no role on 0-1 inputs, we have that $\mathsf{Isol}(a)=g(a)$ holds for all 0-1 inputs $a$. Thus, the polynomial $g$ can be counted by the circuit given by the definition (5) of $\mathsf{Isol}$. This gives the desired upper bound $\mathrm{C}_{0/1}(g)=O(m^3)=O(n^{3/2})$. □

## 5. Proof of Theorem 4

Recall that the $s$-$t$ path polynomial $f=\mathsf{Path}_n$ has one variable $x_{i,j}$ for each edge of a complete undirected graph on $n+2$ nodes $\{s,1,\ldots,n,t\}$. Each monomial of $f$ corresponds to a simple directed path from node $s$ to node $t$.

The upper bound $\mathrm{D}(f)=O(n^3)$ of the *decision* complexity of $f=\mathsf{Path}_n$ follows from the Bellman–Ford dynamic programming algorithm [3, 5]. The circuit is constructed recursively by taking $F_{1,j}=x_{s,j}$ for all $j\in[n]\cup\{t\}$, and using the recursion $F_{l+1,j}=F_{l,j}+\sum_{i\neq j}F_{l,i}\times x_{i,j}$ for $j\in[n]\cup\{t\}$. Monomials of $F_{l,j}$ correspond to walks from node $s$ to node $j$ passing through at most $l$ edges; one edge may be passed more than once, and each pass counts. The output is the polynomial $F = F_{n+1,t}$. Since every $s$-$t$ walk contains a simple $s$-$t$ path, and since in deciding $\{+,\times\}$-circuits we can use the absorption axiom $x + xy = x$, the circuit correctly *decides* $\mathsf{Path}_n$. Thus $\mathrm{D}(\mathsf{Path}_n) = O(n^3)$.

Our goal is now to show that every $\{+,\times\}$-circuit *counting* the $s$-$t$ path polynomial must have exponential size. We do not have a *direct* proof of this lower bound. Instead, we will derive this result indirectly by using some known reductions and lower bounds.

Say that a $\{+,\times\}$-circuit *decides $f$ with threshold* $T$, if for every $a \in \{0,1\}^n$, $F(a) \geqslant T$ holds precisely when $f(a) \geqslant 1$. Here, the threshold $T = T(n)$ may depend on the number $n$ of variables, but not on the input. Note that deciding $\{+,\times\}$-circuits decide with threshold $T = 1$. Let $\mathrm{D}_{\mathrm{thr}}(f)$ denote the smallest size of a $\{+,\times\}$-circuit deciding $f$ with some threshold $T$.

As defined by Valiant [26], and Skyum and Valiant [21], a polynomial $f(x_1,\ldots,x_n)$ is a *monotone projection* of a polynomial $g(y_1,\ldots,y_m)$ if there exists an assignment $\sigma : \{y_1,\ldots,y_m\} \to \{x_1,\ldots,x_n,0,1\}$ such that $f(x_1,\ldots,x_n) = g(\sigma(y_1),\ldots,\sigma(y_m))$. It is clear that then $\mathrm{D}_{\mathrm{thr}}(f) \leqslant \mathrm{D}_{\mathrm{thr}}(g)$.

The *$r$-clique polynomial*, $\mathsf{Clique}_{n,r}$, has $\binom{n}{2}$ variables $x_e$, one for each edge $e$ of $K_n$, and has one monomial $\prod_{e\subseteq S} x_e$ for every subset $S \subseteq [n]$ of size $|S| = r$. Results of Valiant [25] imply that, for every $1 \leqslant r \leqslant n$, $\mathsf{Clique}_{n,r}$ is a monotone projection of the Hamiltonian $s$-$t$ path polynomial $\mathsf{Ham}_m$ for $m = n^{O(1)}$; as noted by Alon and Boppana [1], already $m = 25n^2$ is enough in this case. On the other hand, it is known that, for $r$ about $\sqrt{n}$, the clique polynomial $f = \mathsf{Clique}_{n,r}$ requires $\mathrm{D}_{\mathrm{thr}}(f) \geqslant 2^{n^{\Omega(1)}}$ [8, 15, 11]; see, e.g. [12, Sect. 9.8] for a simpler proof. (In fact, this result holds for more general circuits where arbitrary monotone real valued functions $g : \mathbb{R}^2 \to \mathbb{R}$ can be used as gates.) Since $\mathsf{Clique}_{n,r}$ is a monotone projection of $\mathsf{Ham}_m$, we have that

$$\mathrm{D}_{\mathrm{thr}}(\mathsf{Ham}_m) \geqslant \mathrm{D}_{\mathrm{thr}}(\mathsf{Clique}_{n,r}) = 2^{n^{\Omega(1)}} .$$

It remains therefore to show that

$$\mathrm{C}_{0/1}(\mathsf{Path}_m) \geqslant \mathrm{D}_{\mathrm{thr}}(\mathsf{Ham}_n) \text{ for } m = n^{O(1)}.$$

This can be shown using a standard reduction of $\mathsf{Path}$ to $\mathsf{Ham}$. Let $p = (n+1)\log n$. Given an input graph $G$ on $n+2$ nodes $\{s,1,2,\ldots,n,t\}$, replace each edge $(u,v)$ by a graph on $2p+2$ nodes ($u$, $v$ and $2p$ new nodes) containing exactly $2^p$ paths of length $p+1$ between $u$ and $v$. This way, every $s$-$t$ path of length $l$ in $G$ gives $(2^p)^l$ $s$-$t$ paths in the resulting graph $G'$. This graph has $m = O(pn^2) = O(n^3\log n)$ nodes.

