Electronic Colloquium on Computational Complexity, Report No. 80 (2014)

Lower Bounds for Tropical Circuits and Dynamic Programs

Stasys Jukna *†‡§

June 11, 2014

Abstract

Tropical circuits are circuits with Min and Plus, or Max and Plus operations as gates. Their importance stems from their intimate relation to dynamic programming algorithms. The power of tropical circuits lies somewhere between that of monotone boolean circuits and monotone arithmetic circuits. In this paper we present some lower bounds arguments for tropical circuits, and hence, for dynamic programs.

Keywords: Tropical circuits; dynamic programming; monotone arithmetic circuits; lower bounds

1 Introduction

Understanding the power and limitations of fundamental algorithmic paradigms—such as greedy or dynamic programming—is one of the basic questions in the algorithm design and in the whole theory of computational complexity. In this paper we focus on the dynamic programming paradigm.

Our starting point is a simple observation that many dynamic programming algorithms for optimization problems are just recursively constructed *circuits* over the corresponding semirings. Each such circuit computes, in a natural way, some polynomial over the underlying semiring. Most of known dynamic programming algorithms correspond to circuits over the $(\min,+)$ or $(\max,+)$ semirings, i.e. to *tropical circuits*.[1] For example, the Bellman [5], Ford [7], and Moore [25] dynamic programming algorithm gives a $(\min,+)$ circuit for the st-connectivity problem STCON with only $O(n^3)$ gates, and the Floyd [6] and Warshall [35] dynamic programming algorithm gives a circuit of this size even for the connectivity problem CONN (see Theorem 3 below). Thus, lower bounds for tropical circuits show the limitations of dynamic programming algorithms over the corresponding semirings.

The power of tropical circuits (and hence, of dynamic programming) lies somewhere between that of monotone boolean circuits and monotone arithmetic circuits:

$$\text{monotone boolean } \leqslant \text{ tropical} \leqslant \text{ monotone arithmetic}$$

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

†University of Frankfurt, Institute of Computer Science, Germany

‡Institute of Mathematics and Informatics, Vilnius, Lithuania

§Email: jukna@thi.informatik.uni-frankfurt.de

[1] There is nothing special about the term “tropical”. Simply, this term is used in honor of Imre Simon who lived in Sao Paulo (south tropic). Tropical algebra and tropical geometry are now intensively studied topics in mathematics.

ISSN 1433-8092

and the gaps may be even exponential (we will show this in Section 8).

Monotone *boolean* circuits are most powerful among these three models and, for a long time, only linear lower bounds were known for such circuits. First super-polynomial lower bounds for the k-clique function CLIQUE and the perfect matching function PER were proved by Razborov [31, 30] by inventing his method of approximations. At almost about the same time, explicit exponential lower bounds were also proved by Andreev [3, 4]. Alon and Boppana [1] improved Razborov's lower bound for CLIQUE from super-polynomial until exponential. Finally, Jukna [13] gave a general and easy to apply lower bounds *criterium* for monotone boolean and real-valued circuits, yielding strong lower bounds for a row of explicit boolean functions. These lower bounds hold for tropical circuits as well. Still, all these methods seem to fail for some important polynomials, like STCON or CONN.

On the other hand, monotone *arithmetic* circuits are much easier to analyze: such a circuit cannot produce anything else but the monomials of the computed polynomial, no "simplifications" (like $x^2 = x$) are allowed here. Exponential lower bounds on the monotone arithmetic circuit complexity were proved already by Schnorr [32] (for CLIQUE), and Jerrum and Snir [11] (for PER and some other polynomials). A comprehensive survey on arithmetic (not necessarily monotone) circuits can be found in the book by Shpilka and Yehudayoff [33].

In this paper we summarize our knowledge about the power of tropical circuits. To our best knowledge, no similar attempt was made after the classical paper by Jerrum and Snir [11]. The main message is that not only methods developed for monotone *boolean* circuits, but (sometimes) even those for monotone *arithmetic* circuits can be used to establish limitations of dynamic programming. Although organized as a survey, the paper contains some new results, including:

1. The proof that tropical circuits for optimization problems with homogeneous target polynomials are no more powerful than monotone arithmetic circuits (Theorem 6). This explains why we do not have efficient dynamic programming algorithms for optimization problems whose target polynomials are homogeneous.

2. A new and simpler proof of Schnorr's [32] lower bound on the size of monotone arithmetic circuits computing union-free polynomials (Theorem 12). A polynomial f is union-free if the product of any two of its monomials contains no third monomial of f distinct from these two ones.

3. A handy "rectangle" lower bound yielding super-polynomial lower bounds on the size of tropical circuits computing homogeneous polynomials (Theorem 17 and its applications).

4. A truly exponential lower bound for monotone arithmetic circuits using expander graphs (Theorem 25).

5. A new and simpler proof of Gashkov and Sergeev's [8, 9] lower bound on the size of monotone arithmetic circuits computing k-free polynomials (Theorem 28). A polynomial is k-free if it does not contain a product of two polynomials, both with $> k$ monomials. This extend's Schnorr's bound, since every union-free polynomial is also k-free for $k = 1$.

Finally, let us mention that we are only interested in the *size* of tropical circuits, i.e. in the total number of gates in them. This number corresponds to the minimum number of sub-problems required by dynamic algorithms for the corresponding optimization problem. Another important measure (not dealt with in this paper) is the *depth* of circuits. In the model of tropical circuits, this corresponds to the parallel time of the corresponding dynamic programs. A well-known result of Karchmer and Wigderson [16] for monotone boolean circuit depth of STCON implies that $(\min, +)$ circuits for this problem must have depth $\Omega(\ln^2 n)$; using binary search, this depth is also achievable. By improving a previous lower bound of Yao [36], Goldmann and Hastad [10] proved a lower bound $\Omega(\ln^2 n/\ln\ln)$ also for CONN; moreover, circuits for CONN of polynomial size must have depth $\Omega(\ln^2 n)$. But it remains open whether any of these two functions require monotone boolean circuits of *size* $\Omega(n^3)$.

2 Semirings

A (commutative) semiring is a system $\mathbf{S} = (S, +, \times, \mathbf{0}, \mathbf{1})$, where S is a set, $+$ ("sum") and $\times$ ("product") are binary operations on S, and 0 and 1 are elements of S having the following three properties:

(i) in both $(S, +, \mathbf{0})$ and $(S, \times, \mathbf{1})$, operation are associative and commutative with identities $\mathbf{0}$ and $\mathbf{1}$: $a + \mathbf{0} = a$ and $a \times \mathbf{1} = a$ hold for all $a \in S$;

(ii) product distributes over sum: $a \times (b + c) = (a \times b) + (a \times c)$;

(iii) $a \times \mathbf{0} = \mathbf{0}$ for all $a \in S$ ("annihilation" axiom).

A semiring is *additively-idempotent* if $a + a = a$ holds for all $a \in S$, and is *multiplicatively-cancellative*, if $ac = bc$ implies $a = b$ for every $c \neq \mathbf{0}$. We will use the common conventions to save parenthesis by writing $a \times b + c \times d$ instead of $(a \times b) + (a \times c)$, and replacing $a \times b$ by ab. Also, a^n will stand for $a \times a \times \cdots \times a$ n-times. If desired, we will also assume that the sets $\mathbb{N}$, $\mathbb{Z}$ or $\mathbb{R}$ also contain infinity elements $+\infty$ and/or $-\infty$.

Among important semirings are:

- Arithmetic semiring $\mathbf{A} = (\mathbb{N}, +, \cdot)$ with $\mathbf{0} = 0$ and $\mathbf{1} = 1$.
- Boolean semiring $\mathbf{B} = (\{0, 1\}, \vee, \wedge)$ with $\mathbf{0} = 0$, $\mathbf{1} = 1$.
- Tropical semirings $\mathbf{Min} = (\mathbb{N}, \min, +)$ and $\mathbf{Min}^- = (\mathbb{Z}, \min, +,)$ with $\mathbf{0} = +\infty$ and $\mathbf{1} = 0$, and $\mathbf{Max} = (\mathbb{N}, \max, +)$ and $\mathbf{Max}^- = (\mathbb{Z}, \max, +)$ with $\mathbf{0} = -\infty$ and $\mathbf{1} = 0$.

Note that all these semirings, but $\mathbf{A}$, are additively-idempotent, and that all of them, but $\mathbf{B}$, are multiplicatively-cancellative. Note also that in arithmetic and in tropical semirings one usually allows *real* numbers, not just integers. This corresponds to considering optimization problems with real, not necessarily integral "weights". The point, however, is that lower-bound techniques, we will consider, work already on smaller domains. In fact, they work when, besides ∞ or $-\infty$, the domain contains 0 and 1 or 0 and -1. Roughly speaking, the larger is the domain, the easier is to prove lower bounds over them.

Due to their intimate relation to discrete optimization, we will be mainly interested in tropical semirings, and circuits over these semirings. Lower bounds for such circuits give lower bounds for the number of subproblems used by any dynamic programming algorithm. The semirings $\mathbf{Min}^-$ and $\mathbf{Max}^-$ are isomorphic via the transformation $x \mapsto -x$, so we will not consider $\mathbf{Max}^-$ separately: all results holding for $\mathbf{Min}^-$ hold also for $\mathbf{Max}^-$. These semirings (as well as the boolean semiring $\mathbf{B}$) have many properties not shared by the (most restrictive) arithmetic semiring $\mathbf{A}$. Say, $(a+b)^n = a^n + b^n$ does not hold in $\mathbf{A}$, but holds in every semiring which is additively-idempotent and multiplicatively-cancellative.

3 Polynomials

Let $\mathbf{S} = (S, +, \times, \mathbf{0}, \mathbf{1})$ be a semiring, and let $x_1, \ldots, x_n$ be variables ranging over S. A *monomial* is any product of these variables, where repetitions are allowed. By commutativity and associativity, we can sort the products and write monomials in the usual notation, with the variables raised to exponents. Thus, every monomial $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ is uniquely determined by the vector of exponents $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}^n$, where $x_i^0 = \mathbf{1}$. Note that in tropical semirings, monomials are linear combinations $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n$ (sums, not products). The *degree*, $|p|$, of a monomial $p = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ is the sum $\alpha_1 + \cdots + \alpha_n$ of its exponents. A monomial p_α is *multilinear* if $\alpha \in \{0,1\}^n$, that is, if no variable has degree > 1.

A monomial p_α *contains* a monomial p_β if $\alpha \geqslant \beta$, that is, if $\alpha_i \geqslant \beta_i$ for all $i = 1, \ldots, n$.

By a *polynomial*[2] over $\mathbf{S}$ we will mean a finite sum over $\mathbf{S}$ of monomials, where repetitions of monomials are allowed. Thus, a polynomial is a formal expression of the form $\sum_{\alpha \in A} c_\alpha p_\alpha$ for a finite subset $A \subset \mathbb{N}^n$, and each c_α is a positive integer, representing the multiplicity of the corresponding monomial p_α in f. The sum and product of two polynomials is defined in the standard way. Every polynomial f defines a function $\widehat{f} : S^n \to S$, whose value $\widehat{f}(a)$ at $a = (a_1, \ldots, a_n) \in S^n$ is obtained by substituting a_i for x_i in f. For polynomials f, h, we will write:

- $f = h$ if f and h have the same monomials (appearing not necessarily with the same coefficients);
- $f \rightleftharpoons h$ if f and h coincide as polynomials, that is, if they have the same monomials appearing with the same coefficients;
- $|f|$ to denote the number of *distinct* monomials in f;
- $f \subseteq h$ if f is a *sub-polynomial* of h, i.e., if every monomial of f is also a monomial of h;
- $p \in f$ if p is a monomial of f.

