On the Convexity of a Fragment
of Pure Set Theory with Applications
within a Nelson-Oppen Framework[*]

Domenico Cantone   Pietro Maugeri

Dept. of Mathematics and Computer Science
University of Catania
Catania, Italy

domenico.cantone@unict.it   pietro.maugeri@unict.it

Andrea De Domenico

Scuola Superiore di Catania
University of Catania
Catania, Italy

andrea.dedomenico@studium.unict.it

The Satisfiability Modulo Theories (SMT) issue concerns the satisfiability of formulae from multiple background theories, usually expressed in the language of first-order predicate logic with equality. SMT solvers are often based on variants of the Nelson-Oppen combination method, a solver for the quantifier-free fragment of the combination of theories with disjoint signatures, via cooperation among their decision procedures. When each of the theories to be combined by the Nelson-Oppen method is *convex* (that is, any conjunction of its literals can imply a disjunction of equalities only when it implies at least one of the equalities) and decidable in polynomial time, the running time of the combination procedure is guaranteed to be polynomial in the size of the input formula. In this paper, we prove the convexity of a fragment of Zermelo-Fraenkel set theory, called Multi-Level Syllogistic, most of whose polynomially decidable fragments we have recently characterized.

Keywords: convex theories, satisfiability modulo theories, decision problem, computable set theory.

Introduction

In the process of developing reliable and provably correct software, it is often necessary to express and then subsequently verify properties that belong to different logical languages. Thus, the correctness of a software system depends on being able to prove these conditions, expressed in distinct first-order signatures with equality. The search for a satisfying assignment of a given formula with respect to some background first-order theory is known as the SMT (Satisfiability Modulo Theories) problem.

SMT solvers [2] are particularly useful tools for the automated verification of properties expressed with quantifier-free first-order formulae. Some theories usually integrated with common SMT solvers are the theory of arrays, of bit-vectors, of linear arithmetic, and the theory of uninterpreted functions.

Every background theory used in some SMT solver comes along with its own satisfiability procedure. The problem of modularly combining such special-purpose algorithms is highly non-trivial, since without the appropriate restrictions it is not even decidable [3].

We will now briefly introduce some definitions to understand how to tackle this question and under which assumptions one can do it effectively.

A first-order quantifier-free theory T, identified with the set of its theorems, is *stably infinite* if every formula φ satisfiable in T is satisfiable in an infinite model of T. Let Σ_1 and Σ_2 be signatures for a first-order language. A $(\Sigma_1 \cup \Sigma_2)$-formula φ is *pure* if every literal in φ is a Σ_1-literal or a Σ_2-literal. It is easy to see that every quantifier-free $(\Sigma_1 \cup \Sigma_2)$-formula φ can be *purified*, yet maintaining satisfiability, by (i) substituting every *impure* subterm of the form $f(t)$ with $f(x)$, where x is a new variable, (ii) adding to φ the conjunct $x = t$, and (iii) recursively purifying the term t, if needed.

We say that two theories T_1 and T_2 over the signatures Σ_1 and Σ_2, respectively, are *disjoint* when Σ_1 and Σ_2 do not share any non-logical symbols.[1] The Nelson-Oppen [16] procedure provides a method for combining decision procedures for disjoint, stably infinite theories T_1 and T_2 into one for $T_1 \oplus T_2$, namely the $(\Sigma_1 \cup \Sigma_2)$-theory defined as the deductive closure of the union of the theories T_1 and T_2.

A theory T is *convex* if for all conjunctions of literals φ in T and for all nonempty disjunctions $\bigvee_{i=1}^{n} x_i = y_i$ of equalities, φ implies $\bigvee_{i=1}^{n} x_i = y_i$ in T if and only if φ implies $x_i = y_i$ in T for some $i \in \{1, ..., n\}$.

Examples of convex theories are the theory of Linear Rational Arithmetic $\mathsf{T_{LRA}}$ and the theory of list structure $\mathsf{T_L}$.

