Electronic Colloquium on Computational Complexity, Report No. 72 (2024)

Tropical proof systems

Yaroslav Alekseev* Dima Grigoriev† Edward A. Hirsch‡

April 11, 2024

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 [BIK+96]. Tropical 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, [BE17, GP18, JM18] 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. 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 lower bounds on the tropical degree of derivations of a tropical version of the Knapsack problem and on the size of derivations of a much simplified tropical version of the Binary Value Principle in static tropical proof systems. Also, we establish the non-deducibility of the tropical resolution rule in these systems and discuss the necessity of the use of non-integer coefficients in tropical proofs.

*The Technion, Israel. Email: `tolstreg@gmail.com`

†CNRS, Université de Lille, France. Email: `dmitry.grigoryev@univ-lille.fr`

‡Ariel University, Israel. Email: `edwardh@ariel.ac.il`

ISSN 1433-8092

Contents

1 Introduction

1.1 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) for a lattice with respect to the partial non-strict order composed of the simulations; if one system is strictly stronger than the other one, then the 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.

1.2 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 [Tse68, Hak85, Urq87], 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 [Kra19] for a detailed overview of the area.

[1] This definition deviates from the classical Cook–Reckhow definition [CR79], but for our purpose they are equivalent.

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 [CCT87] uses nonnegative linear combinations of inequalities and the rounding rule

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

as its derivation steps. 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 [Pud97].

Krajíček [Kra98] generalized `CP` to a new system `R(CP)`, also called `Res(CP)`, by allowing to reason about disjunctions of 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

$$\frac{(f_1 \geqslant 0) \vee \Gamma \qquad (f_2 \geqslant 0) \vee \Gamma}{(\alpha_1 f_1 + \alpha_2 f_2 \geqslant 0) \vee \Gamma}\ (\alpha_1, \alpha_2 > 0) \tag{+RES}$$

$$\frac{\sum_i c a_i x_i - d \geqslant 0 \vee \Gamma}{\sum_i a_i x_i - \lceil d/c \rceil \geqslant 0 \vee \Gamma}\ (c, a_i, d \in \mathbb{Z}).$$

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`)` [Kra01], `Res(Lin)` [RT08], `Res(`$\oplus$`)` [IS20]). 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 instead

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

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 [BFI+18] 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 a superpolynomial bound for it [FGI+21]. The daglike versions of `Res(CP)` and `Res(LP)` with unary coefficients are polynomially equivalent [HK06] and no superpolynomial lower bounds are known for them to the date. Very recently, Gläser and Pretsch have shown a superpolynomial bound for Stabbing Planes for the case of binary coefficients by providing a quasipolynomial monotone interpolation [GP23].

1.3 Tropical arithmetic

Tropical (or min-plus) arithmetic involves operations min, $+$ in place of $+, \times$ in classical arithmetic; we refer an interested reader to [MS15] 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 [MS15], also neural networks are a more recent application).

Thus, the main object of tropical arithmetic is a tropical (idempotent) semifield endowed with the operations $\oplus := \min, \odot := +$. As an example one can take the rational numbers $\mathbb{Q}$ or $\mathbb{Q}_\infty := \mathbb{Q} \cup \{\infty\}$, where ∞ plays a role of the neutral element (similar to the role of 0 in classical arithmetic). Observe that 0, in its turn, plays a role of the unity element.

In tropical algebra one introduces *tropical monomials* $m := x_1^{\odot i_1} \odot \cdots \odot x_n^{\odot i_n}$, for nonnegative integer degrees $i_1, \ldots, i_n$. A monomial with a constant coefficient $a \in \mathbb{Q}_\infty$ is called a *tropical term* (at least, in this paper): $a \odot m$. If $i_1 + \ldots + i_n > 1$, then a must be finite (otherwise the monomial is missing, or is equivalent to the constant ∞, similarly to classical monomials with coefficient zero). One can treat a tropical term classically as a linear function $a + i_1 x_1 + \ldots + i_n x_n$. Then one introduces *tropical polynomials* $f := \bigoplus_j t_j$, where t_j are tropical terms (see Sect. 2 for more detailed definitions). 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.

One can consider min-plus equations $f = g$, where f, g are tropical polynomials. One of the central issues in tropical algebra is a criterion of solvability of a system of min-plus equations. 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 [BE17, GP18, JM18, MR18], further extended in [ABG23]. We use a more combinatorial version from [GP18]: we cite a particular case below as Theorem 2.3, while the original result provides also complexity upper bounds, which we do not use in our work.

In this paper, we mainly consider *min-plus inequalities* $f \leqslant g$. Since such an inequality can be expressed as an equation $f = f \oplus g$, we can still use Min-Plus Nullstellensatz for proving that a system of min-plus inequalities has no solutions (Theorem 2.5). Further remarks on the equivalence of these two approaches (equations vs inequalities) are given in Appendix A.

Note that tropical equations [MS15] studied in the literature are a different matter. We stick rather to min-plus equations, which match the common intuition better. On the other hand, the class of systems of min-plus equations is equivalent to the class of systems of tropical equations: namely, one can transform a system of min-plus equations into an equivalent system of tropical equations (within polynomial complexity) and vice versa [GP18].

1.4 Tropical proof systems

Similarly to the already classical "algebraic" proof systems Nullstellensatz and Polynomial Calculus [BIK+96, CEI96] 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 2.6) 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 an 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 be shown by providing, for every monomial in the left-hand side, the coefficient that is strictly greater than the corresponding coefficient on the right-hand side (also, for technical reasons the right-hand side must have a finite constant term).

Similarly to the algebraic proof systems, we introduce a dynamic version of MP-NS: Min-Plus Polynomial Calculus (MP-PC), see Definition 2.9. 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, which we show in Theorems 7.3, 7.5.

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 consider the encoding $\{0, \infty\}$ and can also use more a economical encoding without dual variables.

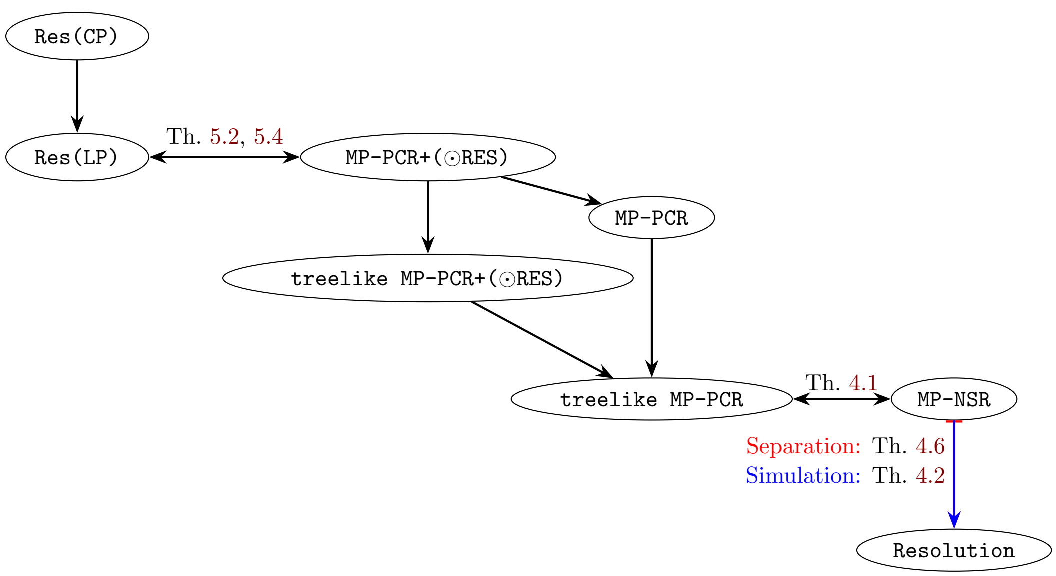

Figure 1: Map of tropical systems with $\{0, 1\}$ dual encoding.

1.5 Our results and methods

Static systems. Static tropical proofs with dual variables over $\{0, 1\}$ turn out to be surprisingly powerful: we prove that they are equivalent to treelike proofs and show that MP-NSR polynomially simulates daglike resolution and has polynomial-size proofs for the propositional pigeonhole principle. This shows that MP-NSR is strictly stronger than resolution; however, its relation to CP remains open. The three methods we use are:

- Simulating a daglike proof using a static proof by putting the daglike proof into the static proof step by step.

  For MP-NSR it means that every step of the simulated proof is split between the sides of the inequality that is an algebraic combination of the input inequalities: the translation of the premises is on the left, and the translation of the conclusion is on the right. Fortunately, every step of a resolution proof can be justified by such an inequality without the necessity to argue about the previous or the subsequent steps. In order to make the algebraic combination contradictory, we multiply these inequalities by decreasing coefficients $1, 1/2, 2/3, 3/4, \ldots$ as the proof progresses, so that in the final algebraic combination every premise (on the left) is matched by the conclusion of some previous step (on the right) with a smaller coefficient. The translation of the input clauses has the constant term 1 on the left-hand side, and the translation of the contradiction has the constant term 0 on the right-hand side, thus the obtained algebraic combination is contradictory.

- Simulating a treelike tropical proof is done by combining the steps of the proof in a single algebraic combination (again, with decreasing coefficients). However, in order to simulate tropical multiplication of a tropical polynomial p we need to multiply 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).

- 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 [Juk12, 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.

Dynamic systems. We prove that MP-PCR+($\odot$RES) using dual variables with $\{0, 1\}$ values is polynomially equivalent to Res(LP). 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. We 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 $\{0, \infty\}$. If we encode Boolean logic using $\{0, \infty\}$, MP-PCR turns out to be polynomially equivalent to Res(∞), which is the unbounded version of the Res(k) proof system [Kra01]. 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 $\{0, \infty\}$.

Systems based on equations. One could imagine that tropical proof systems based on equations instead of inequalities could be weaker. For the static systems, it is clear that it does not change anything right on the level of definitions. We show that in the dynamic setting this is also not the case: the translation of $f \leqslant g$ into $f = f \oplus g$ works successfully in the dynamic case as well. This is a technical proof given in the Appendix.

Lower bounds and non-deducibility results. 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 [AGHT20, PT21] both in MP-NSE and in MP-NSR. 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.

We also show two non-deducibility results. First we show that the inequality $0 \leqslant x$ is not derivable from the axiom $x^{\odot 2} \oplus 1 = x$ (thus showing the difference between two Boolean encodings). After that we establish that the tropical resolution rule cannot be simulated directly neither in MP-PCE, nor in MP-PCR by providing an easy example of premises of these rule that cannot yield the conclusion through an algebraic combination with Boolean axioms (even with auxiliary polynomials remaining in the algebraic combination).

These proof adhere 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 non-deducibility 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. Then we show the existence of a cycle in the graph, which leads to a contradiction. Finally, 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.

Another non-deducibility result concerns the use of non-integer coefficients in static tropical proofs. We show that this is unavoidable in MP-NSE and MP-NSR (the proof goes by a simple comparison of the coefficients) in contrast to MP-PCR.

In addition, we provide exact lower bounds on the degree of refutations of the Tropical Knapsack problem $\bigoplus_{1 \leqslant i \leqslant n} x_i = r$ in MP-NSE. We assume that $r \in \mathbb{Q} \setminus \{0\}$ (respectively, $r \in \mathbb{Q} \setminus \{0, 1\}$) when we manipulate with the Boolean encoding $x^{\odot 2} = x$ (respectively, $x^{\odot 2} \oplus 1 = x$).

Note that the exact bound on the degree equals $n+1$ in case $r < 0$. To achieve this lower bound we consider a dual min-plus system and show that there is a solution for this system. On the contrary, in MP-NSR an upper bound 2 on the degree holds in both $\{0, \infty\}$- and $\{0, 1\}$-Boolean encodings. We mention that in [GP18, 4.6] a linear (respectively, exponential) lower bound on the degree was established for min-plus refutations over $\mathbb{Q}$ (respectively, over $\mathbb{Q}_\infty$), in contrast to the Boolean case studied in the current paper.

1.6 Conclusion

We introduce a new view of previously known proof systems by using tropical arithmetic. This view allows to isolate weaker fragments of Res(CP) (see Figure 1) so that we can 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 provide several steps in this direction (though not for formulas in CNF). We view proving lower bounds for tropical proof systems as a promising direction.

1.7 Organization of the paper

We start with providing the definitions (Section 2) and proving auxiliary facts about them (Section 3). Then we show the upper bound results for static proofs (Section 4). Afterwards we show the equivalence between dynamic proofs augmented with the ($\odot$RES) rule to Res(LP) (Section 5). A similar result for the $\{0, \infty\}$ encoding (with the replacement of Res(LP) by Res(∞)) is proved in Section 6. In Section 7 we prove several lower bounds for the static systems, and also show several impossibility results that justify that some parts of our definitions are essential. Eventually, we formulate numerous open questions (Section 8). In Appendix A we show that dynamic systems based on equations are equivalent to the systems based on inequalities.

2 Definitions

2.1 General notation

We use poly(n) do denote any function with polynomial growth, that is, $n^{O(1)}$.

We allow to write a rational number as p/q even if $\gcd(p, q) \neq 1$.

2.2 Tropical arithmetic basics

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. 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 $c \in \mathbb{Q}_\infty$.

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 $x \odot 9$.

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 ∞. 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). When we use the unary representation, we say this explicitly. 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. Criteria for the existence of common roots for systems of min-plus polynomials $\{(f_1, g_1), \dots, (f_k, g_k)\}$ have been suggested in [BE17, GP18, JM18].

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 $\{f_1 \leqslant g_1, \dots, f_k \leqslant g_k\}$. 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 2.1 ($\succ$ 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 $\Gamma \odot t \succ \Delta \odot t$.*

Proof. 1. Every monomial in $\Gamma \oplus \Gamma'$ that appears only in one of them still has the respective counterpart in $\Delta \oplus \Delta'$ with the same or a lower coefficient.

Every other term in $\Gamma \oplus \Gamma'$ has the form $a \odot m \oplus c \odot m$, where a, c are constants and m is a monomial. There are terms in Δ an Δ', respectively, of the form $b \odot m$ for $b < a$ and $d \odot m$ for $d < c$. Since $\min\{b, d\} < \min\{a, c\}$, Lemma follows.

2. Trivial. □

2.3 Tropical algebraic proof systems

The basic static proof system, MP-NS.

Definition 2.2. Consider a system of min-plus polynomials $F = \{(f_1, g_1), \dots, (f_k, g_k)\}$. An *algebraic combination* of F is a min-plus polynomial (f, g) that can be represented in the form

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

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 2.3 (Min-Plus Nullstellensatz, [GP18, Theorem 3.8] over $\mathbb{Q}_\infty$ without the degree claim)**.** *Consider a symmetric system of min-plus polynomial equations F as in Def. 2.2 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).

Remark 2.4. The theorem can be formulated over $\mathbb{Q}_\infty$ or over $\mathbb{Q}$ (where it is more efficient with respect to the degrees, but we are not talking about the complexity here yet). In fact, the theorem holds over any tropically closed semifield (for example, $\mathbb{R}$), that is, any semifield where one can (classically) divide by an arbitrary integer s which corresponds to tropically taking an s-th root (see [GP18, Remark 3.17]).

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 for the case of systems of inequalities (which correspond to not necessarily symmetric systems of min-plus polynomials), a similar theorem holds as a corollary.

Theorem 2.5. *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. 2.2) 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 also need the additional property that the constant term in g is finite.

Proof. Note that the min-plus polynomials $(f_i \oplus g_i, f_i)$ and $(f_i, f_i \oplus g_i)$ can be obtained as algebraic combinations as follows: the former one is obtained as a tropical sum of (g_i, ∞) and $(0, 0) \odot f_i$, and the latter one is obtained as a tropical sum of (f_i, g_i) and $(0, 0) \odot f_i$.

Apply Theorem 2.3 to the symmetric system that contains $(f_i \oplus g_i, f_i)$ and $(f_i, f_i \oplus g_i)$ for each min-plus polynomial (f_i, g_i) of the original system.

In the algebraic combination provided by this theorem, expand the algebraic combinations for the initial polynomials. Note that this expansion does not change the algebraic combination (the resulting two polynomials) at all. Thus it satisfies the requirements on its terms. □

Definition 2.6 (Min-Plus Nullstellensatz, `MP-NS`)**.** We will call a min-plus algebraic combination (that is, $(t_j)_{j=1}^{K}$ in terms of the definition) satisfying the conditions of this theorem (over $\mathbb{Q}_\infty$, unless otherwise stated) a *Min-Plus Nullstellensatz (`MP-NS`)* refutation of S.

Note 2.7 (The $0 \leqslant c$ "axiom")*.* In Theorem 2.5 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 2.8 (`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 a 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 maximum size of a coefficient in the system and (f, g) (be it the binary or the unary representation), and their degree does not exceed the degree of monomials in f and g.*

Proof. Note that every monomial that has been generated in the algebraic combination as $f_i \odot m_j$ or $g_i \odot m_j$ remains present in f or g (perhaps, with a different coefficient). Thus, we search for polynomials q_i such that $f = \bigoplus_i f_i \odot q_i$ and $g = \bigoplus_i g_i \odot q_i$, and $q_i = \bigoplus_k c_{i,k} \oplus r_k$, where $c_{i,k} \in \mathbb{Q}_\infty$, and r_k' are all formal quotients of the form s/s' for s a monomial in (f, g) and s' a monomial in (f_i, g_i) (for some i) that are indeed monomials.

Take a term $t = d_t \odot n_t$ in f, where d_t is a constant and n_t is a monomial. It must be obtained as $\bigoplus_{i,k} c_{i,k} \odot n_{i,t,k} \odot r_k$, where $c_{i,k}$ is a constant, and $n_{i,t,k} = n_t/r_k$, if this is a correct monomial in f_i (and let us call the corresponding constant $d_{i,t,k}$), or $= \infty$, otherwise. The constants $c_{i,k}$ must satisfy $d_t = \bigoplus_{i,k} c_{i,k} \odot d_{i,t,k}$. Let us adopt the same notation with primes ($'$) for terms in g (with respect to g_i's). We thus obtain a min-plus linear system of equations (also called one-sided min-plus linear system)

$$\begin{aligned} \bigoplus_{i,k} d_{i,t,k} \odot c_{i,k} &= d_t \text{ for each } t \text{ in } f, \\ \bigoplus_{i,k} d'_{i,t,k} \odot c_{i,k} &= d_{t'} \text{ for each } t' \text{ in } g, \end{aligned}$$

over $\mathbb{Q}_\infty$, where $c_{i,k}$'s are the variables. The dimensions of the matrix of this system are polynomial in the sum of the numbers of monomials in $f, g, (f_i)_i, (g_i)_i$, and its entries are coefficients of the terms in these polynomials.

Let us rename the indices and consider one-sided min-plus linear system

$$\bigoplus_{1\leqslant j\leqslant n} a_{i,j}\odot z_j = b_i,\ 1\leqslant i\leqslant m. \tag{2}$$

One can test solvability of (2) within polynomial complexity and produce its solution, provided that (2) is solvable, as follows. For each $1\leqslant j\leqslant n$, find the minimal $z_j^{(0)}$ such that $a_{i,j}+z_j^{(0)}\geqslant b_i$ holds for every $1\leqslant i\leqslant m$ (if $a_{i,j}=\infty$ for all $1\leqslant i\leqslant m$, then we put $z_j:=\infty$). One can directly verify that (2) is solvable iff $(z_1^{(0)},\dots,z_n^{(0)})$ is its solution.

As $z_j^{(0)}$'s are differences between some $a_{i,j}$'s and b_i's, their bit-size, as well as the unary representation size, is bounded by a polynomial in the respective size of the coefficients of the input system. □

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 [Kra98]: 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 2.9 (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 $m=x_1^{\odot j_1}\odot\cdots\odot x_n^{\odot j_n}$ 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 2.10 (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.

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

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

$$\frac{\emptyset}{p\leqslant\infty},\ \text{for any tropical polynomial } p. \tag{WEAK}$$

   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 2.11 (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 2.12 (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 2.13 (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 together with the minimum rule and substitution of the right.

Note 2.14 (Systems based on equations instead of inequalities). Similarly to Theorem 2.3, 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 the refutation system $\texttt{MP-PC}_=$ 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 Appendix A). As inequalities provide a more natural framework and allow to refute more unsolvable systems, we stick to using inequalities.

2.4 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+`($\odot$`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.

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

While this rule is looking very natural, we do not know how to eliminate its use at a polynomial cost. Moreover, we show that its direct simulation in static proof systems is impossible (Theorems 7.3 and 7.5).