In general, $\widehat{f} = \widehat{h}$ does not imply $f \rightleftharpoons h$, and even $f = h$. The arithmetic semiring is here an exception.

Lemma 1. *In the arithmetic semiring* $\mathbf{A}$, $\widehat{f} = \widehat{h}$ *implies* $f \rightleftharpoons h$.

Proof. There are several ways to prove this well-known fact. We follow the argument suggested by Sergey Gashkov (personal communication). Suppose that $\widehat{f} = \widehat{h}$ but $f \not\rightleftharpoons h$. Since $f \not\rightleftharpoons h$, the polynomial $g = f - h$ contains at least one monomial. Let p be a monomial of g of maximum degree. Take all partial derivatives with respect to the variables of p until all they disappear. Since p has maximum degree, we obtain some constant $\neq 0$. But since $\widehat{g} = \widehat{f} - \widehat{h}$ is a zero function, the derivative should be zero, a contradiction. □

[2] Usually, polynomials of more than one variable are called *multivariate*, but we will omit this for shortness.

A polynomial is *homogeneous* if all its monomials have the same degree, and is *multilinear* if all its monomials are multilinear (no variables of degree > 1). For example, $f = x^2y + xyz$ is homogeneous but not multilinear, whereas $g = x + yz$ is multilinear but not homogeneous. In general, multilinear polynomials have the form

$$f(x) \rightleftharpoons \sum_{I \in \mathcal{I}} c_I \prod_{i \in I} x_i\,, \tag{1}$$

where $\mathcal{I} \subseteq 2^{[n]}$ is some family of subsets of $[n] = \{1, \ldots, n\}$, and the c_I are positive integers. Such a polynomial is homogeneous of degree m, if all sets $I \in \mathcal{I}$ have the same cardinality $|I| = m$.

It is important to note that the same polynomial (1) (with all $c_I = 1$) has different interpretations over different semirings:

$$\begin{aligned}
f(x) &\rightleftharpoons \bigvee_{I \in \mathcal{I}} \bigwedge_{i \in I} x_i && \text{over } \mathbf{B} \text{ (existence)}\\
f(x) &\rightleftharpoons \min_{I \in \mathcal{I}} \sum_{i \in I} x_i && \text{over } \mathbf{Min} \text{ and } \mathbf{Min}^- \text{ (minimization)}\\
f(x) &\rightleftharpoons \max_{I \in \mathcal{I}} \sum_{i \in S} x_i && \text{over } \mathbf{Max} \text{ and } \mathbf{Max}^- \text{ (maximization)}\\
f(x) &\rightleftharpoons \sum_{I \in \mathcal{I}} \prod_{i \in S} x_i && \text{over } \mathbf{A} \text{ (counting).}
\end{aligned}$$

4 Circuits and their Polynomials

A *circuit* F over a semiring $\mathbf{S} = (S, +, \times, \mathbf{0}, \mathbf{1})$ is a usual fanin-2 circuit whose inputs are variables $x_1, \ldots, x_n$ and constants $\mathbf{0}$ and $\mathbf{1}$. Gates are fanin-2 $+$ and $\times$. That is, we have a directed acyclic graph with $n + 2$ fanin-0 nodes labeled by $x_1, \ldots, x_n, \mathbf{0}, \mathbf{1}$. At every other node, the sum ($+$) or the product ($\times$) of its entering nodes is computed; nodes with assigned operations are called *gates*. The *size* of F, denoted by $|\mathsf{F}|$, is the number of gates in F.

Like polynomials, circuits are also "syntactic" objects. So, we can associate with every circuit F the unique polynomial F *produced* by F inductively as follows:[3]

1. If $\mathsf{F} = x_i$, then $F \rightleftharpoons x_i$.

2. If $\mathsf{F} = \mathsf{G} + \mathsf{H}$, then $F \rightleftharpoons \sum_{p \in G} p + \sum_{q \in H} q$.

3. If $\mathsf{F} = \mathsf{G} \times \mathsf{H}$, then $F \rightleftharpoons \sum_{p \in G} \sum_{q \in H} pq$.

When producing the polynomial F from a circuit F we only use the generic semiring axioms (i)–(iii) to write the result as a polynomial (sum of monomials). For example, if $\mathsf{F} = x \times (\mathbf{1} + y)$ then $F = x + xy$, even though $\widehat{F} = x$ in $\mathbf{B}$ and $\mathbf{Min}$, and $\widehat{F} = xy$ in $\mathbf{Max}$. It is thus important to note that the produced by a given circuit F polynomial F is the same over *any* semiring!

Definition 1. A circuit F *computes* a polynomial f if $\widehat{F} = \widehat{f}$ (F and f coincide as functions). A circuit F *produces* f if $F = f$ (F and f have the same set of monomials).

[3] We will always denote circuits as upright letters $\mathsf{F}, \mathsf{G}, \mathsf{H}, \ldots$, and their produced polynomials by italic versions $F, G, H, \ldots$.

A circuit F *simultaneously* computes (or produces) a given set $\mathcal{F}$ of polynomials if, for every polynomial $f \in \mathcal{F}$, there is a gate in F at which f is computed (or produced).

When analyzing circuits, the following concept of "parse graphs" is often useful. A *parse-graph* G in F is defined inductively as follows: G includes the root (output gate) of F. If u is a $+$-gate, then exactly one of its inputs is included in G. If u is a $\times$-gate, then both its input gates are included in G. Note that each parse-graph produces exactly one monomial in a natural way, and that each monomial $p \in F$ is produced by at least one parse-graph. If p is multilinear then each parse-graph for p is a tree.

- A circuit is *multilinear*, if for every its product gate $u = v \times w$, the sets of variables of the polynomials produced at gates v and w are disjoint. Note that multilinear circuits can only compute multilinear polynomials, and every multilinear polynomial can be computed by such a circuit. Sometimes, multilinear (in our sense) circuits are called also *syntactically multilinear*.

- A circuit is *homogeneous*, if polynomials produced at its gates are homogeneous.

Lemma 2. *If a circuit over* $\mathbf{Max}$*,* $\mathbf{Min}^{-}$*,* $\mathbf{Max}^{-}$ *or* $\mathbf{A}$ *computes a multilinear polynomial, then the circuit itself must be multilinear.*

Proof. For the arithmetic semiring $\mathbf{A}$, this follows from Lemma 1. To show this for the remaining semirings, let f be a multilinear polynomial, and F be a circuit computing f over a semiring $\mathbf{S}$. Suppose that the circuit is not multilinear. Then the polynomial F produced by F contains a monomial p in which some variable x_i appears more than once. If $\mathbf{S} = \mathbf{Max}$, then we can set $x_i = 1$ and $x_j = 0$ for all $j \neq i$. Then $\widehat{f}(x) \leqslant 1$ but $\widehat{F}(x) \geqslant 2$, a contradiction. If $A = \mathbf{Min}^{-}$, then we can set $x_i = -1$, and $x_j = 0$ for all $j \neq i$. Then $\widehat{f}(x) \geqslant -1$, because all monomials of f get value $\geqslant -1$, but $\widehat{F}(x) \leqslant -2$ since already the monomial p of F gets value $\leqslant -2$, a contradiction. Since the semiring $\mathbf{Max}^{-}$ is isomorphic to $\mathbf{Min}^{-}$, we are done. □

Note, however, that no similar fact holds for semirings $\mathbf{B}$ and $\mathbf{Min}$: here we have $x + x^2 = x$, so that terms of higher degree *can* be eliminated.

We will be interested in the following two complexity measures of polynomials f:

- $\mathbf{S}(f)$ = minimum size of a circuit over semiring $\mathbf{S}$ *computing* f.

- $\mathbf{S}[f]$ = minimum size of a circuit over semiring $\mathbf{S}$ *producing* f.

What we are really interested in is to lower-bound the first measure $\mathbf{S}(f)$. The second measure $\mathbf{S}[f]$ is less interesting: it is the *same* for all semirings $\mathbf{S}$, because the formal polynomial of a given (fixed) circuit is the same over all semirings. In particular, we have that

$$\mathbf{S}[f] = \mathbf{A}[f]$$

holds for every semiring $\mathbf{S}$ and every polynomial f. Still, it will be convenient *not* to focus on the arithmetic semiring $\mathbf{A}$ because the inequality $\mathbf{S}(f) \geqslant \mathbf{S}[f]$ is more informative: it means that computing a given polynomial over $\mathbf{S}$ is not easier than to produce this polynomial. This, for example, happens in the arithmetic semiring $\mathbf{A}$: Lemma 1 implies that $\mathbf{A}(f) \geqslant \mathbf{A}[f]$.

5 Some Prominent Polynomials

For the ease of reference, here we recall some polynomials which we will use later to illustrate the lower bound arguments. Variables x_e of considered polynomials correspond to edges of K_n or $K_{n,n}$. Thus, monomials $\prod_{e\in E} x_e$ correspond to some subgraphs E of K_n or $K_{n,n}$. Here are the polynomials we will use later:

- Permanent polynomial PER_n = all perfect matchings in $K_{n,n}$.
- Hamiltonian cycle polynomial HC_n = all Hamiltonian cycles in K_n.
- k-clique polynomial $\mathrm{CLIQUE}_{n,k}$ = all k-cliques in K_n.
- Spanning tree polynomial ST_n = all spanning trees in K_n rooted in node 1.
- s-t connectivity polynomial STCON_n = all paths from $s = 1$ to $t = n$ in K_n.
- All-pairs connectivity polynomial APSP_n = *set* of $\binom{n}{2}$ polynomials STCON_n corresponding to different pairs of start and target nodes s and t.
- Matrix product polynomial MP_n = special case of APSP_n when only paths of length-2 are considered.
- The connectivity polynomial CONN_n = product of all polynomials of APSP_n.

In Section 11.1 we will show that the first four polynomials require **Min**-circuits of exponential size, whereas the next result shows that the last four polynomials all have **Min**-circuits of polynomial size. The following result holds for every semiring with the absorption axiom $a + ab = a$, including the boolean and **Min** semirings.

Theorem 3 (Floyd [6] and Warshall [35]). *Over semirings* **Min** *and* **B***, the polynomials of* APSP_n *can all be simultaneously computed by a circuit of size* $O(n^3)$*.*

Proof. Inputs for APSP_n are non-negative weights x_{ij} of the edges of K_n. For every pair $i < j$ of distinct nodes of K_n, the goal is to compute the weight of the lightest path between i and j; the weight of a path is the sum of weights of its edges. The idea is to recursively compute the polynomials $f_{i,j}^{(k)}$ for $k = 0, 1, \ldots, n$, whose value is the weight of the lightest walk between i and j whose all inner nodes lie in $[k] = \{1, \ldots, k\}$. Then $f_{i,j}^{(0)} = x_{ij}$, and the recursion is: $f_{i,j}^{(k)} = \min\{f_{i,j}^{(k-1)},\ f_{i,k}^{(k-1)} + f_{k,j}^{(k-1)}\}$. The output gates are $f_{i,j}^{(n)}$ for all $i < j$. The total number of gates is $O(n^3)$. Even though the circuit actually searches for weights of lightest *walks*, it correctly computes APSP because every walk between two nodes i and j also contains a simple path (with no repeated nodes) between these nodes. Since the weights are non-negative, the minimum must be achieved on a simple path. □

Remark 1. Earlier dynamic programming algorithm of Bellman [5] and Ford [7] gives a (structurally) simpler **Min**-circuit for STCON_n. It tries to compute the polynomials $f_j^{(k)}$ whose value is the weight of the lightest walk between 1 and j with at most k edges. Then $f_j^{(1)} = x_{ij}$, and the recursion is: $f_j^{(k)}$ = the minimum of $f_j^{(k-1)}$ and of $f_j^{(k-1)} + x_{i,j}$ over all nodes $i \neq j$. The output gate is $f_n^{(n-1)}$. The circuit also has $O(n^3)$ fanin-2 gates.

