Tropical Proof Systems: Between R(CP) and Resolution

Yaroslav Alekseev
Technion – Israel Institute of Technology, Haifa, Israel

Dima Grigoriev
CNRS, Mathématique, Université de Lille, Villeneuve d'Ascq, 59655, France

Edward A. Hirsch
Department of Computer Science, Ariel University, Israel

Abstract

Propositional proof complexity deals with the lengths of polynomial-time verifiable proofs for Boolean tautologies. An abundance of proof systems is known, including algebraic and semialgebraic systems, which work with polynomial equations and inequalities, respectively. The most basic algebraic proof system is based on Hilbert's Nullstellensatz [7]. Tropical ("min-plus") arithmetic has many applications in various areas of mathematics. The operations are the real addition (as the tropical multiplication) and the minimum (as the tropical addition). Recently, [8, 17, 21] demonstrated a version of Nullstellensatz in the tropical setting.

In this paper we introduce (semi)algebraic proof systems that use min-plus arithmetic. For the dual-variable encoding of Boolean variables (two tropical variables x and $\overline{x}$ per one Boolean variable x) and $\{0,1\}$-encoding of the truth values, we prove that a *static* (Nullstellensatz-based) tropical proof system polynomially simulates *daglike* resolution and also has short proofs for the propositional pigeon-hole principle. Its dynamic version strengthened by an additional derivation rule (a tropical analogue of resolution by linear inequality) is equivalent to the system `Res(LP)` (aka `R(LP)`), which derives nonnegative linear combinations of linear inequalities; this latter system is known to polynomially simulate Krajíček's `Res(CP)` (aka `R(CP)`) with unary coefficients. Therefore, tropical proof systems give a finer hierarchy of proof systems below `Res(LP)` for which we still do not have exponential lower bounds. While the "driving force" in `Res(LP)` is resolution by linear inequalities, dynamic tropical systems are driven solely by the transitivity of the order, and static tropical proof systems are based on reasoning about differences between the input linear functions. For the truth values encoded by $\{0,\infty\}$, dynamic tropical proofs are equivalent to `Res(`∞`)`, which is a small-depth Frege system called also DNF resolution.

Finally, we provide a lower bound on the size of derivations of a much simplified tropical version of the Binary Value Principle in a static tropical proof system. Also, we establish the non-deducibility of the tropical resolution rule in this system and discuss axioms for Boolean logic that do not use dual variables. In this extended abstract, full proofs are omitted.

2012 ACM Subject Classification Theory of computation → Proof complexity

Keywords and phrases Cutting Planes, Nullstellensatz refutations, Res(CP), semi-algebraic proofs, tropical proof systems, tropical semiring

Digital Object Identifier 10.4230/LIPIcs.STACS.2025.8

Related Version *Full Version*: `https://eccc.weizmann.ac.il/report/2024/072/` [3]

Funding *Edward A. Hirsch*: This research was conducted with the support of the State of Israel, the Ministry of Immigrant Absorption, and the Center for the Absorption of Scientists.

Acknowledgements The authors are very grateful to Dmitry Itsykson and Dmitry Sokolov for fruitful discussions, and to Marc Vinyals for his inspiring Proof Complexity Zoo project and for pointing to the recent work of Gläser and Pfetsch.

42nd International Symposium on Theoretical Aspects of Computer Science (STACS 2025).
Editors: Olaf Beyersdorff, Michał Pilipczuk, Elaine Pimentel, and Nguyễn Kim Thắng;
Article No. 8; pp. 8:1–8:20

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction and Organization of this Extended Abstract

This paper introduces tropical proof systems, that is, proof systems that use min-plus arithmetic. To the best of our knowledge, these are the first tropical proof systems described in the literature though one of them is equivalent to a known proof system `Res(LP)` [19], which is a weakened version of `Res(CP)` (`R(CP)`) [23], these systems are working with disjunctions of inequalities. Thus our proof systems not only introduce a new paradigm, but also give a scale of proof systems between `Res(CP)` and resolution (this scale is visualised in Fig. 1).

In this extended abstract, we briefly recall the standard setup for propositional proof complexity and survey previous results concerning relevant proof systems (Sect. 2), recall tropical arithmetic (Sect. 3) and introduce tropical proof systems (Sect. 4), survey our results (Sect. 6), and discuss further directions (Sect. 7). Preliminary versions of full proofs can be found in the preprint [3].

2 General setup

2.1 Propositional proof complexity

A proof system for language L is[1] a deterministic polynomial-time algorithm V such that for every $x \in L$, there is a *proof* $\pi \in \{0,1\}^*$ such that $V(x,\pi) = 1$, and for every $x \notin L$ and every candidate proof π, it holds that $V(x,\pi) = 0$. In this paper, we are interested in proofs for the language **UNSAT** of unsatisfiable Boolean formulas in conjunctive normal form (CNF) and, more broadly, in proofs for the language of unsolvable systems of linear equations (and even their disjunctions) with rational coefficients. Frequently (but not always) a proof of the unsatisfiability of a formula derives semantically implied statements from previously derived (or input) statements (in the case of a formula in CNF, the input statements are Boolean clauses). The existence of a proof system that has a polynomial-size proof for every $x \in L$ is equivalent to $\mathbf{NP} = \mathbf{co\text{-}NP}$, this equivalence of the classes is unlikely and proving or disproving it is far beyond the reach of the current methods.

Propositional proof complexity is a rapidly developing area where we typically prove four kinds of results:

- A superpolynomial lower bound on the size of the shortest proof for a certain (infinite) set of inputs $x_1, x_2 \ldots \in L$ in some specific proof system.
- A polynomial *simulation* between two proof systems, that is, for every $x \in L$, one proof system has a proof of x that has the same or a smaller length (up to a polynomial factor) than the shortest proof of x in the other proof system.
- A polynomial upper bound on the proof size for a certain (infinite) set of inputs $x_1, x_2 \ldots \in L$ in a specific proof system.
- A superpolynomial *separation* between proof systems, which is typically obtained by providing a set of inputs for which we can prove a polynomial size upper bound in one proof system and a superpolynomial size lower bound in another proof system.

When we have both a polynomial simulation and a superpolynomial separation between two specific systems, we say that one system is strictly stronger than the other one. Thus proof systems (for the same language) form a lattice[2] with respect to the partial non-strict order composed of the simulations; if one system is strictly stronger than the other one, then the

[1] This definition deviates from Cook and Reckhow's definition [11], but for our purpose they are equivalent.
[2] Note that we do not require the simulations to be computable in polynomial time (p-simulations) though in most cases the simulations are indeed efficient.

order is strict for these two systems. *Cook's (or Cook–Reckhow's) program* in the propositional proof complexity is the intention for proving superpolynomial lower bounds for stronger and stronger proof systems, thus developing new methods for proving superpolynomial lower bounds, which are the crux of computational complexity.

2.2 Previous proof complexity results relevant to this paper

The area essentially started with superpolynomial (and then exponential) lower bounds for various versions of the resolution proof system [31, 18, 32], where proofs proceed by deriving the resolvent $C \vee D$ of two already derived (or input) clauses $C \vee x$ and $D \vee \overline{x}$ until we derive the empty clause. We refer the reader to Krajíček's book [25] for a detailed overview of the area.

The previously known proof systems that are the most relevant to us are proof systems that work with linear inequalities.

The Cutting Plane (`CP`) proof system [12] uses the rounding rule and nonnegative linear combinations of inequalities

$$\frac{\sum_i ca_ix_i - d \geqslant 0}{\sum_i a_ix_i - \lceil d/c \rceil \geqslant 0}\ (c, a_i, d \in \mathbb{Z}), \qquad \frac{f_1 \geqslant 0 \qquad f_2 \geqslant 0}{\alpha_1 f_1 + \alpha_2 f_2 \geqslant 0}\ (\alpha_1, \alpha_2 > 0)$$

as its derivation steps (here f_1 and f_2 are the affine forms). The derivation starts from linear inequalities expressing Boolean clauses and from the axioms $x_i \geqslant 0$, $1 - x_i \geqslant 0$ for every variable x_i. It finishes with deriving the contradictory inequality $-1 \geqslant 0$. An exponential lower bound for `CP` was proved in [29].