If $G$ has a Hamiltonian $s$-$t$ path (of length $n+1$), then the graph $G'$ has at least $T := (2^p)^{n+1}$ $s$-$t$ paths. If $G$ has no Hamiltonian path, then the longest $s$-$t$ path has at most $n$ edges, and hence, at most $n-1$ inner nodes. The number of $s$-$t$ paths of length $\leqslant n$ is bounded from above by $n \cdot n^{n-1} = n^n$. So, in this case, $G'$ can have at most $(2^p)^n \cdot n^n = l \cdot n^n/2^p = T/n$ $s$-$t$ paths. We have thus shown that every $\{+,\times\}$-circuit counting $\mathsf{Path}_m$ for $m = \Theta(pn^2) = \Theta(n^3\log n)$ decides $\mathsf{Ham}_n$ with threshold $T = (2^p)^{n+1}$. □

## 6. Proof of Lemma 5

Let $f(x_1,\ldots,x_n)$ be a polynomial in which each variable $x_i$ has degree at most $t_i$, and let $S_i \subseteq \mathbb{N}$ be arbitrary subsets of sizes $|S_i| \geqslant t_i + 1$, $i = 1,\ldots,n$.

**Claim 10** (Folklore)**.** *The polynomial $f$ is uniquely determined by its values on $S_1 \times S_2 \times \cdots \times S_n$.*

*Proof.* Induction on $n$. For $n = 1$, the claim is simply the assertion that a non-zero polynomial of degree $t_1$ in one variable can have at most $t_1$ distinct roots. For the induction step, expand the polynomial $f$ by the variable $x_n$:

$$f(x_1, \ldots, x_n) = \sum_{i=0}^{t_n} f_i(x_1, \ldots, x_{n-1}) \cdot x_n^i \,.$$

For each point $a \in S_1 \times \cdots \times S_{n-1}$,

$$f(a, x_n) = \sum_{i=0}^{t_n} f_i(a) \cdot x_n^i$$

is a polynomial of degree at most $t_n$ in one variable, and hence, all its coefficients $f_i(a)$, $i = 0, 1, \ldots, t_n$ can be recovered knowing the values $f(a, b)$ for all $b \in S_{n+1}$. Knowing the values $f_i(a)$ for all $a \in S_1 \times \cdots \times S_{n-1}$ we can, by the induction hypothesis, recover the polynomials $f_i$, and hence, the original polynomial $f$. □

Now let $f$ and $h$ be two polynomials on the same set of $n$ variables such that $f(a) = h(a)$, and hence, also $\overline{f}(a) = \overline{h}(a)$ holds for all $a \in \{0,1\}^n$. (Recall that $\overline{f}$ is obtained from $f$ by removing all nonzero exponents.) Since the polynomials $\overline{f}$ and $\overline{h}$ are multilinear, Claim 10 with all $S_i = \{0,1\}$ yields $\overline{f} = \overline{h}$ (they must coincide as multilinear polynomials), and hence, also $\sup(f) = \sup(h)$ must hold as well.

Let us now prove the second claim of Lemma 5: if $f$ and $h$ are polynomials on the same set of variables, then $f$ and $h$ have the same 0-1 roots if and only if $\min(f) = \min(h)$. The "if" part is trivial, because $f(a) > 0$ happens precisely when $p(a) = 1$ for some monomial $p \in \min(f)$. To prove the "only if" direction, assume that $f$ and $h$ have the same 0-1 roots. Our goal is to show that then $\min(f) = \min(h)$ must hold.

Assume contrariwise that there is a monomial $p \in \mathrm{mon}(f)$ whose set of variables $X_p$ belongs to $\min(f)$ but not to $\min(h)$. If $X_q \not\subseteq X_p$ holds for all monomials $q$ of $h$, then we can set all variables in $X_p$ to 1 and the rest to 0. On the resulting assignment $a = a_p$, we will have $h(a) = 0$ but $f(a) \geqslant p(a) \geqslant 1$, a contradiction. Thus, there must be a monomial $q \in \min(h)$ such that $X_q \subset X_p$; the inclusion must be proper, because $X_p \notin \min(h)$. But then on the input $a_q$, we will have $f(a_q) = 0$ but $h(a_q) \geqslant q(a_q) \geqslant 1$, a contradiction again. □

## 7. Proof of Lemma 6

We will need the following two simple and well-known facts.

A *subadditive weighting* of a circuit is an assignment of nonnegative numbers (weights) to its gates such that the weight of a gate does not exceed the sum of the weights of its inputs.

**Claim 11** (Folklore)**.** *If the output gate gets weight $m$, and every leaf gets weight at most $2m/3$, then there is a gate of weight larger than $m/3$ and at most $2m/3$.*

*Proof.* By starting at the output gate, and traversing the circuit by always choosing the input of larger weight, we can find a gate $v$ of weight $> 2m/3$ such that both its inputs $u$ and $w$ have weights at most $2m/3$. By the subadditivity of weighting, at least one of the gates $u$ and $w$ have then weight larger than $(2m/3)/2 = m/3$ and at most $2m/3$. □

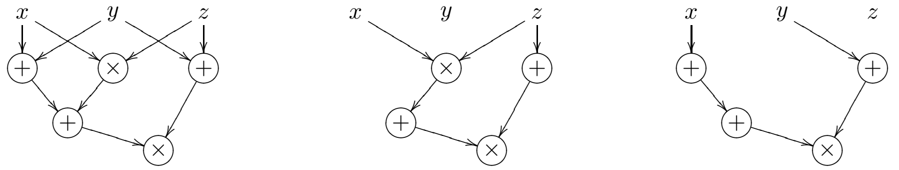

Figure 2: A circuit and two its parse sub-circuits producing, respectively, the monomials $xz^2$ and $xy$.