Polynomial f	Bound	Reference
ST_n	$\mathbf{B}(f) = O(n^3)$, $\mathbf{S}(f) = 2^{\Omega(n)}$	Rem. 2, Thm. 21
CONN_n, STCON_n	$\mathbf{Min}(f) = O(n^3)$	Rem. 2
APSP_n, MP_n	$\mathbf{Min}(f) = \Theta(n^3)$	Thm. 13
PER_n, HC_n	$\mathbf{S}(f) = 2^{\Omega(n)}$	Thm. 21
$\mathrm{CLIQUE}_{n,k}$	$\mathbf{S}(f) \geqslant \binom{n}{k} - 1$	Thm. 14

Table 1: Summary of specific bounds; $\mathbf{S}$ is an arbitrary tropical semiring.

Remark 2. Theorem 3 immediately implies that the polynomials MP_n, CONN_n, and STCON_n can also be computed by **Min**-circuits of size $O(n^3)$. Moreover, over the boolean semiring, the spanning tree polynomial ST represents the same boolean function as CONN. Thus, Theorem 3 also gives $\mathbf{B}(\mathrm{ST}_n) = O(n^3)$.

In the rest of the paper, we will present various lower bound argument for tropical circuits. Table 1 summarizes the resulting specific bounds obtained by these arguments for the polynomials listed above.

6 Reduction to the Boolean Semiring

A semiring $\mathbf{S} = (S, +, \times, \mathbf{0}, \mathbf{1})$ is of *zero-characteristic*, if $\mathbf{1} + \mathbf{1} + \cdots + \mathbf{1} \neq \mathbf{0}$ holds for any finite sum of the unity $\mathbf{1}$. Note that all semirings we consider are of zero-characteristic. The following seems to be a "folklore" result.

Lemma 4. *If a semiring* $\mathbf{S}$ *is of zero-characteristic, then* $\mathbf{S}(f) \geqslant \mathbf{B}(f)$ *holds for every polynomial* f.

Proof. Let F be a circuit over $\mathbf{S}$ computing a given polynomial f. The circuit must correctly compute f on any subset of the domain S. We choose the subset $S_+ = \{\mathbf{0}, \overline{1}, \overline{2}, \ldots\}$, where $\overline{n} = \mathbf{1} + \cdots + \mathbf{1}$ is the n-fold sum of the multiplicative unit element $\mathbf{1}$. Note that $\overline{n} \neq \mathbf{0}$ holds for all $n \geqslant 1$, because $\mathbf{S}$ has zero-characteristic.

Since $\overline{n} + \overline{m} = \overline{n+m}$ and $\overline{n} \times \overline{m} = \overline{n \cdot m}$, $\mathbf{S}_+ = (S_+, +, \times, \mathbf{0}, \mathbf{1})$ is a semiring. Since $S_+ \subseteq S$, the circuit must correctly compute f over this semiring as well. But the mapping $h : S_+ \to \{0, 1\}$ given by $h(\mathbf{0}) = 0$ and $h(\overline{n}) = 1$ for all $n \geqslant 1$, is a homomorphism from $\mathbf{S}_+$ into the boolean semiring $\mathbf{B}$ with $h(x + y) = h(x) \vee h(y)$ and $h(x \times y) = h(x) \wedge h(y)$. So, if we replace each $+$-gate by a logical OR, and each $\times$-gate by a logical AND, then the resulting monotone boolean circuit computes the polynomial f over $\mathbf{B}$. □

Remark 3. One can easily show that, if the input variables can only take boolean values 0 and 1, then $\mathbf{Min}(f) \leqslant 2 \cdot \mathbf{B}(f)$ holds for every multilinear polynomial. Indeed, having a (boolean) circuit F for f, just replace each AND gate $u \wedge v$ by a Min gate $\min(u, v)$, and each OR gate $u \vee v$ by $\min(1, u + v)$. The point however is that tropical circuits must work correctly on much larger domain than $\{0, 1\}$. This is why lower bounds for tropical circuits do not translate to lower bounds for monotone boolean circuits. And indeed, there are explicit polynomials f, like the spanning tree polynomial $f = \mathrm{ST}_n$ such that $\mathbf{B}(f) = O(n^3)$ but $\mathbf{Min}(f) = 2^{\Omega(n)}$; the upper bound is shown in Remark 2, and the lower bound will be shown in Theorem 21.

To prove lower bounds in the boolean semiring—and hence, by Lemma 4, also in any *any* semiring of zero characteristic—one can try to use the following general lower bounds criterion proved in [13] (see also [15, Sect. 9.4] for a simplified proof).

For $a \in \{0,1\}$, an *a-term* of a monotone boolean function is a subset of its variables such that, when all these variables are fixed to the constant a, the function outputs value a, independent of the values of other variables. A family of sets A *covers* a family of sets B if every set in B contains at least one set of A.

By a k-DNF (k-CNF) we will mean a monotone DNF (CNF) with all its monomials (clauses) containing exactly k variables. The *size* of a DNF (or CNF) is the number of its monomials (clauses).

Definition 2. A monotone boolean function $f(x_1,\ldots,x_n)$ is *t-simple* if for every pair of integers $2 \leqslant r, s \leqslant n$ there exists an s-CNF C of size at most $t \cdot (r-1)^s$, an r-DNF D of size at most $t \cdot (s-1)^r$, and a subset $I \subseteq [n]$ of size $|I| \leqslant s-1$ such that either $C \leqslant f$ or $f \leqslant D \vee \bigvee_{i \in I} x_i$ (or both) hold.

The latter condition here means that either the family of all 0-terms of f has a covering consisting of at most $t(r-1)^s$ (out of all $\binom{n}{s}$ possible) s-element subsets, or the family of all 1-terms of f has a covering consisting of at most $s-1$ single variables and at most $t(s-1)^r$ (out of all $\binom{n}{r}$ possible) r-element subsets.

Theorem 5 ([13])**.** *If a monotone boolean function can be computed by a monotone circuit of size t, then f is t-simple.*

Thus, in order to show that f does not have a monotone circuit with t gates, it is enough to show that, for some choice of the parameters $2 \leqslant r, s \leqslant n$ and some choice of "hard to cover" subsets P and Q of 0-terms and 1-terms of f,

(i) either P cannot be covered by $t(r-1)^s$ s-element subsets,

(ii) or Q cannot be covered by $s-1$ single variables and at most $t(s-1)^r$ r-element subsets.

Still, even this "freedom of choice" does not seem to work for $f = \mathrm{STCON}$ or $f = \mathrm{CONN}$. For both these boolean functions, we have no problems with 0-terms: one can take P to be the set of all $|P| = 2^{n-1}-1$ terms corresponding to partitions $[n] = S \cup T$ such that $1 \in S$ and $n \in T$. The corresponding to such a partition 0-term of f consists of all variables x_{ij} with $i \in S$ and $j \in T$. It is clear that setting to 0 all these variables will force f take value 0. Since no s-subset of edges can cover more than $2^{n-\sqrt{s}}$ of the 0-terms in P, we obtain that t must be at least $2^{\sqrt{s}}/(r-1)^s$ in the first case (i). For this bound to be non-trivial, we are forced to take $r = 2$. But then all 1-terms (1-to-n paths) can be covered by only n^2 2-element subsets of edges: just take length-2 paths starting in the source node.

7 Reduction to the Arithmetic Semiring

As we already mentioned in the introduction, circuits over the arithmetic semiring $\mathbf{A}$ are no more powerful than circuits over boolean or tropical semirings. The weakness of circuits computing a given polynomial f over $\mathbf{A}$ lies in the fact (following from Lemma 1) that they cannot produce any "redundant" monomials, those not in f. That is, here we have

$$\mathbf{A}(f) \geqslant \mathbf{A}[f]\,.$$

On the other hand, if the semiring $\mathbf{S}$ is additively-idempotent, then

$$\mathbf{S}(f) \leqslant \mathbf{S}[f]\,.$$

This holds because in an additively-idempotent semiring $\mathbf{S}$ (where $x + x = x$ holds), the multiplicities of monomials have no effect on the represented function. But, in general, we have no converse inequality $\mathbf{S}(f) \geqslant \mathbf{S}[f]$: for some polynomials f, $\mathbf{S}[f]$ may be even exponentially larger than $\mathbf{S}(f)$. Such is, for example, the *s-t* connectivity polynomial $f = \mathrm{STCON}_n$. For this polynomial, we have $\mathbf{Min}(f) = O(n^3)$ (see Remark 2), but it is relatively easy to show that $\mathbf{Min}[f] = 2^{\Omega(n)}$ (see Theorem 22 below).

The polynomial STCON is highly non-homogeneous. The goal of this section is to show that $\mathbf{S}(f)$ just coincides with $\mathbf{S}[f]$, as long as the polynomial f is homogeneous.

Let f be a polynomial. Following Jerrum and Snir [11], define the *lower envelope* of f to be the polynomial f_{le} consisting of all monomials of f of smallest degree. Similarly, the *higher envelope*, f_{he}, of f consists of all monomials of f of largest degree. Note that both polynomials f_{le} and f_{he} are homogeneous, and $f_{\mathrm{le}} = f_{\mathrm{he}} = f$, if f itself is homogeneous.

Theorem 6. *Let f be a polynomial over a semiring $\mathbf{S}$. Then*

(i) $\mathbf{Min}(f) \geqslant \mathbf{A}[f_{\mathrm{le}}]$ *and* $\mathbf{Max}(f) \geqslant \mathbf{A}[f_{\mathrm{he}}]$.

(ii) $\mathbf{Min}(f) = \mathbf{Max}(f) = \mathbf{A}[f]$ *and minimal circuits are homogeneous, if f is homogeneous.*

Item (ii) is an important fact because, when lower bounding $\mathbf{A}[f]$, we can assume that the circuit produces no "redundant" monomials, those not in f. This theorem also has an important implication concerning the power of dynamic programs, which can be roughly stated as follows:

> For optimization problems whose target polynomials are *homogeneous*, dynamic programming is no more powerful than monotone arithmetic circuits!

Proof of Theorem 6. For a polynomial f, let $f_{\min} \subseteq f$ denote the set of all monomials not containing any other monomial of f, and $f_{\max} \subseteq f$ denote the set of all monomials not contained in any other monomial of f. For example, if $f = x + x^2y + yz$, then $f_{\min} = \{x, yz\}$ and $f_{\max} = \{x^2y, yz\}$. Note that $f_{\min} = f_{\max} = f$, if f is homogeneous. Note also that every monomial of f contains (properly or not) at least one monomial of $f_{\min}$, and is contained in at least monomial of $f_{\max}$.

Claim 7. Let f and h be polynomials such that $\widehat{f} = \widehat{h}$ over a semiring $\mathbf{S}$.

(i) If $\mathbf{S} \in \{\mathbf{Min}, \mathbf{Min}^-\}$, then $f_{\min} = h_{\min}$.

(ii) If $\mathbf{S} \in \{\mathbf{Max}, \mathbf{Max}^-\}$, then $f_{\max} = h_{\max}$.

(iii) If $\mathbf{S} \in \{\mathbf{Min}^-, \mathbf{Max}^-\}$ and f is multilinear, then $f = h$.