2.5 Previously known proof systems

For the sake of self-containedness, we provide the definitions of several known proof systems. In what follows we typically denote literals (which are variables or the negations of variables) by $\ell, \ell_1, \ell_2, \ldots$, and variables by $x, x_1, \ldots, v, v_1, \ldots$ without further notice.

`Res(CP)`-like systems. Krajíček [Kra98] suggested the `Res(CP)` system (also known as `Res(CP)`), which works with disjunctions of inequalities. Later, more systems of this kind have been defined.

One considers two kinds of such systems: with coefficients written in binary and with coefficients written in unary, in the latter case a superscript * or ^{1} is applied.

Definition 2.15 (Resolution over Linear Programming, `Res(LP)` [HK06])**.** Consider a system of linear inequalities $F = \{g_1 \geqslant 0, g_2 \geqslant 0, \ldots, g_m \geqslant 0\}$. A ***Res(LP)** derivation* from F is a sequence of disjunctions of linear inequalities with the following inference rules:

Axioms.

$$\frac{\emptyset}{g_i \geqslant 0}, \text{ where } 1 \leqslant j \leqslant m,$$

$$\frac{\emptyset}{x \geqslant 0}, \qquad \frac{\emptyset}{1 - x \geqslant 0},$$

$$\frac{\emptyset}{(x - 1 \geqslant 0) \ \vee \ (-x \geqslant 0)}. \tag{BOOL}$$

Linear combination, or Resolution by a pair of inequalities.

$$\frac{(f_1 \geqslant 0) \vee \Gamma \qquad (f_2 \geqslant 0) \vee \Gamma}{(\alpha_1 f_1 + \alpha_2 f_2 \geqslant 0) \vee \Gamma}, \tag{+RES}$$

where α_1, α_2 are positive constants.

Weakening.

$$\frac{\Gamma}{\Gamma \vee (f \geqslant 0)}.$$

Simplification. We will treat disjunctions as sets formally using the rule

$$\frac{\Gamma \vee (f \geqslant 0) \vee (f \geqslant 0)}{\Gamma \vee (f \geqslant 0)},$$

which we will not mention explicitly.

A `Res(LP)` refutation of F is a `Res(LP)` derivation of $-1 \geqslant 0$ from F.

As a *propositional* proof system, `Res(LP)` refutes a formula in CNF by refuting its translation to inequalities: a clause $\ell_1 \vee \ldots \vee \ell_k$ is translated to $[\ell_1] + \ldots + [\ell_k] \geqslant 1$, where $[x] = x$ and $[\neg x] = 1 - x$ for a variable x.

When the coefficients in the affine forms are represented in binary, one can distinguish between the systems with integer or rational coefficients. In what follows, we assume that all coefficients in `Res(LP)` and its versions are integers.

Definition 2.16 (`Res(CP)` [Kra98])**.** `Res(CP)` augments `Res(LP)` with two rules:

$$\frac{\emptyset}{f - 1 \geqslant 0 \vee -f \geqslant 0}, \tag{INT}$$

$$\frac{\sum_i ca_i x_i - d \geqslant 0 \vee C}{\sum_i a_i x_i - \lceil d/c \rceil \geqslant 0 \vee C}, \tag{RO}$$

where $c, d, a_i \in \mathbb{Z}$ and C is any disjunction of inequalities. (Note that we round to the nontrivial direction.)

Note 2.17 (On (`RO`), (`INT`) and versions of `Res(CP*)`). It can be easily seen that (`RO`) is superfluous and can be polynomially simulated using (`INT`). On the other hand, a version of `Res(CP)` with (`RO`) and without (`INT`) has been considered in [HK06]. They concerned the unary setting only, where it does not matter because the unary version of (`INT`) can be derived step by step using (`BOOL`). In the unary setting `Res(CP*)` and `Res(LP*)` are polynomially equivalent [HK06, Proposition 2].

Res-k. A proof system working with disjunctions of conjunctions was introduced by Krajíček [Kra01]. A definition similar to ours can be found, for example, in [Lau18]; however, we do weakening steps explicitly in order for cut steps to look simpler.

Definition 2.18 (k-DNF Resolution, `Res(`k`)` [Kra01])**.** A proof system `Res(`k`)` operates with k-DNFs. A *`Res(`k`)` refutation* π of an unsatisfiable CNF formula ϕ is an ordered sequence of k-DNFs $\pi = C_1, C_2, \ldots, C_s$ such that $C_s = \emptyset$ is the empty formula. Each C_i either comes from the original formula or is inferred using one of the rules:

$$\frac{\emptyset}{(\ell_1 \wedge \ell_2 \wedge \ldots \wedge \ell_m) \vee \neg\ell_1 \vee \neg\ell_2 \vee \ldots \vee \neg\ell_m}, \tag{Axiom}$$

$$\frac{A \vee (\ell_1 \wedge \ell_2 \wedge \ldots \wedge \ell_m) \quad A \vee \neg\ell_1 \vee \neg\ell_2 \vee \ldots \vee \neg\ell_m}{A}, \tag{Cut}$$

$$\frac{A}{A \vee \ell}. \tag{Weakening}$$

The size of the proof π is the sum of the sizes of C_i.

One can also consider `Res(`k`)` without the restriction on k. Instead of the bounded-depth Frege terminology, we call it `Res(`∞`)` to avoid ambiguity. One can notice that it is a particular case of `Res(LP*)`.

2.6 Encoding of Boolean logic and `MP-NSE`, `MP-PCE`, `MP-NSR`, and `MP-PCR` systems

Economic encoding. We can translate Boolean variables to $\{0, 1\}$ by introducing, for every variable x, the axiom

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

or to $\{0, \infty\}$ by introducing the axiom

$$\frac{\emptyset}{x^{\odot 2} = x}. \tag{0∞/E}$$

We treat 0 as `false`, and 1 and ∞ as `true`. Note that $x \leqslant 1$ follows (in `MP-PC` from (01/E) by weakening, and in `MP-NS` extra terms on the right do not harm at all), while $x \geqslant 0$ does not seem to be derivable from (01/E) (see Prop. 7.1) or (0∞/E). (Still, $x^2 \geqslant x$ can be used as a moral equivalent of $x \geqslant 0$ in both cases.) A Boolean clause $x_1 \vee \ldots \vee x_k \vee \neg y_1 \vee \ldots \vee \neg y_m$ can be translated then as

$$y_1 \oplus \ldots \oplus y_m \leqslant x_1 \odot \ldots \odot x_k. \tag{DE}$$

For $\{0,1\}$ variables an alternative translation is

$$y_1 \odot \ldots \odot y_m \leqslant x_1 \odot \ldots \odot x_k \odot (m-1), \tag{IE}$$

which may be not equivalent to (DE). Using these translations with `MP-NS` and `MP-PC` we obtain *propositional* proof systems `MP-NSE` and `MP-PCE`, respectively, for the language of unsatisfiable formulas in CNF. By default we will be working with the $\{0,1\}$ encoding for the truth value, and will mention the $\{0,\infty\}$ encoding explicitly. If one uses this encoding for a formula in CNF, it is important to mention a specific representation of clauses (DE)/(IE) explicitly.

However, most of this paper is devoted to a richer encoding resulting in stronger and more convenient systems. In Theorem 3.10 we prove that for daglike proofs this richer encoding over $\{0,1\}$ can be polynomially simulated by economic encoding, but the situation with treelike proofs is more tricky and is left for further research.

Dual variable encoding. In this encoding we introduce a "dual variable" for the negation. 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.

Encoding by $\{0,\infty\}$. We include the axioms

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

to ensure that x and $\overline{x}$ are dual and in $\{0,\infty\}$. Note that $(0\infty/E)$ easily follows for both x and $\overline{x}$ (from $x \oplus \overline{x} = 0$ we can derive $(x \odot x) \oplus (x \odot \overline{x}) = x$, from which we can derive $(x \odot x) \oplus \infty = x$, which is equivalent to $x \odot x = x$).

Encoding by $\{0,1\}$. We include the axioms

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

to ensure that x and $\overline{x}$ are dual and in $\{0,1\}$. Again, (01/E) follows for both x and $\overline{x}$.

Note 2.19. 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 $x \odot \overline{x} \leqslant 1$.

In both cases of $\{0,1\}$ and $\{0,\infty\}$ 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)` [RT08] 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, in the $\{0,1\}$ case 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. We delay the proof to Lemma 3.5 to introduce all the required machinery first.

3 Preparatory statements about tropical systems and `Res(LP)`

In this section we prepare formal grounds for further results.

First of all, we prove that we can assume that `Res(LP)` works with integer coefficients as well as with rational coefficients. (This is important, because tropical systems work naturally with rational coefficients, moreover, one cannot avoid using rational coefficients in tropical systems refutations.)

Then we prove several general statements about tropical proofs. We start with proving auxiliary lemmas mostly about treelike proofs (and also the promised equivalence of (D) and (I)).

Eventually, we proceed to showing that the last line in `MP-PCR` does not need to be as complex as in the definition: it can be simply $1 \leqslant 0$.

3.1 Integer vs rational coefficients in `Res(LP)`

We now prove formally that `Res(LP)` with integer coefficients polynomially simulates `Res(LP)` with rational coefficients. In order to do so, we need to multiply each affine form f in the derivation by an appropriate integer constant C, such $C \cdot f$ is an integer affine form. Let $\texttt{Res(LP}_{\mathbb{Z}}\texttt{)}$ be the system that uses only integers in its proof lines (the division is permitted as long as it does not result in non-integral coefficients), and $\texttt{Res(LP}_{\mathbb{Q}}\texttt{)}$ be `Res(LP)` with rational coefficients.

Proposition 3.1. *$\texttt{Res(LP}_{\mathbb{Z}}\texttt{)}$ polynomially simulates $\texttt{Res(LP}_{\mathbb{Q}}\texttt{)}$.*

Proof. We will simulate $\texttt{Res(LP}_{\mathbb{Q}}\texttt{)}$ in $\texttt{Res(LP}_{\mathbb{Z}}\texttt{)}$ by induction. Suppose C is a product of all nominators and denominators occurring in the $\texttt{Res(LP}_{\mathbb{Q}}\texttt{)}$ derivation. We will show that for each clause Γ_i, which was derived at the i-th step of $\texttt{Res(LP}_{\mathbb{Q}}\texttt{)}$ derivation, we can derive $C^i \cdot \Gamma_i$ in $\texttt{Res(LP}_{\mathbb{Z}}\texttt{)}$ derivation, where $C^i \cdot \Gamma_i$ denote the disjunction of inequalities from Γ, multiplied by C^i.

For the axioms, we can trivially do so. Now suppose we derived in $\texttt{Res(LP}_{\mathbb{Z}}\texttt{)}$

$$C \cdot \Gamma_1, C^2 \cdot \Gamma_2, \cdots, C^k \cdot \Gamma_k.$$

We want to derive $C^{k+1} \cdot \Gamma_{k+1}$. If we want to apply a weakening or simplification rule or derive one of the axioms, we simply do it, and multiply the result by the appropriate constant.

Finally, if we need to simulate the resolution rule, we will do the following: we need to derive from

$$(C^r \cdot f_1 \geqslant 0) \vee C^r \cdot \Gamma \text{ and } (C^m \cdot f_2 \geqslant 0) \vee C^m \cdot \Gamma$$

the disjunction

$$\left(\frac{C^{k+1}\cdot\alpha_1}{\beta_1}f_1+\frac{C^{k+1}\cdot\alpha_2}{\beta_2}f_2\geqslant 0\right)\vee C^{k+1}\cdot\Gamma.$$

We do it in two steps: first, we multiply $C^r\cdot\Gamma$ and $C^m\cdot\Gamma$ by C^{k+1-r} and C^{k+1-m}, respectively. This operation produces two clauses:

$$(C^r\cdot f_1\geqslant 0)\vee C^{k+1}\cdot\Gamma \text{ and } (C^m\cdot f_2\geqslant 0)\vee C^{k+1}\cdot\Gamma.$$

After that, since C is a product of all constants in the original derivation, $\frac{C^{k+1}\cdot\alpha_1}{C^r\cdot\beta_1}$ and $\frac{C^{k+1}\cdot\alpha_2}{C^m\cdot\beta_2}$ are integers, and we can apply the resolution rule in $\texttt{Res(LP}_{\mathbb{Z}}\texttt{)}$ to the aforementioned two clauses with those constants to get

$$\left(\frac{C^{k+1}\cdot\alpha_1}{C^r\cdot\beta_1}C^r\cdot f_1+\frac{C^{k+1}\cdot\alpha_2}{C^m\cdot\beta_2}C^r\cdot f_2\geqslant 0\right)\vee C^{k+1}\cdot\Gamma,$$

which completes the induction step.

Observe that the bit-size of our constants is at most polynomial, so the size of resulting derivation is at most polynomial in the size of the initial derivation. □

3.2 Preliminary lemmas and the equivalence of encodings

Lemma 3.2 (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*

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

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

If A_i, B_i have integer coefficients written in unary, then so does the derivation. In any case (unary integer or binary rational coefficients), 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 $j=3,\dots,k$, 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 3.3 (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:*

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

$$b\ \leqslant\ x^{\odot b}\odot\overline{x}^{\odot b}, \tag{4}$$

$$x^{\odot b}\oplus\overline{x}^{\odot i}\ \leqslant\ 0 \textit{ (as well as of the symmetrical inequality), for } 1\leqslant i\leqslant b. \tag{5}$$

The tropical degree of these derivations is $O(b)$. The derivations of (3), (4) contain $O(b)$ (not necessarily distinct) terms, all the coefficients in them and constants are $\leqslant b$. The derivation of (5) contains $O(b^3)$ (not necessarily distinct) terms, all the coefficients in it are zeroes.

Proof. The inequalities (3) and (4) follow from Lemma 3.2.

To show (5) 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 3.2, multiplied by $\overline{x}$) into its left-hand side getting

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

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 (5), 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

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

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 3.2, multiplied by $x^{\odot b}$) on the left. $\square$

Lemma 3.4 (Boolean cut inside the sum, treelike, any encoding)**.** *There is a polynomial-size unary treelike* `MP-PC` *derivation of*

$$\ell_1 \odot \ell_2 \odot \cdots \odot \ell_k \oplus \overline{\ell}_1 \oplus \overline{\ell}_2 \oplus \cdots \oplus \overline{\ell}_k \leqslant \ell_2 \odot \cdots \odot \ell_k \oplus \overline{\ell}_2 \oplus \cdots \oplus \overline{\ell}_k \tag{6}$$

and hence

$$\ell_1 \odot \ell_2 \odot \cdots \odot \ell_k \oplus \overline{\ell}_1 \oplus \overline{\ell}_2 \oplus \cdots \oplus \overline{\ell}_k = 0 \tag{7}$$

from the axioms $x \oplus \overline{x} = 0$ for every variable x. (Thus it works over both $\{0,1\}$ and $\{0,\infty\}$ encoding.)

Proof. Derive

$$\ell_1 \odot \ell_2 \odot \cdots \odot \ell_k \oplus \overline{\ell}_1 \oplus \overline{\ell}_2 \oplus \cdots \oplus \overline{\ell}_k \leqslant \ell_1 \odot \ell_2 \odot \cdots \odot \ell_k \oplus \overline{\ell}_1 \oplus \overline{\ell}_2 \oplus \cdots \oplus \overline{\ell}_k \tag{8}$$

from $0 \leqslant 0$. Observe that by multiplication we can derive from $\overline{\ell}_1 \oplus \ell_1 \leqslant 0$ that

$$\overline{\ell}_1 \odot \ell_2 \odot \cdots \odot \ell_k \oplus \ell_1 \odot \ell_2 \odot \cdots \odot \ell_k \leqslant \ell_2 \odot \cdots \odot \ell_k,$$

from which by using $\overline{\ell}_1 \leqslant \overline{\ell}_1 \odot \ell_2 \odot \cdots \odot \ell_k$ (which is a tropical product of $0 \leqslant \ell_i$ derived by Lemma 3.2 multiplied further by $\overline{\ell}_1$) we can derive

$$\overline{\ell}_1 \oplus \ell_1 \odot \ell_2 \odot \cdots \odot \ell_k \leqslant \ell_2 \odot \cdots \odot \ell_k.$$

Substituting this into the right-hand side (RHS) of (8) we get (6). Continuing in the same way, we get the following chain of inequalities:

$$\bigoplus_{i=1}^{k} \overline{\ell}_i \leqslant \bigodot_{j=1}^{k} \ell_j \oplus \bigoplus_{i=1}^{k} \overline{\ell}_i \leqslant \bigodot_{j=2}^{k} \ell_j \oplus \bigoplus_{i=2}^{k} \overline{\ell}_i \leqslant \ldots \leqslant \ell_k \oplus \overline{\ell}_k \leqslant 0.$$

The opposite inequality in (7) is easy as it is a tropical sum of $0 \leqslant \overline{\ell}_i$ and the product of $0 \leqslant \ell_i$ provided by Lemma 3.2. $\square$

Lemma 3.5 ($(D) \leftrightarrow (I)$)**.** *There are polynomial-size unary treelike derivations of encodings* (D) *and* (I) *from each other in* MP-PCR *with* $\{0,1\}$*-encoding of Boolean variables.*

Proof. (D) *to* (I). Multiply (D) by $\ell_1 \odot \ell_2 \odot \cdots \odot \ell_k$ obtaining

$$\bigoplus_i \ell_i \odot \bar{\ell}_i \odot \bigodot_{j \neq i} \ell_j \leqslant \ell_1 \odot \ell_2 \odot \cdots \odot \ell_k.$$

The right-hand side (RHS) is already as needed. Use the axiom $1 \leqslant \ell_i \odot \bar{\ell}_i$: multiply it by $\bigodot_{j \neq i} \ell_j$ and make a substitution in the left-hand side (LHS) getting

$$\bigoplus_i 1 \odot \bigodot_{j \neq i} \ell_j \leqslant \ell_1 \odot \ell_2 \odot \cdots \odot \ell_k.$$

Eliminate the remaining products of ℓ_i's from the LHS by using a substitution of the respective products of $0 \leqslant \ell_i$ and 1 using Lemma 3.2.

(I) *to* (D). Take a sum of (I) with $\bar{\ell}_1 \oplus \bar{\ell}_2 \oplus \cdots \oplus \bar{\ell}_k \leqslant \bar{\ell}_1 \oplus \bar{\ell}_2 \oplus \cdots \oplus \bar{\ell}_k$ obtaining

$$\bar{\ell}_1 \oplus \bar{\ell}_2 \oplus \cdots \oplus \bar{\ell}_k \oplus 1 \leqslant \ell_1 \odot \ell_2 \odot \cdots \odot \ell_k \oplus \bar{\ell}_1 \oplus \bar{\ell}_2 \oplus \cdots \oplus \bar{\ell}_k \tag{I'}$$

Observe that $\bar{\ell}_1 \leqslant \bar{\ell}_1 \oplus 1$, so we can transform the LHS into $\bar{\ell}_1 \oplus \bar{\ell}_2 \oplus \cdots \oplus \bar{\ell}_k$.

It remains to transform the RHS into 0 using Lemma 3.4.

The opposite inequality in (D) is trivial as it is a tropical sum of $0 \leqslant \bar{\ell}_i$. □

Therefore, MP-PCR (even treelike) with $\{0,1\}$ encoding is the same propositional proof system for the language of unsatisfiable formulas in CNF irrespectively of the clause encoding ((D) vs (I)). A similar (though not literally equivalent) claim can be made for MP-NSR by making use of Theorem 4.1.

3.3 The last line in MP-PCR can be simplified to $1 \leqslant 0$

In fact, the last line in a MP-PCR proof (actually, in any MP-PC proof using nonnegative variables) does not need to be that complex as in the definition: it can be simply $1 \leqslant 0$. To show this, we start with the unary case (either treelike or daglike) and continue with the binary daglike case. This works for any nonnegative variables.

We start with two technical lemmas.

Lemma 3.6 (tropical power, daglike)**.** *Let* A, B *be tropical terms, and* $k \geqslant 1$ *be an integer. Then there is a* MP-PC *derivation of the inequality*

$$A^{\odot k} \leqslant B^{\odot k}$$

along with all the inequalities

$$A^{\odot 2^i} \leqslant B^{\odot 2^i} \text{ (for } i = 1, \ldots, \lfloor \log_2 k \rfloor\text{)}$$

from the inequality $A \leqslant B$*. The number of terms in the proof is* $O(\log_2 k)$*, and the bit-size of coefficients and degrees is at most* $O(\log_2^2 k)$ *times larger than the bit-size of coefficients and degrees in* $A \leqslant B$*.*

Proof. Consider the binary expansion $k = \sum_{i=0}^{d} 2^i b_i$, where $b_i \in \{0,1\}$ and $b_d = 1$. Use Lemma 3.2 for $A \leqslant B$, $A \leqslant B$ to obtain $A^{\odot 2} \leqslant B^{\odot 2}$; then use it for $A^{\odot 2} \leqslant B^{\odot 2}$ to obtain $A^{\odot 4} \leqslant B^{\odot 4}$, etc, until we get to $A^{\odot 2^d} \leqslant B^{\odot 2^d}$. Every use of the lemma takes $O(1)$ terms with coefficients and degrees bit-sizes $O(c)$, where c is the bit-size of the coefficients and degrees in A^i and B^i. The coefficients in $A^{\odot i}$ and $B^{\odot i}$'s are simply multiplied by 2^i, thus the final size of the coefficients and degrees is $O(cd)$, and the number of terms in this proof is $O(d)$.