**Claim 12** (Folklore)**.** *For every gate $u$ in a $\{+,\times\}$-circuit producing a polynomial $F$, the polynomial can be written as $F = PQ + R$, where $P$ is the polynomial produced at $u$.*

(We use capital letters for polynomials only to stress that they are produced by circuits.)

*Proof.* If we replace the gate $u$ by a new variable $y$, the resulting circuit produces a polynomial of the form $yH + R$ for some polynomial $H$, where $R$ does not contain $y$ (albeit $H$ may contain). It remains to substitute all occurrences of the variable $y$ with the polynomial $P$ produced at the gate $u$. □

*Proof of Lemma 6(i).* For a polynomial $f$, let $l(f)$ denote the minimum number of variables in a monomial of $f$. Hence, a product $gh$ of two polynomials is $m$-balanced, if $m/3 < l(g) \leqslant 2m/3$. We have to show that, if $l(f) \geqslant m$ for $m \geqslant 2$, then $\sup(f)$ is a union of at most $s = \mathrm{C}_{0/1}(f)$ supports of $m$-balanced products of polynomials.

To prove this claim, fix a $\{+,\times\}$-circuit of size $s = \mathrm{C}_{0/1}(f)$ counting $f$. Define the *weight* of a gate $u$ as $l(P)$, where $P = P_u$ is the polynomial produced at $u$. Hence, the output gate has weight at least $m \geqslant 2$, and each input gate has weight 1 (which is $\leqslant 2m/3$ since $m \geqslant 2$). Since this weighting is subadditive, Claim 11 gives us a gate $u$ with $m/3 < l(P) \leqslant 2m/3$. By Claim 12, we can write the produced by our circuit polynomial $F$ as a sum $F = PQ + R$. Hence, $\sup(f) = \sup(F) = \sup(PQ) \cup \sup(R)$, where the product $PQ$ is $m$-balanced.

The polynomial $R$ is obtained from $F$ by removing some monomials. If $R$ is empty, then we are done. Otherwise, the polynomial $R$ can be produced by a circuit with one gate fewer (gate $u$ is set to constant 0, and disappears). Moreover, $\mathrm{mon}(R) \subseteq \mathrm{mon}(F)$ implies that $l(R) \geqslant l(F) \geqslant m$ still holds. So, we can repeat the same argument for the polynomial $R$, until the empty polynomial $R$ is obtained. □

*Proof of Lemma 6(ii).* We will now apply Claim 11 not to the entire circuit but to some its sub-circuits. A *parse-subcircuit* of a circuit $\mathrm{F}$ is obtained by setting to 0 one of the two inputs of each sum gate. Such a subcircuit $\mathrm{F}'$ can also be defined inductively as follows. The output gate of $\mathrm{F}$ is included in $\mathrm{F}'$. If a gate $u$ is already included in $\mathrm{F}'$, and if $u$ is a sum gate, then exactly one of the inputs to $u$ are included in $\mathrm{F}'$. If $u$ is a product gate, then both its inputs are included in $\mathrm{F}'$ (see Fig. 2). Note that each parse-subcircuit produces exactly one monomial in a natural way, and that each monomial of the polynomial produced by the entire circuit is produced by at least one parse-subcircuit.

Now let $\mathrm{F}$ be a circuit of size $s = \mathrm{C}_{0/1}(f)$ counting $f$, and $F$ be the polynomial produced by $\mathrm{F}$. By Lemma 5, we have that $\sup(f) = \sup(F)$. For every monomial $p$ of $F$ of length at least $m$, take some parse-subcircuit $\mathrm{F}_p$ producing $p$, and use Claim 11 to find a gate $u$ in $\mathrm{F}_p$ such that the part $p'$ of $p$ produced at $u$ in $\mathrm{F}_p$ has length $l$ satisfying $m/3 < l \leqslant 2m/3$. By Claim 12, we can write the polynomial $F$ as a sum $F = PQ + R$, where $P$ is the polynomial produced at gate $u$ (in the entire circuit). Hence, $p$ appears $m$-balanced in the product $R_u = PQ$. Since we have at most $s$ products $R_u$, and since $\mathrm{mon}(R_u) \subseteq \mathrm{mon}(F)$ implies $\sup(R_u) \subseteq \sup(f)$, we are done. □

## 8. Proof of Theorems 8 and 3

Define the *join* of two families of sets $B$ and $C$ as the family

$$B * C = \{b \cup c \colon b \in B, c \in C\}$$

of all possible unions. Note that the support of a product $gh$ of two polynomials is the join of the supports of $g$ and $h$. Note also that, if no set of $B$ intersects any set of $C$, then we have an upper bound $|A| \leqslant \#_{|b|}(A) \cdot \#_{|c|}(A)$ on the size of the join $A = B * C$ holding for *all* $b \in B$ and $c \in C$. This holds because then $|B| = |B * \{c\}| \leqslant \#_{|c|}(A)$, and similarly $|C| = |\{b\} * C| \leqslant \#_{|b|}(A)$. If, however, sets in $B$ and in $C$ intersect, then it may happen that $|B| \gg |B * \{c\}|$. Still, also then we have a reasonable upper bound.