Proof. To prove item (ii) for the $\mathbf{Min}$-semirings, it is enough to prove it for $\mathbf{Min}$, because $\mathbf{Min}^-$ has larger domain. So, assume that there is a monomial $p \in f_{\min} \setminus h_{\min}$. Let a be an assignment which gives value 1 to all variables of p, and gives value ∞ to the remaining variables. Thus, the value $\widehat{f}(a)$ of f on this assignment is the degree $|p|$ of p. On the other hand, for every monomial q of h, we have that $\widehat{q}(a) = \infty$ if q is not contained in p, and

$\widehat{q}(a) = |q|$ if q is contained in p. Hence, either $\widehat{h}(a) = \infty$ (and hence, $\widehat{f} \neq \widehat{h}$), or $\widehat{h}(a) = |q|$ for some $q \in h_{\min}$ contained in the monomial p. But since $q \neq p$, we have that $\widehat{h}(a) = \widehat{q}(a) = |q|$ is strongly smaller than $|p| = \widehat{f}$. The obtained contradiction shows that $f_{\min} \subseteq h_{\min}$. The converse inclusion $h_{\min} \subseteq f_{\min}$ follows by the same argument. The proof of item (ii) is dual to that of (i).

Item (iii) was proved by Jerrum and Snir [11] using the Farkas lemma about systems of linear inequalities. Here we give a direct proof. Let us consider the semiring $\mathbf{Min}^-$; the argument for $\mathbf{Max}^-$ is similar. Since the polynomial f is multilinear, Lemma 2 implies that the polynomial h must also be multilinear. By (i), every monomial of h must contain at least one monomial of f. Thus, $f \neq h$ can only happen if h contains a monomial (sum) p such that every monomial $q \in f$ misses some variable of p. If we assign -1 to all variables of p, and 0 to the remaining variables, then h takes some value $\leqslant -|p|$. But since each monomial $q \in f$ misses at least one variable of p, the value of each of them, and hence the value of f, is $\geqslant |p| + 1$, a contradiction. □

Claim 7(iii) may fail, if the polynomials are not multilinear: if $f = \min\{x, 2x, 3x\}$ and $h = \min\{x, 3x\}$, then $\widehat{f} = \widehat{h}$ over $\mathbf{Min}^-$, but $f \neq h$.

Claim 8 ([11])**.** Let F be a circuit over some semiring, and F the polynomial produced by F. Then some homogeneous subcircuit of F produces F_{le}, and some homogeneous subcircuit of F produces F_{he}.

Proof. The desired homogeneous subcircuit can be obtain by starting with input gates, and removing (if necessary) one of the wires of every sum gate, at inputs of which polynomials of different degrees are produced. □

We now turn to the actual proof of Theorem 6.

Let us first prove the first claim (i) that $\mathbf{Min}(f) \geqslant \mathbf{A}[f_{\text{le}}]$ holds for every polynomial f (the proof of $\mathbf{Max}(f) \geqslant \mathbf{A}[f_{\text{he}}]$ is similar). Take a minimal circuit F over $\mathbf{Min}$ computing f. Claim 7(i) implies that F must contain all monomials of $f_{\min}$ and, apparently, some extensions of these monomials. Thus, the set of monomials of *minimum* degree must be the same in F and in f, that is $F_{\text{le}} = f_{\text{le}}$ must hold. On the other hand, Claim 8 implies that some (homogeneous) sub-circuit F' of F must *produce* the lower envelope $F_{\text{le}} = f_{\text{le}}$. Thus, $\mathbf{A}[f_{\text{le}}] \leqslant |\mathsf{F}'| \leqslant |\mathsf{F}| = \mathbf{Min}(f)$, as desired.

To prove item (ii) of Theorem 6, assume that our polynomial is homogeneous. Since then $f_{\text{le}} = f_{\text{he}} = f$, item (i) implies that both $\mathbf{Min}(f)$ and $\mathbf{Max}(f)$ must be at least $\mathbf{A}[f]$. That they also cannot exceed $\mathbf{A}[f]$ follows because tropical semirings are additively-idempotent, and hence, the multiplicities of monomials play no role here. □

Let us note that in the arithmetic semiring $\mathbf{A}$, we have a stronger version of Theorem 6(i) allowing one to concentrate on any envelope, not just on the lower or higher ones. Namely, let the *r-th envelope*, f_r, of f be the sum of all monomials of f of degree r. Hence, if d and D are the minimum and the maximum degrees of f, then $f_d = f_{\text{le}}$, $f_D = f_{\text{he}}$, and $f = \sum_{i=d}^{D} f_i$.

Lemma 9. *There is a constant $\epsilon > 0$ such that, for every polynomial f of maximum degree D, and every integer $0 < r \leqslant D$,*

$$\mathbf{A}(f) \geqslant \frac{\epsilon \cdot \mathbf{A}(f_r)}{r^2}$$

Proof. We will prove a somewhat stronger result: if $s = \mathbf{A}(f)$, then for every $0 < r \leqslant D$, there is a homogeneous circuit of size at most $O(r^2 s)$ simultaneously producing $f_0, f_1, \ldots, f_r$. The argument is essentially due to Strassen [34].

Let F be a circuit producing f. We construct the desired circuit F' as follows. For every gate u in F, we define $r+1$ gates in F', which we denote $(u, 0), \ldots, (u, r)$, in such a way that (u, i) produces the i-th envelope of the polynomial produced at u. We construct F' inductively as follows. If u is an input gate, we can clearly define (u, i) as an input gate with the appropriate properties. If $u = v + w$, define $(u, i) = (v, i) + (w, i)$ for all i. If $u = v \times w$, define $(u, i) = \sum_{j=0}^{i} (v, j) \times (w, i-j)$. Induction implies that F' has the claimed property. Every gate in F corresponds to at most $O(r^2)$ gates in F' (each product gate introduces at most $O(r^2)$ additional sum gates), and so $|\mathsf{F}'| = O(r^2 s)$. □

8 Relative Power of Semirings

The relative power of circuits over different semirings is summarized in the following

Theorem 10. *For every multilinear polynomial f, we have*

$$\mathbf{B}(f) \overset{(1)}{\leqslant} \mathbf{Min}(f), \mathbf{Max}(f) \overset{(2)}{\leqslant} \mathbf{Min}^-(f) \overset{(3)}{=} \mathbf{Max}^-(f) \overset{(4)}{=} \mathbf{A}[f]\,.$$

Proof. Inequality (1) follows from Lemma 4, since semirings **Min** and **Max** have zero characteristic, (3) holds since semirings $\mathbf{Min}^-$ and $\mathbf{Max}^-$ are isomorphic, (2) follows from (3) since every circuit computing f on a larger domain must also compute f on any its sub-domain. The last equality (4) follows from Claim 7(iii). □

If f is multilinear *and* homogeneous, then Theorem 6 implies that

$$\mathbf{B}(f) \leqslant \mathbf{Min}(f) = \mathbf{Max}(f) = \mathbf{Min}^-(f) = \mathbf{Max}^-(f) = \mathbf{A}[f]\,.$$

But even if f is multilinear and homogeneous, $\mathbf{B}(f)$ may be exponentially smaller than $\mathbf{Min}(f)$. To see this, take the spanning tree polynomial $f = \mathrm{ST}_n$. This polynomial is multilinear and homogeneous of degree $n-1$, and its boolean version is just the boolean graph-connectivity function. Hence, the Floyd–Warshall dynamic programming algorithm gives $\mathbf{B}(f) = O(n^3)$ (see Remark 2). But a relatively simple argument (see Theorem 21 below) shows that $\mathbf{Min}(f) = 2^{\Omega(n)}$. Thus, we have an exponential gap between $\mathbf{B}(f)$ and $\mathbf{Min}(f)$:

$$\mathbf{Min}(f)/\mathbf{B}(f) = 2^{\Omega(n)} \quad \text{for } f = \mathrm{ST}_n.$$

Exponential separations between $\mathbf{Min}(f)$ and $\mathbf{Max}(f)$, as well as between $\mathbf{Min}(f)$ and $\mathbf{Min}^-(f)$, are given by the *s*-*t* connectivity polynomial $f = \mathrm{STCON}_n$. We know that $\mathbf{Min}(f) = O(n^3)$ (Remark 2), but a simple argument (see Theorem 22) shows that $\mathbf{Max}(f) = 2^{\Omega(n)}$. Hence,

$$\mathbf{Max}(f)/\mathbf{Min}(f) = 2^{\Omega(n)} \quad \text{for } f = \mathrm{STCON}_n.$$

Note that, by Theorem 6, no such gap is possible for *homogeneous* polynomials, so the polynomial $f = \mathrm{STCON}_n$ being non-homogeneous is crucial here.

From now on we concentrate on the lower bound *arguments* themselves.

9 Lower Bounds for Union-Free Polynomials

Let $f(x_1,\ldots,x_n)$ be a polynomial in $n \geqslant 3$ variables. An *enrichment* of f is a polynomial h in $n-1$ variables obtained by taking some variable x_k and replacing it by a sum $x_i + x_j$ or by a product x_ix_j of some other two (not necessarily distinct) variables, where $k \not\in \{i,j\}$. A *progress measure* of polynomials is an assignment of non-negative numbers $\mu(f)$ to polynomials f such that

(i) $\mu(x_i) = 0$ for each variable x_i;

(ii) $\mu(h) \leqslant \mu(f) + 1$ for every enrichment h of f.

Lemma 11. *For every polynomial f, and every progress measure $\mu(f)$, we have $\mathbf{A}[f] \geqslant \mu(f)$.*

Proof. Take a monotone arithmetic circuit F with $s = \mathbf{A}[f]$ gates producing f. We argue by induction on s. If $s = 0$, then $\mathsf{F} = x_i$ in an input variable, and we have $\mathbf{A}[f] = 0 = \mu(f)$. For the induction step, take one gate $u = x_i * x_j$ where $* \in \{+,\cdot\}$. Let $\mathsf{F}'(x_1,\ldots,x_n,y)$ be the circuit with the gate u replaced by a new variable y. Hence, $|\mathsf{F}'| = |\mathsf{F}| - 1$ and $F(x_1,\ldots,x_n)$ is an enrichment of $F'(x_1,\ldots,x_n,y)$. By the induction hypothesis, we have that $|\mathsf{F}'| \geqslant \mu(F')$. Together with $\mu(F) \leqslant \mu(F') + 1$, this yields $|F| = |F'| + 1 \geqslant \mu(F') + 1 \geqslant \mu(F)$. □

Definition 3. A sub-polynomial $g \subseteq f$ of a polynomial f is *union-free* if the product of any two monomials p and q of g contains no third monomial of f distinct from p and from q.

In particular, a multilinear polynomial f of minimum degree m is union-free, if no subset of $\lceil m/2 \rceil$ variables is contained in more than one monomial of f. Indeed, if a product pq of some two monomials $p \neq q$ of f contains some third monomial r of f, then $|p \cap r|$ or $|q \cap r|$ must be least $\lceil m/2 \rceil$.

Theorem 12 (Schnorr [32])**.** *For every polynomial f, we have $\mathbf{A}[f] \geqslant \nu(f) - 1$, where*

$$\nu(f) := \max\{|g| \colon g \subseteq f \text{ is a union-free sub-polynomial}\}\,.$$

In particular, $\mathbf{A}[f] \geqslant |f| - 1$ is the polynomial f itself is union-free.

Proof. It is enough to show that the measure $\mu(f) = \nu(f) - 1$ is a progress measure. The first condition (i) is clearly fulfilled, since $\nu(x_i) = 1$. To verify the second condition (ii), let $f(x_1,\ldots,x_n,y)$ be a polynomial, and $h(x_1,\ldots,x_n)$ be its enrichment. Our goal is to show that $\nu(f) \geqslant \nu(h) - 1$ (and hence, also $\mu(f) \geqslant \mu(h) - 1$). We only consider the "hard" case when y is replaced by a sum of variables: $h(x_1,\ldots,x_n) = f(x_1,\ldots,x_n,u+v)$, where $u,v \in \{x_1,\ldots,x_n\}$.