Use Lemma 3.2 to multiply tropically the obtained inequalities for those powers 2^i where $b_i = 1$. It adds $O(d)$ terms to the proof and the bit-size of the coefficients and degrees is at most $O(d{\cdot}cd)$. □

For every tropical polynomial $p = \bigoplus_i c_i \odot m_i$, where c_i are constants and m_i are pairwise distinct monomials, define

$$\mathrm{lb}(p) := \min_i c_i.$$

Obviously, for nonnegative variables this is the lower bound on the value of p.

Lemma 3.7 (tropical polynomial, estimated from below)**.** *For a tropical polynomial p, we can derive $\mathrm{lb}(p) \leqslant p$ from the inequalities $0 \leqslant x$ for every variable x*

(1) in `treelike` `MP-PC` using $O(\mathrm{degtr}(p)\mu(p))$ additional terms of degree $O(\mathrm{degtr}(p))$, and the coefficients in the derivation will be among 0 and the coefficients of p;

(2) in `MP-PC` using $O(\log_2 \mathrm{degtr}(p) + n)$ additional terms, where n is the number of variables; the coefficients and the degrees in the derivation will have bit-size $O(c \cdot \log_2^2 \mathrm{degtr}(p))$, where c is the bit-size of the coefficients and the degrees in p.

Proof. (1) Use Lemma 3.2 for the axioms to derive $0 \leqslant m$ for any monomial m, further use the multiplication by constants c_i, and the minimum rule.

(2) Use Lemma 3.6 for taking powers of the variables, then tropically multiply them using Lemma 3.2. Further use the multiplication by constants c_i, and the minimum rule. □

Theorem 3.8 (last line, simplified)**.** *Given the last line $\Gamma \leqslant \Delta$ according to the definition of an `MP-PC` refutation (with any encoding that has $O(1)$-size derivations of the nonnegativity statements $0 \leqslant x$ for variables), there is a polynomial-size derivation of $1 \leqslant 0$ in `MP-PC` from this last line and the nonnegativity statements:*

(1) in the treelike mode, with coefficients and degrees written in unary,

(2) in the daglike mode, with coefficients and degrees written in binary.

Proof. Note that by substituting (`WEAK`) on the right-hand side of the last line of a `MP-PC` refutation we can always assume that the last line has the form

$$\bigoplus_i a_i m_i \leqslant \bigoplus_i b_i m_i, \tag{9}$$

where m_i's are monomials, $a_i > b_i$ are constants and a_0, b_0 are the constant terms (all of the constants here except (possibly) a_0 are finite.

Let $\varepsilon := \min_{i \geqslant 0}(a_i - b_i) > 0$. The value of ε may be as small as $\Omega(1/\nu^2)$, where ν is the maximum absolute value of a denominator in the last line.

We now treat the two items of the statements separately. In both cases we reduce the general situation to much easier cases and then treat them together.

Namely, for the general case assume two conditions:

- the last line has non-constant terms, and
- $\min_i(a_i) \leqslant b_0$.

(The cases where one of these conditions is false are considered to be easier and are treated later.)

1. The unary treelike case. We substitute $\varepsilon \odot b_i \leqslant a_i$ multiplied by m_i to the left-hand side of our last line getting

$$\varepsilon \odot \bigoplus_i b_i m_i \leqslant \bigoplus_i b_i m_i.$$

Let $E := \bigoplus_i b_i m_i$.

Now $\mathrm{lb}(E) \leqslant \mathrm{lb}(A) \leqslant b_0$. For $i = 1, \ldots, \lceil (b_0 - \mathrm{lb}(E))/\varepsilon \rceil$, tropically multiply the obtained inequality $\varepsilon \odot E \leqslant E$ by $\varepsilon^{\odot i}$ and substitute all the obtained inequalities into each other getting

$$\varepsilon \odot L \odot E \leqslant \ldots \leqslant (3\varepsilon) \odot E \leqslant (2\varepsilon) \odot E \leqslant \varepsilon \odot E \leqslant E, \tag{10}$$

where $L = \lceil (b_0 - \mathrm{lb}(E))/\varepsilon \rceil \cdot \varepsilon \geqslant b_0 - \mathrm{lb}(E)$ is a constant. Substitute to the left-hand side of (10) the inequality $\mathrm{lb}(E) \leqslant E$ provided by Lemma 3.7 and drop the non-constant terms $b_i m_i$ ($i \neq 0$) from the right-hand side using (`WEAK`) obtaining

$$L + \varepsilon + \mathrm{lb}(E) \leqslant b_0.$$

As $L \geqslant b_0 - \mathrm{lb}(E)$, this is a constant inequality with the difference between the sides at least ε.

Assume that the original last line contains K terms, d is its tropical degree, and c is the maximum unary size of a degree or of a nominator or a denominator of a coefficient. The number of terms in this derivation is $O(Kc/\varepsilon) = O(c^2 K)$, and the coefficients and the degrees have the size $O(c)$. Lemma 3.7 adds $O(dK)$ terms of a similar size of the coefficients and degrees.

The binary daglike case. Let $k = \lceil (b_0 - \mathrm{lb}(E))/\varepsilon \rceil$. The proof of the general case proceeds the same way as in the treelike unary case, but we use another item of Lemma 3.7 and perform the derivation of (10) more efficiently: after we derive $(2\varepsilon) \odot E \leqslant E$, we multiply it by 2ε to derive $(4\varepsilon) \odot E \leqslant E$, etc, until we arrive at $\left(2^{\lceil \log_2 k \rceil} \varepsilon\right) \odot E \leqslant E$. It is easy to see that the fact that we arrived at a slightly larger L than before does not matter.

Let c be now the maximum binary size of a degree or of a nominator or a denominator of a coefficient. The number of terms in our derivation is $O(K \log_2 k)$, and the coefficients and the degrees have the bit-size $O(c \cdot \log_2^2 k)$; Lemma 3.7 adds a similar number of terms of a similar bit-size of the coefficients and degrees.

Easier cases. (a) If $\min_i(a_i) > b_0$, we take (9) and substitute to its left-hand side the inequality provided by Lemma 3.7, then we drop the non-constant terms from the right-hand side using (`WEAK`), and arrive at a constant inequality. Obviously, the complexity of this derivation does not exceed the complexity we got in other estimations.

(b) If we have a constant inequality, multiply it tropically by $-b_0$, then proceed to growing the constant on the left (which is at least ε) similarly to the derivation of (10) (this is done differently in the treelike and the daglike cases) in order to make the left-hand side at least 1. Further substitute 1 for the left-hand side if necessary.

Let c be now the size (either unary or binary, whatever is applicable) of the coefficients and the degrees in the original last line. The number of terms in our derivation can be as large as $O(1/\varepsilon) = O(c)$ in the treelike case, and as large as $\lceil \log_2(1/\varepsilon) \rceil = O(c)$ in the binary case. The size of the coefficients and the degrees is also $O(c)$. $\square$

3.4 A note on economic encoding

Most of this paper is devoted to the dual encoding of Boolean logic. However, lower bounds may be easier to prove in the economic encoding. In this subsection we show that derivations in dual encoding can be transformed into derivations in economic encoding at the expense of multiplying the whole proof by a certain monomial.

We start by introducing relevant notation.

Definition 3.9. Let $L(p)$ be the transformation that replaces every pair of contrary variables in a term in p by the constant 1.

For a polynomial or an inequality φ, define $r(\varphi)$ as the product of (positive) variables, each raised to the degree with which the corresponding negative variable occurs in φ.

For example, $L(x \odot y \odot z \odot \overline{x} \odot \overline{y} \oplus (-1/2) \odot z^{\odot 2} \odot \overline{z}^{\odot 2}) = 2 \odot z \oplus (3/2)$ and $r(1 \odot x \odot \overline{y}^{\odot 2} \odot \overline{z}) = y^{\odot 2} \odot z$.

Note that these two functions composed as $L(p \odot r(p))$ eliminate the negative variables from p. We are now ready to transform the derivations.

Theorem 3.10. *1. If*

$$f \leqslant g \tag{11}$$

is derivable in `MP-PCR` (resp., `MP-NSR`) from a set of inequalities $\{f_i \leqslant g_i\}_i$ (and Boolean axioms), then $L(f \odot m \leqslant g \odot m)$ is derivable in `MP-PCE` (resp., `MP-NSE`) from $\{L(f_i \odot m_i \leqslant g_i \odot m_i)\}_i$ and Boolean axioms, where $m_i = r(f_i \leqslant g_i)$ and $m = \prod_x x^{d(x)}$, where x ranges over all variables, and $d(x) = d_0(x) + \max_J \sum_{j \in J} d_j(x)$, where d_0 is the maximum degree of $\overline{x}$ in the input axioms and Boolean axioms, d_j is the degree of $\overline{x}$ in the j-th application of the tropical multiplication rule, and J is a set of possible numbers j that ranges over all paths from an axiom to (11).

The number of steps in this transformation increases linearly, the degree increases as stated above (that is, also linearly), and the coefficients increase linearly as well.

2. `MP-PCE` with (IE) translation polynomially simulates `MP-PCR`. `MP-NSE` with (IE) translation polynomially simulates `MP-NSE` with (I) translation when the degree of the original proof is polynomial.

Proof. 1. First of all, we transform the `MP-PCR` proof by the induction on its construction into a `MP-PCR` proof satisfying the condition of Claim 1 without L.

For the induction base, we multiply each initial inequality φ (including the Boolean axiom $x \oplus \overline{x} = 0$ but excluding the Boolean axiom $x \odot \overline{x} = 1$) by $r(\varphi)$. To prove the induction step, consider three cases regarding what was the last step of the `MP-PCR` derivation of $f \leqslant g$:

Product. We replace the multiplication by p by the multiplication by $p \odot r(p)$. This adds exactly the respective $d_j(x)$ to the degree of each variable x by the definition of r.

Minimum. Given $f_i \leqslant g_i$ and $f_k \leqslant g_k$ in the original proof, and $f_i \odot m_i \leqslant g_i \odot m_i$ and $f_k \odot m_k \leqslant g_k \odot m_k$ by the induction hypothesis, we multiply them by M/m_i and M/m_k respectively, where $M = \mathrm{lcm}(m_i, m_k)$. After that, we take the minimum.

Transitivity. Given $f_i \leqslant g_i$ and $g_i \leqslant g_k$ in the original proof, and $f_i \odot m_i \leqslant g_i \odot m_i$ and $g_i \odot m_k \leqslant g_k \odot m_k$ by the induction hypothesis, we multiply them by M/m_i and M/m_k respectively, where $M = \mathrm{lcm}(m_i, m_k)$. After that, we use the transitivity rule.

It is easy to see that if we replace each inequality $f' \leqslant g'$ in this proof by $L(f' \leqslant g')$, it will become a valid MP-PCE derivation. What happens to the Boolean axioms? One of them was multiplied by x, and is now transformed into the Boolean axiom for the economic encoding $L(x\odot x\oplus x\odot\overline{x} = x) = (x^{\odot 2}\oplus 1 = x)$; the other one became the trivial axiom $L(x\odot\overline{x} = 1) = (1 = 1)$.

There is nothing specific to daglike computations in this proof, so the result holds for the treelike case (and, through Theorem 4.1, for MP-NSR vs MP-NSE) as well.

2. Note that (I) transforms into (DI).

To conform to the definition of tropical proofs over $\mathbb{Q}_\infty$ (and get rid of the all-∞ solution) we must obtain a finite constant in the right-hand side of the final inequality. We use the $x \leqslant 1$ part of the axiom $x \leqslant x^{\odot 2} \oplus 1$ in order to do this: take a term that is already present in the last line of our proof and add the proof of its upper bound into the linear combination (multiplying it by a small constant, if necessary).

In MP-PCE, we get rid of $x^{\odot 2}$ in the axiom by dropping it using $x^{\odot 2} \leqslant \infty$; then this upper bound (for any term) is proved efficiently using Lemmas 3.2 and 3.6. For the treelike case we have to use Lemma 3.2, therefore the number of steps is proportional to the degree of the smallest degree monomial in the last line of the (transformed) proof. We then convert a treelike proof into a linear combination using Theorem 4.1. □

Remark 3.11 (Proofs over $\mathbb{Q}_\infty$ vs $\mathbb{Q}$). For MP-NSE, if we formulated Theorem 3.10 over $\mathbb{Q}$ instead of $\mathbb{Q}_\infty$, we would have the same complexity bound in Claim 2 as for MP-PCE (the only difference for MP-NS over $\mathbb{Q}$ is the absence of the requirement to have a finite constant in the right-hand side of the linear combination, cf. Theorem 2.5 and Definition 2.6). However, over $\mathbb{Q}_\infty$ we need to have a finite constant on the right-hand side, and it is not possible to simply upper bound a (potentially exponential) degree monomial efficiently, cf. Theorem 7.15. This does not exclude alternative ways for the simulation.

Remark 3.12. Note that Theorem 3.10 does not apply to systems using ($\odot$RES), as this rule multiplies two terms. However, for a generalization of ($\odot$RES)

$$\frac{t\odot m \oplus f\odot m \leqslant m \qquad t'\odot m \oplus f\odot m \leqslant m}{t\odot t'\odot m^{\odot 2} \oplus f\odot m^{\odot 2} \leqslant m^{\odot 2}},\ \text{where } t, t' \text{ are terms, and } m \text{ is a monomial,}$$

an analogue of Theorem 3.10 holds for MP-PCR (vs MP-PCE) extended with this generalized rule at the expense of replacing $d(x)$ by $d(x)\cdot 2^s$, where s is the maximum number of resolution steps on a path from a leaf to the root in the input proof, as each time the degree doubles.

4 The power of static tropical proofs

When discussing the coefficients in this section, we mean finite coefficients unless otherwise stated.

4.1 Min-Plus Nullstellensatz vs treelike Min-Plus Polynomial Calculus

In this subsection we are not using any Boolean axioms, the statements are very general. It is intuitively clear that MP-NS has a flavour of a treelike version of MP-PC, in particular, an MP-NS proof serves as an MP-PC proof. The next statement makes the converse formal (though the coefficients bit-size may become linear in the size of the proof).

Theorem 4.1. *1. Assume that there is an s-step* **`treelike`** *MP-PC derivation* $p_1 \leqslant q_1, \ldots, p_s \leqslant q_s$. *Let* $R > 0$ *be an integer, and let* $c_s = 1/R$. *Then there is an algebraic combination of the input inequalities used in this derivation that evaluates to*

$$\Gamma \oplus p_s^- \leqslant q_s^+ \oplus \Delta,$$

where the tropical polynomial $p_s^- \succeq p_s$, *the tropical polynomial* $q_s^+ \preceq q_s \odot c_s$, *the monomials in* p_s^- *and* q_s^+ *can possibly occur in* $\Gamma \succ \Delta$, *and the bit-size of this algebraic combination is bounded by a polynomial in the bit-size of the original MP-PC derivation both when the coefficients and the tropical exponents are written in unary (both nominators and the denominator, the latter being the same for all coefficients in the proof), and when they are written in binary.*

2. As proof systems for the language of min-plus polynomial systems that have no roots,

(a) MP-NS polynomially simulates **`treelike`** *MP-PC,*

(b) when coefficients (both nominators and the denominator, the latter being the same for all coefficients in the proof) and tropical exponents are written in unary, MP-NS still polynomially simulates **`treelike`** *MP-PC.*

Proof. 1. We proceed by induction on the construction of the proof. The base (input inequalities) is trivial. Assume that for every $i' \leqslant i - 1$, we have already constructed an algebraic combination

$$\Gamma \oplus p^- \leqslant q^+ \oplus \Delta, \tag{12}$$

for every inequality $p \leqslant q$ that took at most i' steps to derive in the original `treelike MP-PC` derivation (that is, its proof tree contained at most $i' + 1$ nodes). Here $\Gamma \succ \Delta$, the tropical polynomial $p^- \succeq p$, and $q^+ \preceq q \odot c_{i'}$, where $c_j = j/(sR)$. Further, assume that

- the number of different monomials in (12) is at most the number of different monomials in the original derivation of $p \leqslant q$,
- the maximum tropical degree of monomials in (12) is the maximum tropical degree of monomials in the original derivation plus the sum of the degrees of terms in the multiplication rules along a path from a leaf (an input inequality) to the root ($p \leqslant q$),
- each coefficient in (12) is of the form $a + \sum_{a'}(a' + a'')$, where $a = k/(sR)$ (for some integer k, $0 \leqslant k \leqslant s$), a' is an instance of a coefficient in the original subproof, and a'' is the sum of the coefficients appearing in the terms by which we tropically multiply on a path from the node where a' occurs to the root ($p \leqslant q$).

We now prove that we can do the same for an inequality that has an i-step `treelike MP-PC` derivation. Assume that its premises have been derived using i_1 and i_2 (if applicable) steps, respectively. We consider all possible rules through which this inequality could be derived from its premises. In the following proof, we use Lemma 2.1 many times without mentioning it explicitly. In order to simplify the presentation, we do not cut terms with identical monomials.

Minimum. Take the tropical sum of the algebraic combinations constructed for the premises.

Tropical multiplication. For the tropical multiplication by a term t, tropically multiply by t the algebraic combination constructed for the premise.

Transitivity. Consider the application of this rule

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

and the algebraic combinations for its premises that we have due to the induction hypothesis

$$\begin{aligned} \Gamma_1 \oplus p^- &\leqslant h^+ \oplus \Delta_1, \\ \Gamma_2 \oplus h^- &\leqslant r^+ \oplus \Delta_2, \end{aligned}$$

where $h^+ \preceq h \odot c_{i_1}$, $r^+ \preceq r \odot c_{i_2}$, $p^- \succeq p$, and $h^- \succeq h$.

Tropically multiply the second premise by $c_{i_1} \odot 1/(sR)$ and take the tropical sum with the first premise. We get

$$\begin{aligned} &\overbrace{\Gamma_1 \oplus \Gamma_2 \odot (c_{i_1} \odot 1/(sR)) \oplus h^- \odot (c_{i_1} \odot 1/(sR))}^{\Gamma} \oplus p^- \\ \leqslant\ &\underbrace{\Delta_1 \oplus \Delta_2 \odot (c_{i_1} \odot 1/(sR)) \oplus h^+}_{\Delta} \oplus r^+ \odot (c_{i_1} \odot 1/(sR)). \end{aligned}$$

As $p^- \succeq p$ and $r^+ \odot (c_{i_1} \odot 1/(sR)) \preceq r \odot (c_{i_1} + c_{i_2} + 1/(sR))$, these polynomials satisfy the induction hypothesis (note that $i = i_1 + i_2 + 1$). Also the new Γ and Δ, as designated in the equation, satisfy the induction hypothesis, since $h^+ \preceq h \odot c_{i_1}$.

It is also easy to observe that the complexity parameters in the induction hypothesis are also maintained through the induction step (we merge two linear combinations changing only coefficients). The only item to be checked is the coefficients. The coefficients added to the coefficients in the combinations for the premises are of two kinds: (a) in the transitivity rule, we add coefficients with the denominator sR, and the obtained sum of the added coefficients is kept within the specified range, (b) in the tropical multiplication rule, we add the coefficient of the term by which we multiply. Note also that the coefficients in Γ and Δ come from h (tropically multiplied by the corresponding constant $j/(sR)$) only.

2. To prove the polynomial simulation claim, observe that we can apply the first claim of our theorem to the last line $p_s \leqslant q_s$ of the `MP-PC` *refutation* (so $p_s \succ q_s$ and q_s has a finite constant term). Let R be large enough so that $1/R$ is smaller than the difference between any two coefficients (for the same monomial) on the left and on the right that establish $p_s \succ q_s$. If we have used the axioms $g \leqslant \infty$ for g not occurring in the right-hand side of an input inequality, we simply drop it from the algebraic combination (along with its multipliers); it can never harm the correctness of the refutation. Thus we obtained a valid `MP-NS` refutation. (The condition to have the same denominator, where needed, can be easily maintained by representing the constants using the denominator being the least common multiple of the old denominator and sR.) □

4.2 Min-Plus NSR over $\{0, 1\}$ variables polynomially simulates daglike Resolution

We now prove that even an apparently weak and static system `MP-NSR` is able to simulate daglike `Resolution`.