**Lemma 13.** *Let $B * C$ be a join of two families, and $B * C \subseteq A$. Suppose that every set in $B * C$ has size at least $m$, and that $B$ or $C$ has a set of size $r$. Then*

$$|B * C| \leqslant \#_r(A) \cdot \#_{m-r}(A)\,.$$

*Proof.* Assume w.l.o.g. that the family $B$ contains a set $b$ of size $|b| = r$, and let $A_b = \{b\} * C \subseteq A$. Associate with every $a \in A_b$ the family

$$C_a = \{c \in C \colon b \cup c = a\}\,.$$

These families give a partition of $C$ into $|A_b|$ pairwise disjoint subfamilies. Since all sets in $A_b$ contain the set $b$ of size $|b| = r$, we have that

$$|A_b| \leqslant \#_r(A)\,.$$

On the other hand, for each $a \in A_b$, all sets in $C_a$, and hence, also all sets in $B * C_a$ contain the set $a \setminus b$ of size $|a \setminus b| \geqslant m - r$, implying that

$$|B * C_a| \leqslant \#_{m-r}(A)$$

holds for all $a \in A_b$. Now, every set $b' \cup c'$ in $B * C$ belongs to $B * C_a$ for $a = b \cup c'$. So,

$$\begin{aligned} |B * C| &\leqslant \sum_{a \in A_b} |B * C_a| \leqslant \sum_{a \in A_b} \#_{m-r}(A) \\ &\leqslant |A_b| \cdot \#_{m-r}(A) \leqslant \#_r(A) \cdot \#_{m-r}(A)\,. \end{aligned}$$ □

*Proof of Theorem 8.* Let $f = g + h$ be a polynomial such that $l(g) \geqslant m \geqslant 2$, and $l(h) < m/3$; here, as before, $l(f)$ denotes the minimum number of variables in a monomial of $f$. By Lemma 6(ii), there are $s = \mathrm{C}_{0/1}(f)$ products $PQ$ of polynomials such that $\sup(PQ) \subseteq \sup(f)$, and every monomial of $g$ appears $m$-balanced in at least one of these products.

**Claim 14.** *If $\sup(PQ) \subseteq \sup(f)$, and if at least one monomial of $g$ appears $m$-balanced in $PQ$, then $\sup(PQ) \subseteq \sup(g)$ and $|\sup(PQ)| \leqslant \#_r(g) \cdot \#_{m-r}(g)$ for some $m/3 < r \leqslant 2m/3$.*

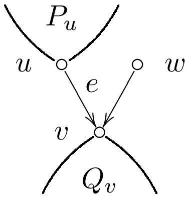

Figure 3: For an edge $e = (u, v)$, the polynomial $Q_e$ produced after $e$ is the polynomial $Q_e = Q_v$ produced after the gate $v$, if $v = u + w$ is a sum gate, and is $Q_e = Q_v P_w$, if $v = u \times w$ is a product gate, where $P_w$ is the polynomial produced before the gate $w$.

*Proof.* To show the inclusion $\sup(PQ) \subseteq \sup(g)$, assume contrariwise that there are $a, a' \in \sup(P)$ and $b, b' \in \sup(Q)$ such that $a \cup b \in \sup(g)$, $m/3 < |a| \leqslant 2m/3$ but $a' \cup b' \in \sup(h)$. Since $|b'| = l$ for some $l < m/3$, the union $a \cup b'$ has size $l < m/3 < |a \cup b'| \leqslant 2m/3 + l < m$, and hence, cannot belong to $\sup(f)$, a contradiction with $\sup(PQ) \subseteq \sup(f)$. Thus, $\sup(PQ)$ must lie entirely within $\sup(g)$, as claimed.

To show the upper bound on $|\sup(PQ)|$, let $A = \sup(g)$, $B = \sup(P)$ and $C = \sup(Q)$. Since $l(g) \geqslant m$, and $\sup(PQ) \subseteq \sup(g)$, we have that every set in $B * C = \sup(PQ)$ has at least $m$ elements. On the other hand, since some monomial of $g$ appears $m$-balanced in $PQ$, some set in $B$ must have $r$ elements, for some $m/3 < r \leqslant 2m/3$. For this $r$, Lemma 13 yields $|A * B| = |\sup(PQ)| \leqslant \#_r(A) \cdot \#_{m-r}(A)$, as desired. □

Thus, every monomial of $g$ belongs to at least one of $s$ products $PQ$ of polynomials such that $|\sup(PQ)| \leqslant \#_r(g) \cdot \#_{m-r}(g)$ for some $m/3 < r \leqslant 2m/r$. By taking such an $r$ maximizing $\#_r(g) \cdot \#_{m-r}(g)$, the desired lower bound $s \geqslant |\sup(g)|/\#_r(g) \cdot \#_{m-r}(g)$ follows. □

*Proof of Theorem 3.* Recall that our polynomial $f$ has the form $f = g + h$ with $g = \mathsf{Per}_n$ and $h = \sum_{i,j \in [n]} x_{ij}$. Hence, $l(g) = n$ and $l(h) = 1 < n/3$. By Theorem 8, there is an integer $r$ between $n/3$ and $2n/3$ such that $\mathrm{C}_{0/1}(f) \geqslant |\sup(g)|/\#_r(g) \cdot \#_{m-r}(g) \geqslant n!/r!(n-r)! = 2^{\Omega(n)}$. On the other hand, on every 0-1 input $a$, we have that $f(a) = 0$ if and only if $h(a) = 0$, because $g(0, \ldots, 0) = 0$. Hence, the circuit $h$ decides $f$, implying that $\mathrm{D}(f) = \mathrm{D}(h) \leqslant n^2$. □