To present the proof idea, we first consider the case when no monomial of f contains more than one occurrence of the variable y. Then every monomial yp of f turns into two monomials up and vp of h. To visualize the situation, we may consider the bipartite graph $G \subseteq f \times h$, where every monomial $yp \in f$ is connected to two monomials $up, vp \in h$; each monomial $q \in f$ without y is connected to $q \in h$.

Take now a union-free subset $C \subseteq h$ of size $|C| = \nu(h)$. Since *both* neighbors up and vp of every monomial yp of f belong to h, the set of neighbors $D \subseteq f$ of $C \subseteq h$ is also a union-free subset of f. A simple (but crucial) observation is that at most one monomial in D can have two neighbors in C: were there two monomials $p \neq q$ such that all four monomials

up, vp, uq, vq belong to C, then C would be not union-free, because $up \times vq$ contains uq (and vp). Thus,

$$\nu(f) \geqslant |D| \geqslant |C| - 1 = \nu(h) - 1\,.$$

In general (if y can have any degrees in f), a monomial $y^k p$ of f has $k+1$ neighbors $u^i v^{k-i} p$, $i = 0, 1, \ldots, k$ in h. We only have to show that at most one monomial in D can have two neighbors in C. For this, assume that there are two monomials $p \neq q$ such that all four monomials $u^a v^{k-a} p, u^b v^{k-b} p, u^c v^{l-c} q, u^d v^{l-d} q$ belong to C. Assume w.l.o.g. that $a = \max\{a, b, c, d\}$. Then the product $u^a v^{k-a} p \times u^c v^{l-c} q$ contains $u^a v^{l-c} q$, and (since $c \leqslant a$) contains the monomial $u^a v^{l-a} q$ of h, contradicting the union-freeness of C. □

Remark 4. It is not difficult to see that we have a stronger inequality $\nu(f) \geqslant \nu(h)$, if the variable y is replaced by the product uv (instead of the sum $u+v$). Thus, in fact, Theorem 12 gives a lower bound on the number of sum gates.

9.1 Applications

Recall that the dynamic programming algorithm of Floyd–Warshall implies that the all-pairs shortest path polynomial APSP_n, and hence, also the matrix product polynomial MP_n, have **Min**-circuits of size $O(n^3)$; see Theorem 3. On the other hand, using Theorem 12 one can show that this algorithm is optimal: a cubic number of gates is also necessary.

Theorem 13. *Both* $\mathbf{Min}(\mathrm{APSP}_n)$ *and* $\mathbf{Min}(\mathrm{MP}_n)$ *are* $\Theta(n^3)$.

Proof. It is enough to show that $\mathbf{Min}(\mathrm{MP}_n) = \Omega(n^3)$. Recall that $\mathrm{MP}_n(x, y)$ is the set of all n^2 polynomials $f_{ij} = \sum_{k \in [n]} x_{ik} y_{kj}$. Take a set z of n^2 new variables, and consider the *triangle polynomial*

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

Since $\mathrm{TR} = \sum_{i,j \in [n]} z_{ij} f_{ij}$, we have that $\mathbf{S}(\mathrm{MP}_n) \geqslant \mathbf{S}(\mathrm{TR}_n) - 2n^2$ holds in any semiring, including the **Min**-semiring. On the other hand, since the polynomial $f = \mathrm{TR}$ is homogeneous, Theorem 6 implies that $\mathbf{Min}(f) = \mathbf{A}[f]$. So, it remains to show that $\mathbf{A}[f] = \Omega(n^3)$ holds for $f = \mathrm{TR}_n$.

To do this, observe that every monomial $p = x_{ik} y_{kj} z_{ij}$ of f is uniquely determined by any choice of any two of its three variables. This implies that p cannot be contained in a union of any two monomials distinct from p. Thus, the polynomial f is union-free, and its Schnorr's measure is $\nu(f) = n^3 - 1$. Theorem 12 yields $\mathbf{A}[f] \geqslant \nu(f) = n^3 - 1$, as desired. □

Schnorr's theorem allows one to obtain even exponential lower bounds. Recall that the k-clique polynomial $\mathrm{CLIQUE}_{n,k}$ has $m = \binom{n}{k}$ monomials $\prod_{i \neq j \in S} x_{ij}$ corresponding to subsets $S \subseteq [n]$ of size $|S| = k$. This is a multilinear homogeneous polynomial of degree $\binom{k}{2}$.

By Lemma 4, an exponential lower bound for $\mathrm{CLIQUE}_{n,s}$ over the tropical **Min** follows from Razborov's lower bound for this polynomial over the boolean semiring **B** [31]. However, the proof over **B** is rather involved. On the other hand, in the tropical semiring **Min** such a bound comes quite easily.

Theorem 14. *For* $f = \mathrm{CLIQUE}_{n,k}$*, both* $\mathbf{Min}(f)$ *and* $\mathbf{Max}(f)$ *are at least* $\binom{n}{k} - 1$.

Proof. The polynomial $f = \mathrm{CLIQUE}_{n,k}$ is homogeneous. So, by Theorems 6 and 12, it is enough to show that $\mathrm{CLIQUE}_{n,k}$ is union-free. To show this, assume for the sake of contradiction, that the union of two distinct k-cliques A and B contains all edges of some third clique C. Since all three cliques are distinct and have the same number of nodes, C must contain a node u which does not belong to A and a node v which does not belong to B. This already leads to a contradiction because either the node u (if $u = v$) or the edge $\{u, v\}$ (if $u \neq v$) of C would remain uncovered by the cliques A and B. □

Kerr [19] earlier proved $\mathbf{Min}(\mathrm{MP}_n) = \Omega(n^3)$ using a different argument, which essentially employs the fact the **Min**-semiring contains more than two distinct elements. Since this "domain-dependent" argument may be of independent interest, we sketch it.

Proof. (Due to Kerr [19]) Let F be a **Min**-circuit computing all n^2 polynomials

$$f_{ij}(x) = \min\{x_{ik} + y_{kj} \colon k = 1, \ldots, n\}\,.$$

By Claim 7(i), for each polynomial f_{ij} there must be a gate u_{ij}, the polynomial F_{ij} produced at which is of the form $F_{ij} = \min\{f_{ij}, G_{ij}\}$, where G_{ij} is some set of monomials (sums), each containing at least one monomial of f_{ij}.

Assign to every monomial $p = x_{ik} + y_{kj}$ of f_{ij} a gate u_p with the following two properties: (i) p is produced at u_p, and (ii) there is a path from u_p to u_{ij} containing no sum-gates. Since $a + a = a$ does not hold in **Min**, at least one such gate must exist for each of the monomials $x_{ik} + y_{kj}$.

It remains therefore to show that no other term $x_{ab} + y_{bc}$ gets the same gate u_p. To show this, assume the opposite. Then at the gate u_p some sum

$$\min\{x_{ik}, \alpha, \ldots\} + \min\{y_{kj}, \ldots\}$$

is computed, where $\alpha \in \{x_{ab}, y_{bc}\}$ is a single variable distinct from x_{ik} and y_{kj}. Set $\alpha := 0$, $x_{ik} = y_{kj} := 1$ and set all remaining variables to 2. Then the first minimum in the sum above evaluates to 0, and we obtain that $\widehat{F}_{ij}(x) \leqslant 1$. But $\widehat{f}_{ij}(x) = 2$ because the term $x_{ik} + y_{kj}$ gets value $1 + 1 = 2$, and the remaining terms of f_{ij} get values $\geqslant 2 + 0 = 2$. This gives the desired contradiction. □

Remark 5. Using far more subtle arguments, Paterson [27], and Mehlhorn and Galil [24] succeeded to prove a cubic lower bound $\Omega(n^3)$ for MP_n even over the boolean semiring **B**.

10 Cuts

In the proof of Lemma 11, we eliminated one-by-one the "next to the inputs" gates. We can, however, eliminate also "deeper" gates.

Let F be a circuit over some semiring $\mathbf{S} = (S, +, \times, \mathbf{0}, \mathbf{1})$. For a gate u in F, let $\mathrm{pol}(u)$ denote the polynomial produced at u, and let $\mathsf{F}_{u=\mathbf{0}}$ denote the circuit obtained from F by replacing the gate u by the additive identity $\mathbf{0}$. Recall that $a \times \mathbf{0} = \mathbf{0}$ holds for all $a \in S$. Hence, the polynomial $F_{u=\mathbf{0}}$ consists of only those monomials of F that do not "use" the gate u for their production. To avoid trivialities, we will always assume that $\mathsf{F}_{u=\mathbf{0}} \neq \mathsf{F}$, i.e. that there are no "redundant" gates.

Lemma 15 (Decomposition by Gates)**.** *For every gate u in F, the polynomial F produced by F can be written as a sum $F = F_u + F_{u=\mathbf{0}}$, where $F_u = \mathrm{pol}(u) \times \mathrm{ext}(u)$ for some polynomial* $\mathrm{ext}(u)$.

Proof. If we replace the gate u by a new variable y, the resulting circuit produces a polynomial of the form

$$F'(x_1, \ldots, x_n, y) = \sum_{i \in I} y^{k_i} p_i + \sum_{j \in J} q_j$$

where all $k_i \geqslant 1$, and none of the monomials p_i and q_j contains y. Hence, F' has the form

$$F'(x_1, \ldots, x_n, y) = y \times \Big(\sum_{i \in I} y^{k_i - 1} p_i \Big) + F'(x_1, \ldots, x_n, \mathbf{0}) \,,$$

where $F'(x_1, \ldots, x_n, \mathbf{0}) = F_{u=\mathbf{0}}(x_1, \ldots, x_n)$. It remains to replace the variable y by the polynomial $\mathrm{pol}(u)$ produced at the gate u. □

Remark 6. Roughly speaking, the number $|F_u|$ of monomials in the polynomial F_u is the "contribution" of the gate u to the production of the entire polynomial F. Intuitively, if this contribution is small for many gates, then there must be many gates in F. More formally, associate with each monomial $p \in F$ some of its parse-graphs F_p in F. Observe that $u \in \mathsf{F}_p$ implies $p \in F_u$. Thus, double-counting yields

$$|\mathsf{F}| = \sum_{u \in \mathsf{F}} 1 \geqslant \sum_{u \in \mathsf{F}} \sum_{p \in F\colon u \in \mathsf{F}_p} \frac{1}{|F_u|} = \sum_{p \in F} \sum_{u \in \mathsf{F}_p} \frac{1}{|F_u|} \geqslant |F| \cdot \min_{p \in F} \sum_{u \in \mathsf{F}_p} \frac{1}{|F_u|} \,.$$

So, in principle, one can obtain strong lower bounds on the total number of gates in F by showing that this latter minimum cannot be too small.

The polynomial $\mathrm{ext}(u)$ in Lemma 15 can be defined by associating polynomials with paths in the circuit F. Let π be a path from a gate u to the output gate, $u_1, \ldots, u_m$ be all product gates along this path (excluding the first gate u, if it itself is a product gate), and $w_1, \ldots, w_m$ be input gates to these product gates *not lying* on the path π. We associate with π the polynomial $\mathrm{pol}(\pi) := \mathrm{pol}(w_1) \times \mathrm{pol}(w_2) \times \cdots \times \mathrm{pol}(w_m)$. Then

$$\mathrm{ext}(u) = \sum_{\pi} \mathrm{pol}(\pi) \,,$$

where the sum is over all paths π from v to the output gate.

Lemma 15 associates sub-polynomials of F with *nodes* (gates) of F. In some situations, it is more convenient to associate sub-polynomials with *edges*. For this, associate with every edge (u, v), where $v = u * w$ is some gate with $* \in \{+, \times\}$ of F, the polynomial

$$\mathrm{ext}_u(v) := A \times \mathrm{ext}(v) \quad \text{where} \quad A = \begin{cases} \mathbf{1} & \text{if } * = +; \\ \mathrm{pol}(w) & \text{if } * = \times. \end{cases}$$

That is, $\mathrm{ext}_u(v) = \mathrm{ext}(v)$ if v is a sum gate, and $\mathrm{ext}_u(v) = \mathrm{pol}(w) \times \mathrm{ext}(v)$ if v is a product gate.