Krajíček [23] generalized `CP` to a new system `R(CP)`, also called `Res(CP)`, by allowing to reason about disjunctions of *affine* inequalities (the disjunctions are interpreted as sets, trivially false constant inequalities are dropped out, and a disjunction can be weakened by adding new inequalities to it). The two rules above are generalized to

$$\frac{\sum_i ca_ix_i - d \geqslant 0 \vee \Gamma}{\sum_i a_ix_i - \lceil d/c \rceil \geqslant 0 \vee \Gamma}\ (c, a_i, d \in \mathbb{Z}), \quad \frac{(f_1 \geqslant 0) \vee \Gamma \qquad (f_2 \geqslant 0) \vee \Gamma}{(\alpha_1 f_1 + \alpha_2 f_2 \geqslant 0) \vee \Gamma}\ (\alpha_1, \alpha_2 > 0). \ (\texttt{+RES})$$

Also the notion of the negation of an inequality is introduced through the rule

$$\frac{\emptyset}{f - 1 \geqslant 0 \vee -f \geqslant 0}.$$

The same idea has been used to define other proof systems (for example, `Res(`k`)` [24], `Res(Lin)` [30], `Res(`$\oplus$`)` [20]). In particular, Hirsch and Kojevnikov stripped `Res(CP)` of the negation and the rounding rule and defined the system `Res(LP)` that uses the splitting rule

$$\frac{\emptyset}{(x - 1 \geqslant 0)\ \vee\ (-x \geqslant 0)}\ (x \text{ is a variable}).$$

No superpolynomial size lower bounds for `Res(CP)` or `Res(LP)` are known. Derivations can be daglike (as usual) or treelike (where we have to re-derive a statement again every time we use it). Beame et al. defined the Stabbing Planes proof system [6] that is equivalent to `treelike Res(CP)`. While usually the coefficients of linear inequalities are written in *binary*, one can consider weaker proof systems when they are written in *unary*. In the unary coefficients setting, Fleming et al. have shown a quasipolynomial simulation of Stabbing Planes in `CP` (with binary coefficients) thus obtaining an exponential lower bound for it [14]. Very recently, Gläser and Pfetsch have shown an exponential bound for Stabbing Planes for the case of binary coefficients by providing a quasipolynomial monotone interpolation [15]. The daglike versions of `Res(CP)` and `Res(LP)` with unary coefficients are polynomially equivalent [19] and no superpolynomial lower bounds are known for them to the date.

3 Tropical arithmetic

Tropical (or min-plus) arithmetic involves operations $\min, +$ in place of $+, \times$ in classical arithmetic; we refer the interested reader to [27] for the introduction and survey of tropical arithmetic and in particular its history and the origin of the name "tropical". Tropical arithmetic has several sources including algebraic geometry (valuations), mathematical physics, and optimization, and, respectively, numerous applications (some of them can be found in [27], also neural networks are a more recent application).

We consider a tropical semifield based on $\mathbb{Q} \cup \{+\infty\}$. Many of the results of this paper can be also formulated and proved using a similar semifield based on $\mathbb{Q}$.

Tropical operations. We consider the min-plus (or tropical) semifield defined by the set $\mathbb{Q}_\infty = \mathbb{Q} \cup \{+\infty\}$ endowed with two operations: the tropical addition $\oplus$ and the tropical multiplication $\odot$ defined in the following way:

$$a \oplus b = \min\{a, b\}, \quad a \odot b = a + b,$$

where min and $+$ are the usual (traditional) arithmetic operations extended to work with the neutral element ∞: namely, $a \oplus \infty = a$ and $a \odot \infty = \infty$. A tropical *power* n of a is defined as

$$a^{\odot 0} = 0, \qquad a^{\odot n} = \underbrace{a \odot \ldots \odot a}_{n \text{ copies}},$$

where n is a positive integer. Sometimes we use a bigger $\bigoplus$ to facilitate reading.

Tropical polynomials.

▶ **Definition 1.** *A* tropical monomial *is a tropical product of tropical powers of variables. For a vector of variables $\vec{x} = (x_1, \ldots, x_n)$ and a vector of integers $I = (i_1, \ldots, i_n)$ we introduce the notation*

$$\vec{x}^I = x_1^{\odot i_1} \odot \cdots \odot x_n^{\odot i_n}.$$

Then $\mathbf{degtr}(x^I) = i_1 + \ldots + i_n$ *is called the (total) (tropical)* degree *of this monomial.*

Note that we never use the word "monomial" for a submonomial, that is, a subset of monomial (in other words, the monomial $x \odot y$ does *not* occur in $x \odot y^{\odot 2} \oplus x \odot y \odot z$).

In this paper, a (tropical, or min-plus) *term* $t = c \odot m$ is a tropical product of a tropical monomial m and a constant $c \in \mathbb{Q}_\infty$. One can treat a tropical term classically as a linear function $a + i_1 x_1 + \ldots + i_n x_n$. By analogy with the traditional arithmetic (and its zero), a constant term is the only situation where the coefficient $c = \infty$ is meaningful (since $\infty \odot m = \infty$). We assume that if a term is non-constant, it has a finite coefficient. This is important when we say "monomial m *occurs*" somewhere: we mean that a term based on m occurs. The degree of a term is the degree of its monomial.

Note that when we work with constants, we use traditional operations and treat the constant as a whole, for example, $x \odot (10 - 2 + 1)$ is the same as $x \odot 9$.

▶ **Definition 2.** *Let $x_1, \ldots, x_n$ be variables, and let $\mathcal{I}$ be a finite set of their power vectors ($\mathcal{I} \subseteq \mathbb{N}_0^n$). A* tropical polynomial *is an element of $(\mathbb{Q}_\infty, \oplus, \odot)[x_1, \ldots, x_n]$, that is, the tropical sum of a set of tropical terms $t_I(\vec{x}) = c_I \odot \vec{x}^I$ with distinct power vectors $I \in \mathcal{I}$:*

$$f(\vec{x}) = \bigoplus_{I \in \mathcal{I}} t_I(\vec{x}).$$

If $\mathcal{I} = \emptyset$, we identify this polynomial with the constant polynomial ∞.

In other words, tropical polynomials are members of the $(\mathbb{Q}_\infty, \oplus, \odot)$-linear space spanned by the monomials (for example, $1 \oplus x^{\odot 2} \odot y \oplus 2 \odot x$ and ∞ are tropical polynomials). One can treat f as a concave piecewise linear function.

Tropical addition and multiplication are correctly defined on tropical polynomials as $\infty \odot m = \infty$ and $a \odot m \oplus b \odot m = \min\{a, b\} \odot m$ for any monomial m, and thus we never need more than one term per monomial.

Complexity of tropical polynomials. We usually write the coefficients and the exponents in binary, so the bit-size of x^{2^n} is polynomial (which is important when we estimate the size of a proof that uses tropical polynomials). The degree of a tropical polynomial f, denoted by $\mathbf{degtr}(f)$, is the maximal degree of its terms. Let $\boldsymbol{\mu}(f)$ be the number of terms in f (it is strictly positive).

Min-plus polynomials and inequalities. A *min-plus polynomial* is a pair of tropical polynomials $(f(\vec{x}), g(\vec{x}))$. The degree of a min-plus polynomial is the maximum of the degrees of f and g. A point $\vec{a} \in \mathcal{R}^n$ is a root of this polynomial if the following equality holds: $f(\vec{a}) = g(\vec{a})$. We can apply tropical operations component-wise to min-plus polynomials, thus min-plus polynomials can be summed using the tropical addition $\oplus$ and can be tropically multiplied by a tropical monomial using tropical multiplication $\odot$, and these operations preserve the common roots of the involved polynomials. Thus, the closure of a set of min-plus polynomials under these operations is a (tropical) ideal. One of the central issues in tropical algebra is a criterion for the existence of common roots for systems of min-plus polynomials $\{(f_1, g_1), \ldots, (f_k, g_k)\}$. In classical algebra such a criterion is provided by Hilbert's Nullstellensatz (over an algebraically closed field). In tropical algebra a criterion of solvability has been formulated as a Min-Plus Nullstellensatz [8, 17, 21, 26], further extended in [1].

In this paper we will deal with a more convenient (albeit equivalent) framework of the problem of the existence of common roots for systems of min-plus polynomial inequalities $\{f_1 \leqslant g_1, \ldots, f_k \leqslant g_k\}$. A *min-plus polynomial inequality* is a pair of tropical polynomials f, g that we write as $f \leqslant g$ or (f, g). A point $\vec{a} \in \mathcal{R}^n$ is a root of min-plus inequality $f \leqslant g$ if $f(\vec{a}) \leqslant g(\vec{a})$. Note that $\vec{a}$ is a root of $f \leqslant g$ iff it is a root of $(f \oplus g, f)$. In what follows, we abuse the notation by writing $f = g$ instead of the two inequalities $f \leqslant g$ and $g \leqslant f$.

Note that while one can consider solving min-plus equations and inequalities over $\mathbb{Q}$ or over $\mathbb{Q}_\infty$, tropical polynomials will always have coefficients in $\mathbb{Q}_\infty$, in particular, ∞ is a tropical polynomial equivalent to "the empty tropical polynomial".

An order on tropical polynomials. For tropical polynomials L and R, let $L \succeq R$ denote the component-wise $\geqslant$ of the coefficients of the respective monomials in L and R.

Let $L \succ R$ denote the component-wise $>$ of the coefficients of the respective monomials in L and R, *where R may also contain extra monomials not present in L.*

Note that if $L \succ R$, then it is impossible for $R \leqslant L$ to have finite roots.

We define $\preceq$ and $\prec$ similarly. The following lemma is easy to see.