## 9. Proof of Theorem 9

By Claim 12, we know that, for every gate $u$ in a given $\{+, \times\}$-circuit $\mathrm{F}$, the produced by the circuit polynomial $F$ can be written as $F = P_u Q_u + R$, where $P_u$ is the polynomial produced at $u$, $Q_u$ is the polynomial produced "after" the *gate* $u$, and $R$ is the polynomial produced by the circuit after the gate $u$ is replaced with constant 0. For our argument, it will be convenient to introduce the notion of a polynomial $Q_e$ produced after an *edge* $e = (u, v)$ (see Fig. 3):

$$Q_e = \begin{cases} Q_v & \text{if } v = u + w, \\ Q_v P_w & \text{if } v = u \times w. \end{cases}$$

A set $E$ of edges of $\mathrm{F}$ is a *cut*, if every input-output path in $\mathrm{F}$ contains an edge in $E$.

**Claim 15.** *If $E$ is a cut, then* $\mathrm{mon}(F)$ *is a union of* $\mathrm{mon}(P_u Q_e)$ *over all edges $e = (u, v)$ in $E$.*

*Proof.* Take a monomial $p$ of the produced polynomial $F$, and let $\mathrm{F}_p$ be any parse-subcircuit producing $p$. Since $E$ forms a cut, the graph $\mathrm{F}_p$ must contain some edge $e = (u, v) \in E$. Then the monomial $p$ has the form $p = p'p''$ where $p'$ is the monomial produced by the subgraph of $\mathrm{F}_p$ rooted in $u$. Thus $p'$ belongs to the polynomial $P_u$ produced in $\mathrm{F}$ before the edge $e$, and $p''$ belongs to the polynomial $Q_e$ produced after the edge $e$. Hence, $p$ belongs to $P_u Q_e$, as desired. □

*Proof of Theorem 9.* Let $\mathrm{F}$ be a $\{+,\times\}$-circuit of size $s = \mathrm{C}_{0/1}(f)$ counting $f$, and let $F$ be the polynomial produced by $\mathrm{F}$. By Lemma 5, we know that $\sup(F) = \sup(f)$. Hence, the polynomial $F$ is also $(k,l)$-free. We first transform the circuit $\mathrm{F}$ to a circuit $\mathrm{F}'$ as follows. For every product gate $v = u \times w$ in $\mathrm{F}$, one of whose inputs, say $u$, is *small* in that $|\min(P_u)| \leqslant l$ holds, we remove the edge $(u,v)$ and replace $v$ by a unary (fanin-1) gate $v = P_u \times w$ of "scalar" multiplication by this fixed (small) polynomial $P_u$. If both inputs produce small polynomials, then we eliminate only one of them. It is clear that $\mathrm{F}'$ produces the same polynomial $F$. In particular, $\sup(F') = \sup(f)$ holds as well.

Say that an edge $e = (u,v)$ of $\mathrm{F}'$ is *light*, if $|\min(P_u Q_e)| \leqslant kl^2$. To finish the proof of the first claim in Theorem 9, it is enough, by Claim 15, to show that every input-output path in $\mathrm{F}'$ must contain at least one light edge.

To show this, take an arbitrary input-output path in $\mathrm{F}'$, and let $e = (u,v)$ be the last edge along this path such that $|\min(P_u)| \leqslant k$; hence, $|\min(P_v)| > k$. Such an edge must exist because $|\min(x_i)| = 1 \leqslant k$, and since we can assume that $|\min(F)| > k$ (for otherwise the theorem would trivially hold). Together with $\min(P_v Q_v) \subseteq \min(F)$ and $|\min(P_v)| > k$, the $(k,l)$-freeness of $F$ implies that

$$|\min(Q_v)| \leqslant l\,.$$

If $v$ is a sum gate, then $Q_e = Q_v$, and hence, also $|\min(Q_e)| \leqslant l$. So, the edge $e$ is light in this case:

$$|\min(P_u Q_e)| \leqslant |\min(P_u)| \cdot |\min(Q_e)| \leqslant kl\,.$$

So, assume that $v$ is a product gate. Let $u$ and $w$ be the inputs to $v$ in the original circuit $\mathrm{F}$. Since $|\min(P_u)| \leqslant k \leqslant l$, we have that $|\min(P_w)| \leqslant l$ must hold as well, for otherwise the edge $e = (u,v)$ could not exist in $\mathrm{F}'$ (would be already eliminated when going from $\mathrm{F}$ to $\mathrm{F}'$). Hence,

$$|\min(Q_e)| = |\min(P_w Q_v)| \leqslant l^2\,.$$

So, the edge $e$ is light also in this case:

$$|\min(P_u Q_e)| \leqslant |\min(P_u)| \cdot |\min(Q_e)| \leqslant kl^2\,.$$

Since the total number of edges in $\mathrm{F}'$ is at most $2s$, we have thus shown that the support $\sup(F') = \sup(f)$ is a union of at most $2s$ families $\sup(PQ)$ with $|\min(PQ)| \leqslant kl^2$. Since every minimal set of a union of two families must be minimal in at least one of these families, this implies that $\min(f)$ is contained in (albeit not necessarily equal to) the union of the families $\min(PQ)$. Hence, the desired lower bound $s \geqslant |\min(f)|/2lk^2$. □