A *node-cut* in a circuit is a set U of its nodes (gates) such that every input-output path contains a node in U. Similarly, an *edge-cut* is a set E of edges such that every input-output path contains an edge in E. Recall that, in our notation, "$f = h$" for two polynomials f and h only means that their *sets* of monomials are the same—their multiplicities (coefficients) may differ.

Lemma 16 (Cuts)**.** *If U is a node-cut and E an edge-cut in a circuit F, then*

$$F = \sum_{u \in U} \mathrm{pol}(u) \times \mathrm{ext}(u) = \sum_{(u,v)\in E} \mathrm{pol}(u) \times \mathrm{ext}_u(v)\,.$$

Proof. The fact that all monomials of the last two polynomials are also monomials of F follows from their definitions. So, it is enough to show that every monomial $p \in F$ belongs to both these monomials. For this, take a parse graph F_p of p. Since U forms a node-cut, the graph F_p must contain some node $u \in U$. The monomial p has a form $p = p'p''$ where p' is the monomial produced by the subgraph of F_p rooted in u. Hence, $p' \in \mathrm{pol}(u)$ and $p'' \in \mathrm{ext}(u)$. Similarly, since E forms an edge-cut, the graph F_p contains some edge $(u,v) \in E$. The monomial p has the form $p = p'p''$ where p' is the monomial produced by the subgraph of F_p rooted in u. Hence, $p' \in \mathrm{pol}(u)$ and $p'' \in \mathrm{ext}_u(v)$. □

11 Rectangle Bound

For a polynomial f and a natural number r, let $\mu_r(f)$ denote the maximum number of monomials in f containing a fixed monomial of degree r. In particular, $\mu_0(f) = |f|$ is the total number of distinct monomials of f, and $\mu_r(f)$ can only decrease as r increases. Moreover, $\mu_d(f) = 1$ where d is the maximum degree of f, and $g \subseteq f$ implies $\mu_r(g) \leqslant \mu_r(f)$.

Theorem 17 (Rectangle Bound)**.** *For every homogeneous polynomial f of degree $m \geqslant 2$, and every tropical semiring $\mathbf{S}$, there is an integer $m/3 < r \leqslant 2m/3$ such that*

$$\mathbf{S}(f) \geqslant \frac{|f|}{\mu_r(f) \cdot \mu_{m-r}(f)}\,.$$

Proof. Let F be a minimal circuit over $\mathbf{S}$ computing f. Since f is homogeneous, Theorem 6(ii) implies that $F = f$ and the circuit F is homogeneous. Define the weight l_u of a gate $u \in \mathsf{F}$ be the degree $\deg(\mathrm{pol}(u))$ of the (homogeneous) polynomial $\mathrm{pol}(u)$ produced at u. Hence, leaves (input gates) get weight 1, the output gate gets weight m. Since the minimum degree measure is clearly subadditive, the weighting is subadditive: $l_u \leqslant l_v + l_w$ holds for every gate $u = v * w$ of F.

Claim 18. Let $0 < \epsilon < 1$, and let l_u be a subadditive weighting of the gates of F. If m is the weight of the output gate, and if each input gate receives weight $\leqslant \epsilon m$, then there exists a gate u of weight $\epsilon m/2 < l_u \leqslant \epsilon m$.

Proof. Start at the output gate of F, and traverse the circuit (in the reverse order of edges) by always choosing the input of maximal weight until a gate v of weight $l_v > \epsilon m$ is found such that $l_u, l_w \leqslant \epsilon m$ holds for both gates u and w feeding into v. Assume w.l.o.g. that $l_u \geqslant l_w$. Since $l_v \leqslant l_u + l_w \leqslant 2l_u$, the gate u has the desired weight $\epsilon m/2 < l_u \leqslant \epsilon m$. □

By a *degree-balanced rectangle* in f we will mean a product of two homogeneous polynomials $A \times B \subseteq f$ such that $m/3 < \deg(A) \leqslant 2m/3$. (Note that in tropical semirings, polynomials A are minimums of sums, hence, rectangles here have the form $A + B$.)

Claim 19. The polynomial f can be written as a sum of at most $|\mathsf{F}|$ degree-balanced rectangles.

Proof. We proceed by induction on $s = |\mathsf{F}|$. If $s = 1$, then f is a product of two (not necessarily distinct, if f is not multilinear) input variables, $f = x_i x_j$. Since $\deg(f) = 2$, and $\deg(x_i) = \deg(x_j) = 1$, f itself is a degree-balanced rectangle.

By Claim 18 (with $\epsilon = 2/3$), there exists a gate u of weight $m/3 < l_u \leqslant 2m/3$. By Lemma 15, we can write F as $F = F_u + F_{u=\mathbf{0}}$ where $F_u = A \times B$ with $m/3 < \deg(A) \leqslant 2m/3$. The polynomial $F_{u=\mathbf{0}}$ is obtained from F by removing some monomials. If $F_{u=\mathbf{0}}$ is empty, then we are done. Otherwise, $F_{u=\mathbf{0}}$ is a homogeneous polynomial of degree m which can be computed by a circuit with at most $s-1$ gates (the gate u is eliminated). By the induction hypothesis, $F_{u=\mathbf{0}}$ can be written as a sum of $s-1$ degree-balanced rectangles. Hence, the entire polynomial $f = F$ can be written as a sum of s products, as desired. □

By Claim 19, the number $|\mathsf{F}|$ of gates in F is at least the number $|f|$ of monomials in f divided by the largest possible number of a degree-balanced rectangle in f. So, it remains to upper-bound this latter number.

Claim 20. Let A and B be polynomials of maximum degrees a and b over a tropical semiring. If $A \times B \subseteq f$, then $|A \times B| \leqslant \mu_a(f) \cdot \mu_b(f)$.

Proof. Fix a monomial $p \in g$ of degree $|p| = a$, and a monomial $q \in h$ of degree $|q| = b$. Since $\{p\} \times h \subseteq f$, we have that $|h| = |\{p\} \times h| \leqslant \mu_{|p|}(f) = \mu_a(f)$, where the first equality holds because tropical semirings are not multiplicatively idempotent ($a \times a \neq a$ for all $a \neq \mathbf{1}$, that is, $a + a \neq a$ for all $a \neq \pm\infty$). Similarly, since $g \times \{q\} \subseteq f$, we have that $|g| = |g \times \{q\}| \leqslant \mu_{|q|}(f) = \mu_b(f)$. □

Now we can finish the proof of the theorem as follows. By Claim 19, the polynomial f can be written as a sum of $s = |\mathsf{F}|$ products $A_i \times B_i$ of homogeneous polynomials A_i and B_i, where the degree $a_i = \deg(A_i)$ of A_i satisfies $m/3 < a_i \leqslant 2m/3$; hence, $\deg(B_i) \geqslant m - a_i$. For every $i = 1, \ldots, s$, Claim 20 gives $|A_i \times B_i| \leqslant \mu_{a_i}(f) \cdot \mu_{m-a_i}(f)$, and hence, $|f| \leqslant \sum_{i=1}^{s} \mu_{a_i}(f) \cdot \mu_{m-a_i}(f) \leqslant s \cdot \mu_r(f) \cdot \mu_{m-r}(f)$ for some $m/3 < r \leqslant 2m/3$. □

11.1 Applications

The Rectangle Bound allows one to easily obtain *exponential* lower bounds for some explicit polynomials.

Theorem 21. *Let* $\mathbf{S}$ *be some tropical semiring, and* $f \in \{\mathrm{PER}_n, \mathrm{HC}_n, \mathrm{ST}_n\}$. *Then* $\mathbf{S}(f) = 2^{\Omega(n)}$.

Using a tighter analysis (in the spirit of Remark 6) and more involved computations, Jerrum and Snir [11] obtained even *tight* lower bounds for PER_n and HC_n.

Proof. Since all these three polynomials are homogeneous, we can apply Theorem 17 to them. First, consider the permanent function $f = \mathrm{PER}_n$. This is a homogeneous polynomial of degree n with $|f| = n!$ monomials. Since $\mu_r(f) = (n-r)!$, Theorem 17 (with $r = n/3$) gives $\mathbf{S}(f) \geqslant n!/(n-r)!r! = \binom{n}{r} \geqslant 3^{n/3}$.

The argument for HC_n is almost the same: the only difference is that now the monomials correspond to symmetric, not to all permutations.

So, let us consider the spanning tree polynomial $f = \mathrm{ST}_n$. This a homogeneous polynomial of degree $n-1$ with $|f| = n^{n-2}$ monomials. Each monomial $x_{2,\pi(2)} x_{3,\pi(3)} \cdots x_{n,\pi(n)}$ corresponds to one of the functions $\pi : \{2, 3, \ldots, n\} \to [n]$ such that $\forall i\ \exists k$: $\pi^{(k)}(i) = 1$. Each such function π gives a spanning tree, where $\pi^{-1}(i)$ is the set of children of the node i in the tree. Now, if we fix some r edges, then r values of functions π whose spanning trees contain these edges are fixed. Thus, $\mu_r(f) \leqslant (n-r)^{n-r-2}$. Theorem 17 (with $r = n/3$) gives $\mathbf{S}(f) = 2^{\Omega(n)}$. □

The three polynomials above are homogeneous. To show that the Rectangle Bound works also for non-homogeneous polynomials, consider the *s-t* connectivity polynomial $f = \mathrm{STCON}_n$. We know that $\mathbf{Min}(f) = O(n^3)$ (Remark 2). But over the **Max**-semiring, f requires circuits of exponential size.

Theorem 22. *If* $f = \mathrm{STCON}_n$*, then* $\mathbf{Min}(f) = O(n^3)$ *but* $\mathbf{Max}(f)$ *and* $\mathbf{Min}[f]$ *are both* $2^{\Omega(n)}$.

Proof. Consider the higher envelope f_{he} of f. This is a homogeneous polynomial of degree $m = n-1$. By Theorem 6(i), we have that $\mathbf{Max}(f) \geqslant \mathbf{Max}[f_{\mathrm{he}}]$. Monomials of f_{he} correspond to 1-to-n paths with exactly $n-2$ inner nodes. Hence, $|f_{\mathrm{he}}| = (n-2)!$. If we fix some set of r edges, then at most $(n-2-r)!$ monomials of f_{he} can contain all these edges; hence, $\mu_r(f) \leqslant (n-2-r)!$. Thus, again, Theorem 17 (with $r = n/3$) gives a lower bound:

$$\mathbf{Max}(f) \geqslant \mathbf{Max}[f'] \geqslant \frac{(n-2)!}{(n-2-r)!(r-1)!} = 2^{\Omega(n)}\,.$$

Since $\mathbf{Max}(f) \leqslant \mathbf{Max}[f] = \mathbf{Min}[f]$, the same lower bound on $\mathbf{Min}[f]$ also follows. □

12 Truly Exponential Lower Bounds

Note that the lower bounds above have the forms $2^{\Omega(\sqrt{n})}$, where n is the number of variables. Truly exponential lower bounds $2^{n/2}$ on the monotone circuit size of multilinear polynomials of n variables were announced by Kasim-Zade [17, 18] and Kuznetsov [20]. Using some ideas of [17, 18, 20], Gashkov [8] proposed a general lower bounds argument for monotone arithmetic circuits and used it to prove a $2^{2n/3}$ lower bound. These bounds are obtained via an appropriate modification of Schnorr's approach (Section 9); the method was further developed and new lower bounds were proved by Gashkov and Sergeev [9].