▶ **Lemma 3** ($\succ$ inside $\oplus, \odot$). *Let $\Gamma, \Delta, \Gamma', \Delta'$ be tropical polynomials.*

1. *If $\Gamma \succ \Delta$ and $\Gamma' \succ \Delta'$, then $\Gamma \oplus \Gamma' \succ \Delta \oplus \Delta'$.*
2. *For a tropical term $t \neq \infty$, if $\Gamma \succ \Delta$, then $\Gamma \odot t \succ \Delta \odot t$.*

4 Tropical proof systems

Similarly to the already classical "algebraic" proof systems Nullstellensatz and Polynomial Calculus [7, 10] based on Hilbert's Nullstellensatz, we introduce proof systems that rely on the Min-Plus Nullstellensatz. The most general static proof system MP-NS (Min-Plus Nullstellensatz, Definition 7) for the language of unsolvable linear inequalities requires a proof that is a contradictory algebraic combination of the input inequalities and trivial axioms $0 \leqslant 0$, $f \leqslant \infty$. That is, for a system of min-plus inequalities $f_i \leqslant g_i$, the proof is a contradictory inequality $\bigoplus_{j=1}^{K} p_j \leqslant \bigoplus_{j=1}^{K} q_j$ for some $K \geqslant 1$, where for each $1 \leqslant j \leqslant K$ we have $(p_j, q_j) = (t_j \odot f_{i_j}, t_j \odot g_{i_j})$ for some term t_j and some $1 \leqslant i_j \leqslant k$. The contradiction must follow immediately from the coefficients of the inequality; namely, for every monomial present in the left-hand side, its coefficient must be strictly greater than the coefficient of the same monomial in the right-hand side (also, for technical reasons the right-hand side must have a finite constant term).

For example, the system of inequalities $\{x \leqslant y, \quad y \leqslant z, \quad z+1 \leqslant x, \quad 2x \leqslant 0\}$, which is written tropically as $\{x \leqslant y, \quad y \leqslant z, \quad z \odot 1 \leqslant x, \quad x^{\odot 2} \leqslant 0\}$, can be refuted by tropically multiplying its inequalities by $x \odot \frac{1}{3}$, $x \odot \frac{2}{3}$, x, and $\frac{1}{3}$, respectively. This results in

$$\underline{x^{\odot 2} \odot \frac{1}{3}} \oplus \underline{\underline{y \odot x \odot \frac{2}{3}}} \oplus \underline{\underline{z \odot x \odot 1}} \quad \leqslant \quad \underline{\underline{y \odot x \odot \frac{1}{3}}} \oplus \underline{\underline{z \odot x \odot \frac{2}{3}}} \oplus \underline{x^{\odot 2} \odot 0} \oplus \frac{1}{3}.$$

One can see that the requirement on the coefficients is satisfied.

Similarly to algebraic proof systems, we introduce a dynamic version of MP-NS: Min-Plus Polynomial Calculus (MP-PC), see Definition 11. It derives the contradiction of the same sort step by step by tropically adding inequalities, tropically multiplying them by terms, and substituting inequalities into other inequalities.

We also consider the additional *tropical resolution* rule

$$\frac{t \oplus f \leqslant 0 \qquad t' \oplus f \leqslant 0}{(t \odot t') \oplus f \leqslant 0}, \text{ where } t, t' \text{ are terms,} \tag{$\odot$RES}$$

which is a counterpart of (+RES) in Res(LP) and Res(CP). When we add this rule to our systems, we mention this explicitly. While this rule is not needed for the completeness of our tropical proof systems, on the one hand, and is looking very natural, on the other hand, its elimination from the system may be expensive, as shown in Theorem 27.

The proof systems MP-NS and MP-PC can be transformed into proof systems for **UNSAT** using several possibilities to encode the truth values, Boolean variables and Boolean clauses. In the "default" setting, we encode the truth values by $\{0, 1\}$, introduce the dual variable $\overline{x}$ for every variable x, and transform a clause into the corresponding linear inequality (which, in tropical terms, is $1 \leqslant m$ for a multilinear monomial m). These proof systems are called MP-NSR and MP-PCR; the diagram of connections between them and known systems is given in Figure 1. One can also considered different encodings (without dual variables or with values in $\{0, \infty\}$), the detailed treatment of these is delayed to the full version of the paper.

4.1 The basic static proof system, MP-NS

▶ **Definition 4.** *Consider a system of min-plus polynomials $F = \{(f_1, g_1), \ldots, (f_k, g_k)\}$. An* algebraic combination *of F is a min-plus polynomial (f, g) that can be represented as*

$$(f, g) = \left(\bigoplus_{j=1}^{K} p_j, \bigoplus_{j=1}^{K} q_j \right), \tag{1}$$

for some $K \geqslant 1$, where for each $1 \leqslant j \leqslant K$ we have $(p_j, q_j) = (t_j \odot f_{i_j}, t_j \odot g_{i_j})$ for some term t_j and some $1 \leqslant i_j \leqslant k$. We will abuse the language by calling an "algebraic combination" both the min-plus polynomial (f, g) and the composition (1), that is, t_j's.

We call a system of min-plus polynomials *symmetric* if it always includes (f_i, g_i) together with (g_i, f_i). The possibility of refuting min-plus systems of equations (and inequalities) using min-plus proofs is based on the following theorem.

▶ **Theorem 5** (Min-Plus Nullstellensatz, [17, Theorem 3.8] over $\mathbb{Q}_\infty$ without the degree claim)**.** *Consider a symmetric system of min-plus polynomial equations F as in Def. 4 in n variables.*

The system F has no roots over the tropical semifield $\mathbb{Q}_\infty$ iff we can construct an algebraic min-plus combination

$$(f, g) = \left(\bigoplus_{j=1}^{K} p_j, \bigoplus_{j=1}^{K} q_j \right)$$

of F such that for each monomial m occurring in f, and also for the constant monomial even if it is infinite, its coefficient in f is greater than the coefficient of this monomial in g (in particular, m must be present in g).

It can be easily observed that one direction of the theorem is trivial: indeed, if there is an algebraic combination (f, g) satisfying the conditions of the theorem (recall also that in terms of integer operations, the "coefficient" is the additive constant in a standard arithmetic linear combination of variables), so the system F is unsatisfiable. The finite constant term in g saves us from the parasite all-∞ solution.

It is easy to see that in the case of systems of inequalities (which correspond to not necessarily symmetric systems of min-plus polynomials), a similar result holds as a corollary.

▶ **Theorem 6.** *Consider a system of min-plus polynomial inequalities S in n variables over $\mathbb{Q}_\infty$. Let $F = S \cup \{(0, 0)\} \cup \{(g_i, \infty) \mid (f_i, g_i) \in S\}$.*

The system S has no roots over the tropical semifield $\mathbb{Q}$ iff we can construct an algebraic min-plus combination

$$(f, g) = \left(\bigoplus_{j=1}^{K} p_j, \bigoplus_{j=1}^{K} q_j \right)$$

of F (in terms of Def. 4) such that for each monomial $m \neq \infty$ occurring in f, its coefficient is greater than the coefficient of this monomial in g (in particular, m must be present in g).

Over the semifield $\mathbb{Q}_\infty$ we need an additional property: the constant term in g is finite.

▶ **Definition 7** (Min-Plus Nullstellensatz, `MP-NS`)**.** *We will call a min-plus algebraic combination (that is, $(t_j)_{j=1}^K$ in terms Def. 4) satisfying the conditions of Theorem 6 (over $\mathbb{Q}_\infty$, unless otherwise stated) a* Min-Plus Nullstellensatz (`MP-NS`) *refutation of S.*

▶ Note 8 (The $0 \leqslant c$ "axiom")**.** In Theorem 6 we have added the axioms $0 \leqslant 0$ and $g \leqslant \infty$ to `MP-NS`. Note that, for any constant $c \geqslant 0$, the inequality $0 \leqslant c$ can be easily derived as a tropical sum of $0 \leqslant \infty$ and $0 \leqslant 0$ tropically multiplied by c. In what follows we will use it without further notice both for `MP-NS` and for our dynamic proof system described later.

In fact, the "last line" of the proof (that is, (f, g) in terms of the theorem, after combining similar terms) can be thought of as a refutation itself: the composition of this algebraic combination can be easily reconstructed, and its complexity parameters are bounded by a

polynomial in the complexity of (f, g). (In what follows, when we speak about the size of a rational number, we mean the size of its nominator plus the size of its denominator; for ∞ this is zero.)