Theorem 4.2. *MP-NSR with the dual $\{0,1\}$ encoding (I) polynomially simulates `Resolution`. Moreover, in the resulting MP-NSR proof the nominators and denominators in the rational constants, as well as the degrees of monomials, are polynomially bounded w.r.t. the number of monomials in the proof. The maximum degree of monomials in the resulting proof is bounded by the resolution width (that is, the maximum number of variables occurring in a clause of the simulated resolution proof).*

Proof. 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

$$\frac{A \vee x \quad A \vee \neg x}{A}, \tag{13}$$

and a weakening step

$$\frac{A}{A \vee \ell}, \tag{14}$$

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 $1 \leqslant [A]$:

$$1 \leqslant 0 \odot [A]. \tag{15}$$

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

  $$c_i \odot x \odot [A] \oplus c_i \odot \overline{x} \odot [A] \leqslant c_i \odot [A]. \tag{16}$$

  Observe that $[A \vee v] = [A] \odot v$ for every variable v, so the terms in (16) are exactly the translation of (13) multiplied by c_i.

- For a weakening step, we would like to multiply $0 \leqslant [\ell]$ by $c_i \odot [A]$ obtaining

  $$c_i \odot [A] \leqslant c_i \odot [A] \odot [\ell]. \tag{17}$$

  Observe that the terms in (17) are exactly the translation of (14) 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 (17), 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 (15) (for all the initial clauses A), (16), and (17) (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. $\square$

4.3 A short proof of the propositional pigeon-hole principle in Min-Plus NSR over $\{0, 1\}$ variables

Definition 4.3 (PHP)**.** The propositional pigeon-hole principle ($\mathtt{PHP}_n^m$, for short, for $m > n$) consists of the following clauses:

$$\bigvee_{1\leqslant j\leqslant n} x_{ij} \text{ for } 1 \leqslant i \leqslant m,$$
$$\overline{x}_{i'j} \vee \overline{x}_{ij} \text{ for } 1 \leqslant i < i' \leqslant m, 1 \leqslant j \leqslant n,$$

which translates in the (I) encoding to

$$1 \leqslant \bigodot_{j=1}^{n} x_{ij} \text{ for } 1 \leqslant i \leqslant m, \tag{18}$$
$$1 \leqslant \overline{x}_{i'j} \odot \overline{x}_{ij} \text{ for } 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n. \tag{19}$$

We will construct a `treelike MP-PCR` proof and then apply Theorem 4.1 to get a `MP-NSR` proof. Our proof resembles the `treelike CP`* proof of `PHP` from [Juk12, Proposition 19.5], however, it does not use the rounding rule as we do not have it.

Note that there is a short `treelike MP-PCR` derivation of

$$x_{i'j} \odot x_{ij} \leqslant 1 \text{ for } 1 \leqslant i < i' \leqslant m, 1 \leqslant j \leqslant n. \tag{20}$$

from (19) and the axioms: tropically multiply (19) by $x_{i'j} \odot x_{ij}$ substitute the axiom $x_{kj} \odot \overline{x}_{kj} \leqslant 1$ for $k = i$ and then for $k = i'$. Therefore, we will use (20) in our proof.

Before continuing to the main proof, we prove a lemma.

Lemma 4.4 (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. 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

$$V_j \leqslant 1 \odot v_j. \tag{21}$$

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 3.2 to the result obtaining

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

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

$$V_j \leqslant 1 \odot \overline{v}_j^{\odot(j-2)}. \tag{22}$$

Stage 3. Take the tropical sum of (21) and (22) and substitute its right-hand side with $v_j \oplus \overline{v}_j^{j-2} \leqslant 0$ (due to Lemma 3.3) multiplied by 1 eventually obtaining $V_j \leqslant 1$. □

Remark 4.5. Note that this is essentially a `treelike Res(LP)` proof that does not use the full strength of (`+RES`): this rule is applied when one premise is an inequality and not a disjunction of inequalities.

Theorem 4.6. *For any $n > m$, the dual (I) encoding of $\mathtt{PHP}_n^m$ has `treelike MP-PCR` refutations that contain $O(n^4)$ (not necessarily distinct) terms, tropical degree $O(mn)$, and integer coefficients of value at most $O(n)$.*

Proof. Apply Lemma 4.4 to $x_{1j}, \ldots, x_{mj}$ for each $j = 1, \ldots, n$ separately. Multiply the results using Lemma 3.2 getting

$$\bigodot_{j=1}^{n} \bigodot_{i=1}^{m} x_{ij} \leqslant n. \tag{23}$$

Now multiply all the inequalities (18) using Lemma 3.2 getting

$$m \leqslant \bigodot_{i=1}^{m} \bigodot_{j=1}^{n} x_{ij} \tag{24}$$

Eventually, substitute (23) into the right-hand side of (24) arriving at the contradiction $m \leqslant n$. The complexity easily follows from the lemmas. □

Corollary 4.7. *For any $n > m$, the dual (I) encoding of $\mathtt{PHP}_n^m$ has polynomial-size `MP-NSR` refutations with coefficients (both nominators and the denominator, the latter one being the same for all the coefficients) and tropical exponents written in unary.*

Proof. Use Theorems 4.1 and 4.6. The denominator in Theorem 4.1 is proportional to the size of the refutation in Theorem 4.6, and R can be chosen to be 2 as the treelike refutation uses integers only. □

5 Encoding Boolean logic by $\{0, 1\}$ with dual variables, the dynamic case

5.1 Min-Plus PCR with tropical resolution polynomially simulates resolution over linear inequalities

We would love to prove that `MP-PCR` polynomially simulates `Res(LP)`. However, the latter contains the "resolution" rule (`+RES`) that apparently makes a problem. Therefore, we extend our tropical system by a simular rule in order to show the simulation, and leave the equivalence between the original `MP-PCR` and `Res(LP)` as an open question.

Translation. For any affine form $f = c + \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$ with integer coefficients we define the following translation:

$$[f] = c' \odot g_1 \odot g_2 \odot \ldots \odot g_n,$$

where $g_i = x_i^{\odot \alpha_i}$, if $\alpha_i \geqslant 0$, or $g_i = \overline{x}_i^{\odot - \alpha_i}$ if $\alpha_i < 0$ and

$$c' = c + \sum_{i : \alpha_i < 0} \alpha_i \text{ as a sum of integers.}$$

In other words, we informally change every variable x_i with negative coefficient to $1 - \bar{x}_i$ and then translate the linear combination to min-plus operations literally.

Proposition 5.1. *For any linear forms f and g we can transform in a polynomial number of steps $[f + g]$ into $[f] \odot [g]$ wherever it occurs in a min-plus inequality.*

Proof. All we need is to substitute $x_i \odot \overline{x}_i = 1$. □

A line of `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

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

Polynomial simulation. We simulate the `Res(LP)` proof line by line.

Theorem 5.2. *MP-PCR+($\odot$RES) polynomially simulates `Res(LP)`.*

Proof. We show that each inference rule of `Res(LP)` can be simulated in `MP-PCR+(`$\odot$`RES)` (in our translation).

- For every input clause, its translation (I) does the job.
- The translations of $x \geqslant 0$ and $1 - x \geqslant 0$ are $\overline{x} \odot (-1) \leqslant 0$ and $x \odot (-1) \leqslant 0$, see Note 2.19.
- The translation of (`BOOL`) is $\overline{x} \oplus x \leqslant 0$, which is our axiom.
- To derive $[(-\alpha_1 f_1 - \alpha_2 f_2)] \oplus \tilde{\Gamma} \leqslant 0$ from $[-f_1] \oplus \tilde{\Gamma} \leqslant 0$ and $[-f_2] \oplus \tilde{\Gamma} \leqslant 0$ we use the ($\odot$`RES`) rule. Let us represent each α_i in the binary notation as $\alpha_i = \beta_0 2^0 + \beta_1 2^1 + \ldots + \beta_k 2^k$. We derive all inequalities of the form
$$\left[-2^j f_i\right] \oplus \tilde{\Gamma} \leqslant 0$$
using j applications of the ($\odot$`RES`) rule and the use of Prop. 5.1. After that, we use the ($\odot$`RES`) rule and Prop. 5.1 once again to sum up these inequalities for $\beta_j \neq 0$ and get
$$[(-\alpha_1 f_1 - \alpha_2 f_2)] \oplus \tilde{\Gamma} \leqslant 0.$$
- To derive $[-f] \oplus \tilde{\Gamma} \leqslant 0$ from $\tilde{\Gamma} \leqslant 0$ we use Note 2.13.
- Now observe that $[-f] \oplus [-f] \oplus \tilde{\Gamma} \leqslant 0$ is the same as $[-f] \oplus \tilde{\Gamma} \leqslant 0$ since $[-f] \oplus [-f]$ and $[-f]$ denote the same min-plus polynomial. □

Note that if the coefficients are written in unary, then we can also simulate Krajíček's extension of Cutting Planes, because `Res(CP*)` is polynomially simulated by `Res(LP*)` [HK06, Proposition 2] (see also Note 2.17).

Corollary 5.3. *MP-PCR+($\odot$RES) polynomially simulates `Res(CP*)`.*

In fact, the coefficients and tropical exponents of the min-plus polynomials can be kept small in this case (that is, also written in unary).

5.2 Resolution over linear inequalities simulates Min-Plus PCR with tropical resolution

Translation. For any min-plus monomial (with possibly zero exponents)

$$f = c \odot x_1^{\odot\alpha_1} \odot x_2^{\odot\alpha_2} \odot \ldots \odot x_n^{\odot\alpha_n} \odot \overline{x}_1^{\odot\beta_1} \odot \overline{x}_2^{\odot\beta_2} \odot \ldots \odot \overline{x}_n^{\odot\beta_n},$$

we define the following translation:

$$\{f\} = c' + (\alpha_1 - \beta_1)x_1 + (\alpha_2 - \beta_2)x_2 + \ldots + (\alpha_n - \beta_n)x_n,$$

where

$$c' = c + \sum_{i=1}^{n} \beta_i.$$

Again, informally this is simply replacing $\bar{x}_i$ by $1 - x_i$.

We will translate every line of the tropical proof, that is, a min-plus inequality

$$f_1 \oplus f_2 \oplus \cdots \oplus f_t \leqslant g_1 \oplus g_2 \oplus \cdots \oplus g_k,$$

into the disjunctions of inequalities, one for each $1 \leqslant j \leqslant k$:

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

Polynomial simulation. We will simulate the derivation step by step.

Theorem 5.4. *Res(LP) polynomially simulates MP-PCR+($\odot$RES).*

Proof. First of all, recall from Prop. 3.1 that we can assume that `Res(LP)` is working with rationals (and not necessarily integers).

We simulate each of the `MP-PCR+(`$\odot$`RES)` inference rules in the following way:

- We can derive axioms in `MP-PCR+(`$\odot$`RES)`.
  - The representation of the initial clauses ((I), in the case of `Res(LP)`) goes through our translation literally.
  - The translation of (`WEAK`) can be dropped. Its use in the $\oplus$ rule is simulated by weakening the clauses, its use in the minimum rule is simulated by dropping the respective clauses, and its use in the tropical multiplication rule is equivalent to the use of (`WEAK`) itself.
  - Axioms $x \odot \overline{x} \leqslant 1$ and $x \odot \overline{x} \geqslant 1$ are translated into $1 \leqslant 1$, which is trivial. The axiom $x \oplus \overline{x} \leqslant 0$ is translated into $x \leqslant 0 \vee 1 - x \leqslant 0$, which is an axiom of `Res(LP)`. Finally, $x \oplus \overline{x} \geqslant 0$ is translated into $-x \leqslant 0$ and $1 - x \geqslant 0$, which are axioms of `Res(LP)`.
  - We can derive inequalities of the form $x \leqslant \alpha$, where $\alpha \geqslant 0$, which is also trivially translated.

- Tropical multiplication by a term s,

$$\frac{f_1 \oplus f_2 \oplus \ldots \oplus f_t \leqslant g_1 \oplus g_2 \oplus \ldots \oplus g_k}{f_1 \odot s \oplus f_2 \odot s \oplus \ldots \oplus f_t \odot s \leqslant g_1 \odot s \oplus g_2 \odot s \oplus \ldots \oplus g_k \odot s},$$

in fact does not need any simulation at all: in `Res(LP)` it looks like

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

for every $1 \leqslant j \leqslant k$. Observe that for any two min-plus terms s_1 and s_2, $\{s_1\} + \{s_2\} = \{s_1 \odot s_2\}$. This means that in particular, that the inequalities $\{f_i \odot s\} \leqslant \{g_j \odot s\}$ and $\{f_i\} \leqslant \{g_j\}$ are identical.

- The minimum rule in the original derivation can be simulated by weakening. Indeed, if from

$$f_1 \oplus f_2 \oplus \ldots \oplus f_t \leqslant g_1 \oplus g_2 \oplus \ldots \oplus g_k \text{ and } f'_1 \oplus f'_2 \oplus \ldots \oplus f'_{t'} \leqslant g'_1 \oplus g'_2 \oplus \ldots \oplus g'_{k'}$$

we derive

$$f_1 \oplus f_2 \oplus \ldots \oplus f_t \oplus f'_1 \oplus f'_2 \oplus \ldots \oplus f'_{t'} \leqslant g_1 \oplus g_2 \oplus \ldots \oplus g_k \oplus g'_1 \oplus g'_2 \oplus \ldots \oplus g'_{k'},$$

then in `Res(LP)` we need to derive, for every $1 \leqslant j \leqslant k$ and $1 \leqslant s \leqslant k'$,

$$\bigvee_{i=1}^{t} \{f_i\} \leqslant \{g_j\} \vee \bigvee_{i=1}^{t'} \{f'_i\} \leqslant \{g_j\}, \qquad \bigvee_{i=1}^{t} \{f_i\} \leqslant \{g'_s\} \vee \bigvee_{i=1}^{t'} \{f'_i\} \leqslant \{g'_s\},$$

from

$$\bigvee_{i=1}^{t} \{f_i\} \leqslant \{g_j\}, \qquad \bigvee_{i=1}^{t'} \{f'_i\} \leqslant \{g_s\}.$$

It is easy to see that the derivation of those clauses can be done by weakening.

- Let us simulate the transitivity rule. In `MP-PCR`, from

$$p_1 \oplus p_2 \oplus \ldots \oplus p_t \leqslant h_1 \oplus h_2 \oplus \ldots \oplus h_k$$

and

$$h_1 \oplus h_2 \oplus \ldots \oplus h_k \leqslant r_1 \oplus r_2 \oplus \ldots \oplus r_q$$

we derive

$$p_1 \oplus p_2 \oplus \ldots \oplus p_t \leqslant r_1 \oplus r_2 \oplus \ldots \oplus r_q.$$

This means, that in `Res(LP)` we need to derive, for $i \leqslant q$ and $b \leqslant k$,

$$\bigvee_{j=1}^{t} \{p_j\} \leqslant \{r_i\}, \tag{25}$$

from

$$\bigvee_{j=1}^{t} \{p_j\} \leqslant \{h_b\} \qquad \text{and} \qquad \bigvee_{u=1}^{k} \{h_u\} \leqslant \{r_i\}.$$

We do it in k steps by using a procedure that after s steps will give us

$$\bigvee_{j=1}^{t} \{p_j\} \leqslant \{r_i\} \vee \{h_{s+1}\} \leqslant \{r_i\} \vee \{h_{s+2}\} \leqslant \{r_1\} \vee \ldots \vee \{h_k\} \leqslant \{r_i\}\,. \tag{26}$$

At step $s+1$ of this procedure we apply the resolution rule t times in the following way: by the r-th application of this rule we derive from (26) and

$$\begin{aligned}&\bigvee_{j=1}^{t} \{p_j\} \leqslant \{r_i\}\\ &\vee \{h_{s+2}\} \leqslant \{r_i\} \vee \ldots \vee \{h_k\} \leqslant \{r_i\}\\ &\vee \{p_r\} \leqslant \{h_{s+1}\} \vee \{p_{r+1}\} \leqslant \{h_{s+1}\} \vee \ldots \vee \{p_t\} \leqslant \{h_{s+1}\}\end{aligned}$$

the following disjunction:

$$\begin{aligned}&\bigvee_{j=1}^{t} \{p_j\} \leqslant \{r_i\}\\ &\vee \{h_{s+2}\} \leqslant \{r_i\} \vee \ldots \vee \{h_k\} \leqslant \{r_i\}\\ &\vee \{p_{r+1}\} \leqslant \{h_{s+1}\} \vee \{p_{r+2}\} \leqslant \{h_{s+1}\} \vee \ldots \vee \{p_t\} \leqslant \{h_{s+1}\}\end{aligned}$$

by resolving $\{p_r\} \leqslant \{h_{s+1}\}$ and $\{h_{s+1}\} \leqslant \{r_i\}$. Note that at the first resolution step we resolve with a weakened

$$\{p_1\} \leqslant \{h_{s+1}\} \vee \{p_2\} \leqslant \{h_{s+1}\} \vee \ldots \vee \{p_t\} \leqslant \{h_{s+1}\}\,.$$

After t resolution steps, we will get the desired disjunction

$$\bigvee_{j=1}^{t} \{p_j\} \leqslant \{r_i\} \vee \{h_{s+2}\} \leqslant \{r_i\} \vee \{h_{s+3}\} \leqslant \{r_1\} \vee \ldots \vee \{h_k\} \leqslant \{r_i\}\,.$$

So, after k steps of our procedure, we will get (25).

- The simulation of the ($\odot$`RES`) rule is easy. If from

  $$f_1 \oplus g_1 \oplus \ldots \oplus g_t \leqslant 0 \text{ and } f_2 \oplus g_1 \oplus \ldots \oplus g_t \leqslant 0$$

  we derive

  $$(f_1 \odot f_2) \oplus g_1 \oplus \ldots \oplus g_t \leqslant 0,$$

  then in `Res(LP)` we need to derive

  $$\{f_1 \odot f_2\} \leqslant 0 \vee \{g_1\} \leqslant 0 \vee \{g_2\} \leqslant 0 \vee \ldots \vee \{g_m\} \leqslant 0$$

  from

  $$\begin{aligned}&\{f_1\} \leqslant 0 \vee \{g_1\} \leqslant 0 \vee \{g_2\} \leqslant 0 \vee \ldots \vee \{g_m\} \leqslant 0 \text{ and}\\ &\{f_2\} \leqslant 0 \vee \{g_1\} \leqslant 0 \vee \{g_2\} \leqslant 0 \vee \ldots \vee \{g_m\} \leqslant 0.\end{aligned}$$

  Since $\{f_1 \odot f_2\} = \{f_1\} + \{f_2\}$, this is a straightforward application of the (`+RES`) rule.

As by Theorem 3.8 we can assume that the last line is $1 \leqslant 0$, we are done. □

Corollary 5.5. *`MP-PCR+(`$\odot$`RES)` that uses $\{0,1\}$ encoding with dual variables is polynomially equivalent to `Res(LP)`.*

6 Encoding Boolean logic by $\{0, \infty\}$ with dual variables, the dynamic case

All derivations in this section assume the $\{0, \infty\}$ dual encoding.

6.1 Min-Plus PCR over $\{0, \infty\}$ encoding polynomially simulates $\texttt{Res}(\infty)$.

Theorem 6.1. *MP-PCR over $\{0, \infty\}$ polynomially simulates $\texttt{Res}(\infty)$.*

Proof. We are going to simulate a $\texttt{Res}(\infty)$ refutation step by step. Each step of the $\texttt{Res}(\infty)$ refutation derives a clause of the form

$$X_1 \vee X_2 \vee \ldots \vee X_r,$$

where each X_i is a conjunction of variables or its negations. We will naturally transform such a clause into a min-plus equation

$$\tilde{X}_1 \oplus \tilde{X}_2 \oplus \cdots \oplus \tilde{X}_r = 0,$$

where $\tilde{X}_i = \overline{x}_1^{\alpha_1} \odot \overline{x}_2^{\alpha_2} \odot \cdots \odot \overline{x}_s^{\alpha_s}$ whenever $X_i = x_1^{\alpha_1} \wedge x_2^{\alpha_2} \wedge \ldots \wedge x_s^{\alpha_s}$. Note that the empty clause is translated into $\infty = 0$.

Suppose that we derived such translations for the initial fragment of the $\texttt{Res}(\infty)$ refutation. We consider the cases how the next line

$$T_1 \vee T_2 \vee \ldots \vee T_s,$$

could be derived (here, T_i is a conjunction of variables and/or their negations) and show how its translation can be derived in $\texttt{MP-PCR}$.