The construction of the corresponding multilinear polynomials in these works is algebraic. Say, the monomials of the polynomial $f(x,y)$ of $2n$ variables constructed in [17, 18] have the form $x_1^{a_1}\cdots x_n^{a_n}y_1^{b_1}\cdots y_n^{b_n}$ where $a \in \{0,1\}^n$ and $b = a^3$ (we view vector a as an element of $GF(2^n)$ when rising it to the 3rd power). That is, monomials correspond to points of the cubic parabola $\{(a,a^3)\colon a \in GF(2^n)\}$. The monomials of the polynomial constructed in [8] are defined using triples (a,b,c) with $a,b,c \in GF(2^n)$ satisfying $a^3+b^7+c^{15} = 1$. The constructed polynomials are $(1,1)$-free, and the desired lower bounds follow from a general lower bound of Gashkov and Sergeev [9] for (k,l)-free polynomials (see Sect. 13 for this bound).

Without knowing these results, Raz and Yehudayoff [29] have recently also proved a truly exponential lower bound $2^{\Omega(n)}$ using discrepancy arguments and exponential sum estimates. In this section we use some ideas from [14] to show that truly exponential lower bounds can be also proved using graphs with good expansion properties. Numerically, our bounds are worse than those in [17, 18, 20, 8, 9] (have smaller constants), but the construction of polynomials is quite simple (modulo the construction of expander graphs).

Say that a partition $[n] = S \cup T$ is *balanced* if $n/3 \leqslant |S| \leqslant 2n/3$. Define the *matching number* $m(G)$ of a graph $G = ([n], E)$ as the largest number m such that, for every balanced partition of nodes of G, at least m crossing edges form an induced matching. An edge is crossing if it joins a node in one part of the partition with a node in the other part. Being an induced matching means that no two endpoints of any two edges of the matching are joined by a crossing edge.

Our construction of hard polynomials is based on the following lemma. Associate with every graph $G = ([n], E)$ the multilinear polynomial $f_G(x_1, \ldots, x_n)$ whose monomials are $\prod_{i \in S} x_i$ over all subsets $S \subseteq [n]$ such that the induced subgraph $G[S]$ has an odd number of edges of G.

Lemma 23. *For every non-empty graph G on n nodes, we have*

$$\mathbf{A}(f_G) \geqslant 2^{m(G)-2}\,.$$

We postpone the proof of this lemma and turn to its application.

The following simple claim gives us a general lower bound on the matching number $m(G)$. Say that a graph is *s-mixed* if every two disjoint s-element subsets of its nodes are joined by at least one edge.

Claim 24. If an n-node graph G of maximum degree d is s-mixed, then $m(G) \geqslant (\lfloor n/3 \rfloor - s)/(2d+1)$.

Proof. Fix an arbitrary balanced partition of the nodes of G into two parts. To construct the desired induced matching, formed by crossing edges, we repeatedly take a crossing edge and remove it together with all its neighbors. At each step we remove at most $2d+1$ nodes. If the graph is s-mixed, then the procedure will run for m steps as long as $\lfloor n/3 \rfloor - (2d+1)m$ is at least s. □

Thus, we need graphs of small degree that are still s-mixed for small s. Examples of such graphs are expander graphs. A *Ramanujan graph* is a regular graph $G_{n,q}$ of degree $q+1$ on n nodes such that $\lambda(G) \leqslant 2\sqrt{q}$, where $\lambda(G)$ is the second largest (in absolute value) eigenvalue of the adjacency matrix of G. Explicit constructions of Ramanujan graphs on n nodes for every prime $q \equiv 1 \bmod 4$ and infinitely many values of n were given by Margulis [22], Lubotzky, Phillips and Sarnak [21]; these were later extended to the case where q is an arbitrary prime power by Morgenstern [26], and Jordan and Livné [12].

Theorem 25. *If $f_G(x_1, \ldots, x_n)$ is the multilinear polynomial associated with the Ramanujan graph $G = G_{n,64}$, then*

$$\mathbf{A}(f_G) \geqslant 2^{0.001n}\,.$$

Proof. The Expander Mixing Lemma ([2, Lemma 2.3]) implies that, if G is a d-regular graph on n nodes, and if $s > \lambda(G) \cdot n/d$, then G is s-mixed. Now, the graph $G = G_{n,q}$ is d-regular with $d = q+1$ and has $\lambda(G) \leqslant 2\sqrt{q}$. Hence, the graph G is s-mixed for $s = 2n/\sqrt{q} > 2\sqrt{q}n/(q+1)$.

Our graph $G = G_{n,64}$ is a regular graph of degree $d = 65$, and is s-mixed for $s = 2n/\sqrt{64} = n/4$. Lemma 23 gives the desired lower bound. □

Proof of Lemma 23. Following Raz and Yehudayoff [29], we call polynomial $f(x_1, \ldots, x_n)$ a *product polynomial*, if f is a product of two polynomials on disjoint sets of variables, each of size at least $n/3$, that is, if $f = g(Y) \times h(Z)$ for some partition $Y \cup Z = \{x_1, \ldots, x_n\}$ of variables with $|Y|, |Z| \geqslant n/3$, and some two polynomials g and h on these variables. Note that we do not require that, say, the polynomial $g(Y)$ must depend on all variables in Y: some of them may have zero degrees in g.

Claim 26 ([29])**.** If $\mathsf{F}(x_1,\ldots,x_n)$ is a multilinear circuit of size s with $n \geqslant 3$ input variables, then the polynomial F can be written as a sum of at most $s+1$ product polynomials.

Proof. Induction on s, similar to that in the proof of Claim 19. For a gate u, let X_u be the set of variables in the corresponding subcircuit of F. Let v be the output gate of F. If v is an input gate, then F itself is a product polynomial, since $n \geqslant 3$. So, assume that v is not an input gate. If $|X_v| \leqslant 2n/3$, then the polynomial F itself is a product polynomial, because $F = F \times \mathbf{1}$. So, assume that $|X_v| > 2n/3$. Every gate u in F entered by gates u_1 and u_2 admits $|X_u| \leqslant |X_{u_1}| + |X_{u_2}|$. Thus, there exists a gate u in F such that $n/3 \leqslant |X_u| \leqslant 2n/3$. By Lemma 15, we can write F as $F = F_u + F_{u=\mathbf{0}}$ where $F_u = g_u \times h$ with $n/3 \leqslant |X_u| \leqslant 2n/3$ and some polynomial h. Moreover, since the circuit is multilinear, the set X_h of variables in the polynomial h must be disjoint from X_u, implying that $|X_h| \geqslant n - |X_u| \geqslant n/3$. Thus, $g_u \times h$ is a product polynomial. Since the circuit $F_{u=\mathbf{0}}$ has size at most $s-1$, the desired decomposition of F follows from the induction hypothesis. □

By the *characteristic function* of a multilinear polynomial $f(x_1,\ldots,x_n)$ we will mean the (unique) boolean function which accepts a binary vector $\alpha \in \{0,1\}^n$ if and only if the polynomial f contains the monomial $x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n} = \prod_{i\colon a_i=1} x_i$. (Note that this boolean function needs not to be monotone.) In particular, the characteristic function of our polynomial f_G is the quadratic boolean function

$$\phi(x) = \sum_{\{i,j\}\in E} x_i x_j \bmod 2\,.$$

That is, $\phi(a) = 1$ if the subgraph $G[S]$ induced by the set of nodes $S = \{i\colon a_i = 1\}$ has an odd number of edges. Since $\phi(x)$ is a non-zero polynomial of degree 2 over $GF(2)$, we have that $|f_G| = |\phi^{-1}(1)| \geqslant 2^{n-2}$.

Claim 27. For every graph G on n nodes, every product sub-polynomial of f_G contains at most $2^{n-m(G)}$ monomials.

Proof. Let $G \times H$ be a product polynomial contained in f_G. This polynomial gives a partition $x = (y,z)$ of the variables into two parts, each containing at least $n/3$ variables. Let $g(y)$ and $h(z)$ be the characteristic functions of G and H, and $r(x) = g(y) \wedge h(z)$. Then $|G \times H| = |r^{-1}(1)|$, and it is enough to show that $|r^{-1}(1)| \leqslant 2^{n-m(G)}$. When doing this, we will essentially use the fact that $r \leqslant \phi$, which follows from the fact that all monomials of $G \times H$ are also monomials of f_G.

By the definition of $m(G)$, some set $M = \{y_1z_1,\ldots,y_mz_m\}$ of $m = m(G)$ crossing edges y_iz_i forms an induced matching of G. Given an assignment α of constants 0 and 1 to the $n-2m$ variables outside the matching M, define vectors $a, b \in \{0,1\}^m$ and a constant $c \in \{0,1\}$ as follows:

- $a_i = 1$ iff an odd number of neighbors of y_i get value 1 under α,
- $b_i = 1$ iff an odd number of neighbors of z_i get value 1 under α,
- $c = 1$ iff the number of edges whose both endpoints get value 1 under α is odd.

Then the subfunction ϕ_α of ϕ obtained after restriction α is

$$\begin{aligned}\phi_\alpha(y_1,\ldots,y_m,z_1,\ldots,z_m) &= \sum_{i=1}^m y_iz_i + \sum_{i=1}^m y_ia_i + \sum_{i=1}^m b_iz_i + c \mod 2\\ &= IP_m(y\oplus b, z\oplus a)\oplus IP_m(a,b)\oplus c\,,\end{aligned}$$

where $IP_n(y_1,\ldots,y_m,z_1,\ldots,z_m)=\sum_{i=1}^m y_iz_i \mod 2$ is the inner product function. Since a,b and c are *fixed*, the corresponding $2^m\times 2^m$ ±1 matrix H with entries $H[y,z]=(-1)^{\phi_\alpha(y,z)}$ is a Hadamard matrix (rows are orthogonal to each other). Lindsey's Lemma (see, e.g. [15, p. 479]) implies that no monochromatic submatrix of H can have more than 2^m 1-entries.

Now, the obtained subfunction $r_\alpha = g_\alpha(y_1,\ldots,y_m)\wedge h_\alpha(z_1,\ldots,z_m)$ of $r=g(y)\wedge h(z)$ also satisfies $r_\alpha(a,b)\leqslant \phi_\alpha(a,b)$ for all $a,b\in\{0,1\}^m$. Since the set of all pairs (a,b) for which $r_\alpha(a,b)=1$ forms a *submatrix* of H, this implies that r_α can accept at most 2^m such pairs. Since this holds for each of the 2^{n-2m} assignments α, the desired upper bound $|r^{-1}(1)|\leqslant 2^m\cdot 2^{n-2m}=2^{n-m}$ follows.

This completes the proof of Claim 27, and hence, the proof of Lemma 23. □

13 Bounds for (k,l)-free Polynomials

A polynomial f is (k,l)*-free* if f does not contain a product of two polynomials, one with $>k$ monomials and the other with $>l$ monomials; (k,k)-free polynomials are called just k*-free.* In particular, every union-free polynomial (see Sect. 9) is 1-free. An (a,b)*-rectangle* is a product $A\times B$ of two polynomials such that $|A|\leqslant a$ and $|B|\leqslant b$; hence, $|A\times B|\leqslant ab$. Note that if $A\times B\subseteq f$, and if f is k-free, then we only know that $\min\{|A|,|B|\}\leqslant k$: the total number $|A\times B|$ of monomials in the rectangle $A\times B$ may be arbitrarily large.