▶ **Proposition 9** (MP-NS derivation reconstruction)**.** *Given a system of min-plus inequalities (f_i, g_i) and given their algebraic combination as two polynomials (f, g), we can find the terms t_j's of this algebraic combination in polynomial time, their number is bounded by a polynomial in the number of monomials in the system and (f, g), their coefficient size is bounded by a polynomial in the size of coefficients in the system and (f, g). and their degree does not exceed the degree of monomials in f and g.*

▶ Remark 10. Now we say a few words about the complexity of constructing an MP-NS refutation given a system of min-plus equations, or more generally, inequalities (including strict ones). First, one can estimate a bound on the degree of a refutation (algebraic combination) with the help of [17, Theorem 3.8] in the case of min-plus equations, which was extended to the case of min-plus inequalities in Theorem 3.1 [1]. For a given bound on the degree, an algebraic combination can be treated as a system of min-plus **strict linear** inequalities (whose unknowns are the rational coefficients of an algebraic combination). Solvability of a system of min-plus linear inequalities (including strict ones) is reduced in [5] (within polynomial complexity) to solvability of a system of min-plus linear equations (with integer coefficients and thereby, integer unknowns).

One can apply to a system of min-plus linear equations one of the algorithms to solve it (see e.g., [9, 2, 16]). The complexity of each of these algorithms is polynomial in the number of unknowns and equations and in the absolute values of integer coefficients of the system. Observe that this complexity bound is not polynomial in the size of the input because the complexity depends on the absolute values of the coefficients rather than on their bit-sizes. It is a longstanding open problem whether a system of min-plus linear equations is solvable within polynomial complexity. However, this problem belongs to the class $\mathbf{NP} \cap \mathbf{co\text{-}NP}$ (see e.g., [2, 16]).

4.2 The basic dynamic proof system, MP-PC

We also consider a dynamic version of MP-NS called the Min-Plus Polynomial Calculus (MP-PC). It has some informal resemblance to Krajíček's original quantifier-free propositional LK(CP) proof system [23]: it uses both sides of a "sequent" while Res(CP) used only one because of the presence of an efficient negation, which we are missing. However, the "sequents" of our system contain tropical terms (affine functions) and not inequalities.

We will sometimes use equations to abbreviate pairs of two opposite inequalities.

▶ **Definition 11** (Min-Plus Polynomial Calculus, MP-PC)**.** *Consider a system of min-plus polynomial inequalities $S = \{f_1 \leqslant g_1, \dots, f_m \leqslant g_m\}$ in n variables. A* Min-Plus PC (MP-PC) *refutation of F is a list of min-plus inequalities*

$$p_1 \leqslant q_1, \dots, p_K \leqslant q_K$$

such that

1. *In the last inequality, for each monomial $m = x_1^{\odot j_1} \odot \dots \odot x_n^{\odot j_n}$ in p_K there is a matching monomial in q_K, and the coefficient in the monomial in p_K is greater than the corresponding coefficient in q_K. Moreover, the constant term in q_K must be present and must be finite.*

▶ Note 12 ($0/1$ variables in $\mathbb{Q}_\infty$). Later on, in our systems dealing with $\{0,1\}$ variables, all monomials become bounded from the above and thus the requirement on the constant term can be satisfied automatically.

2. *Each inequality $p_i \leqslant q_i$ is obtained from the previously derived inequalities using the following rules.*

   Axioms*:*

   $$\frac{\emptyset}{f_j \leqslant g_j}, \quad \textit{where } 1 \leqslant j \leqslant m,$$

   $$\frac{\emptyset}{0 \leqslant 0},$$

   $$\frac{\emptyset}{p \leqslant \infty}, \ \textit{for any tropical polynomial } p. \qquad (\texttt{WEAK})$$

   Minimum. *We can take a minimum of two previously derived inequalities:*

   $$\frac{p \leqslant q \qquad p' \leqslant q'}{p \oplus p' \leqslant q \oplus q'}.$$

   Tropical multiplication*:*

   $$\frac{p \leqslant q}{p \odot t \leqslant q \odot t},$$

   where t is a term.

   Transitivity of the order*:*

   $$\frac{p \leqslant h \qquad h \leqslant r}{p \leqslant r}.$$

▶ Note 13 (Substitutions). It is easy to see that by combining transitivity with other rules we can substitute inequalities into each other on the left or on the right, for example,

$$\frac{p \oplus h \leqslant q \qquad r \leqslant h}{p \oplus r \leqslant q} \qquad \frac{p \leqslant q \oplus h \qquad h \leqslant r}{p \leqslant q \oplus r}.$$

and do it even inside monomials by multiplying the substitution by an appropriate term. In what follows, we refer to these derivations as **substitutions**.

▶ Note 14 (Tropical product). Note that we can take the tropical product ($\odot$) of two inequalities by first multiplying one of them by the left-hand-side of the other one and then applying the transitivity rule. We will discuss the complexity issues of constructing tropical products of inequalities later.

▶ Note 15 (Natural weakening). Note also that we can weaken inequalities by dropping a summand from the right-hand side or adding a summand to the left-hand side. This is simulated using the (WEAK) axiom with the minimum rule and substitution on the right.

▶ Note 16 (Systems based on equations instead of inequalities). Similarly to Theorem 5, it is possible to talk about symmetric systems and thus min-plus equations, even in the context of dynamic proof systems. For example, one could define a refutation system for symmetric systems with the same rules except for the axiom (WEAK), and with an additional rule to swap an equation ($f = g \longrightarrow g = f$). This apparently weaker proof system turns out to be polynomially equivalent to MP-PC for symmetric systems (see full version of this paper). As inequalities provide a more natural framework and allow to refute more unsolvable systems, we stick to using inequalities.

4.3 The tropical resolution rule

As usual, when we consider stronger systems that include additional rules, we denote them by "system+rule", for example, MP-PC+(⊙RES).

In what follows f denotes any tropical monomial.

The following rule can be viewed as the generalization of the resolution-like rule (+RES) in Res(CP)-like systems (though we limit it very much) or as tropical multiplication of two inequalities, each one being in the tropical sum.

$$\frac{t \oplus f \leqslant 0 \qquad t' \oplus f \leqslant 0}{(t \odot t') \oplus f \leqslant 0}, \text{ where } t, t' \text{ are terms.} \tag{⊙RES}$$

While this rule is looking very natural, we do not know how to eliminate its use at a polynomial cost. Moreover, we will show later that its direct simulation in the static proof systems is impossible.

4.4 Encoding of Boolean logic: MP-NSR and MP-PCR systems

In this extended abstract we concentrate on the following encoding. We use 0 for false and 1 for true and introduce a "dual variable" for the negation of each variable. Note that we use $\neg\Phi$ as the Boolean negation of a Boolean formula Φ (without distinguishing Φ from $\neg\neg\Phi$) while keeping the notation $\overline{x}$ for dual variables. Recall that we denote literals (which are variables or the negations of variables) by $\ell, \ell_1, \ell_2, \ldots$ without further notice.

We thus obtain from (the systems for refuting conjunctions of min-plus inequalities) MP-NS and MP-PC the propositional proof systems MP-NSR and MP-PCR, respectively. In order to do that we translate a formula in CNF into a conjunction of tropical inequalities. Namely, we translate each clause into an inequality and also add additional inequalities (axioms) to ensure that variables are Boolean.

Boolean axioms. We include the axioms

$$\frac{\emptyset}{x \odot \overline{x} = 1} \quad (01/\odot) \qquad\qquad \frac{\emptyset}{x \oplus \overline{x} = 0} \quad (01/\oplus)$$

to ensure that x and $\overline{x}$ are dual and in $\{0, 1\}$.

▶ Note 17. For any binary variable x we can derive from $(01/\oplus)$ in MP-PC that $0 \leqslant x$ and $x \leqslant 1$. The first inequality can be derived from $0 \leqslant x \oplus \overline{x}$ by simplification. The latter inequality can be derived in the following way: from $0 \leqslant \overline{x}$ we can derive $x \leqslant x \odot \overline{x}$, from which we can derive $x \leqslant 1$ using $x \odot \overline{x} \leqslant 1$.

Translations of Boolean clauses. We can encode a Boolean clause $\ell_1 \vee \ell_2 \vee \ldots \vee \ell_k$ using the equation

$$\overline{\ell}_1 \oplus \overline{\ell}_2 \oplus \cdots \oplus \overline{\ell}_k \leqslant 0. \tag{D}$$

Note that clauses are encoded in Res(Lin) [30] in exactly the same way (the absence of the dual variables does not matter as re-encoding is done by a simple linear substitution).

However, there is another possibility to encode a clause, which is used in CP and similar proof systems:

$$1 \leqslant \ell_1 \odot \ell_2 \odot \cdots \odot \ell_k. \tag{I}$$

It is not difficult to see that in the case of MP-PCR these encodings are equivalent. A formal proof of this statement can be found in the full version of the paper.

5 Preliminary lemmas and the equivalence of encodings

Before we come to the main results, we state several technical lemmas about derivations in tropical systems.

▶ **Lemma 18** (tropical product, treelike, no axioms). *For $1 \leqslant i \leqslant k$, let A_i, B_i be tropical terms. Then there is a* `treelike MP-PC` *derivation of all the inequalities*

$$\bigodot_{i=1}^{j} A_i \leqslant \bigodot_{i=1}^{j} B_i, \text{ for } j \leqslant k,$$

from the inequalities $A_i \leqslant B_i$ (each used once).