## 10. Conclusion and Open Problems

The weakness of monotone arithmetic circuits, i.e. of $\{+,\times\}$-circuits, *computing* a given polynomial $f$ is stipulated by the fact that the produced by the circuit polynomial $F$ must just (syntactically) coincide with $f$. In particular, then $\mathrm{mon}(F) = \mathrm{mon}(f)$ must hold. On the other pole are $\{+,\times\}$-circuits just *deciding* $f$. These are, in fact, monotone boolean circuits, where the idempotence axiom $x^2 = x$ as well as the absorption axiom $x + xy = x$ can be used, and hence, here we only have a weaker property $\min(F) = \min(f)$. While proving lower bounds in the latter (boolean) model is a relatively difficult task, the severe restriction of the former (arithmetic) model makes this task much easier.

| Circuits | $x+x=x$ | $x^2=x$ | $x+xy=x$ | Property |
|---|---|---|---|---|
| Computing | – | – | – | $F=f$ |
| Counting | – | ✓ | – | $\overline{F}=\overline{f}$ |
| Approximating | ✓ | ✓ | – | $\sup(F)=\sup(f)$ |
| Tropical | ✓ | – | ✓ | $\mathrm{Min}(F)=\mathrm{Min}(f)$ |
| Deciding/Boolean | ✓ | ✓ | ✓ | $\min(F)=\min(f)$ |

Table 1: Summary of which axioms are allowed (✓) in which kind of $\{+,\times\}$-circuits. The last column indicates what property the produced by a circuit polynomial $F$ must satisfy; here $\overline{f}$ is the linearization of $f$ obtained by removing all nonzero exponents. Tropical circuits are circuits with $x\oplus y=\min(x,y)$ and $x\otimes y=x+y$ functions as gates. Finally, $\mathrm{Min}(f)$ is the set of all *monomials* of $f$ that contain no other monomial of $f$ as a proper factor. The property $\mathrm{Min}(F)=\mathrm{Min}(f)$ holds only if $f$ is multilinear [10, 13].

In this paper we considered an intermediate model of *counting* $\{+,\times\}$-circuits. In this case, it is required that the values of $F$ must coincide with those of $f$ on only 0-1 inputs: on other inputs, the values may be different. Thus, counting circuits are $\{+,\times\}$-circuits that are allowed to use the idempotence axiom $x^2=x$ (but not the absorption axiom $x+xy=x$). These circuits have an intermediate structural property that $\sup(F)=\sup(f)$ must hold (Lemma 5). We have shown that counting circuits can be exponentially smaller than computing circuits (Theorem 2), and that deciding circuits can be exponentially smaller than counting circuits (Theorem 3).

A next natural question was whether lower-bounds arguments for the weak (computing) model can be extended to work also for the intermediate (counting) model? We have shown that such an extension is possible for two lower-bounds arguments (Theorems 8–9). In fact, our proofs of these bounds hold for $\{+,\times\}$-circuits that only "approximate" a given polynomial $f$ in that $\sup(F)=\sup(f)$ holds for the produced by the circuit polynomial $F$ (coefficients play no role in our arguments). Approximating circuits can use both idempotence axioms $x+x=x$ and $x^2=x$. (Table 1 summarizes the axioms allowed in various types of circuits.) So, these bounds also hold for $\{\cup,*\}$-circuits constructing a given family $A\subseteq 2^X$ of subsets of a (fixed) finite set. Inputs are single element sets $\{x\}$ with $x\in X$, and gates are set-theoretic union ($\cup$) and join ($*$) of families. A special case of Theorem 8 (for $h=0$) gives that, if every set in $A$ has at least $m\geqslant 2$ elements, then there is an integer $m/3<r\leqslant 2m/3$ such that every $\{\cup,*\}$-circuit constructing $A$ must have at least $|A|/\#_r(A)\cdot\#_{m-r}(A)$ gates.

A "complementary" in a sense to counting $\{+,\times\}$-circuits model, also lying between computing $\{+,\times\}$-circuits and deciding $\{+,\times\}$-circuits, is that of *tropical* circuits, i.e. $\{\min,+\}$-circuits. These are $\{+,\times\}$-circuits, where the sum is interpreted as $\min\{x,y\}$, and the product as $x+y$. Such a circuit *computes* a given polynomial $f$ of $n$ variables, if $\hat{F}(a)=\hat{f}(a)$ holds for all $a\in\mathbb{N}^n$, where $\hat{f}$ is the "tropicalization" of $f$:

$$f(x)=\sum_{e\in\mathbb{N}^n}c_e\prod_{i=1}^{n}x_i^{e_i}\qquad\text{turns to}\qquad\hat{f}(x)=\min_{\substack{e\in\mathbb{N}^n\\ c_e\neq 0}}\sum_{i=1}^{n}e_ix_i\,.$$

For example, if $f=xy^2+3y^2z^3$, then $\hat{f}=\min\{x+2y,2y+3z\}$. Tropical circuits are important, because many dynamic programming algorithms for minimization problems are just recursively constructed tropical circuits.

The difference from counting $\{+,\times\}$-circuits is that now the absorption axiom $x + xy = x$ is allowed, but the idempotence axiom $x^2 = x$ is not ($x + x \neq x$ unless $x = 0$). As shown in [10, 13], lower bounds for computing $\{+,\times\}$-circuits hold also for tropical circuits, as long as the target polynomial $f$ is multilinear: in this case we have that $\mathrm{T}(f) \geqslant \mathrm{C}(f_{\mathrm{le}})$, where $\mathrm{T}(f)$ is the minimum size of a tropical circuit computing $f$. In particular, for polynomials which are multilinear and homogeneous (all monomials have the same number of variables), tropical circuits are no more powerful than computing $\{+,\times\}$-circuits. Still, for non-homogeneous polynomials, tropical circuits can be exponentially more powerful than even counting $\{+,\times\}$-circuits. In fact, both gaps $\mathrm{C}_{0/1}(f)/\mathrm{T}(f)$ and $\mathrm{T}(f)/\mathrm{C}_{0/1}(f)$ can be exponential, meaning that tropical and counting $\{+,\times\}$-circuits are incomparable.