Theorem 28. *Let* F *be a circuit over some semiring. If the produced polynomial* F *is* (k,l)*-free for some* $1\leqslant k\leqslant l$*, then* F *can be written as a sum of at most* $2|\mathsf{F}|$ (k,l^2)*-rectangles. In particular,*

$$|\mathsf{F}|\geqslant \frac{|F|}{2kl^2}\,.$$

Proof. Our argument is a mix of ideas of Gashkov and Sergeev [9], and Pippenger [28]. Since F is (k,l)-free, every product gate $u=v\times w$ in F must have an input, say w, at which a "small" set $A=|\mathrm{pol}(w)|$ of $|A|\leqslant l$ monomials is produced. We thus can remove the edge (w,u) and replace u by a unary (fanin-1) gate $u=v\times A$ of scalar multiplication by this fixed (small) polynomial A. If both inputs produce small polynomials, then we eliminate only one of them. What we achieve by doing this is that input gates remain the same as in the original circuit (variables $x_1,\ldots,x_n$ and constants $\mathbf{0},\mathbf{1}$), each product gate has fanin 1, and for every edge (u,v) in the resulting circuit F', we have an upper bound

$$|\mathrm{ext}_u(v)|\leqslant l\cdot|\mathrm{ext}(v)|\,. \tag{2}$$

Say that an edge (u,v) in F' is *legal* if both $|\mathrm{pol}(u)|\leqslant k$ and $|\mathrm{ext}_u(v)|\leqslant l^2$ hold. Let E be the set of all legal edges. By Lemma 16, it remains to show that E forms an edge-cut of F'.

To show this, take an arbitrary input-output path P in F', and let $e=(u,v)$ be the last gate of P with $|\mathrm{pol}(u)|\leqslant k$. If v is the output gate, then $\mathrm{ext}(v)$ is a trivial polynomial $\mathbf{1}$, and

Bound	Conditions	Ref.
$\mathbf{B}(f) > t$	f is not t-simple (Def. 2)	Thm. 5
$\mathbf{S}(f) = \mathbf{S}[f]$	f is homogeneous	Thm. 6
$\mathbf{S}[f] \geqslant \|f\|$	f is union-free (Def. 3)	Thm. 12
$\mathbf{S}(f) \geqslant \dfrac{\|f\|}{\mu_r(f) \cdot \mu_{m-r}(f)}$	f homogeneous of degree m	Thm. 17
$\mathbf{S}[f] \geqslant \dfrac{\|f\|}{2kl^2}$	$A \times B \subseteq f$ implies $\|A\| \leqslant l$ or $\|B\| \leqslant k$	Thm. 28

Table 2: A summary of general lower bounds. Here $\mathbf{S}$ is an arbitrary tropical semiring, $\mu_r(f)$ is the maximum possible number of monomials of f containing a fixed monomial of degree r, and r is some integer $m/3 < r \leqslant 2m/3$.

hence, $|\mathrm{ext}_u(v)| \leqslant l$ by (2), meaning that (u, v) is a legal edge. Suppose now that v is not the output gate. Then $|\mathrm{pol}(u)| \leqslant k$ but $|\mathrm{pol}(v)| > k$. Held also $|\mathrm{ext}_u(v)| > l^2$, then (2) would imply that $|\mathrm{ext}(v)| \geqslant |\mathrm{ext}_u(v)|/l > l$. Together with $|\mathrm{pol}(v)| > k$ and $\mathrm{pol}(v) \times \mathrm{ext}(v) \subseteq F$, this would contradict the (k, l)-freeness of F. Thus, $|\mathrm{pol}(u)| \leqslant k$ and $|\mathrm{ext}_u(v)| \leqslant l^2$, meaning that (u, v) is a legal edge. □

Together with Theorem 6, Theorem 28 yields the following lower bound over tropical semirings for polynomials, whose only lower or higher envelopes are (k, l)-free.

Corollary 29. *Let f and g be polynomials such that f_{le} and g_{he} are (k, l)-free for some $1 \leqslant k \leqslant l$. Then*

$$\mathbf{Min}(f) \geqslant \frac{|f_{\mathrm{le}}|}{2kl^2} \quad \textit{and} \quad \mathbf{Max}(g) \geqslant \frac{|g_{\mathrm{he}}|}{2kl^2} .$$

Remark 7. By a deeper analysis of circuit structure, Gashkov and Sergeev [8, 9] were able to even estimate the numbers of sum and product gates: every monotone arithmetic circuit computing a (k, l)-free polynomial f of n variables must have at least $|f|/K - 1$ sum gates, and at least $2\sqrt{|f|/K} - n - 2$ product gates, where $K = \max\{k^3, l^2\}$.

Remark 8. Every boolean $n \times n$ matrix $A = (a_{ij})$ defines a bi-linear polynomial $f_A(x, y) = \sum_{i,j} a_{ij} x_i y_j$ on $2n$ variables, as well as a set $Ax = (f_1, \ldots, f_n)$ of n linear polynomials $f_i = \sum_j a_{ij} x_j$. Call a boolean matrix A (k, l)-*free*, if it does not contain any $(k + 1, l + 1)$ all-1 submatrix. It is clear that the polynomial f_A is (k, l)-free if and only if the matrix A is (k, l)-free.

The results of Mehlhorn [23] and Pippenger [28] imply that, if A is k-free, then $\mathbf{B}(Ax) \geqslant |A|/4k^3$, where $|A|$ is the number of 1-entries in A. This, however, does not immediately imply a similar lower bound on $\mathbf{B}(f_A)$ for the single-output version f_A and, in fact, no such bound is known so far. On the other hand, Theorem 28 gives such a bound at least for tropical circuits: $\mathbf{Min}(f_A) = \mathbf{Max}(f) = \mathbf{A}(f_A) \geqslant |A|/2k^3$, where the equalities follow from Theorem 6, because the polynomial f_A is homogeneous.

14 Conclusion and Open Problems

In this paper we summarized known and presented some new lower-bound arguments for tropical circuits, and hence, for the dynamic programming paradigm; Table 2 gives a short overview. We have also shown these bounds already yield strong (even exponential) lower bounds for a full row of important polynomials (see Table 1). Still, the known arguments seem to fail for non-homogeneous polynomials like CONN or STCON.

Open Problem 1. *Does* $\mathbf{B}(f) = \Omega(n^3)$ *or at least* $\mathbf{Min}(f) = \Omega(n^3)$ *hold for* $f = \mathrm{STCON}_n$ *and/or* $f = \mathrm{CONN}_n$*?*

Note that the lower bound $\Omega(n^3)$ for the all-pairs-shortest-paths polynomial APSP_n, given in Theorem 13 does not automatically imply the same lower bounds for CONN: a circuit for CONN needs *not* to compute the polynomials of APSP on *separate* gates.

One could show $\mathbf{Min}(\mathrm{CONN}) = \Omega(n^3)$ by showing that monotone arithmetic circuits for the following "multiplicative version" of the triangle polynomial TR_n require $\Omega(n^3)$ gates. Recall that $\mathrm{TR}_n(x, y, z) = \sum_{i,j\in[n]} z_{ij} f_{ij}$, where $f_{ij} = \sum_{k\in[n]} x_{ik}y_{kj}$. We already know (see the proof of Theorem 13) that $\mathbf{A}(\mathrm{TR}_n) = \Theta(n^3)$, and hence also $\mathbf{Min}(\mathrm{TR}_n) = \Theta(n^3)$ since the polynomial is homogeneous. Replace now the outer sum by product, and consider the polynomial $\mathrm{TR}^*_n = \prod_{i,j\in[n]} z_{ij} f_{ij}$.

Open Problem 2. *Does* $\mathbf{A}(\mathrm{TR}^*_n) = \Omega(n^3)$*?*

If true, this would yield $\mathbf{Min}(\mathrm{CONN}_n) = \Omega(n^3)$, because the polynomial TR^*_n is homogeneous (of degree $m = 3n^2$).

In Section 8, we mentioned an exponential gap $\mathbf{Max}(f)/\mathbf{Min}(f) = 2^{\Omega(n)}$ achieved on $f = \mathrm{STCON}_n$.

Open Problem 3. *Can the gap* $\mathbf{Min}(f)/\mathbf{Max}(f)$ *also be super-polynomial for some* f*?*

Acknowledgements

I am thankful to Georg Schnitger 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.

[2] N. Alon and Fan R.K. Chung. Explicit constructions of linear sized tolerant networks. *Discrete Math.*, 72:15–19, 1989.

[3] A.E. Andreev. On a method for obtaining lower bounds for the complexity of individual monotone functions. *Soviet Math. Dokl.*, 31(3):530–534, 1985.

[4] A.E. Andreev. A method for obtaining efficient lower bounds for monotone complexity. *Algebra and Logics*, 26(1):1–18, 1987.

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

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

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

[8] 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.

[9] 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.

[10] M. Goldmann and J. Hastad. Monotone circuits for connectivity have depth log n to the power (2-o(1)). *SIAM J. Comput.*, 27:1283–1294, 1998.

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

[12] J.W. Jordan and R. Livné. Ramanujan local systems on graphs. *Topology*, 36(5):1007–1–24, 1997.

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

[14] S. Jukna. Expanders and time-restricted branching programs. *Theoret. Comput. Sci.*, 409(3):471–476, 2008.

[15] S. Jukna. *Boolean Function Complexity: Advances and Frontiers.* Springer-Verlag, 2012.

[16] M. Karchmer and A. Wigderson. Monotone circuits for connectivity require super-logarithmic depth. *SIAM J. Discrete Math.*, 3:255–265, 1990.

[17] O.M. Kasim-Zade. On arithmetical complexity of monotone polynomials. In *Proc. of All-Union Conf. on Theoretical Problems in Kybernetics*, volume 1, pages 68–69, 1986. (in Russian).

[18] O.M. Kasim-Zade. On the complexity of monotone polynomials. In *Proc. of All-Union Seminar on Discrete Math. and its Appl.*, pages 136–138, 1986. (in Russian).

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

[20] S.E. Kuznetsov. Monotone computations of polynomials and schemes without null-chains. In *Proc. of 8-th All-Union Conf. on Theoretical Problems in Cybernetics*, volume 1, pages 108–109, 1985. (in Russian).

[21] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[22] G.A. Margulis. Explicit constructions of concentrators. *Problems of Inf. Transm.*, pages 323–332, 1975.

[23] K. Mehlhorn. Some remarks on Boolean sums. *Acta Informatica*, 12:371–375, 1979.

[24] K. Mehlhorn and Z. Galil. Monotone switching circuits and boolean matrix product. *Computing*, 16(1-2):99–111, 1976.

[25] E.F. Moore. The shortest path through a maze. In *Proc. Internat. Sympos. Switching Theory*, volume II, pages 285–292. Harvard Univ. Press 1959, 1957.

[26] M. Morgenstern. Existence and explicit constructions of $q+1$ regular ramanujan graphs for every prime power q. *J. Comb. Theory Ser. B*, 62(1):44–62, 1994.

[27] M. Paterson. Complexity of monotone networks for boolean matrix product. *Theor. Comput. Sci.*, 1(1):13–20, 1975.

[28] N. Pippenger. On another Boolean matrix. *Theor. Comput. Sci.*, 11:49–56, 1980.

[29] 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.

[30] A.A. Razborov. A lower bound on the monotone network complexity of the logical permanent. *Math. Notes Acad. of Sci. USSR*, 37(6):485–493, 1985.

[31] A.A. Razborov. Lower bounds for the monotone complexity of some boolean functions. *Soviet Math. Dokl.*, 31:354–357, 1985.

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

[33] A. Shpilka and A. Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends in Theoret. Comput. Sci.*, 5(3-4):207–388, 2009.

[34] V Strassen. Vermeidung von divisionen. *The Journal für die Reine und Angewandte Mathematik*, 264:182–202, 1973.

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

[36] A.C. Yao. A lower bound for the monotone depth of connectivity. In *35th Ann. Symp. on Foundations of Computer Science*, 1994.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de