The derivation contains $O(k)$ (not necessarily different) terms and the bit-size of every coefficient (respectively, the tropical exponent) in the derivation is upper bounded by $O(k \cdot b)$, where b is the maximum bit-size of a coefficient (respectively, a tropical exponent) in any of the A_i, B_i. In particular, the coefficients (resp., tropical exponents) in the derivation are sums of the original coefficients (resp., tropical exponents).

Proof. Start with $A_1 \leqslant B_1$. Tropically multiply it by A_2 and tropically multiply $A_2 \leqslant B_2$ by B_1 to conclude $A_1 \odot A_2 \leqslant B_1 \odot B_2$ by transitivity.

Continue in the same way for $j = 3, \ldots, k$, multiplying $A_j \leqslant B_j$ by $\bigodot_{i=1}^{j-1} A_i$, multiplying the previously derived $\bigodot_{i=1}^{j-1} A_i \leqslant \bigodot_{i=1}^{j-1} B_i$ by B_j, and applying the transitivity rule. ◀

▶ **Lemma 19** (powers of axioms, treelike). *For a variable x and an integer $b > 0$, there are* `treelike MP-PCR` *derivations from the axioms of the following inequalities:*

$$x^{\odot b} \odot \overline{x}^{\odot b} \leqslant b, \tag{2}$$

$$b \leqslant x^{\odot b} \odot \overline{x}^{\odot b}, \tag{3}$$

$$x^{\odot b} \oplus \overline{x}^{\odot i} \leqslant 0 \text{ (as well as of the symmetrical inequality), for } 1 \leqslant i \leqslant b. \tag{4}$$

The tropical degree of these derivations is $O(b)$. The derivations of (2), (3) contain $O(b)$ (not necessarily distinct) terms, all the coefficients in them and constants are $\leqslant b$. The derivation of (4) contains $O(b^3)$ (not necessarily distinct) terms, all the coefficients in it are zeroes.

Proof. The inequalities (2) and (3) follow from Lemma 18.

To show (4) for $i = 1$, proceed by induction on b (starting with $b = 1$). Tropically multiply the axiom $x \oplus \overline{x} \leqslant 0$ by $x^{\odot(b-1)}$ and substitute $\overline{x} \leqslant \overline{x} \odot x^{\odot(b-1)}$ (which is $0 \leqslant x^{\odot(b-1)}$, provided by Lemma 18, multiplied by $\overline{x}$) into its left-hand side getting

$$x^{\odot b} \oplus \overline{x} \leqslant x^{\odot(b-1)}.$$

Tropically add $\overline{x}$ to both sides and substitute the induction hypothesis for $b-1$ on the right obtaining the desired inequality.

The inequality $x^{\odot b} \oplus \overline{x} \leqslant 0$ provided by the previous argument is the starting point for deriving (4), now by the induction on i (where $i = 1$ is the base). Take it and tropically multiply it by $\overline{x}^{\odot(i-1)}$ obtaining

$$x^{\odot b} \odot \overline{x}^{\odot(i-1)} \oplus \overline{x}^{\odot i} \leqslant \overline{x}^{\odot(i-1)}.$$

Tropically add $x^{\odot b}$ to both sides, substitute the induction hypothesis on the right. Substitute $x^{\odot b} \leqslant x^{\odot b} \odot \overline{x}^{\odot(i-1)}$ (which is $0 \leqslant \overline{x}^{\odot(i-1)}$, provided by Lemma 18, multiplied by $x^{\odot b}$) on the left. ◀

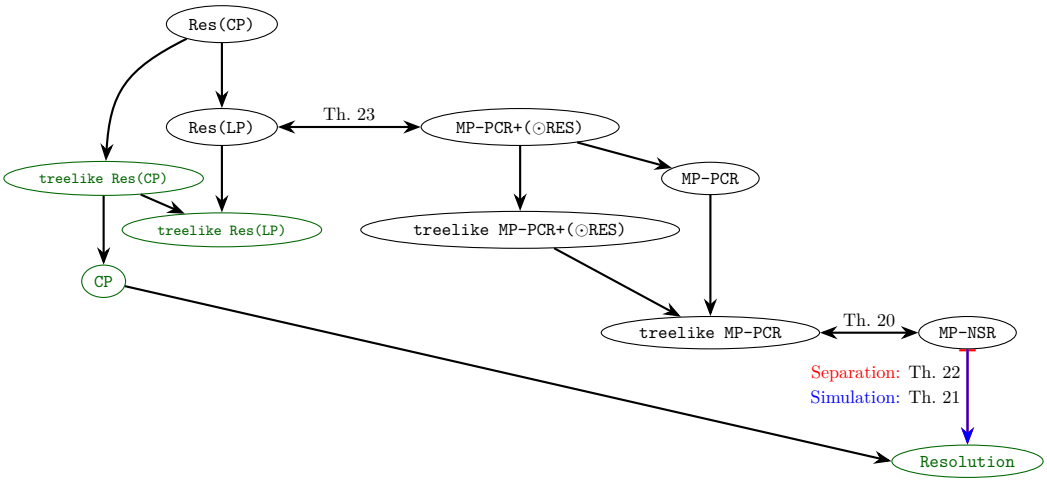

Figure 1 Map of tropical systems with $\{0,1\}$ dual encoding. An arrow $\Pi \to \Psi$ means polynomial simulation of Π by Ψ. Proof systems known to be not polynomially bounded are shown in green.

6 Our results and methods

6.1 Static systems: Already stronger than Resolution

Static tropical proofs with dual variables over $\{0,1\}$ turn out to be surprisingly powerful. We start with a natural statement that static tropical proofs are equivalent to treelike proofs:

▶ **Theorem 20.** *MP-NS polynomially simulates treelike MP-PC.*

Proof Sketch. Simulating a treelike tropical proof is done by combining the steps of the proof in a single algebraic combination with *decreasing coefficients*. Namely, when we go down (towards the root) the proof tree, which becomes now the formula tree of the algebraic combination, we tropically multiply subformulas by small positive coefficients. A similar idea is demonstrated in more detail in the proof of the next Theorem 21. ◀

Note that when we convert a treelike proof into a formula, the tropical multiplication of a tropical polynomial p applies to the whole subtree deriving p, thus this strategy does not work for simulating daglike tropical proofs (if p is multiplied by different terms t_i, we need to repeat it as many times).

However, we show that MP-NSR polynomially simulates *daglike* resolution. While the simulation of the treelike tropical proof is technical but intuitively straightforward, the simulation of the Resolution proof system is trickier due to its daglike nature.

▶ **Theorem 21.** *MP-NSR polynomially simulates Resolution.*

Proof. We simulate a resolution proof by putting it into the static proof step by step. For a disjunction $A = \ell_1 \vee \ldots \vee \ell_k$, define its translation $[A] = 0 \odot \ell_1 \odot \ldots \odot \ell_k$ with the meaning that it is true iff $[A] > 0$. In particular, every initial clause A is translated into $1 \leqslant [A]$, as we expect in MP-NSR.

Translate a Resolution proof into an MP-NSR proof as follows. Let s be the number of steps in the Resolution proof. We can assume that steps can be of two kinds: a resolution step

$$\frac{A \vee x \quad A \vee \neg x}{A}, \tag{5}$$

and a weakening step

$$\frac{A}{A \vee \ell}, \tag{6}$$

where A is a clause, x is a variable, and ℓ is a literal.

We now compose our algebraic combination.

For every initial clause A, we take its translation $1 \leqslant [A]$:

$$1 \leqslant 0 \odot [A]. \tag{7}$$

At step $i = 1, 2, \ldots, s$, we do the following. Let $c_i = i/(s+1)$.

- For a resolution step, multiply the axiom $x \oplus \overline{x} \leqslant 0$ by $c_i \odot [A]$ obtaining

$$c_i \odot x \odot [A] \oplus c_i \odot \overline{x} \odot [A] \leqslant c_i \odot [A]. \tag{8}$$

  Observe that $[A \vee v] = [A] \odot v$ for every variable v, so the terms in (8) are exactly the translation of (5) multiplied by c_i.
- For a weakening step, we would like to multiply $0 \leqslant [\ell]$ by $c_i \odot [A]$ obtaining

$$c_i \odot [A] \leqslant c_i \odot [A] \odot [\ell]. \tag{9}$$

  Observe that the terms in (9) are exactly the translation of (6) multiplied by c_i.

  Strictly speaking, $0 \leqslant [\ell]$ is not an axiom, while $0 \leqslant [\neg\ell] \oplus [\ell]$ is. Formally, we must multiply the latter (rather than the former) by $c_i \odot [A]$. However, this leaves only extra terms in the right-hand side compared to (9), which cannot harm our MP-NSR refutation.

Note that the last step's right-hand side is $c_s \odot [\emptyset]$, that is, $1 - 1/(s+1)$.

Our algebraic combination is a tropical sum of all inequalities (7) (for all the initial clauses A), (8), and (9) (for all steps of the Resolution proof).