**Proposition 16.** *There are multilinear polynomials $f$ and $g$ of $n$ variables such that both $\mathrm{C}_{0/1}(f)/\mathrm{T}(f)$ and $\mathrm{T}(g)/\mathrm{C}_{0/1}(g)$ are $2^{\Omega(\sqrt{n})}$.*

*Proof.* To show the first gap, consider the permanent polynomial $f = \mathsf{Per}_m + \sum_{i,j=1}^{m} x_{ij}$ on $n = m^2$ variables. Theorem 3 gives $\mathrm{C}_{0/1}(f) = 2^{\Omega(m)}$. But $\mathrm{T}(f) \leqslant m^2 = n$ because $f$ can be computed by a tropical circuit $F = \sum_{i,j} x_{ij}$ whose tropicalization is $\hat{F} = \min_{i,j}(x_{ij})$: since variables cannot take negative values, the minimum will be achieved on a single variable. Thus, $\mathrm{C}_{0/1}(f)/\mathrm{T}(f) = 2^{\Omega(m)}$.

To show the second gap, take the multilinear polynomial $g$ considered in the proof of Theorem 2. The polynomial $g$ is the linearization of the polynomial $\mathsf{Isol}_n$ on $n = m^2$ variables given by (5), and has $\mathrm{C}_{0/1}(g) = O(n^{3/2})$. On the other hand, every monomial of $g$ has degree between $m$ and $2m$, and the monomials of degree $m$ correspond to perfect matchings. Thus, the lower envelope $g_{\mathrm{le}}$ of $g$ is just the permanent polynomial, i.e. $g_{\mathrm{le}} = \mathsf{Per}_m$. Since $\mathrm{C}(\mathsf{Per}_m) \geqslant \mathrm{C}_{0/1}(\mathsf{Per}_m) = 2^{\Omega(m)}$ (see Corollary 1) and $\mathrm{T}(g) \geqslant \mathrm{C}(g_{\mathrm{le}})$, the desired lower bound $\mathrm{T}(g) = 2^{\Omega(m)}$ follows. □

As we mentioned above, $\mathrm{T}(f) \geqslant \mathrm{C}(f_{\mathrm{le}})$ holds for every multilinear polynomial $f$. Thus, if the lower envelope $f_{\mathrm{le}}$ requires large monotone arithmetic circuits, then the polynomial $f$ itself requires large tropical circuits. This, however, does not hold for polynomials whose lower envelopes have small $\{+,\times\}$-circuits. An important example in this respect is the $s$-$t$ path polynomial $f = \mathsf{Path}_n$. Even though we have $\mathrm{C}(f) = 2^{\Omega(n)}$ [10], the lower envelope of $f$ consist of just one variable $x_{s,t}$, implying that $\mathrm{C}(f_{\mathrm{le}}) = 0$. And indeed, the Bellman–Ford algorithm (see Sect. 5) gives $\mathrm{T}(f) = O(n^3)$.

**Problem 1.** *Does $\mathrm{T}(f) = \Omega(n^3)$ hold for $f = \mathsf{Path}_n$?*

This would show that the Bellman–Ford algorithm is optimal, if only Min and Plus operations can be used. It is worth to mention that the optimality of the other prominent dynamic programming algorithm—that of Floyd–Warshall [4, 28] for the all-pairs shortest paths problem—is already known. The corresponding to this problem "polynomial" $f_n$ is actually a *set* of $s$-$t$ path polynomials $\mathsf{Path}_n$ for all choices of the source and target nodes $s$ and $t$. Thus, unlike for $\mathsf{Path}_n$, every circuit for $f_n$ must already have $\Omega(n^2)$ distinct output gates. The Ford–Warshall algorithm gives $\mathrm{T}(f_n) = O(n^3)$. On the other hand, Kerr [14] has shown that also $\mathrm{T}(f_n) = \Omega(n^3)$ holds.

In Sect. 5, we have shown that the monotone counting complexity of $\mathsf{Path}_n$ is exponential in $n$. But, unlike bounds given in Sect. 3, our proof for $\mathsf{Path}$ indirect and is based on two rather non-trivial known results: the fact that the clique polynomial $\mathsf{Clique}$ requires exponential monotone real circuits, and is a projection of the Hamiltonian $s$-$t$ path polynomial $\mathsf{Ham}$.

**Problem 2.** *Give a direct proof of $\mathrm{C}_{0/1}(f) = 2^{n^{\Omega(1)}}$ for $f = \mathsf{Path}_n$.*

Finally, it would be interesting to extend to the case of counting $\{+,\times\}$-circuits one of the first lower-bounds arguments for computing $\{+,\times\}$-circuits suggested by Schnorr in [17]. Namely, he proved that $\mathrm{C}(f) \geqslant |\mathrm{mon}(f)| - 1$ holds, if the polynomial $f$ is *separated* in the following sense: for every two monomials $p \neq q$ of $f$, their product $pq$ does not contain any third monomial $r \not\in \{p, q\}$ of $f$ as a factor (see also [13, Sect. 8] for a somewhat simpler proof). This criterion allows to easily prove strong lower bounds for some polynomials. For example, using it, one can easily show that $\mathrm{C}(f) \geqslant \binom{n}{r} - 1$ holds for the $r$-clique polynomial $f = \mathsf{Clique}_{n,r}$. This polynomial is separated, because the union of no two $r$-cliques (sets of edges of complete subgraphs of $K_n$ with $r$ nodes) can contain a third $r$-clique.