The non-logical symbols of the theory of $\mathsf{T_{LRA}}$ are $+, -, \leqslant, 0, 1$; following [4, Chapter 3.4.2], its axioms (universally quantified) are:

$$
\begin{array}{ll}
x + 0 = x, & x + (-x) = 0, \\
(x + y) + z = x + (y + z), & x + y = y + x, \\
x \leqslant y \wedge y \leqslant x \rightarrow x = y, & x \leqslant y \vee y \leqslant x, \\
x \leqslant y \rightarrow x + z \leqslant y + z, & x \leqslant y \wedge y \leqslant z \rightarrow x \leqslant z, \\
nx = 0 \rightarrow x = 0, & (\exists y)\, x = ny \quad \text{(for each positive integer } n\text{),}
\end{array}
$$

where nx stands for $\underbrace{x + \cdots + x}_{n \text{ times}}$. After [16], the non-logical symbols of the theory of list structure $\mathsf{T_L}$ are car, cdr, cons, and atom, and its axioms are:

$$
\begin{array}{l}
\mathsf{car}(\mathsf{cons}(x, y)) = x, \\
\mathsf{cdr}(\mathsf{cons}(x, y)) = y, \\
\neg\mathsf{atom}(x) \rightarrow \mathsf{cons}(\mathsf{car}(x), \mathsf{cdr}(x)) = x, \\
\neg\mathsf{atom}(\mathsf{cons}(x, y)),
\end{array}
$$

where (i) cons is a binary function, with $\mathsf{cons}(x, y)$ representing the list constructed by prepending the object x to the list y, (ii) car and cdr are unary functions, the left and right projections, respectively, and (iii) atom is true if and only if x is a single-element list.

Given two disjoint stable infinite theories T_1 and T_2, the Nelson-Oppen combination technique establishes the satisfiability of a conjunction of pure formulae $\varphi_1 \wedge \varphi_2$ (where φ_i has signature Σ_i) in $T_1 \oplus T_2$ from the decision procedures for φ_1 and φ_2. The key idea is to propagate equalities $x = y$ to φ_2 whenever $T_1 \cup \varphi_1$ implies $x = y$, and conversely. This iterative process can be performed quickly in polynomial time, when the theories involved are convex. On the other hand, case-splitting would occur when dealing

---

[1]Besides propositional connectives, logical symbols comprise equality.

with non-convex theories, since only one of the equalities of the disjunct implied by φ_i must be chosen at every step.

In [19, 21, 20], variants of the Nelson-Oppen method were used to combine theories involving sets/multisets of urelements (i.e., objects with no internal structure) with the theory of integers and with the theory of cardinal numbers in presence of a cardinality operator. The SMT problem in the context of the theory of finite sets is considered in [1].

In this paper, we start an investigation for combining decidable fragments of pure Zermelo-Fraenkel set theory (in which sets are recursively built up from other sets) with other theories within the Nelson-Oppen framework. More specifically, our main result is that the theory Multi-Level Syllogistic (the basic language of computable set theory—MLS for short) is convex and therefore its decision procedure (and those of its several polynomial fragments [8, 10]) can be efficiently combined with the decision procedures of other basic decidable theories, such as for instance the theory of lists and the theory of linear rational arithmetic, since set theory is plainly stably infinite.

———————

The paper is organized as follows. Section 1 introduces the syntax and semantics of the theory MLS of our interest. Then, in Section 2, we prove the main result of the paper, namely that the theory MLS is convex. We also review several fragments of MLS endowed with polynomial-time decision procedures, since these inherit convexity from MLS and are therefore particularly interesting for efficient combinations with other convex decidable theories. Subsequently, in Section 3, we prove the non-convexity of various extensions of MLS. Finally, in Section 4, we provide some closing remarks and plans for future research.

1 Syntax and semantics of MLS

Multi-Level Syllogistic (MLS) is the quantifier-free propositional closure of atoms of the types:

$$x = \varnothing, \quad x = y, \quad x \subseteq y, \quad x \in y, \quad x = y \setminus z, \quad x = y \cup z, \quad x = y \cap z, \tag{1}$$

where x, y, z stand for set variables. We denote by $Vars(\varphi)$ the collection of the set variables occurring in any MLS-formula φ.

The satisfiability problem for MLS has been first solved in the seminal paper [14]. Its NP-completeness (and that of its extension MLSS with the singleton operator) has been later proved in [11]. Several extensions of MLS have been proved decidable over the years, giving rise to the field of Computable Set Theory (see [9, 12, 18, 13] for an in-depth account).