The constant terms of the combination are 1 in the left-hand side, from the initial clauses, and $1 - 1/(s+1)$ in the right-hand side, from the last clause; $1 > 1 - 1/(s+1)$.

Every other monomial in the left-hand side has its counterpart in the right-hand side, from the previous steps of the proof. The coefficient is smaller in the simulation of the previous steps and in the initial clauses (thus, on the right-hand side).

It is clear that the total number of terms appearing in the proof is bounded by a polynomial in s, the degree of every monomial is bounded by the width of the resolution proof, and the nominators and denominators of the rational coefficients are also bounded by a polynomial in s. ◀

We also show that MP-NSR has polynomial-size proofs for *the propositional pigeonhole principle*, thus it is strictly stronger than Resolution. We consider the following translation of the pigeonhole principle:

$$1 \leqslant \bigodot_{j=1}^{n} x_{ij} \text{ for } 1 \leqslant i \leqslant m,$$

$$1 \leqslant \overline{x}_{i'j} \odot \overline{x}_{ij} \text{ for } 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n.$$

▶ **Theorem 22.** *For any $n > m$, PHP_n^m has polynomial-size MP-NSR refutations.*

Proof. For the refutation of the propositional pigeonhole principle, we construct a treelike MP-PCR proof and then convert it into a static proof. We use the overall strategy for a treelike CP proof [22, Proposition 19.5]. The main step of this proof is the inductive

derivation of long inequalities $\sum_i x_{ij} \leqslant 1$ stating that every hole contains at most one pigeon, from short inequalities $x_{ij} + x_{i'j} \leqslant 1$. In CP this is done using the rounding rule, however, in MP-NSR we do not have it. Instead, we consider the cases for the newly added pigeon using tropical tools. More precisely, we will prove the following lemma

▶ **Lemma** (short to long inequalities). *Let $v_1 \dots v_k, \overline{v}_1, \dots, \overline{v}_k$ be variables. Given the Boolean axioms and the set of inequalities $v_i \odot v_{i'} \leqslant 1$ for $1 \leqslant i < i' \leqslant k$, one can construct a* `treelike MP-PCR` *derivation of $\bigodot_{i=1}^{k} v_i \leqslant 1$, which contains $O(k^4)$ terms, has tropical degree $O(k)$, and its coefficients are zeroes and ones.*

Proof of Lemma. Denote $V_j = \bigodot_{i=1}^{j} v_i$. We proceed by the induction on the number of variables constructing a `treelike MP-PCR` derivation of $V_j \leqslant 1$.

The base ($j = 2$) is trivial. The induction step comes in three stages.

Stage 1. Take the induction hypothesis for $j - 1$ and tropically multiply it by v_j getting

$$V_j \leqslant 1 \odot v_j. \tag{10}$$

Stage 2. For $i = 1, \dots, j-1$, construct also the following derivation: tropically multiply the initial inequality $v_i \odot v_j \leqslant 1$ by $\overline{v}_j$ and substitute its left-hand side by the axiom $1 \leqslant v_j \odot \overline{v}_j$ multiplied by v_i. Multiply the result by (-1) obtaining $v_i \leqslant \overline{v}_j$. Apply Lemma 18 to multiply these inequalities for $i = 1, \dots, j-1$:

$$\bigodot_{i=1}^{j-1} v_i \leqslant \overline{v}_j^{\odot(j-1)}.$$

Further multiply it by v_j and substitute $v_j \odot \overline{v}_j \leqslant 1$ multiplied by $\overline{v}_j^{\odot(j-2)}$ into it obtaining

$$V_j \leqslant 1 \odot \overline{v}_j^{\odot(j-2)}. \tag{11}$$

Stage 3. Take the tropical sum of (10) and (11) and substitute its right-hand side with $v_j \oplus \overline{v}_j^{j-2} \leqslant 0$ (due to Lemma 19) multiplied by 1 eventually obtaining $V_j \leqslant 1$. ◀

Given the lemma, we apply it to $x_{1j}, \dots, x_{mj}$ for each $j = 1, \dots, n$ separately. Multiply the results to get

$$\bigodot_{j=1}^{n} \bigodot_{i=1}^{m} x_{ij} \leqslant n.$$

On the other hand, by multiplying the initial inequalities, we get

$$m \leqslant \bigodot_{i=1}^{m} \bigodot_{j=1}^{n} x_{ij}$$

After substitution of the first equation into the right-hand side of the second equation, we arrive at the contradiction $m \leqslant n$. ◀

This shows that MP-NSR is strictly stronger than resolution; however, its relation to CP remains open. This makes MP-NSR a nice frontier proof system, for which (as a proof system for unsatisfiable formulas in CNF) we do not know any superpolynomial lower bounds.

6.2 Dynamic systems: Going up to Res(LP)

We do not know whether MP-PCR simulates Res(LP). The additional ($\odot$RES) rule strengthening MP-PCR is needed for that. We prove the following equivalence.

▶ **Theorem 23.** *MP-PCR+($\odot$RES) with $\{0,1\}$ encoding is polynomially equivalent to Res(LP).*

Proof Sketch. We simulate a Res(LP) proof step by step. A line of a Res(LP) refutation of the form $f_1 \geqslant 0 \vee f_2 \geqslant 0 \vee \ldots \vee f_k \geqslant 0$ is translated into the min-plus inequality

$$[-f_1] \oplus [-f_2] \oplus \cdots \oplus [-f_k] \leqslant 0,$$

where for a linear inequality $f \geqslant 0$, its translation $[-f]$ is given by the natural tropical term semantically equivalent to $-f$. To simulate the "main" rule (+RES) deriving a nonnegative linear combination, we split its coefficients into bits, simulate linear combinations for this easy case, and then sum everything together using ($\odot$RES).

In the other direction, a min-plus inequality $f_1 \oplus f_2 \oplus \cdots \oplus f_t \leqslant g_1 \oplus g_2 \oplus \cdots \oplus g_k$ is translated into the disjunctions of inequalities, one for each $1 \leqslant j \leqslant k$:

$$\bigvee_{i=1}^{t} \{f_i\} \leqslant \{g_j\},$$

where $\{\cdot\}$ again defines the natural semantically equivalent translation of tropical terms into linear inequalities. One can prove that a dynamic tropical proof can always be finished by a constant inequality $1 \leqslant 0$ (this is done in the same vein as simulating treelike proofs by static proofs, but now dynamically). Therefore, we do not need to deal with a complicated last line of the tropical proof in our simulation by Res(LP). ◀

Systems over $\{0,\infty\}$. One can consider systems that encode false and true by $\{0,\infty\}$ instead of $\{0,1\}$. The axioms ($01/\odot$) and ($01\oplus$) are then replaced by

$$\frac{\emptyset}{x \odot \overline{x} = \infty} \quad (0\infty/\odot), \qquad \frac{\emptyset}{x \oplus \overline{x} = 0} \quad (0\infty/\oplus)$$

to ensure that x and $\overline{x}$ are dual and in $\{0,\infty\}$. With this encoding, MP-PCR becomes equivalent to a different proof system (additional rules are not needed in this setting):

▶ **Theorem 24.** *MP-PCR that uses $\{0,\infty\}$ encoding with dual variables is polynomially equivalent to Res(∞), the unbounded version of the Res(k) proof system [24].*

The proof is similar to the $\{0,1\}$ case; the main difference is that for $\{0,\infty\}$ tropical operations are essentially conjunction and disjunction, so it remains to process accurately statements like $f = c$ for a term f and a constant $c \in \mathbb{Q} \cup \{\infty\}$, and prove the corresponding translations of MP-PCR rules in Res(∞). The other direction goes almost literally by translating clauses composed of DNFs into the corresponding min-plus inequalities over $\{0,\infty\}$.

6.3 Lower bounds

We prove the lower bound k on the size of refutations of a much simplified tropical version $x^{\odot k} = c$ (where $c \in \mathbb{Q} \setminus \mathbb{N}_0$) of the (generalized) Binary Value Principle [4, 28] in MP-NSR.

▶ **Theorem 25.** *The size of MP-NSR refutations of a tropical binomial $x^{\odot k} = c$ for $c \in \mathbb{Q}$ is greater than k.*

In particular, for $x^{\odot 2^n} = -1$ this is an exponential lower bound when the coefficients and the degrees of tropical proofs are represented in binary.

The proof adheres to the following ideology. The MP-NS refutations are based on comparing coefficients in left- and right-hand sides in algebraic combinations. Having this in mind, when talking about size in MP-NSR, we construct a directed graph on monomials occurring in a tropical algebraic combination. We do it in a way such that some specific function on the vertices of the graph related to the coefficients is strictly monotone along any arrow. To establish the lower bound on the size of refutations of $x^{\odot k} = c$ in MP-NSR we prove that any cycle in this graph should contain at least k arrows.