Cut. Then the following clauses have been previously derived in $\texttt{Res}(\infty)$:

$$A \vee (\neg \ell_1 \wedge \neg \ell_2 \wedge \ldots \wedge \neg \ell_m) \text{ and } A \vee \ell_1 \vee \ell_2 \vee \ldots \vee \ell_m,$$

where $A = T_1 \vee T_2 \vee \ldots \vee T_s$. By the assumption, we have $\texttt{MP-PCR}$ derivations of

$$\tilde{A} \oplus \bigodot_{i=1}^{m} \ell_i = 0 \text{ and } \tilde{A} \oplus \overline{\ell}_1 \oplus \overline{\ell}_2 \oplus \ldots \oplus \overline{\ell}_m = 0$$

From those equations, we can derive

$$(\tilde{A} \odot \overline{\ell}_1) \oplus (\overline{\ell}_1 \odot \bigodot_{i=1}^{m} \ell_i) = \overline{\ell}_1,$$

$$\ldots$$

$$(\tilde{A} \odot \overline{\ell}_m) \oplus (\overline{\ell}_m \odot \bigodot_{i=1}^{m} \ell_i) = \overline{\ell}_m,$$

$$(\tilde{A} \odot \bigodot_{i=1}^{m} \ell_i) \oplus (\overline{\ell}_1 \odot \bigodot_{i=1}^{m} \ell_i) \oplus \ldots \oplus (\overline{\ell}_m \odot \bigodot_{i=1}^{m} \ell_i) = \bigodot_{i=1}^{m} \ell_i.$$

Now, using $\ell_i \odot \overline{\ell}_i = \infty$, we can derive

$$\begin{aligned}
&\tilde{A} \odot \overline{\ell}_1 = \overline{\ell}_1,\\
&\ldots\\
&\tilde{A} \odot \overline{\ell}_m = \overline{\ell}_m,\\
&\tilde{A} \odot \bigodot_{i=1}^{m} \ell_i = \bigodot_{i=1}^{m} \ell_i.
\end{aligned}$$

Combining those equations in a tropical sum, we get

$$(\tilde{A} \odot \overline{\ell}_1) \oplus (\tilde{A} \odot \overline{\ell}_2) \oplus \cdots \oplus (\tilde{A} \odot \overline{\ell}_m) \oplus (\tilde{A} \odot \bigodot_{i=1}^{m} \ell_i) = \overline{\ell}_1 \oplus \overline{\ell}_2 \oplus \cdots \oplus \overline{\ell}_m \oplus \bigodot_{i=1}^{m} \ell_i.$$

By Lemma 3.4 the right-hand side is zero. Since for each i, $\tilde{A} \odot \overline{\ell}_i \geqslant \tilde{A}$, one can derive

$$\tilde{A} \oplus \tilde{A} \oplus \ldots \oplus \tilde{A} \leqslant 0,$$

which is equivalent to $\tilde{A} \leqslant 0$. Using Lemma 3.2 to derive $\tilde{A} \geqslant 0$we conclude that $\tilde{A} = 0$.

Weakening. In this case the `Res(∞)` derivation contained $T_1 \vee T_2 \vee \ldots \vee T_r$, where $r < s$, and we already derived its `MP-PCR` translation

$$\tilde{T}_1 \oplus \tilde{T}_2 \oplus \ldots \oplus \tilde{T}_r = 0.$$

Then by taking the minimum with $\tilde{T}_{r+1} \oplus \cdots \oplus \tilde{T}_s$, we can derive

$$\tilde{T}_1 \oplus \tilde{T}_2 \oplus \ldots \oplus \tilde{T}_s = 0 \oplus \tilde{T}_{r+1} \oplus \cdots \oplus \tilde{T}_s \leqslant 0.$$

Since $\tilde{T}_i \geqslant 0$ by Lemma 3.2, we get the desired translation of `Res(∞)` line.

Axioms. Use Lemma 3.4. □

6.2 `Res(∞)` polynomially simulates Min-Plus PCR over $\{0, \infty\}$ encoding

Translation. For any pair of min-plus monomials (with possibly zero exponents)

$$\begin{aligned}
f &= c \odot \overline{x}_1^{\odot\alpha_1} \odot \overline{x}_2^{\odot\alpha_2} \odot \ldots \odot \overline{x}_n^{\odot\alpha_n} \odot x_1^{\odot\beta_1} \odot x_2^{\odot\beta_2} \odot \ldots \odot x_n^{\odot\beta_n},\\
g &= c' \odot \overline{x}_1^{\odot\alpha'_1} \odot \overline{x}_2^{\odot\alpha'_2} \odot \ldots \odot \overline{x}_n^{\odot\alpha'_n} \odot x_1^{\odot\beta'_1} \odot x_2^{\odot\beta'_2} \odot \ldots \odot x_n^{\odot\beta'_n}
\end{aligned}$$

we define the following translation:

$$\{f \leqslant g\} = \left(\bigwedge_{\alpha_i \neq 0} x_i \wedge \bigwedge_{\beta_i \neq 0} \overline{x}_i\right) \vee \left(\bigvee_{\alpha'_i \neq 0} \overline{x}_i \vee \bigvee_{\beta'_i \neq 0} x_i\right),$$

if $c \leqslant c' \neq \infty$ and

$$\{f \leqslant g\} = \left(\bigvee_{\alpha'_i \neq 0} \overline{x}_i \vee \bigvee_{\beta'_i \neq 0} x_i\right),$$

if $c > c'$. Note that here if g is a constant monomial, then $\left(\bigvee_{\alpha'_i \neq 0} x_i \vee \bigvee_{\beta'_i \neq 0} \overline{x}_i\right) = \texttt{false}$, and if f is a constant monomial, then $\left(\bigwedge_{\alpha_i \neq 0} x_i \wedge \bigwedge_{\beta_i \neq 0} \overline{x}_i\right) = \texttt{true}$. Eventually, if $c' = \infty$, then $\{f \leqslant g\} = \texttt{true}$.

We will translate every line of the tropical proof, that is, a min-plus inequality

$$f_1 \oplus f_2 \oplus \cdots \oplus f_t \leqslant g_1 \oplus g_2 \oplus \cdots \oplus g_k,$$

into disjunctions of inequalities, one for each $1 \leqslant j \leqslant k$:

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

In the next lemma, by the derivation for a "rule" $\frac{A,\ B}{C}$ we mean a derivation of its conclusion from its premises.

Lemma 6.2. *There is a polynomial-size* $\texttt{Res}(\infty)$ *derivation for*

$$\frac{\{f \leqslant g\} \quad \{g \leqslant h\}}{\{f \leqslant h\}}.$$

Proof. Assume

$$\begin{aligned} f &= c \odot \overline{x}_1^{\odot\alpha_1} \odot \overline{x}_2^{\odot\alpha_2} \odot \ldots \odot \overline{x}_n^{\odot\alpha_n} \odot x_1^{\odot\beta_1} \odot x_2^{\odot\beta_2} \odot \ldots \odot x_n^{\odot\beta_n}, \\ g &= c' \odot \overline{x}_1^{\odot\alpha'_1} \odot \overline{x}_2^{\odot\alpha'_2} \odot \ldots \odot \overline{x}_n^{\odot\alpha'_n} \odot x_1^{\odot\beta'_1} \odot x_2^{\odot\beta'_2} \odot \ldots \odot x_n^{\odot\beta'_n}, \\ h &= c'' \odot \overline{x}_1^{\odot\alpha''_1} \odot \overline{x}_2^{\odot\alpha''_2} \odot \ldots \odot \overline{x}_n^{\odot\alpha''_n} \odot x_1^{\odot\beta''_1} \odot x_2^{\odot\beta''_2} \odot \ldots \odot x_n^{\odot\beta''_n}. \end{aligned}$$

If h has the coefficient ∞, then the derivation is trivial. So, we can assume that c'' is finite. Let us denote

$$\begin{aligned} \{f = c\} &= \left(\bigwedge_{\alpha_i \neq 0} x_i \wedge \bigwedge_{\beta_i \neq 0} \overline{x}_i\right), \\ \{g = c'\} &= \left(\bigwedge_{\alpha'_i \neq 0} x_i \wedge \bigwedge_{\beta'_i \neq 0} \overline{x}_i\right), \\ \{g = \infty\} &= \left(\bigvee_{\alpha'_i \neq 0} \overline{x}_i \vee \bigvee_{\beta'_i \neq 0} x_i\right), \\ \{h = \infty\} &= \left(\bigvee_{\alpha''_i \neq 0} \overline{x}_i \vee \bigvee_{\beta''_i \neq 0} x_i\right). \end{aligned}$$

So one needs to derive

$$\frac{(\{f = c\} \wedge (c \leqslant c')) \vee \{g = \infty\} \quad (\{g = c'\} \wedge (c' \leqslant c'')) \vee \{h = \infty\}}{(\{f = c\} \wedge (c \leqslant c'')) \vee \{h = \infty\}},$$

where the relations between the constants denote logical constants $\texttt{true}$ and $\texttt{false}$. We consider possible cases of c, c', c'' ordering:

- If $c, c' > c''$ (c or c' is possibly infinite), then the second premise of the translation equals the conclusion (namely, they both equal $\{h = \infty\}$), so the derivation is trivial.
- If $c' \leqslant c''$, we can assume $c > c'$ (c is possibly infinite). Then one can derive

$$\frac{\{g = \infty\} \quad \{g = c'\} \vee \{h = \infty\}}{\{h = \infty\}},$$

by using the cut rule, since $\{g = \infty\}$ is a negation of $\{g = c'\}$, from which one can derive by weakening

$$\frac{\{h = \infty\}}{(\{f = c\} \wedge (c \leqslant c'')) \vee \{h = \infty\}}.$$

- Finally, if $c \leqslant c''$, we can assume $c \leqslant c'$ (c' is possibly infinite) . Then one can derive

$$\frac{\{f = c\} \vee \{g = \infty\} \quad (\{g = c'\} \wedge (c' \leqslant c'')) \vee \{h = \infty\}}{\{f = c\} \vee \{h = \infty\}},$$

by applying either the cut rule if $c' \leqslant c''$, or the weakening rule otherwise. □

Polynomial simulation. We will simulate the derivation step by step.

Theorem 6.3. *`Res(∞)` polynomially simulates `MP-PCR` over* $\{0, \infty\}$.

Proof. We simulate each of the inference rules in the following way:

- We can derive axioms in `MP-PCR` over $\{0, \infty\}$.
  - The representation of the initial clauses goes through our translation literally.
  - The translation of (`WEAK`) can be dropped since $\{f \leqslant \infty\}$ is translated into `true` value.
  - Axioms $x \odot \overline{x} \geqslant \infty$ and $x \odot \overline{x} \leqslant \infty$ are translated into $x \vee \overline{x}$ (an axiom of `Res(∞)`) and `true` (which is trivial). The axiom $x \oplus \overline{x} \leqslant 0$ is translated into $x \vee \overline{x}$. Finally, $x \oplus \overline{x} \geqslant 0$ is translated into $\{0 \leqslant x\}$ and $\{0 \leqslant \overline{x}\}$, both of which are `true`.
- Tropical multiplication by a term t,

$$\frac{f_1 \oplus f_2 \oplus \ldots \oplus f_s \leqslant g_1 \oplus g_2 \oplus \ldots \oplus g_k}{f_1 \odot t \oplus f_2 \odot t \oplus \ldots \oplus f_s \odot t \leqslant g_1 \odot t \oplus g_2 \odot t \oplus \ldots \oplus g_k \odot t},$$

is translated into the following:

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

for every $1 \leqslant j \leqslant k$. If $t = \infty$, then the conclusion is trivially equal to `true`. Otherwise each $\{f_i \odot t \leqslant g_j \odot t\}$ can be derived from $\{f_i \leqslant g_j\}$ in the following way: suppose

$$f = c \odot \overline{x}_1^{\odot \alpha_1} \odot \overline{x}_2^{\odot \alpha_2} \odot \ldots \odot \overline{x}_n^{\odot \alpha_n} \odot x_1^{\odot \beta_1} \odot x_2^{\odot \beta_2} \odot \ldots \odot x_n^{\odot \beta_n},$$
$$g = c' \odot \overline{x}_1^{\odot \alpha'_1} \odot \overline{x}_2^{\odot \alpha'_2} \odot \ldots \odot \overline{x}_n^{\odot \alpha'_n} \odot x_1^{\odot \beta'_1} \odot x_2^{\odot \beta'_2} \odot \ldots \odot x_n^{\odot \beta'_n}$$
$$t = c'' \odot \overline{x}_1^{\odot \alpha''_1} \odot \overline{x}_2^{\odot \alpha''_2} \odot \ldots \odot \overline{x}_n^{\odot \alpha''_n} \odot x_1^{\odot \beta''_1} \odot x_2^{\odot \beta''_2} \odot \ldots \odot x_n^{\odot \beta''_n}$$

If $c < c'$, then one wants to derive

$$\left(\bigwedge_{\alpha_i \neq 0} x_i \wedge \bigwedge_{\beta_i \neq 0} \overline{x}_i \wedge \bigwedge_{\alpha''_i \neq 0} x_i \wedge \bigwedge_{\beta''_i \neq 0} \overline{x}_i\right) \vee \left(\bigvee_{\alpha'_i \neq 0} x_i \vee \bigvee_{\beta'_i \neq 0} \overline{x}_i \vee \bigvee_{\alpha''_i \neq 0} \overline{x}_i \vee \bigvee_{\beta''_i \neq 0} x_i\right)$$

from

$$\left(\bigwedge_{\alpha_i \neq 0} x_i \wedge \bigwedge_{\beta_i \neq 0} \overline{x}_i\right) \vee \left(\bigvee_{\alpha'_i \neq 0} x_i \vee \bigvee_{\beta'_i \neq 0} \overline{x}_i\right).$$

This is a derivation of the form

$$\frac{\overline{A} \vee B}{(\overline{A} \wedge \bigwedge_{i=1}^{s} y_i) \vee B \vee \bigvee_{i=1}^{s} \overline{y}_i},$$

where A is a disjunction of literals and its negation $\overline{A}$ is the conjunction of their negations. It can be done in the following way:

$$\frac{\emptyset}{(\overline{A} \wedge \bigwedge_{i=1}^{s} y_i) \vee A \vee \bigvee_{i=1}^{s} \overline{y}_i}, \qquad \frac{(\overline{A} \wedge \bigwedge_{i=1}^{s} y_i) \vee A \vee \bigvee_{i=1}^{s} \overline{y}_i \qquad \overline{A} \vee B}{(\overline{A} \wedge \bigwedge_{i=1}^{s} y_i) \vee B \vee \bigvee_{i=1}^{s} \overline{y}_i}.$$

- The minimum and transitivity rules are simulated literally as in Theorem 5.4. The only difference is that the resolution step is performed using Lemma 6.2 instead of (`+RES`).

As by Theorem 3.8 we can assume that the last inequality in the derivation was $1 \leqslant 0$, we are done. □

Corollary 6.4. *`MP-PCR` that uses $\{0, \infty\}$ encoding with dual variables is polynomially equivalent to `Res(`∞`)`.*

7 Lower bounds and non-deducibility

In this section we prove lower bounds and results on non-deducibility.

We discuss our definitions and show some evidence that several subtle details are indeed important. Namely, we prove that $0 \leqslant x$ (which is present in `MP-PCR` and is semantically true in `MP-PCE`) cannot be derived in `MP-PCE` and that the tropical resolution rule cannot be directly simulated in `MP-PCE` as well as in `MP-PCR`. We also show that for `MP-NSE` and `MP-NSR` proofs, non-integer coefficients are important in a sharp contrast to `MP-PCR` proofs.

We then prove a lower bound on the size of `MP-PCE` and `MP-PCR` derivations of a much simplified tropical version of the Binary Value Principle, which provides exponential lower bounds for these systems. We also establish lower bounds on the tropical degree of derivations of a tropical version of the Knapsack problem.

7.1 "Derivations" in MP-NS and the inability to derive $0 \leqslant x$ in MP-PCE

We show that $0 \leqslant x$ cannot be derived in MP-NSE or MP-PCE for $\{0,1\}$ variables. However, what does it mean to "derive" in MP-NS, which is a static system? How can we represent this inequality in order to make use of it? In principle, we can allow it to come in the form $\Gamma \oplus c \leqslant x \oplus \Delta$ with two tropical polynomials $\Gamma \succ \Delta$: such inequality can be useful because Γ and Δ (possibly multiplied by the same polynomial) will later simply contribute to the last line of the derivation (see Lemma 2.1, and see the proof of Theorem 4.1 for an example of such derivation). This could increase the number of terms and the degree, but we leave the complexity issues apart for now, because we show that in our case it is simply impossible.

Proposition 7.1. *$\Gamma \oplus c \leqslant x \oplus \Delta$ is not derivable in MP-PC from (01/E) for any $c \in \mathbb{Q}_\infty$ and any $\Gamma \succ \Delta$.*

Proof. Assume the contrary. Convert the MP-PC derivation into a treelike one (note that in this proposition we are not concerned with the complexity). By Theorem 4.1 there must be an algebraic combination of the form

$$\Bigg(\bigoplus_{0\leqslant i\leqslant d}(b_i \odot x \oplus a_i \odot (x^{\odot 2} \oplus 1)) \odot x^{\odot i} \oplus \bigoplus_{0\leqslant \ell\leqslant d+2} e_\ell \odot x^{\odot \ell},$$

$$\bigoplus_{0\leqslant i\leqslant d}(b_i \odot (x^{\odot 2} \oplus 1) \oplus a_i \odot x) \odot x^{\odot i} \oplus \bigoplus_{0\leqslant \ell\leqslant d+2} e_\ell \odot x^{\odot \ell}\Bigg)$$

$$= (c \oplus \Gamma, x \oplus \Delta), \quad (27)$$

where $\Gamma \succ \Delta$, $d \geqslant 0$, $a_i, b_i \in \mathbb{Q}_\infty$, and $e_\ell \in \mathbb{Q}_\infty$ (note that we do not include the use of the axiom (WEAK), because additional monomials on the left do not relax these conditions). W.l.o.g. one can assume that $b_d < \infty$. In what follows we refer to the first/second component of the pair in (27) as the left/right-hand side.

Lemma 7.2. *For $1 \leqslant i \leqslant d$, $b_i > b_{i-1}$. For $0 \leqslant j \leqslant d$, $b_j < a_j$.*

Proof of Lemma. We prove lemma by inverse induction on i. For the base of induction comparing the coefficients in (27) at the monomial $x^{\odot(d+2)}$, we get that

$$\min\{b_d, e_{d+2}\} < \min\{a_d, e_{d+2}\}$$

since $\Gamma \succ \Delta$, hence $b_d = \min\{b_d, e_{d+2}\}$ and $b_d < a_d$. Comparing the coefficients at $x^{\odot(d+1)}$, we get that

$$\min\{a_d, b_{d-1}, e_{d+1}\} < \min\{a_{d-1}, b_d, e_{d+1}\},$$

provided that $d \geqslant 1$. Therefore, $b_d < a_d$ implies that the minimum on the left cannot be attained at a_d (as it is greater than b_d on the right), hence $b_{d-1} = \min\{a_d, b_{d-1}, e_{d+1}\}$ and $b_{d-1} < b_d,\ b_{d-1} < a_{d-1}$.

For the inductive step, comparing the coefficients at $x^{\odot i}$ for some $2 \leqslant i \leqslant d$, we get that

$$\min\{b_i + 1, a_{i-1}, b_{i-2}, e_i\} < \min\{a_i + 1, b_{i-1}, a_{i-2}, e_i\}.$$

Since $b_i + 1 \geqslant b_i > b_{i-1},\ a_{i-1} > b_{i-1}$ by the inductive hypothesis, we conclude that the minimum on the left is attained at b_{i-2}, hence $b_{i-2} < b_{i-1},\ b_{i-2} < a_{i-2}$. $\square$

Coming back to the proof of the proposition, denote by c_1 the coefficient at x of Γ and by c_0 the coefficient at x of Δ. Then the coefficient at x in the left-hand side of (27) equals

$$c_1 = \min\{a_1, b_0, e_1\} \tag{28}$$

The coefficient at x in the right-hand side of (27) equals

$$\min\{0, c_0\} = \min\{a_0, b_1, e_1\}. \tag{29}$$

Since $c_0 < c_1$ due to $\Gamma \succ \Delta$, we conclude from (28), (29) that

$$\min\{a_0, b_1, e_1\} < \min\{a_1, b_0, e_1\}$$

which leads to a contradiction because $a_0 > b_0,\ b_1 > b_0,\ e_1 \geqslant e_1$ taking into account Lemma 7.2. $\square$

7.2 The importance of the tropical resolution rule

Recall that we were able to show the polynomial equivalence between `MP-PCR` and `Res(LP)` only after we added the rule ($\odot$`RES`) to `MP-PCR`. Despite the fact that this rule is not needed for the completeness of `MP-PCR`, it may have a substantial impact on the strength of the system.