The semantics of MLS is defined in the most natural way by means of *set assignments*.

A SET ASSIGNMENT M is any map from a *finite* collection of set variables V, denoted $\mathrm{dom}(M)$, into the von Neumann universe $\mathcal{V}$.

We recall that $\mathcal{V}$ is the cumulative hierarchy constructed in stages by transfinite recursion over the class On of all ordinals. Specifically,

$$\mathcal{V} := \bigcup_{\alpha \in On} \mathcal{V}_\alpha,$$

where, recursively,

$$\mathcal{V}_\alpha := \bigcup_{\beta < \alpha} \mathscr{P}(\mathcal{V}_\beta),$$

for every $\alpha \in On$, with $\mathscr{P}(\cdot)$ denoting the powerset operator.

The notion of rank of a set is strictly connected to the construction steps of the von Neumann hierarchy. Specifically, for any set $s \in \mathscr{V}$, the rank of s (denoted $\mathsf{rk}(s)$) is defined as the least ordinal α such that $s \subseteq \mathscr{V}_\alpha$. The rank function is extended to set assignments M, by putting $\mathsf{rk}(M) := \max\{\mathsf{rk}(Mx) \mid x \in \mathsf{dom}(M)\}$.

The set operators and relators of MLS are interpreted according to their usual semantics. Thus, given a set assignment M, we put:

$$M(x \star y) := Mx \star My$$

and

$$M(x = y) = \mathsf{true} \iff Mx = My,$$
$$M(x \in y) = \mathsf{true} \iff Mx \in My,$$
$$M(x = y \star z) = \mathsf{true} \iff Mx = M(y \star z),$$

where $\star \in \{\cup, \cap, \setminus\}$ and $x, y, z \in \mathsf{dom}(M)$.

Finally, for all MLS-formulae φ and ψ, we put by structural recursion:

$$M(\neg \varphi) := \neg M(\varphi), \qquad\qquad M(\varphi \wedge \psi) := M\varphi \wedge M\psi,$$
$$M(\varphi \vee \psi) := M\varphi \vee M\psi, \qquad\qquad M(\varphi \to \psi) := M\varphi \to M\psi.$$

An MLS-formula φ is SATISFIABLE if there exists a set assignment M over $Vars(\varphi)$ such that $M\varphi = \mathsf{true}$, in which case we also write $M \models \varphi$ and say that M is a MODEL for φ. If φ is satisfied by all set assignments, we say that φ is TRUE and write $\models \varphi$.

By way of disjunctive normal form, the satisfiability problem for MLS can be reduced to the satisfiability problem for conjunctions of MLS-literals, namely MLS-atoms of types (1) and their negation. In addition, for the purposes of simplifying some proofs, we can further restrict ourselves to MLS-conjunctions involving a minimal number of literal types. As shown in [8], all the atoms in (1) and their negations can be rewritten in terms of atoms of type $x \in y$ and $x = y \setminus z$ only by repeatedly applying the following equivalences much as rewrite rules (the existential quantifiers are then just dropped while the quantified variables are replaced by fresh ones):

- $\models x = \varnothing \longleftrightarrow x = x \setminus x$,
- $\models x \neq \varnothing \longleftrightarrow (\exists w) w \in x$,
- $\models x \notin y \longleftrightarrow (\exists w)(x \in w \wedge w = w \setminus y)$,
- $\models x = y \longleftrightarrow (\exists e)(x = y \setminus e \wedge e = e \setminus e)$,
- $\models x = y \cap z \longleftrightarrow (\exists w)(w = y \setminus z \wedge x = y \setminus w)$,
- $\models x = y \cup z \longleftrightarrow (\exists e, w)(w = x \setminus y \wedge w = z \setminus y \wedge e = y \setminus x \wedge e = e \setminus e)$,
- $\models x \subseteq y \longleftrightarrow x = y \cap x$,
- $\models x \neq y \longleftrightarrow (\exists v, w, z)(w = x \cup y \wedge z = x \cap y \wedge v \in w \wedge v \notin z)$,
- $\models x \neq y \star z \longleftrightarrow (\exists w)(x \neq w \wedge w = y \star z)$,

where $\star \in \{\cup, \cap, \setminus\}$.