Proof. Consider a refutation

$$(f,g) := \bigoplus_{i,j} x^{\odot i} \odot \bar{x}^{\odot j} \odot \big(a_{i,j} \odot (x \oplus \bar{x}, 0) \oplus b_{i,j} \odot (0, x \oplus \bar{x}) \\ \oplus\, d_{i,j} \odot (x \odot \bar{x}, 1) \oplus e_{i,j} \odot (1, x \odot \bar{x}) \oplus u_{i,j} \odot (x^{\odot k}, c) \oplus v_{i,j} \odot (c, x^{\odot k})\big),$$

where $a_{i,j}, b_{i,j}, d_{i,j}, e_{i,j}, u_{i,j}, v_{i,j} \in \mathbb{Q}_\infty$ and $f \succ g$.

We construct a directed graph H (See Fig. 2) whose vertices are tropical monomials m appearing in g. We distinguish 7 cases regarding from which summand in the right-hand side of the refutation a monomial m emerges in g:

$$m = x^{\odot i} \odot \bar{x}^{\odot j},\ c(m) = a_{i,j}; \tag{12}$$
$$m = x^{\odot (i+1)} \odot \bar{x}^{\odot j},\ c(m) = b_{i,j}; \tag{13}$$
$$m = x^{\odot i} \odot \bar{x}^{\odot (j+1)},\ c(m) = b_{i,j}; \tag{14}$$
$$m = x^{\odot i} \odot \bar{x}^{\odot j},\ c(m) = d_{i,j} + 1; \tag{15}$$
$$m = x^{\odot (i+1)} \odot \bar{x}^{\odot (j+1)},\ c(m) = e_{i,j}; \tag{16}$$
$$m = x^{\odot i} \odot \bar{x}^{\odot j},\ c(m) = u_{i,j} + c; \tag{17}$$
$$m = x^{\odot (i+k)} \odot \bar{x}^{\odot j},\ c(m) = v_{i,j} \tag{18}$$

for suitable i, j. If several cases apply to the same monomial, we choose one of them in an arbitrary way.

Draw an arrow in H from m to

$$x \odot m = x^{\odot (i+1)} \odot \bar{x}^{\odot j} \text{ in case (12)}; \tag{19}$$
$$x^{\odot i} \odot \bar{x}^{\odot j} \text{ in case (13)}; \tag{20}$$
$$x^{\odot i} \odot \bar{x}^{\odot j} \text{ in case (14)}; \tag{21}$$
$$x^{\odot (i+1)} \odot \bar{x}^{\odot (j+1)} \text{ in case (15)}; \tag{22}$$
$$x^{\odot i} \odot \bar{x}^{\odot j} \text{ in case (16)}; \tag{23}$$
$$x^{\odot (i+k)} \odot \bar{x}^{\odot j} \text{ in case (17)}; \tag{24}$$
$$x^{\odot i} \odot \bar{x}^{\odot j} \text{ in case (18)}. \tag{25}$$

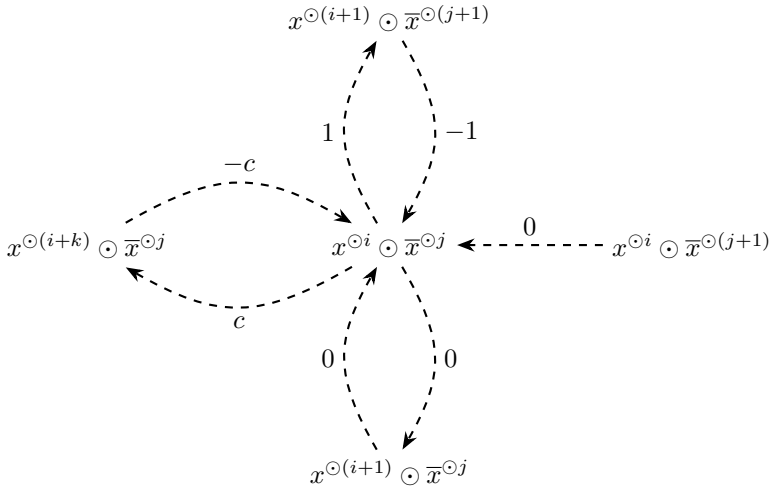

Figure 2 Possible arrows in a fragment of the graph H in Theorem 25 (not all arrows are present in a specific proof!). Coefficients decrease more than by the value shown on the arrows (according to (26)–(32)).

Since $f \succ g$, these arrows indeed correspond to strict inequalities on the coefficients:

$$c(x^{\odot(i+1)} \odot \bar{x}^{\odot j}) < c'(x^{\odot(i+1)} \odot \bar{x}^{\odot j}) \leqslant c(x^{\odot i} \odot \bar{x}^{\odot j}) \text{ in cases (12), (19);} \tag{26}$$

$$c(x^{\odot i} \odot \bar{x}^{\odot j}) < c'(x^{\odot i} \odot \bar{x}^{\odot j}) \leqslant c(x^{\odot(i+1)} \odot \bar{x}^{\odot j}) \text{ in cases (13), (20);} \tag{27}$$

$$c(x^{\odot i} \odot \bar{x}^{\odot j}) < c'(x^{\odot i} \odot \bar{x}^{\odot j}) \leqslant c(x^{\odot i} \odot \bar{x}^{\odot(j+1)}) \text{ in cases (14), (21);} \tag{28}$$

$$c(x^{\odot(i+1)} \odot \bar{x}^{\odot(j+1)}) < c'(x^{\odot(i+1)} \odot \bar{x}^{\odot(j+1)}) \leqslant c(x^{\odot i} \odot \bar{x}^{\odot j}) - 1 \text{ in cases (15), (22);} \tag{29}$$

$$c(x^{\odot i} \odot \bar{x}^{\odot j}) < c'(x^{\odot i} \odot \bar{x}^{\odot j}) \leqslant c(x^{\odot(i+1)} \odot \bar{x}^{\odot(j+1)}) + 1 \text{ in cases (16), (23);} \tag{30}$$

$$c(x^{\odot(i+k)} \odot \bar{x}^{\odot j}) < c'(x^{\odot(i+k)} \odot \bar{x}^{\odot j}) \leqslant c(x^{\odot i} \odot \bar{x}^{\odot j}) - c \text{ in cases (17), (24);} \tag{31}$$

$$c(x^{\odot i} \odot \bar{x}^{\odot j}) < c'(x^{\odot i} \odot \bar{x}^{\odot j}) \leqslant c(x^{\odot(i+k)} \odot \bar{x}^{\odot j}) + c \text{ in cases (18), (25).} \tag{32}$$

There exists a cycle Z in the graph H. To justify the required lower bound k when the numbers of arrows of types (24), (25) differ, note that the degree of x changes at most by one in all other types of arrows.

When they are equal, we observe that the number of arrows of type (23) in Z is greater than the number of arrows of type (22), because the coefficient at a tropical monomial increases (respectively, decreases) by 1 along an arrow of type (23) due to (16) (respectively, of type (22) due to (15)), while the coefficient does not change along arrows of types (19), (20), (21) due to (12), (13), (14), respectively. This leads to a contradiction since the tropical degree with respect to $\bar{x}$ of a tropical monomial decreases (respectively, increases) by 1 along an arrow of type (23) (respectively, (22)), while this tropical degree does not increase along arrows of other types. ◀

6.4 Non-deducibility results

We also show two non-deducibility results. First we notice that one could encode Boolean logic without dual variables by replacing the axioms (01/$\cdot$) and (01/$\oplus$) by semantically equivalent

$$\frac{\emptyset}{x^{\odot 2} \oplus 1 = x}. \tag{01/E}$$

We show that the inequality $0 \leqslant x$ is not derivable from (01/E) (thus showing the difference between two Boolean encodings). Formally, we prove the following theorem.

▶ **Theorem 26.** *$\Gamma \oplus c \leqslant x \oplus \Delta$ is not derivable in MP-NS from (01/E) for any $c \in \mathbb{Q}_\infty$ and any $\Gamma \succ \Delta$.*

After that we establish that the tropical resolution rule cannot be simulated directly in MP-PCR by providing an easy example of premises of these rules that cannot yield the conclusion through an algebraic combination with Boolean axioms (even with auxiliary polynomials remaining in the algebraic combination). More precisely, the next theorem states that there is no inference of the inequality $x^{\odot 2} \leqslant 0$ from the axioms in MP-NSR. Note that this demonstrates that one cannot infer the tropical resolution rule ($\odot$RES): namely, from $t \oplus f \leqslant 0,\ t' \oplus f \leqslant 0$ to infer $t \odot t' \oplus f \leqslant 0$, setting $t := t' := x, f := x^{\odot 2}$.

▶ **Theorem 27.** *For any $\Gamma \succ \Delta$, there is no MP-NSR inference of $\Gamma \oplus x^{\odot 2} \leqslant 0 \oplus \Delta$ from the axioms of these systems.*

This proof uses techniques similar to those of the size lower bounds. To prove non-deducibility in MP-NSR, we again construct a directed graph on monomials occurring in a tropical algebraic combination, such that some specific function on the vertices of the graph related to the coefficients is strictly monotone along any arrow. Then we show the existence of a cycle in the graph, which leads to a contradiction.