Below we first prove that there is no direct simulation of this rule in `MP-NSE`, and then prove that for `MP-NSR` as well.

The next theorem states that there is no inference of the inequality $x^{\odot 2} \leqslant 0$ from $x^{\odot 2} \oplus x \leqslant 0$ in `MP-NSE`. 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 7.3. *For any $\Gamma \succ \Delta$, there is no `MP-NSE` inference of $\Gamma \oplus x^{\odot 2} \leqslant 0 \oplus \Delta$ from $x^{\odot 2} \oplus x \leqslant 0$ and the axiom $x^{\odot 2} \oplus 1 = x$.*

Proof. Suppose the contrary, then there exists an inference

$$(x^{\odot 2} \oplus \Gamma, 0 \oplus \Delta) = \bigoplus_{0 \leqslant i \leqslant k} x^{\odot i} \odot (a_i \odot (x^{\odot 2} \oplus x, 0) \oplus b_i \odot (x, x^{\odot 2} \oplus 1) \oplus c_i \odot (x^{\odot 2} \oplus 1, x)) \tag{30}$$

for suitable k, where $a_i, b_i, c_i \in \mathbb{Q}_\infty$ and $\Gamma \succ \Delta$.

Lemma 7.4. $a_j, c_j > b_j, 1 \leqslant j \leqslant k,\ b_{j+1} > b_j, 1 \leqslant j < k.$

We prove Lemma by the inverse induction on j. Comparing the coefficients at the tropical monomial $x^{\odot(k+2)}$ in both sides of (30), we get that

$$\min\{a_k, c_k\} > b_k \tag{31}$$

due to the condition $\Gamma \succ \Delta$, provided that $k \geqslant 1$, which justifies the base of induction for $j = k$.

After that similarly, comparing the coefficients at $x^{\odot(k+1)}$, we obtain that

$$\min\{a_k, a_{k-1}, b_k, c_{k-1}\} > \min\{c_k, b_{k-1}\}, \tag{32}$$

provided that $k \geqslant 2$. The minimum in the right-hand side of (32) cannot be attained at c_k due to (31), hence $\min\{a_k, a_{k-1}, b_k, c_{k-1}\} > b_{k-1}$, which justifies Lemma for $j = k - 1$.

To prove the inductive step (in a similar way as above) comparing the coefficients at $x^{\odot(j+2)}$ for $j \geqslant 1$, we get that

$$\min\{a_{j+1}, a_j, b_{j+1}, c_{j+2}+1, c_j\} > \min\{a_{j+2}, b_{j+2}+1, b_j, c_{j+1}\}. \tag{33}$$

The minimum at the right-hand side of (33) can be attained only at b_j since $\min\{a_{j+2}, b_{j+2}+1, c_{j+1}\} > b_{j+1}$ according to the inductive hypothesis, which completes the inductive step and the proof of the Lemma. □

Coming back to the proof of the Theorem we denote by $\Gamma_{x^{\odot 2}},\ \Delta_{x^{\odot 2}},\ \Gamma_0, \Delta_0 \in \mathbb{Q}_\infty$ the coefficients in $\Gamma,\ \Delta$ at the corresponding monomials. Comparing the coefficients in both sides of (30) at $x^{\odot 2}$ and making use of (33) for $j=0$, we obtain that

$$\min\{0, \Gamma_{x^{\odot 2}}\} = \min\{a_1, a_0, b_1, c_2+1, c_0\},\ \Delta_{x^{\odot 2}} = \min\{a_2, b_2+1, b_0, c_1\},\ \Gamma_{x^{\odot 2}} > \Delta_{x^{\odot 2}}. \tag{34}$$

In a similar way, comparing the coefficients at $x^{\odot 0}=0$ and making use of (33) for $j=-2$, we obtain that

$$\Gamma_0 = c_0+1,\ \min\{0, \Delta_0\} = \min\{a_0, b_0+1\},\ \Gamma_0 > \Delta_0. \tag{35}$$

We distinguish 3 cases.

1) $\min\{0, \Gamma_{x^{\odot 2}}\} = 0,\ \min\{0, \Delta_0\} = 0$ (see (34), (35)).

Then either $a_0 = 0$ or $b_0+1=0$ due to (35). When $a_0=0$, comparing the coefficients at x (see (33) for $j=-1$) we get a contradiction

$$0 = a_0 > \min\{a_1, b_1+1, c_0\} \geqslant \min\{a_1, a_0, b_1, c_2+1, c_0\} = 0,$$

where the latter equality follows from (34). Otherwise, when $b_0+1=0$, again comparing the coefficients at x, we get a contradiction as well:

$$-1 = b_0 > \min\{a_1, b_1+1, c_0\} \geqslant \min\{a_1, a_0, b_1, c_2+1, c_0\} = 0.$$

2) $\min\{0, \Gamma_{x^{\odot 2}}\} = 0,\ \Delta_0 = \min\{0, \Delta_0\} < 0$.

Then (35) entails that either $\Delta_0 = a_0$ or $\Delta_0 = b_0+1$. In the former case we get a contradiction:

$$0 > \Delta_0 = a_0 \geqslant \min\{a_1, a_0, b_1, c_2+1, c_0\} = 0,$$

taking into account (34). In the latter case we again get a contradiction comparing the coefficients at x (see (33) for $j=-1$):

$$-1 > \Delta_0 - 1 = b_0 > \min\{a_1, b_1+1, c_0\} \geqslant \min\{a_1, a_0, b_1, c_2+1, c_0\} = 0.$$

3) $0 > \min\{0, \Gamma_{x^{\odot 2}}\} = \Gamma_{x^{\odot 2}}$.

Lemma 7.4 implies that $\min\{a_2, b_2+1, c_1\} > b_1$, therefore $\Delta_{x^{\odot 2}} = b_0$, see (34), taking into account that $\Gamma_{x^{\odot 2}} > \Delta_{x^{\odot 2}}$. Comparing the coefficients at x (see (33) for $j=-1$) leads to a contradiction:

$$\Delta_{x^{\odot 2}} = b_0 > \min\{a_1, b_1+1, c_0\} \geqslant \min\{a_1, a_0, c_2+1, b_1, c_0\} = \Gamma_{x^{\odot 2}}. \qquad \square$$

The next theorem states that there is no `MP-NSR` inference of the inequality $x^{\odot 2} \leqslant 0$ from $x^{\odot 2} \oplus x \leqslant 0$ with the axioms $(01/\oplus), (01/\odot)$. Similarly to the explanation above (before Theorem 7.3)), it means that the tropical resolution rule ($\odot$`RES`) cannot be directly simulated in this system.

Theorem 7.5. *For any $\Gamma \succ \Delta$, there is no* `MP-NSR` *inference of $\Gamma \oplus x^{\odot 2} \leqslant 0 \oplus \Delta$ from $x^{\odot 2} \oplus x \leqslant 0$ and the axioms $x \oplus \bar{x} = 0,\ x \odot \bar{x} = 1$.*

Proof. Suppose the contrary, then there exists an inference $(f, g) =$

$$\bigoplus_{i,j \geqslant 0} x^{\odot i} \odot \bar{x}^{\odot j} \odot (u_{i,j} \odot (x^{\odot 2} \oplus x, 0) \oplus a_{i,j} \odot (x \oplus \bar{x}, 0) \oplus b_{i,j} \odot (0, x \oplus \bar{x}) \oplus d_{i,j} \odot (x \odot \bar{x}, 1) \oplus e_{i,j} \odot (1, x \odot \bar{x})),$$

where $u_{i,j}, a_{i,j}, b_{i,j}, d_{i,j}, e_{i,j} \in \mathbb{Q}_\infty$ and $(f, g) = (x^{\odot 2} \oplus \Gamma, 0 \oplus \Delta)$ for suitable tropical polynomials Γ, Δ such that $\Gamma \succ \Delta$. Denote by $f_m, g_m \in \mathbb{Q}_\infty$ the coefficients at tropical monomial m in f, g, respectively. In particular,

$$f_{x^{\odot 2}} = \min\{0, \Gamma_{x^{\odot 2}}\},\ g_0 = \min\{0, \Delta_0\} \tag{36}$$

(cf. the proof of Theorem 7.3).

Construct a directed graph H whose vertices are tropical monomials m occurring in g. We distinguish 6 cases:

$$m = x^{\odot i} \odot \bar{x}^{\odot j},\ g_m = u_{i,j}; \tag{37}$$

$$m = x^{\odot i} \odot \bar{x}^{\odot j},\ g_m = a_{i,j}; \tag{38}$$

$$m = x^{\odot (i+1)} \odot \bar{x}^{\odot j},\ g_m = b_{i,j}; \tag{39}$$

$$m = x^{\odot i} \odot \bar{x}^{\odot (j+1)},\ g_m = b_{i,j}; \tag{40}$$

$$m = x^{\odot i} \odot \bar{x}^{\odot j},\ g_m = d_{i,j} + 1; \tag{41}$$

$$m = x^{\odot (i+1)} \odot \bar{x}^{\odot (j+1)},\ g_m = e_{i,j}. \tag{42}$$

If m falls into more than one case, we choose one of these cases in an arbitrary way.

Construct an arrow in H from m to a vertex as follows:

$$x^{\odot (i+1)} \odot \bar{x}^{\odot j} \text{ in case (37)}; \tag{43}$$

$$x^{\odot (i+1)} \odot \bar{x}^{\odot j} \text{ in case (38)}; \tag{44}$$

$$x^{\odot i} \odot \bar{x}^{\odot j} \text{ in case (39)}; \tag{45}$$

$$x^{\odot i} \odot \bar{x}^{\odot j} \text{ in case (40)}; \tag{46}$$

$$x^{\odot (i+1)} \odot \bar{x}^{\odot (j+1)} \text{ in case (41)}; \tag{47}$$

$$x^{\odot i} \odot \bar{x}^{\odot j} \text{ in case (42)}. \tag{48}$$

Since $F \succ G$ and taking into account (36) we get that

$$g_{x^{\odot (i+1)} \odot \bar{x}^{\odot j}} < f_{x^{\odot (i+1)} \odot \bar{x}^{\odot j}} \leqslant g_{x^{\odot i} \odot \bar{x}^{\odot j}} \text{ in cases (37), (43) (provided that } g_x < 0 \text{ when } m = x); \tag{49}$$

$$g_{x^{\odot (i+1)} \odot \bar{x}^{\odot j}} < f_{x^{\odot (i+1)} \odot \bar{x}^{\odot j}} \leqslant g_{x^{\odot i} \odot \bar{x}^{\odot j}} \text{ in cases (38), (44) (provided that } g_x < 0 \text{ when } m = x); \tag{50}$$

$$g_{x^{\odot i}\odot\bar{x}^{\odot j}} < f_{x^{\odot i}\odot\bar{x}^{\odot j}} \leqslant g_{x^{\odot(i+1)}\odot\bar{x}^{\odot j}} \text{ in cases (39), (45) (provided that } g_{x^{\odot 3}} < 0 \text{ when } m = x^{\odot 3}); \tag{51}$$

$$g_{x^{\odot i}\odot\bar{x}^{\odot j}} < f_{x^{\odot i}\odot\bar{x}^{\odot j}} \leqslant g_{x^{\odot i}\odot\bar{x}^{\odot(j+1)}} \text{ in cases (40), (46)}$$
$$\text{(provided that } g_{x^{\odot 2}\odot\bar{x}} < 0 \text{ when } m = x^{\odot 2}\odot\bar{x}); \tag{52}$$

$$g_{x^{\odot(i+1)}\odot\bar{x}^{\odot(j+1)}} < f_{x^{\odot(i+1)}\odot\bar{x}^{\odot(j+1)}} \leqslant g_{x^{\odot i}\odot\bar{x}^{\odot j}} - 1 \text{ in cases (41), (47)}; \tag{53}$$

$$g_{x^{\odot i}\odot\bar{x}^{\odot j}} < f_{x^{\odot i}\odot\bar{x}^{\odot j}} \leqslant g_{x^{\odot(i+1)}\odot\bar{x}^{\odot(j+1)}} + 1 \text{ in cases (42), (48)}$$
$$\text{(provided that } g_{x^{\odot 3}\odot\bar{x}} < -1 \text{ when } m = x^{\odot 3}\odot\bar{x}). \tag{54}$$

Observe that the reservations in (49)-(52), (54) concern the cases when the head of a corresponding arrow equals $x^{\odot 2}$.

We draw a (uniquely defined) path P in H starting with the vertex $0 = x^{\odot 0}$ (it occurs in H due to (36)). We claim that along P the function

$$g_m + \mathrm{degtr}_{\bar{x}} m \tag{55}$$

strictly decreases. This would lead to a contradiction since P eventually contains a cycle. One can directly verify the claim studying the cases (49)-(54). Observe that at the beginning of P at the vertex 0 the value of the function (55) is non-positive due to (36). Therefore, the value of the function (55) of the head of the first arrow of P is negative, hence the reservations in cases (49)-(52), (54) are fulfilled (it happens when P arrives at the tropical monomial $x^{\odot 2}$). This proves the claim and the Theorem. □

7.3 Using integer coefficients in Min-Plus Nullstellensatz refutations is not always enough

Since a system of min-plus equations $x^{\odot 2} \oplus 1 = x,\ x^{\odot 2} = 1$ has no solutions, by Theorem 2.5 it has some `MP-NS` refutation (over $\mathbb{Q}_\infty$). In contrast, we show that this system does not admit `MP-NS` refutations with coefficients in $\mathbb{Z}_\infty$ (of any complexity!). Afterwards we show that in `MP-PCR` we can assume that the coefficients are integers.

Proposition 7.6. *There are no `MP-NSE` refutations of $x^{\odot 2} = 1$ with integer coefficients.*

Proof. Assume the contrary, then there exists a refutation

$$(f,g) = \bigoplus_{k\in\mathbb{Z}} x^{\odot k} \odot (a_k \odot (x^{\odot 2}\oplus 1, x) \oplus b_k \odot (x, x^{\odot 2}\oplus 1) \oplus c_k \odot (x^{\odot 2}, 1) \oplus d_k \odot (1, x^{\odot 2}))$$

where just a finite number of the coefficients $a_k, b_k, c_k, d_k \in \mathbb{Z}_\infty$ are finite (while not all of them are infinite) and $f \prec g$.

Let us consider the minimal coefficients (scalars) and the smallest tropical degrees in this refutation. Namely, denote $e := \min_k\{a_k, b_k, c_k, d_k\} \in \mathbb{Z}$ and take the minimal k for which the minimum in e is attained. If $e = a_k$ then comparing the coefficients at the tropical monomial $x^{\odot(k+1)}$ in $f,\ g$, we get that

$$\min\{a_{k-1}, a_{k+1}+1, b_k, c_{k-1}, d_{k+1}+1\} < \min\{a_k, b_{k-1}, b_{k+1}+1, c_{k+1}+1, d_{k-1}\},$$

which leads to a contradiction with the minimality of e. The same argument works when either $e = b_k$ or $e = d_k$ (in both latter cases one compares the coefficients at $x^{\odot(k+2)}$).

Thus, it remains to study the case $e = c_k$. Comparing the coefficients at $x^{\odot k}$ in (f, g), we get that

$$\min\{a_{k-2}, a_k + 1, b_{k-1}, c_{k-2}, d_k + 1\} + 1 \leqslant c_k + 1,$$

this is the place where we are taking into account that all the considered coefficients are integers. If either $a_k + 1 \leqslant c_k$ or $d_k + 1 \leqslant c_k$ then we get a contradiction with the minimality of e. If either $a_{k-2} \leqslant c_k$ or $b_{k-1} \leqslant c_k$, or $c_{k-2} \leqslant c_k$, then we get a contradiction with the minimality of k. ☐

Proposition 7.7. *There are no* `MP-NSR` *refutations of* $x^{\odot 2} = 1$ *with integer coefficients.*

Proof. Suppose the contrary, let $(f, g) :=$

$$\bigoplus_{k,\ell\in\mathbb{Z}} x^{\odot k} \odot \bar{x}^{\odot \ell} \odot \big(a_{k,\ell} \odot (x \oplus \bar{x}, 0) \oplus b_{k,\ell} \odot (0, x \oplus \bar{x}) \oplus c_{k,\ell} \odot (x \odot \bar{x}, 1) \oplus d_{k,\ell} \odot (1, x \odot \bar{x}) \oplus e_{k,\ell} \odot (x^{\odot 2}, 1) \oplus h_{k,\ell} \odot (1, x^{\odot 2})\big)$$

be a refutation where all (the finite number of finite) coefficients belong to $\mathbb{Z}$, while not all of them are infinite, and $f \prec g$.

Comparing the coefficients $f_{k,\ell}, g_{k,\ell}$ of f, g, respectively, at a tropical monomial $x^{\odot k} \odot \bar{x}^{\odot \ell}$, one obtains that

$$f_{k,\ell} = \min\{a_{k-1,\ell}, a_{k,\ell-1}, b_{k,\ell}, c_{k-1,\ell-1}, d_{k,\ell} + 1, e_{k-2,\ell}, h_{k,\ell} + 1\} <$$
$$g_{k,\ell} = \min\{a_{k,\ell}, b_{k-1,\ell}, b_{k,\ell-1}, c_{k,\ell} + 1, d_{k-1,\ell-1}, e_{k,\ell} + 1, h_{k-2,\ell}\}.$$

Denote by $m \in \mathbb{Z}$ the minimum among all the coefficients of the refutation. If m is attained at one of $a_{k,\ell}, b_{k-1,\ell}, b_{k,\ell-1}, d_{k-1,\ell-1}, h_{k-2,\ell}$, we get a contradiction with the latter inequality.

Thus, one can assume that either $m = c_{k,\ell}$ or $m = e_{k,\ell}$, and we take k to be the minimal possible. First, consider the case $m = c_{k,\ell}$. Then $g_{k,\ell} = m + 1$ (taking into account that all the coefficients are integers). Therefore, $f_{k,\ell} = m$ and $f_{k,\ell} = \min\{c_{k-1,\ell-1}, e_{k-2,\ell}\}$. This contradicts to the minimality of k. Now we consider the case $m = e_{k,\ell}$. Arguing in a similar way, we again conclude that $g_{k,\ell} = m+1$ and $f_{k,\ell} = m = \min\{c_{k-1,\ell-1}, e_{k-2,\ell}\}$ and again get a contradiction with the minimality of k. ☐

We now show that in `MP-PCR` we can get rid of non-integer coefficients. First of all, we prove a more efficient daglike version of Lemma 3.3 (part (5)):

Lemma 7.8 (Power of axioms, daglike version)**.** *There is a polynomial-size* `MP-PC` *derivation of* $x^d \oplus \overline{x}^d = 0$ *from* $x \oplus \overline{x} = 0$*.*

Proof. It suffices to derive it for $d = 2^{\lceil \log b \rceil}$ (then we can substitute $x^b \leqslant x^d$, $\overline{x}^b \leqslant \overline{x}^d$, which are $0 \leqslant x^{d-b}$, $0 \leqslant \overline{x}^{d-b}$, provided by Lemma 3.6 and multiplied by x^b and $\overline{x}^b$ respectively).

We proceed by induction on b. Tropically multiply the induction hypothesis $x^{\odot b} \oplus \overline{x}^{\odot b} \leqslant 0$ by $x^{\odot b}$ and substitute $\overline{x}^{\odot b} \leqslant \overline{x}^{\odot b} \odot x^{\odot b}$ (which is $0 \leqslant x^{\odot b}$, provided by Lemma 3.6, multiplied by $\overline{x}^{\odot b}$) into its left-hand side getting

$$x^{\odot 2b} \oplus \overline{x}^b \leqslant x^b.$$

Tropically add $\overline{x}^b$ to both sides and substitute the induction hypothesis on the right obtaining

$$x^{\odot 2b} \oplus \overline{x}^{\odot b} \leqslant 0. \tag{56}$$

Tropically multiply the latter inequality (56) by $\overline{x}^{\odot b}$ obtaining

$$x^{\odot 2b} \odot \overline{x}^{\odot b} \bigoplus \overline{x}^{\odot 2b} \leqslant \overline{x}^{\odot b}.$$

Tropically add $x^{\odot 2b}$ to both sides, substitute (56) on the right. Substitute $x^{\odot 2b} \leqslant x^{\odot 2b} \odot \overline{x}^{b}$ (which is $0 \leqslant \overline{x}^{\odot b}$, provided by Lemma 3.6 and multiplied by $x^{\odot 2b}$) on the left. □

Proposition 7.9. *`MP-PC` with integer coefficients simulates `MP-PC` with rational coefficients (as proof systems for unsolvable systems of tropical inequalities). For `MP-PCR`, this is a polynomial simulation.*

Proof. Let γ be the least common multiple of all denominators appearing in the derivation. We arithmetically (not tropically!) multiply the derivation by γ. Namely, we take each term of the initial inequalities to the tropical power γ. For the translation of clauses and for the axiom $x \odot \overline{x} = 1$ this can be done with a derivation of size polynomial in $\log \gamma$ using Lemma 3.6. For the axiom $x \oplus \overline{x} = 0$ this can be done using Lemma 7.8 as efficiently.