Henceforth, we will restrict ourselves to MLS-formulae that are conjunctions of atoms of the following two types only:

$$x \in y, \quad x = y \setminus z. \tag{2}$$

In the rest of the paper, these will be simply referred to as MLS-conjunctions.

Finally, as a piece of notation, for any given *finite* set $\mathscr{L}$ of literals, we write $\bigwedge \mathscr{L}$ (resp., $\bigvee \mathscr{L}$) to denote the conjunction (resp., disjunction) of all the literals in $\mathscr{L}$.

2 Convexity of MLS

Our main goal is to prove that the theory MLS is convex, namely that, for any MLS-conjunction φ and any given finite *nonempty* set $\mathscr{E}$ of equalities among variables, we have:

$$\models \varphi \longrightarrow \bigvee \mathscr{E} \quad \Longrightarrow \quad \models \varphi \longrightarrow x = y, \text{ for some equality } x = y \text{ in } \mathscr{E}.$$

To prove that the theory MLS is convex, we will proceed by way of contradiction.

Thus, let us suppose that there exists an MLS-conjunction φ (namely a conjunction of literals of type (2)) and a finite, nonempty set $\mathscr{E}$ of equalities among variables such that:

(C1) $\models \varphi \longrightarrow \bigvee \mathscr{E}$;

(C2) $\not\models \varphi \longrightarrow x = y$, for any $x = y$ in $\mathscr{E}$
  (that is, for every $x = y$ in $\mathscr{E}$ there exists some set assignment $M_{x,y}$ such that $M_{x,y} \models \varphi \wedge x \neq y$).

It is not restrictive to additionally assume that $Vars(\mathscr{E}) \subseteq Vars(\varphi)$.[2]

In view of condition (C2), our conjunction φ is satisfiable. Among all the models for φ, we select one, say M, that satisfies as few as possible equalities in $\mathscr{E}$, namely such that the cardinality of $\mathscr{E}_M^+ := \{\ell \in \mathscr{E} \mid M \models \ell\}$ is *minimal*. We also set $\mathscr{E}_M^- := \{\neg \ell \mid \ell \in \mathscr{E} \setminus \mathscr{E}_M^+\}$, so $\mathscr{E}_M^-$ is the collection of the inequalities $x \neq y$ such that $x = y$ is in $\mathscr{E}$ and $M \not\models x = y$ (hence, $M \models x \neq y$).

Plainly, we have $M \models \varphi \wedge \bigwedge \mathscr{E}_M^+ \wedge \bigwedge \mathscr{E}_M^-$. Notice that, while $\bigwedge \mathscr{E}_M^-$ may be empty, the conjunction $\bigwedge \mathscr{E}_M^+$ must contain at least one literal, since $M \models \bigvee \mathscr{E}$ by condition (C1).

Let $\overline{\ell}$ be any equality $\overline{x} = \overline{y}$ in $\bigwedge \mathscr{E}_M^+$, which will be referred to in the rest of our proof as the *designated equality of $\mathscr{E}$*. We will prove that the conjunction

$$\varphi^* \stackrel{\text{Def}}{:=} \varphi \wedge \bigwedge \left(\mathscr{E}_M^+ \setminus \{\overline{\ell}\} \right) \wedge \bigwedge \mathscr{E}_M^- \wedge \overline{x} \neq \overline{y}$$

is satisfiable, thereby contradicting the assumed minimality of M, since for every model M^* for φ^* we would have $\mathscr{E}_{M^*}^+ = \mathscr{E}_M^+ \setminus \{\overline{\ell}\}$, and therefore $|\mathscr{E}_{M^*}^+| < |\mathscr{E}_M^+|$.

Before diving into the details of the proof, we provide an overview of how the set assignment M can be suitably enlarged into another set assignment M^* that satisfies all the conjuncts of $\varphi \wedge \bigwedge \mathscr{E}_M^+ \wedge \bigwedge \mathscr{E}_M^-$ but the designated equality $\overline{\ell}$, thus proving that φ^* is satisfiable.