7 Conclusion and Further Research

In this paper we introduced a new view of previously known proof systems by using tropical arithmetic. This view allowed us to isolate weaker fragments of Res(CP) (see Figure 1) so that we could hope for proving superpolynomial lower bounds on the proof size for them. The weakest of these fragments, static tropical proof systems, allow for different (and more elementary) methods of proving lower bounds. We provided several steps in this direction (though not for formulas in CNF). We view proving lower bounds for tropical proof systems as a promising direction.

The "knowledge border" for Boolean formulas in CNF lies between treelike Res(CP), where exponential lower bounds have been recently proved using quasipolynomial monotone interpolation [15], treelike Res(Lin) with semantic weakening, where exponential lower bounds are known for PHP [28], regular Res($\oplus$), where exponential lower bounds for the binary pigeon-hole principle have been proved recently [13], on the one hand, and, on the other hand, Res(LP*) as well as Res(Lin) and Res($\oplus$), where the question is so far open. In the non-CNF case, exponential lower bounds are known also for the Binary Value Principle in daglike Res(Lin) [28].

Tropical proof systems refine these borders. The static system MP-NSR lies between daglike Resolution and (through, for example, MP-PCR and Res(LP)) Res(CP). In the non-CNF case, we have shown an exponential lower bound on the refutations of a greatly simplified version of the Binary Value Principle in MP-NSR.

Several promising directions are (all questions concern $\{0,1\}$-variables encodings):

1. We were able to show the polynomial simulation of Res(LP) only after we added the rule ($\odot$RES) to MP-PCR.
   - **a.** It gives an additional hope to prove **lower bounds for MP-PCR** as it may be weaker than Res(LP).
   - **b.** Or maybe the two systems are polynomially equivalent even without this rule? (We only proved that it cannot be simulated directly in a rule-by-rule fashion.)

2. Fleming et al. [14] prove that CP quasipolynomially simulates treelike Res(CP*). While Res(CP*) and Res(LP*) are polynomially equivalent, this is not necessarily true for their treelike versions. In fact, treelike Res(LP) has very limited ability to work with integer arithmetic at all, because it is unable to make rounding with big coefficients efficiently. Can we quasipolynomially simulate treelike Res(LP) in CP? Perhaps, we can quasipolynomially simulate MP-NSR in CP?
3. Relations between MP-NSR and CP are unclear, both for unary and binary coefficients, and even for treelike CP.
4. Relations between treelike MP-PCR+($\odot$RES) and treelike Res(LP) are also unclear. Even polynomial simulation of MP-NSR in treelike Res(LP) does not seem to be trivial.

References

1 Marianne Akian, Antoine Béreau, and Stéphane Gaubert. The tropical Nullstellensatz and Positivstellensatz for sparse polynomial systems. In *Proc. ACM Intern. Symp. Symb. Algebr. Comput.*, pages 43–52, 2023. doi:10.1145/3597066.3597089.

2 Marianne Akian, Stéphane Gaubert, and Alexander Guterman. The correspondence between tropical convexity and mean payoff games. In *19 Intern. Symp. Math. Theory of Networks and Systems, Budapest*, pages 1295–1302, 2012.

3 Yaroslav Alekseev, Dima Grigoriev, and Edward A. Hirsch. Tropical proof systems. *Electron. Colloquium Comput. Complex.*, TR24-072, 2024. URL: https://eccc.weizmann.ac.il/report/2024/072.

4 Yaroslav Alekseev, Dima Grigoriev, Edward A. Hirsch, and Iddo Tzameret. Semialgebraic proofs, IPS lower bounds, and the τ-conjecture: Can a natural number be negative? *SIAM Journal on Computing*, 53(3):648–700, 2024. doi:10.1137/20M1374523.

5 Xavier Allamigeon, Uli Fahrenberg, Stéphane Gaubert, Ricardo D. Katz, and Axel Legay. Tropical Fourier-Motzkin elimination, with an application to real-time verification. *Int. J. Algebra Comput.*, 24(5):569–607, 2014. doi:10.1142/S0218196714500258.

6 Paul Beame, Noah Fleming, Russell Impagliazzo, Antonina Kolokolova, Denis Pankratov, Toniann Pitassi, and Robert Robere. Stabbing Planes. In Anna R. Karlin, editor, *9th Innovations in Theoretical Computer Science Conference (ITCS 2018)*, volume 94 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 10:1–10:20, Dagstuhl, Germany, 2018. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ITCS.2018.10.

7 Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proc. London Math. Soc.*, 73(3):1–26, 1996. doi:10.1112/plms/s3-73.1.1.

8 Aaron Bertram and Robert Easton. The tropical Nullstellensatz for congruences. *Adv. Math*, 308:36–82, 2017.

9 Peter Butkovic. *Max-linear systems: theory and algorithms*. Springer, 2010.

10 Matthew Clegg, Jeffery Edmonds, and Russell Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, pages 174–183, New York, 1996. doi:10.1145/237814.237860.

11 Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *J. Symb. Log.*, 44(1):36–50, 1979. doi:10.2307/2273702.

12 W. Cook, C.R. Coullard, and Gy. Turán. On the complexity of cutting-plane proofs. *Discrete Applied Mathematics*, 18(1):25–38, 1987. doi:10.1016/0166-218X(87)90039-4.

13 Klim Efremenko, Michal Garlik, and Dmitry Itsykson. Lower bounds for regular resolution over parities. ECCC TR23-187, 2023.

14 Noah Fleming, Mika Göös, Russell Impagliazzo, Toniann Pitassi, Robert Robere, Li-Yang Tan, and Avi Wigderson. On the power and limitations of branch and cut. In Valentine Kabanets, editor, *36th Computational Complexity Conference, CCC 2021, July 20-23, 2021, Toronto, Ontario, Canada (Virtual Conference)*, volume 200 of *LIPIcs*, pages 6:1–6:30. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPICS.CCC.2021.6.

15 Max Gläser and Marc E. Pfetsch. Sub-exponential lower bounds for branch-and-bound with general disjunctions via interpolation. Technical Report 2308.04320, arXiv, 2023.

16 Dima Grigoriev. Complexity of solving tropical linear systems. *Comput. Complexity*, 22:71–88, 2013. doi:10.1007/S00037-012-0053-5.

17 Dima Grigoriev and Vladimir V. Podolskii. Tropical effective primary and dual Nullstellensätze. *Discrete and Computational Geometry*, 59(3):507–552, 2018. doi:10.1007/s00454-018-9966-3.

18 Armin Haken. The intractability of resolution. *Theoret. Comput. Sci.*, 39(2-3):297–308, 1985. doi:10.1016/0304-3975(85)90144-6.

19 Edward A. Hirsch and Arist Kojevnikov. Several notes on the power of Gomory-Chvátal cuts. *Ann. Pure Appl. Log.*, 141(3):429–436, 2006. doi:10.1016/j.apal.2005.12.006.

20 Dmitry Itsykson and Dmitry Sokolov. Resolution over linear equations modulo two. *Ann. Pure Appl. Log.*, 171(1), 2020. doi:10.1016/J.APAL.2019.102722.

21 Daniel Joo and Kalina Mincheva. Prime congruences of additively idempotent semirings and a Nullstellensatz for tropical polynomials. *Selecta Math.*, 24:2207–2233, 2018.

22 Stasys Jukna. *Boolean Function Complexity*. Springer, 2012.

23 Jan Krajícek. Discretely ordered modules as a first-order extension of the cutting planes proof system. *J. Symb. Log.*, 63(4):1582–1596, 1998. doi:10.2307/2586668.

24 Jan Krajícek. On the weak pigeonhole principle. *Fundamenta Mathematicae*, 170(1–3):123–140, 2001.

25 Jan Krajíček. *Proof Complexity*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2019.

26 Diane Maclagan and Felipe Rincon. Tropical ideals. *Compos. Math.*, 154:640–670, 2018.

27 Diane Maclagan and Bernd Sturmfels. *Introduction to Tropical Geometry*. Springer, 2015.

28 Fedor Part and Iddo Tzameret. Resolution with counting: Dag-like lower bounds and different moduli. *Comput. Complex.*, 30(1):2, 2021. doi:10.1007/S00037-020-00202-X.

29 Pavel Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *The Journal of Symbolic Logic*, 62(3):981–998, 1997. URL: http://www.jstor.org/stable/2275583, doi:10.2307/2275583.

30 Ran Raz and Iddo Tzameret. Resolution over linear equations and multilinear proofs. *Ann. Pure Appl. Logic*, 155(3):194–224, 2008. doi:10.1016/j.apal.2008.04.001.

31 Grigori Tseitin. On the complexity of derivations in propositional calculus. In *Studies in constructive mathematics and mathematical logic. Part II*, pages 115–125. Consultants Bureau, New-York-London, 1968.

32 Alasdair Urquhart. Hard examples for resolution. *J. ACM*, 34(1):209–219, 1987. doi:10.1145/7531.8928.