**Problem 3.** *Can Schnorr's argument for* $\mathrm{C}(f)$ *be extended to* $\mathrm{C}_{0/1}(f)$*?*

*Acknowledgments*

I am thankful to Tsuyoshi Ito, Emil Jeřábek, and Igor Sergeev for interesting discussions.

## References

[1] N. Alon and R. Boppana. The monotone circuit complexity of boolean functions. *Combinatorica*, 7(1):1–22, 1987. 11

[2] W. Baur and V. Strassen. The complexity of partial derivatives. *Theoret. Comput. Sci.*, 22:317–330, 1983. 4

[3] R. Bellman. On a routing problem. *Quarterly of Appl. Math.*, 16:87–90, 1958. 10

[4] R.W. Floyd. Algorithm 97, shortest path. *Comm. ACM*, 5:345, 1962. 18

[5] L.R. Ford. Network flow theory. Technical Report P-923, The Rand Corp., 1956. 10

[6] S.B. Gashkov. On one method of obtaining lower bounds on the monotone complexity of polynomials. *Vestnik MGU, Series 1 Mathematics, Mechanics*, 5:7–13, 1987. 2, 7, 7

[7] S.B. Gashkov and I.S. Sergeev. A method for deriving lower bounds for the complexity of monotone arithmetic circuits computing real polynomials. *Math. Sbornik*, 203(10):33–70, 2012 (in Russian). English translation in: Sbornik: Mathematics, 203(10) (2012) 1411–1147. 2, 7, 7, 9

[8] A. Haken and S.A. Cook. An exponential lower bound for the size of monotone real circuits. *J. Comput. Syst. Sci.*, 58(2):326–335, 1999. 11

[9] L. Hyafil. On the parallel evaluation of multivariate polynomials. *SIAM J. Comput.*, 8(2):120–123, 1979. 5

[10] M. Jerrum and M. Snir. Some exact complexity results for straight-line computations over semirings. *J. ACM*, 29(3):874–897, 1982. 2, 3, 3, 4, 4, 5, 5, 17, 18, 18

[11] S. Jukna. Combinatorics of monotone computations. *Combinatorica*, 9(1):1–21, 1999. Preliminary version: ECCC Report Nr. 26, 1996. 6, 6, 11

[12] S. Jukna. *Boolean Function Complexity: Advances and Frontiers.* Springer-Verlag, 2012. 3, 6, 6, 11

[13] S. Jukna. Lower bounds for tropical circuits and dynamic programs. *Theory of Comput. Syst.*, 2014. DOI: 10.1007/s00224-014-9574-4. 7, 17, 18, 19

[14] L.R. Kerr. *The effect of algebraic structure on the computation complexity of matrix multiplications.* PhD thesis, Cornell Univ., Ithaca, N.Y., 1970. 18

[15] P. Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *J. Symb. Log.*, 62(3):981–998, 1997. 11

[16] R. Raz and A. Yehudayoff. Multilinear formulas, maximal-partition discrepancy and mixed-sources extractors. *J. Comput. Syst. Sci.*, 77(1):167–190, 2011. Preliminary version in: Proc. of 49th FOCS, 2008. 5

[17] C.P. Schnorr. A lower bound on the number of additions in monotone computations. *Theor. Comput. Sci.*, 2(3):305–315, 1976. 2, 9, 19

[18] R. Sengupta and H. Venkateswaran. A lower bound for monotone arithmetic circuits computing 0-1 permanent. *Theor. Comput. Sci.*, 209(1–2):389–398, 1998. 3, 3, 4

[19] E. Shamir and M. Snir. On the depth complexity of formulas. *Math. Syst. Theory*, 13:301–322, 1980. 2

[20] J. Singer. A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.*, 43(3):377–385, 1938. 8

[21] S. Skyum and L. G. Valiant. A complexity theory based on boolean algebra. *J. ACM*, 32(2):484–502, 1985. 11

[22] M. Snir. Size-depth trade-offs for monotone arithmetic circuits. *Theor. Comput. Sci.*, 82(1):85–93, 1991. 2

[23] V. Strassen. Die Berechnungskomplexitäat von elementarsymmetrischen Funktionen und von Interpolationskoefizienten. *Numerische Mathematik*, 20:238–251, 1973. 4

[24] P. Tiwari and M. Tompa. A direct version of Shamir and Snir's lower bounds on monotone circuit depth. *Inf. Process. Lett.*, 49(5):243–248, 1994. 2

[25] L. G. Valiant. Completeness classes in algebra. In *Proc. of 11h Annual ACM Symp. on Theory of Computing*, pages 249–261, 1979. 11

[26] L.G. Valiant. The complexity of enumeration and reliability problems. *SIAM J. Comput.*, 8(3):410–421, 1979. 11

[27] L.G. Valiant. Negation can be exponentially powerful. *Theor. Comput. Sci.*, 12:303–314, 1980. 2, 5

[28] S. Warshall. A theorem on boolean matrices. *J. ACM*, 9:11–12, 1962. 18

ECCC ISSN 1433-8092

http://eccc.hpi-web.de