Proof overview

The construction of M^* consists in two phases: the first one, the BOOLEAN PHASE, takes care of the satisfiability of the Boolean literals of φ^*, namely the literals in φ^* of type $x = y \setminus z$, $x = y$, and $x \neq y$, whereas the second one, the MEMBERSHIP PHASE, takes care of the satisfiability of the membership literals of φ^*, namely those of the form $x \in y$.

In order to model $\overline{x} \neq \overline{y}$, we add to exactly one between $M\overline{x}$ and $M\overline{y}$ a new member $\mathfrak{s}$ not already occurring in $\bigcup_{x \in Vars(\varphi)} Mx$. The set $\mathfrak{s}$ must be chosen with care to prevent that no set produced during the

---

[2] Indeed, without disrupting conditions (C1) and (C2), for any variable $x \in Vars(\mathscr{E})$ one may add to φ the literal $x \in w$, where w stands for some fresh variable.

subsequent membership phase is new to the current set assignment. In addition, the set $\mathfrak{s}$ must be added to the right sets Mx in order that the resulting assignment keeps satisfying all of the Boolean literals in $\varphi \wedge \bigwedge \mathscr{E}_M^+ \wedge \bigwedge \mathscr{E}_M^-$ other than the designated equality $\overline{x} = \overline{y}$. The first problem is solved by selecting as $\mathfrak{s}$ any set of rank strictly greater than that of M. As for the second condition, recalling that, by (C2), the conjunction $\varphi \wedge \overline{x} \neq \overline{y}$ is satisfiable, we can select a model $\overline{M}$ for it. Therefore $\overline{M}\overline{x} \neq \overline{M}\overline{y}$, and so we can pick some element $\mathfrak{t}$ belonging to exactly one of the sets $\overline{M}\overline{x}$ and $\overline{M}\overline{y}$. By adding our special set $\mathfrak{s}$ as an element to all and only those sets Mx such that $\mathfrak{t} \in \overline{M}x$, for $x \in Vars(\varphi)$, we obtain a new assignment, which will be denoted M_0. It turns out that M_0 correctly models all the conjuncts in φ^*, but the membership literals $x \in y$ for which $M_0x \neq Mx$. We denote by V_0 the collection of variables x in φ such that $M_0x \neq Mx$.

Example 2.1. *We illustrate the Boolean phase of our enlargement process with the following* MLS-*conjunction*

$$\varphi \stackrel{\text{Def}}{=} x = \overline{y} \setminus z \wedge x = \overline{x} \setminus w \wedge x \neq \overline{y} \wedge \overline{y} \in w \wedge w \in v \wedge z \in v$$

and with the equality $\overline{x} = \overline{y}$.

Let M and $\overline{M}$ be the set assignments over $Vars(\varphi) = \{v, w, x, \overline{x}, \overline{y}, z\}$ so defined, where to enhance readability we use the shorthand $\{\emptyset\}^2 := \{\{\emptyset\}\}$—likewise, $\{\emptyset\}^4$ will denote the set $\{\{\{\{\emptyset\}\}\}\}$:

$$Mx = \emptyset, \qquad M\overline{x} = M\overline{y} = \{\emptyset\}, \qquad Mz = Mw = \{\emptyset, \{\emptyset\}\}, \qquad Mv = \{\{\emptyset, \{\emptyset\}\}\},$$

$$\overline{M}x = \emptyset, \qquad \overline{M}\overline{y} = \overline{M}z = \{\emptyset\}, \qquad \overline{M}\overline{x} = \overline{M}w = \{\emptyset\}^2, \qquad \overline{M}v = \{\{\emptyset\}, \{\emptyset\}^2\}.$$

It can easily be checked that $M \models \varphi \wedge \overline{x} = \overline{y}$ and $\overline{M} \models \varphi \wedge \overline{x} \neq \overline{y}$ hold.