We also take to the power γ all side monomials appearing in the tropical multiplication rule. This way we get a valid derivation, where all terms are taken to the power γ, in particular, all coefficients are arithmetically multiplied by γ. Since we can assume by Theorem 3.8 that the last line of the initial derivation was $1 \leqslant 0$, the last line of the new derivation is $\gamma \leqslant 0$, which can be simplified by taking the minimum with $1 \leqslant 1$. □

7.4 Exact bounds on the degree of Min-Plus Nullstellensatz refutations for Tropical Knapsack in the economic encoding

In this subsection we consider tropical versions of the Knapsack system in the economic encoding (see Subsection 2.6). See also [Gri02] where exact bounds were established on the degree of Positivstellensatz proofs of the classical Knapsack system.

Definition 7.10. (i) A $(0,\infty)$-Tropical Knapsack is the following min-plus equation parameterized by a constant $r \in \mathbb{Q} \setminus \{0\}$:

$$\bigoplus_{1 \leqslant i \leqslant n} x_i = r.$$

(ii) A $(0,1)$-Tropical Knapsack is the following min-plus equation parameterized by a constant $r \in \mathbb{Q} \setminus \{0,1\}$:

$$\bigoplus_{1 \leqslant i \leqslant n} x_i = r.$$

Consider a system of min-plus equations $f_j^{(\ell)} = f_j^{(r)}$, $1 \leqslant j \leqslant k$ where

$$f_j^{(\ell)} = \bigoplus_m a_{j,m} \odot m, \qquad f_j^{(r)} = \bigoplus_m b_{j,m} \odot m, \qquad a_{j,m}, b_{j,m} \in \mathbb{Q}$$

and m ranges over some finite set of tropical monomials. Its Min-Plus Nullstellensatz refutation is defined by a system of tropical terms of the form $y_{j,t} \odot t$, $y_{j,t} \in \mathbb{Q}_\infty$ where $1 \leqslant j \leqslant k$, and t is a tropical monomial: according to Theorem 2.5 we require that for any tropical monomial w it holds that

$$\bigoplus_{m \odot t = w;\, j} a_{j,m} \odot y_{j,t} \prec \bigoplus_{m \odot t = w;\, j} b_{j,m} \odot y_{j,t}. \tag{57}$$

Note that in the case of $\mathbb{Q}_\infty$ the coefficient $(AY)_0$ corresponding to the constant monomial is finite, which excludes the solution where $\forall j, t\ y_{j,t} = \infty$.

Introduce matrices A, B whose rows are numerated by monomials w and whose columns are numerated by pairs (j, t) corresponding to the variables $y_{j,t}$. An $(w, y_{j,t})$-entry of A (respectively, of B) equals $a_{j,m}$ (respectively, $b_{j,m}$), provided that $w = m \odot t$. Thus, one can rewrite (57) as $A \odot Y \prec B \odot Y$ where the coordinates of vector Y are $\{y_{j,t} : j, t\}$. Clearly, both matrices A, B have the same size.

Following [GP18, Corollary 3.12] consider a dual to (57) system of min-plus inequalities

$$A^T \odot Z \succeq B^T \odot Z \tag{58}$$

where A^T, B^T denote the transposed matrices, and Z is a vector.

Lemma 7.11. *([GP18, Corollary 3.12 (iii)]) A linear system of min-plus inequalities (57) has no solution over $\mathbb{Q}_\infty$ distinct from $(\infty, \dots, \infty)$ iff (58) has a solution over $\mathbb{Q}$.*

Theorem 7.12. *The minimal degree of* `MP-NSE` *refutations of the $(0, \infty)$-Tropical Knapsack equals*

(i) 2 *when* $r > 0,\ r \neq \infty$;

(ii) $n + 1$ *when* $r < 0$.

Proof. To prove (i) we construct the tropical sum (so, an algebraic min-plus combination) of the following equations obtained by $\odot$-multiplying the axioms by 1, $(-r) \cdot x_i$, and $(-r/2)$, respectively:

$$\begin{aligned} x_1 \oplus \cdots \oplus x_n &= r, \\ x_i &= (-r) \odot x_i \odot (x_1 \oplus \cdots \oplus x_n), \text{ for } 1 \leqslant i \leqslant n, \\ (-r/2) \odot x_i^{\odot 2} &= (-r/2) \odot x_i, \text{ for } 1 \leqslant i \leqslant n. \end{aligned}$$

As a result we obtain the following Min-Plus Nullstellensatz refutation:

$$x_1 \oplus \cdots \oplus x_n \oplus (-r/2) \odot (x_1^{\odot 2} \oplus \cdots \oplus x_n^{\odot 2}) \succ r \oplus (-r) \odot \bigoplus_{1 \leqslant i,j \leqslant n} x_i \odot x_j \oplus (-r/2) \odot (x_1 \oplus \cdots \oplus x_n).$$

Here and below in the proofs of the upper bounds in Theorem 7.13 the sign $>$ in Nullstellensatz refutations means that for each tropical monomial its coefficient at the left-hand side is greater than the corresponding coefficient at the right-hand side (cf. Theorem 2.5).

To prove the upper bound in (ii) denote $S := x_1 \oplus \cdots \oplus x_n$. Given $S = r$, we construct the tropical sum of the following equations (note that $S^{\odot 0} = 1$):

$$\begin{aligned} S^{\odot(i+1)} &= r \odot S^{\odot i}, \text{ for } 0 \leqslant i \leqslant n, \\ (r/2) \odot m \odot x_j &= (r/2) \odot m \odot x_j^{\odot 2}, \text{ for } 1 \leqslant j \leqslant n, \end{aligned}$$

where m ranges over all tropical monomials of tropical degree $n - 1$.

As a result we obtain the following Min-Plus Nullstellensatz refutation:

$$\bigoplus_{1 \leqslant i \leqslant n+1, i \neq n} S^{\odot i} \oplus (r/2) \odot S^{\odot n} \succ r \odot \bigoplus_{0 \leqslant j \leqslant n} S^{\odot j} \oplus (r/2) \odot S^{\odot(n+1)}.$$

To prove the lower bound in (ii) assume the contrary, that is, there is Min-Plus Nullstellensatz refutation of the $(0, \infty)$-Tropical Knapsack of degree at most n (cf. (57)). Recall that we assume that the system contains $q = p$ together with each min-plus equation $p = q$, so there are $2(n + 2)$ equations. Our purpose is to show that a system of min-plus linear equations $A^T \odot Z = B^T \odot Z$ has a solution over $\mathbb{Q}$ (cf. (58)) where A, B are matrices corresponding to the $(0, \infty)$-Tropical Knapsack (cf. (57)).

Now we describe matrices A^T, B^T explicitly. The columns of A^T, B^T are numerated by tropical monomials w of degrees at most n. The rows of A^T, B^T are partitioned into $2(n + 1)$ blocks according to the number of equation $1 \leqslant j \leqslant 2(n + 1)$. To each tropical monomial t of degree at most $n - 2$ and $j = 2j' - 1,\ 1 \leqslant j' \leqslant n$ corresponds a row (t, j) in the j-th blocks of matrices A^T, B^T. The matrix A^T has its $((t, j), w)$-entry equal to 0 iff $t \odot x_j^{\odot 2} = w$, the matrix B^T has its $((t, j), w)$-entry equal to 0 iff $t \odot x_j = w$. Symmetrically, for $j = 2j',\ 1 \leqslant j' \leqslant n$, the matrix A^T has its $((t, j), w)$-entry equal to 0 iff $t \odot x_j = w$, the matrix B^T has its $((t, j), w)$-entry equal to 0 iff $t \odot x_j^{\odot 2} = w$. For all other monomials w, the entries numerated by $(t, j),\ 1 \leqslant j \leqslant 2n$ equal ∞.

Also to each tropical monomial t of degree at most $n-1$ corresponds a row in the blocks number $(2n+1)$ and $(2n+2)$. The matrix A^T has its $((t, 2n+1), w)$-entry equal to 0 iff $t \odot x_i = w$ for some $1 \leqslant i \leqslant n$, and the matrix B^T has its $((t, 2n + 1), w)$-entry equal to r iff $t = w$. Symmetrically, the matrix A^T has its $((t, 2n + 2), w)$-entry equal to r iff $t = w$, and the matrix B^T has its $((t, 2n + 2), w)$-entry equal to 0 iff $t \odot x_i = w$ for some $1 \leqslant i \leqslant n$. All other entries equal ∞.

For a tropical monomial w denote by $|w|$ the number of pairwise distinct variables among $x_1, \ldots, x_n$ occurring in w. We claim that for $Z_w := r \cdot |w| \in \mathbb{Q}$ the vector Z is a solution of the system $A^T \odot Z = B^T \odot Z$ (cf. (58)).

Indeed, for a row numerated by (t, j) from block $j = 2j' - 1$, $1 \leqslant j' \leqslant n$ one can note that this row in A^T (respectively, in B^T) contains a single finite entry at $((t, j), t \odot x_j^{\odot 2})$ (respectively, at $((t, j), t \odot x_j)$) equal to 0. Also for a row numerated by (t, j) for $j = 2j'$, $1 \leqslant j' \leqslant n$, one can note that this row in A^T (respectively, in B^T) contains a single finite entry at $((t, j), t \odot x_j)$ (respectively, at $((t, j), t \odot x_j^{\odot 2})$) equal to 0. Obviously, $|t \odot x_j^{\odot 2}| = |t \odot x_j|$. Hence both $(t, 2j' - 1)$ and $(t, 2j')$ coordinates of the vector $A^T \odot Z$ and of the vector $B^T \odot Z$ equal $r \cdot |t \odot x_j^{\odot 2}| = r \cdot |t \odot x_j|$.

For a row numerated by $(t, 2n + 1)$ from the block $(2n + 1)$ in A^T its finite entries equal 0 and they are located at $((t, 2n+1), t \odot x_i)$, $1 \leqslant i \leqslant n$. Hence the $(t, 2n+1)$-th coordinate of the vector $A^T \odot Z$ equals

$$\min_{1 \leqslant i \leqslant n} \{r \cdot |t \odot x_i|\} = r(|t| + 1) \tag{59}$$

since the degree of t is at most $n - 1$, and therefore there exists a variable $x_i, 1 \leqslant i \leqslant n$ not occurring in t (recall also that $r < 0$). On the other hand, the only finite entry of B^T at the row numerated by t equals r and it is located at $((t, 2n + 1), t)$. Hence the $(t, 2n + 1)$-th coordinate of the vector $B^T \odot Z$ equals $r + r \cdot |t|$, which proves the coincidence of the $(t, 2n + 1)$-th coordinates of the vectors $A^T \odot Z$ and $B^T \odot Z$ due to (59). By the same token one establishes the coincidence of the coordinates $(t, 2n + 2)$, which completes the proof of the claim.

Thus, $A^T \odot Z = B^T \odot Z$, which contradicts to the assumption that there exists a `MP-NSE` refutation of the $(0, \infty)$-Tropical Knapsack of degree at most n taking into account Lemma 7.11. $\square$

Theorem 7.13. *The minimal degree of `MP-NSE` refutations of the* $(0, 1)$-Tropical Knapsack *equals* *(i)* 2 *when* $r>0,\ r\neq 1$*;*

(ii) $n+1$ *when* $r<0$.

Proof. *(i)* When $r>1$ choose $0>\alpha\in\mathbb{Q},\ r+\alpha>1$, for example $\alpha:=(1-r)/2$. The upper bound in this case is justified by the following Min-Plus Nullstellensatz refutation:

$$x_1 \oplus \cdots \oplus x_n \oplus (r+\alpha) \leqslant x_1^{\odot 2} \oplus 1 \oplus \cdots \oplus x_n^{\odot 2} \oplus 1 \oplus \alpha \odot (x_1 \oplus \cdots \oplus x_n).$$

When $0<r<1$ choose $\beta,\gamma\in\mathbb{Q}$ such that $-r<\beta<0<\gamma<1-r$, for example $\beta:=-r/2,\gamma:=(1-r)/2$. Take the tropical sum (so, the algebraic min-plus combination) of the following equations:

$$\begin{aligned} \gamma \odot (x_1 \oplus \cdots \oplus x_n) &= (\gamma + r), \\ (\beta + r) \odot x_i &= \beta \odot x_i \odot (x_1 \oplus \cdots \oplus x_n),\ \text{for } 1 \leqslant i \leqslant n, \\ x_i^{\odot 2} \oplus 1 &= x_i,\ \text{for } 1 \leqslant i \leqslant n. \end{aligned}$$

As a result we obtain the following Min-Plus Nullstellensatz refutation:

$$\gamma \odot (x_1 \oplus \cdots \oplus x_n) \oplus (\beta + r) \odot x_1 \oplus (x_1^{\odot 2} \oplus 1) \oplus \cdots \oplus (\beta + r) \odot x_n \oplus (x_n^{\odot 2} \oplus 1) \succ$$

$$(\gamma + r) \oplus \beta \odot x_1 \odot (x_1 \oplus \cdots \oplus x_n) \oplus x_1 \oplus \cdots \oplus \beta \odot x_n \odot (x_1 \oplus \cdots \oplus x_n) \oplus x_n.$$

(ii) To prove the upper bound in (ii) denote

$$L_j := \bigoplus_{1 \leqslant i_1 < \cdots < i_k \leqslant n;\ i_1 \neq j, \ldots, i_k \neq j} x_{i_1} \odot \cdots \odot x_{i_k},\ 1 \leqslant j \leqslant n$$

and $L:=(x_j\oplus 0)\odot L_j$, being the tropical sum of all tropical multilinear monomials (in particular, it does not depend on j). Take the tropical sum of the following $n+1$ equalities:

$$(x_1 \oplus \cdots \oplus x_n) \odot L = r \odot L,$$

$$(r/2) \odot x_j \odot L_j = (r/2) \odot (x_j^{\odot 2} \oplus 1) \odot L_j,\ 1 \leqslant j \leqslant n.$$

As a result we obtain the following desired Min-Plus Nullstellensatz refutation:

$$\bigoplus_{1 \leqslant j \leqslant n} ((r/2) \odot x_j \oplus x_j^{\odot 2}) \odot L_j \succ r \odot L \oplus \bigoplus_{1 \leqslant j \leqslant n} ((r/2) \odot x_j^{\odot 2} \odot L_j.$$

The proof of the lower bound is similar to the proof of the lower bound in Theorem 7.12. The vector $Z_w:=r\cdot|w|$ is the same. The only difference is in the rows of the first $2n$ blocks of the matrices A^T,B^T. To $1\leqslant j\leqslant 2n$ and a tropical monomial t of degree at most $n-1$ corresponds a row (t,j) in the j-th blocks in A^T and in B^T.

For $j=2j'-1$, this row of A^T contains just two finite entries: at $((t,j),t\odot x_j^{\odot 2})$, equal to 0, and at $((t,j),t)$, equal to 1. The (t,j)-th row of B^T contains a single finite entry at $((t,j),t\odot x_j)$ equal to 0. Hence the (t,j)-th coordinate of the vector $A^T\odot Z$ (or respectively, of the vector $B^T\odot Z$) equals

$$\min\{r \cdot |t \odot x_j^{\odot 2}|, 1 + r \cdot |t|\} = r \cdot |t \odot x_j^{\odot 2}|$$

taking into account that $r < 0$ (or respectively, $r \cdot |t \odot x_j|$). Since $|t \odot x_j^{\odot 2}| = |t \odot x_j|$ we get that the (t, j)-th coordinates of the vectors $A^T \odot Z$, $B^T \odot Z$ coincide.

For $j = 2j'$, the equality holds by symmetry.

The blocks $(2n+1)$ and $(2n+2)$ of the rows in the matrices A^T, B^T are the same as in the matrices A^T, B^T in the proof of Theorem 7.12, so the proof of coincidence of the corresponding coordinates of the vectors $A^T \odot Z$, $B^T \odot Z$ literally follows the corresponding proof of Theorem 7.12. $\square$

Remark 7.14. Now we demonstrate that unlike Theorems 7.12, 7.13, when we use the dual encoding of Boolean variables (see Subsection 2.6) for both $\{0, \infty\}$ and $\{0, 1\}$, an upper bound 2 on the degree of refutations holds.

First consider $\{0, \infty\}$. In the case of $r < 0$, we can take the tropical sum of

$$\begin{aligned} \bigoplus_{1 \leqslant i \leqslant n} x_i &\leqslant r, \\ r/2 &\leqslant (r/2) \odot (x_i \oplus \bar{x}_i), \text{ for } 1 \leqslant i \leqslant n, \end{aligned}$$

and get the refutation

$$r/2 \oplus \bigoplus_{1 \leqslant i \leqslant n} x_i \succ r \oplus (r/2) \odot \bigoplus_{1 \leqslant i \leqslant n} (x_i \oplus \bar{x}_i).$$

In the case of $r > 0$ we take the tropical sum of the following inequalities

$$\begin{aligned} r \odot (\bigoplus_{1 \leqslant i \leqslant n} x_i) &\leqslant (\bigoplus_{1 \leqslant i \leqslant n} x_i)^{\odot 2}, \\ (r/2) \odot (x_i^{\odot 2} \oplus x_i \odot \bar{x}_i) &\leqslant (r/2) \odot x_i, \text{ for } 1 \leqslant i \leqslant n, \\ \infty &\leqslant (r/3) \odot x_i \odot \bar{x}_i, \text{ for } 1 \leqslant i \leqslant n, \\ r \odot (\bigoplus_{1 \leqslant i \leqslant n} x_i) &\leqslant r \end{aligned}$$

For $\{0, 1\}$, it can be demonstrated as follows. The dual encoding misses the axiom $x_i^{\odot 2} \oplus 1 = x_i$. Instead, it contains the axioms $x_i \oplus \overline{x}_i = 0$, $1 \leqslant i \leqslant n$. Thus we get the equation $(r/2) \odot x_1 \oplus \cdots \oplus (r/2) \odot x_n \oplus (r/2) \odot \overline{x}_1 \oplus \cdots \oplus (r/2) \odot \overline{x}_n = r/2$. First consider the case $r < 0$. Taking the tropical sum of the latter equation with the equation $r = x_1 \oplus \cdots \oplus x_n$ we arrive at the Min-Plus Nullstellensatz refutation

$$x_1 \oplus \cdots \oplus x_n \oplus r/2 \succ (r/2) \odot x_1 \oplus \cdots \oplus (r/2) \odot x_n \oplus (r/2) \odot \overline{x}_1 \oplus \cdots \oplus (r/2) \odot \overline{x}_n \oplus r.$$

Now consider the case $r > 1$. Take the tropical sum (so, the algebraic min-plus combination) of the following equations:

$$\begin{aligned} r &= x_1 \oplus \cdots \oplus x_n, \\ (r-1)/3 \odot x_i &= (r-1)/3 \odot (x_i^{\odot 2} \oplus x_i \odot \overline{x}_i), \text{ for } 1 \leqslant i \leqslant n, \\ (r-1)/2 \odot x_i \odot \overline{x}_i &= (r+1)/2, \text{ for } 1 \leqslant i \leqslant n. \end{aligned}$$

As a result we obtain a Min-Plus Nullstellensatz refutation

$$\begin{aligned} &\bigoplus_{1 \leqslant i \leqslant n} x_i \oplus (r-1)/3 \odot \bigoplus_{1 \leqslant i \leqslant n} (x_i^{\odot 2} \oplus x_i \odot \overline{x}_i) \oplus (r+1)/2 \\ &\qquad \prec r \oplus (r-1)/3 \odot \bigoplus_{1 \leqslant i \leqslant n} x_i \oplus (r-1)/2 \odot \bigoplus_{1 \leqslant i \leqslant n} x_i \odot \overline{x}_i. \end{aligned}$$

Finally, consider the case $0 < r < 1$. Denote $\alpha := (1-r)/2,\ \gamma := \min\{r, \alpha\},\ \delta := \gamma/2$. Take the tropical sum of the following equations:

$$\begin{aligned} r \odot x_i &= x_i \odot (x_1 \oplus \cdots \oplus x_n),\ \text{for } 1 \leqslant i \leqslant n, \\ 1 &= x_i \odot \overline{x}_i,\ \text{for } 1 \leqslant i \leqslant n, \\ \alpha \odot (x_1 \oplus \cdots \oplus x_n) &= r + \alpha, \\ \delta \odot (x_i^{\odot 2} \oplus x_i \odot \overline{x}_i) &= \delta \odot x_i,\ \text{for } 1 \leqslant i \leqslant n. \end{aligned}$$

As a result we obtain a Min-Plus Nullstellensatz refutation:

$$\gamma \odot \bigoplus_{1 \leqslant i \leqslant n} x_i \oplus 1 \oplus \delta \odot \bigoplus_{1 \leqslant i \leqslant n} (x_i^{\odot 2} \oplus x_i \odot \overline{x}_i) \succ \bigoplus_{1 \leqslant i,j \leqslant n} x_i \odot x_j \oplus \bigoplus_{1 \leqslant i \leqslant n} x_i \odot \overline{x}_i \oplus (r+\alpha) \oplus \delta \odot \bigoplus_{1 \leqslant i \leqslant n} x_i.$$

7.5 Size bounds for refutations of a tropical binomial

In this subsection we prove lower bounds on the size of Min-Plus Nullstellensatz refutations for a tropical binomial $x^{\odot k} = c$ with the $\{0, 1\}$ Boolean encoding axioms. Note that there are short MP-PCR refutations of this binomial for $c > k$ and $c < 0$, because we can take the axioms $x \leqslant 1$, $x \geqslant 0$ to the respective power by Lemma 3.6.

We start with the economical encoding and then continue to the dual encoding.

Theorem 7.15. *The size of MP-NSE refutations of a tropical binomial $x^{\odot k} = c$ for $c \in \mathbb{Q}$ is greater than k.*

Proof. Consider a refutation

$$(f, g) := \bigoplus_i x^{\odot i} \odot (a_i \odot (x^{\odot 2} \oplus 1, x) \oplus b_i \odot (x, x^{\odot 2} \oplus 1) \oplus u_i \odot (x^{\odot k}, c) \oplus v_i \odot (c, x^{\odot k})),$$

where $a_i, b_i, u_i, v_i \in \mathbb{Q}_\infty$ and $f \succ g$.

Construct a directed graph G whose vertices are tropical monomials of g. For each tropical monomial m of g denote by $c(m), c'(m) \in \mathbb{Q}$ the coefficient at m in g (respectively, in f). We distinguish 5 cases:

$$m = x^{\odot(i+1)},\ c(m) = a_i; \tag{60}$$

$$m = x^{\odot(i+2)},\ c(m) = b_i; \tag{61}$$

$$m = x^{\odot i},\ c(m) = b_i + 1; \tag{62}$$

$$m = x^{\odot i},\ c(m) = u_i + c; \tag{63}$$

$$m = x^{\odot(i+k)},\ c(m) = v_i \tag{64}$$

for suitable i. When a tropical monomial m falls in more than one case, we choose for it any one among these cases.

Draw an arrow in G from a vertex m to a vertex

$$x \odot m = x^{\odot(i+2)} \text{ in case (60)}; \tag{65}$$

$$x^{\odot(i+1)} \text{ in case (61)}; \tag{66}$$

$$x^{\odot(i+1)} \text{ in case (62);} \tag{67}$$

$$x^{\odot(i+k)} \text{ in case (63);} \tag{68}$$

$$x^{\odot i} \text{ in case (64).} \tag{69}$$

Since $f \succ g$ we get that

$$c(x^{\odot(i+2)}) < c'(x^{\odot(i+2)}) \leqslant c(x^{\odot(i+1)}) \text{ in cases (60), (65);} \tag{70}$$

$$c(x^{\odot(i+1)}) < c'(x^{\odot(i+1)}) \leqslant c(x^{\odot(i+2)}) \text{ in cases (61), (66);} \tag{71}$$

$$c(x^{\odot(i+1)}) + 1 < c'(x^{\odot(i+1)}) + 1 \leqslant c(x^{\odot i}) \text{ in cases (62), (67);} \tag{72}$$

$$c(x^{\odot(i+k)}) + c < c'(x^{\odot(i+k)}) + c \leqslant c(x^{\odot i}) \text{ in cases (63), (68);} \tag{73}$$

$$c(x^{\odot i}) - c < c'(x^{\odot i}) - c \leqslant c(x^{\odot(i+k)}) \text{ in cases (64), (69).} \tag{74}$$

There exists a cycle Z in the graph G. First assume that the numbers of arrows in Z of types (68) and (69) are not equal. Then Z contains at least k arrows of types (65), (66), (67) because along each arrow of type (68) (respectively, (69)) the tropical degree of a tropical monomial increases (respectively, decreases) by k, while along each arrow of types (65), (66), (67) the tropical degree changes at most by 1.

Now we assume that Z contains an equal numbers of arrows of types (68) and (69). This leads to a contradiction since the coefficients at tropical monomials decrease along arrows of types (65), (66), (67) due to (70), (71), (72) (taking into account (63), (64), (73), (74)). $\square$

We now establish a similar lower bound when using the axioms $(01/\oplus), (01/\odot)$.

Theorem 7.16. *The size of MP-NSR refutations of a tropical binomial $x^{\odot k} = c$ for $c \in \mathbb{Q}$ is greater than k.*

Proof. Consider a refutation

$$(f, g) := \bigoplus_{i,j} x^{\odot i} \odot \bar{x}^{\odot j} \odot$$

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

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

Similarly to Theorem 7.15 construct a directed graph H whose vertices are tropical monomials m of g. We distinguish 7 cases:

$$m = x^{\odot i} \odot \bar{x}^{\odot j},\ c(m) = a_{i,j}; \tag{75}$$

$$m = x^{\odot(i+1)} \odot \bar{x}^{\odot j},\ c(m) = b_{i,j}; \tag{76}$$

$$m = x^{\odot i} \odot \bar{x}^{\odot(j+1)},\ c(m) = b_{i,j}; \tag{77}$$

$$m = 1 \odot x^{\odot i} \odot \bar{x}^{\odot j},\ c(m) = d_{i,j} + 1; \tag{78}$$

$$m = x^{\odot(i+1)} \odot \bar{x}^{\odot(j+1)},\ c(m) = e_{i,j}; \tag{79}$$

$$m = c \odot x^{\odot i} \odot \bar{x}^{\odot j},\ c(m) = u_{i,j} + c; \tag{80}$$

$$m = x^{\odot(i+k)} \odot \bar{x}^{\odot j},\ c(m) = v_{i,j} \tag{81}$$

for suitable i, j. Similar to the proof of Theorem 7.15, when a tropical monomial m falls in more than one case, we choose for it any one among these cases.

Draw an arrow in H from m to

$$x \odot m = x^{\odot(i+1)} \odot \bar{x}^{\odot j} \text{ in case (75);} \tag{82}$$

$$x^{\odot i} \odot \bar{x}^{\odot j} \text{ in case (76);} \tag{83}$$

$$x^{\odot i} \odot \bar{x}^{\odot j} \text{ in case (77);} \tag{84}$$

$$x^{\odot(i+1)} \odot \bar{x}^{\odot(j+1)} \text{ in case (78);} \tag{85}$$

$$1 \odot x^{\odot i} \odot \bar{x}^{\odot j} \text{ in case (79);} \tag{86}$$

$$x^{\odot(i+k)} \odot \bar{x}^{\odot j} \text{ in case (80);} \tag{87}$$

$$c \odot x^{\odot i} \odot \bar{x}^{\odot j} \text{ in case (81).} \tag{88}$$

Since $f \succ g$ we get that

$$c(x^{\odot(i+1)} \odot \bar{x}^{\odot j}) < c'(x^{\odot(i+1)} \odot \bar{x}^{\odot j}) \leqslant c(x^{\odot i} \odot \bar{x}^{\odot j}) \text{ in cases (75), (82);} \tag{89}$$

$$c(x^{\odot i} \odot \bar{x}^{\odot j}) < c'(x^{\odot i} \odot \bar{x}^{\odot j}) \leqslant c(x^{\odot(i+1)} \odot \bar{x}^{\odot j}) \text{ in cases (76), (83);} \tag{90}$$

$$c(x^{\odot i} \odot \bar{x}^{\odot j}) < c'(x^{\odot i} \odot \bar{x}^{\odot j}) \leqslant c(x^{\odot i} \odot \bar{x}^{\odot(j+1)}) \text{ in cases (77), (84);} \tag{91}$$

$$c(x^{\odot(i+1)} \odot \bar{x}^{\odot(j+1)}) < c'(x^{\odot(i+1)} \odot \bar{x}^{\odot(j+1)}) \leqslant c(x^{\odot i} \odot \bar{x}^{\odot j}) - 1 \text{ in cases (78), (85);} \tag{92}$$

$$c(x^{\odot i} \odot \bar{x}^{\odot j}) < c'(x^{\odot i} \odot \bar{x}^{\odot j}) \leqslant c(x^{\odot(i+1)} \odot \bar{x}^{\odot(j+1)}) + 1 \text{ in cases (79), (86);} \tag{93}$$

$$c(x^{\odot(i+k)} \odot \bar{x}^{\odot j}) < c'(x^{\odot(i+k)} \odot \bar{x}^{\odot j}) \leqslant c(x^{\odot i} \odot \bar{x}^{\odot j}) - c \text{ in cases (80), (87);} \tag{94}$$

$$c(x^{\odot i} \odot \bar{x}^{\odot j}) < c'(x^{\odot i} \odot \bar{x}^{\odot j}) \leqslant c(x^{\odot(i+k)} \odot \bar{x}^{\odot j}) + c \text{ in cases (81), (88).} \tag{95}$$

There exists a cycle Z in the graph H. As in the proof of Proposition 7.15 one can justify the required lower bound k when the numbers of arrows of types (87), (88) differ.

When they are equal we observe that the number of arrows of type (86) in Z is greater than the number of arrows of type (85), because the coefficient at a tropical monomial increases (respectively, decreases) by 1 along an arrow of type (86) due to (79) (respectively, of type (85) due to (78)), while the coefficient does not change along arrows of types (82), (83), (84) due to (75), (76), (77), 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 (86) (respectively, (85)), while this tropical degree does not increase along arrows of types (82), (83), (84). □

Remark 7.17. Remark 3.11 mentions that treelike `MP-NSR` proofs can be transformed into `MP-NSE` proofs by Theorem 3.10 more efficiently over $\mathbb{Q}$ instead of $\mathbb{Q}_\infty$. The proof of Theorem 7.15 does not use the presence of a finite constant in the right-hand side and also can be easily generalized to refutations of $x^{\odot(k+d)} = c \odot x^d$. Therefore, Theorem 7.16 has also an indirect proof from the proof transformation construction in Theorem 3.10: the proof of the binomial $x^{\odot k} = c$ is transformed into a proof of the above-mentioned binomial for d being the degree of the `MP-NSR` proof; if the original proof was of polynomial size, the new proof is of polynomial size as well, which contradicts Theorem 7.15.

8 Further Research and Open Questions

Tropical proof systems provide an alternative view to the study of propositional proof systems that deal with Boolean operations over linear inequalities. This gives hopes for attacking longstanding open problems from new directions.

The "knowledge border" for Boolean formulas in CNF lies between `treelike Res(CP)`, where superpolynomial lower bounds are known because of the quasipolynomial monotone interpolation [GP23], treelike `Res(Lin)` with semantic weakening, where exponential lower bounds are known for `PHP` [PT21], regular `Res(`$\oplus$`)`, where exponential lower bounds for the binary pigeon-hole principle have been proved recently [EGI23], 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)` [PT21].

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)`. Systems without dual variables seem to be weaker and proving lower bounds for them seems even more feasible. 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 both in `MP-NSR` and `MP-NSE`.

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. [FGI+21] 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.

Acknowledgements

The authors are 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.

References

[ABG23] 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.

[AGHT20] Yaroslav Alekseev, Dima Grigoriev, Edward A. Hirsch, and Iddo Tzameret. Semi-algebraic proofs, IPS lower bounds and the τ-conjecture: Can a natural number be negative? In *STOC-2020*, pages 54–67, 2020. Full version is to appear in SICOMP.

[BE17] Aaron Bertram and Robert Easton. The tropical Nullstellensatz for congruences. *Adv. Math*, 308:36–82, 2017.

[BFI+18] 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.

[BIK+96] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proc. London Math. Soc.*, 73(3):1–26, 1996.

[CCT87] W. Cook, C.R. Coullard, and Gy. Turán. On the complexity of cutting-plane proofs. *Discrete Applied Mathematics*, 18(1):25–38, 1987.

[CEI96] 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.

[CR79] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *J. Symb. Log.*, 44(1):36–50, 1979.

[EGI23] Klim Efremenko, Michal Garlik, and Dmitry Itsykson. Lower bounds for regular resolution over parities. ECCC TR23-187, 2023.

[FGI+21] 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.

[GP18] Dima Grigoriev and Vladimir V. Podolskii. Tropical effective primary and dual Nullstellensätze. *Discrete and Computational Geometry*, 59(3):507–552, 2018.

[GP23] 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.

[Gri02] Dima Grigoriev. Complexity of Positivstellensatz proofs for the knapsack. *Computational Complexity*, 10:139–154, 2002.

[Hak85] Armin Haken. The intractability of resolution. *Theoret. Comput. Sci.*, 39(2-3):297–308, 1985.

[HK06] Edward A. Hirsch and Arist Kojevnikov. Several notes on the power of Gomory-Chvátal cuts. *Ann. Pure Appl. Log.*, 141(3):429–436, 2006.

[IS20] Dmitry Itsykson and Dmitry Sokolov. Resolution over linear equations modulo two. *Ann. Pure Appl. Log.*, 171(1), 2020.

[JM18] Daniel Joo and Kalina Mincheva. Prime congruences of additively idempotent semirings and a Nullstellensatz for tropical polynomials. *Selecta Math.*, 24:2207–2233, 2018.

[Juk12] Stasys Jukna. *Boolean Function Complexity.* Springer, 2012.

[Kra98] Jan Krajícek. Discretely ordered modules as a first-order extension of the cutting planes proof system. *J. Symb. Log.*, 63(4):1582–1596, 1998.

[Kra01] Jan Krajícek. On the weak pigeonhole principle. *Fundamenta Mathematicae*, 170(1–3):123–140, 2001.

[Kra19] Jan Krajíček. *Proof Complexity.* Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2019.

[Lau18] Massimo Lauria. A note about k-DNF resolution. *Information Processing Letters*, 137:33–39, 2018.

[MR18] D. Maclagan and F. Rincon. Tropical ideals. *Compos. Math.*, 154:640–670, 2018.

[MS15] Diane Maclagan and Bernd Sturmfels. *Introduction to Tropical Geometry.* Springer, 2015.

[PT21] Fedor Part and Iddo Tzameret. Resolution with counting: Dag-like lower bounds and different moduli. *Comput. Complex.*, 30(1):2, 2021.

[Pud97] Pavel Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *The Journal of Symbolic Logic*, 62(3):981–998, 1997.

[RT08] Ran Raz and Iddo Tzameret. Resolution over linear equations and multilinear proofs. *Ann. Pure Appl. Logic*, 155(3):194–224, 2008.

[Tse68] 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.

[Urq87] Alasdair Urquhart. Hard examples for resolution. *J. ACM*, 34(1):209–219, 1987.

A Working with min-plus equations instead of min-plus inequalities

Similarly to the transition from Theorem 2.3 to Theorem 2.5, one could define Min-Plus Polynomial Calculus working with equations instead of inequalities. It, however, does not weaken the proof system.

Definition A.1. [Min-Plus Polynomial Calculus with Equations, $\texttt{MP-PC}_=$] Consider a system of min-plus polynomial equations $F = \{(f_1 = g_1), \ldots, (f_m = g_m)\}$ in n variables. A $\texttt{MP-PC}_=$ refutation of F is a list of min-plus equations

$$(p_1 = q_1), (p_2 = q_2), \ldots, (p_K = q_K),$$

kept as ordered pairs of tropical polynomials, such that

1. For each monomial $m = x_1^{\odot j_1} \odot \cdots \odot x_n^{\odot j_n}$, its coefficient in p_K is greater than its coefficient in q_K; q_K must include a finite constant term.
2. Each of the pairs $(p_i = q_i)$ was derived via one of the following derivation rules
   - We can take pair of the initial polynomials: $(p_i = q_i) = (f_j = g_j)$ for some $1 \leqslant j \leqslant m$. Or we can take the axiom $(p_i = q_i) = (0 = 0)$.
   - We can always swap two polynomials: $(p_i = q_i) = (q_j = p_j)$ for some $1 \leqslant j < i$.
   - We can take a minimum of two previously derived pairs of polynomials:
   $$(p_i = q_i) = (p_j \oplus p_K = q_j \oplus q_K)$$
   where $1 \leqslant j, k < i$.
   - We can multiply a previously derived pair of min-plus polynomials by any term $t = c \odot x_1^{\odot j_1} \odot \cdots \odot x_n^{\odot j_n}$:
   $$(p_i = q_i) = (p_j \odot t = q_j \odot t)$$
   where $1 \leqslant j < i$.
   - Finally, if we have derived pairs of polynomials $(p_j = q_j) = (p_K = q_j)$ and $(p_K = q_K)$, then we can **substitute** polynomial q_K instead of the polynomial p_j. Formally, we can derive the following pair:
   $$(p_i = q_i) = (q_K = q_j)$$
   where $p_j = p_K$ and $1 \leqslant j, k < i$.

Theorem A.2. *Suppose a system of min-plus equations $F = \{(f_1 = g_1), \ldots, (f_m = g_m)\}$ (where each equation is interpreted as a pair of inequalities) has an* $\texttt{MP-PC}$ *refutation of size S. Then there is an* $\texttt{MP-PC}_=$ *refutation of F of size* $\mathrm{poly}(S)$.

Proof. Suppose we have a $\texttt{MP-PC}$ refutation

$$(p_1 \leqslant q_1), (p_2 \leqslant q_2), \ldots, (p_K \leqslant q_K).$$

We are going to simulate our derivation step by step. For each inequality $(p_i \leqslant q_i)$ we will derive equation

$$(p_i = q_i \oplus p_i)$$

in $\mathtt{MP\text{-}PC}_=$. For the input inequalities we clearly can derive that $(f_j = g_j \oplus f_j)$ by tropically adding $f_j = f_j$. Translation of the axioms is also trivial: $0 \leqslant 0$ becomes $0 = 0$, and $p \leqslant \infty$ becomes $p = p$.

Suppose we have already derived equations

$$(p_1 = q_1 \oplus p_1)\,, (p_2 = q_2 \oplus p_2)\,, \ldots, (p_i = q_i \oplus p_i)\,.$$

Now we need to simulate each rule of $\mathtt{MP\text{-}PC}$:

- The minimum rule is easy to simulate: from

$$(p_j = q_j \oplus p_j) \text{ and } (p_k = q_k \oplus p_k)$$

  we can derive

$$(p_j \oplus p_k = q_j \oplus p_j \oplus q_k \oplus p_k)$$

- The tropical multiplication rule is also easy to simulate:

$$(p_j = q_j \oplus p_j)$$

  we can derive

$$(p_j \odot t = (q_j \odot m) \oplus (p_j \odot t))\,.$$

- To simulate the transitivity rule

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

  that is,

$$\frac{p = p \oplus h \qquad h = h \oplus r}{p = p \oplus r},$$

  we simply make an xor of the second equation with p and apply the transitivity rule for equations getting $p = p \oplus h \oplus r$. After that we perform weakening on the right using the following procedure: given $p = p \oplus h \oplus r$, get rid of h by first adding $r = r$ to this equation and then making substitutions of equations $p \oplus r = p \oplus h \oplus r = p$ combined with swap.

At the end, we get an equation of the form

$$p_K = q_K \oplus p_K,$$

where for each monomial $m = x_1^{\odot j_1} \odot \cdots \odot x_n^{\odot j_n}$ its coefficient in p_K is greater than its coefficient in q_K. Now observe that with our notation this means that for each monomial $m = x_1^{\odot j_1} \odot \cdots \odot x_n^{\odot j_n}$ its coefficient in p_K is greater than its coefficient in $q_K \oplus p_K$. The same applies to the presence of a finite free term in q_K (respectively, $q_K \oplus p_K$). Thus, $p_K = q_K \oplus p_K$ is a correct ending line for the $\mathtt{MP\text{-}PC}_=$ refutation. $\square$

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il