Let $\mathfrak{s} := \{\emptyset\}^4$, so that $\mathrm{rk}(\mathfrak{s}) = 4 > 3 = \mathrm{rk}(Mv) = \mathrm{rk}(M)$. Since $\emptyset \in \overline{M}\overline{y} \setminus \overline{M}\overline{x}$, we can put $\mathfrak{t} := \emptyset$, and so we have:

$$M_0 u = \begin{cases} \{\emptyset, \mathfrak{s}\} & \text{if } u = \overline{y} \\ \{\emptyset, \{\emptyset\}, \mathfrak{s}\} & \text{if } u = z \\ Mu & \text{otherwise} \end{cases}$$

and $V_0 = \{\overline{y}, z\}$.

Plainly, M_0 satisfies all literals in $\varphi \wedge \overline{x} \neq \overline{y}$ but the literals $\overline{y} \in w$ and $z \in v$.   □

The subsequent membership phase performs the following enlargement step, for $k = 0, 1, 2, \ldots$, until needed:

extend the assignment M_k by putting, for each $u \in V_k$,

$$M_{k+1}u := M_k u \cup \{M_k v \mid v \in V_k \text{ and } Mv \in Mu\},$$

while setting $M_{k+1}u := M_k u$ for the remaining variables u in $Vars(\varphi)$, and define V_{k+1} as the collection of variables u in $Vars(\varphi)$ such that $M_{k+1}u \neq M_k u$.

For $k = 0, 1, 2, \ldots$, it turns out that each M_k correctly models all the Boolean literals in φ^* and all the membership literals in φ^* but those of the form $x \in y$ with $x \in V_{k+1}$. Hence, as soon as some V_k is empty, the assignment M_k is plainly a model for φ^*, and so the membership phase can stop. By the well-foundedness of the membership relation, such a situation occurs in at most $\overline{n} := |Vars(\varphi)|$ steps, and therefore $M_{\overline{n}}$ is a model for φ^*, proving that φ^* is satisfiable.

Example 2.1 (cont'd). *We continue our example by illustrating the membership phase of our enlargement process. We recall that $\mathsf{V}_0 = \{\bar{y}, z\}$. Since $M\bar{y} \in Mw = Mz$ and $Mz \in Mv$, we have $\mathsf{V}_1 = \{z, w, v\}$, $M_1 z = \{\emptyset, \{\emptyset\}, \mathfrak{s}, \{\emptyset, \mathfrak{s}\}\}$, $M_1 w = \{\emptyset, \{\emptyset\}, \{\emptyset, \mathfrak{s}\}\}$, $M_1 v = \{\{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \mathfrak{s}\}\}$, and $M_1 u = M_0 u$ for all $u \neq z, w, v$. Next, since $Mw \in Mv$ and $Mz \in Mv$, we have $\mathsf{V}_2 = \{v\}$, $M_2 u = M_1 u$ for all $u \neq v$, and*
$$M_2 v = \{\{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \mathfrak{s}\}, \{\emptyset, \{\emptyset\}, \mathfrak{s}, \{\emptyset, \mathfrak{s}\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \mathfrak{s}\}\}\}.$$
Finally, since $Mv \notin \bigcup_{u \in Vars(\varphi)} Mu$, we can actually stop. In fact, at this point we have

$$M_2 = M_3 = M_4 = \cdots.$$

Plainly, $M_2 \models \varphi \wedge \bar{x} \neq \bar{y}$.   □

Proof details

For any $V \subseteq Vars(\varphi)$, we will use the notation MV to denote the set $\{Mv \mid v \in V\}$. Let $\mathfrak{s}$ be any fixed set whose rank is larger than the rank of M, namely such that $\mathrm{rk}(\mathfrak{s}) > \mathrm{rk}(M)$.

We define by recursion two sequences $\{\mathsf{V}_n\}_{n \in \mathbb{N}}$ and $\{M_n\}_{n \in \mathbb{N}}$, respectively of subsets of $Vars(\varphi)$ and of set assignments over $Vars(\varphi)$, by putting:

$$\mathsf{V}_0 := \{u \in Vars(\varphi) \mid \mathfrak{t} \in \overline{M}u\}, \tag{3}$$

$$\mathsf{V}_n := \{u \in Vars(\varphi) \mid Mu \cap M\mathsf{V}_{n-1} \neq \emptyset\}, \quad \text{for } n \geqslant 1, \tag{4}$$

and

$$M_0 v := \begin{cases} Mv \cup \{\mathfrak{s}\} & \text{if } v \in \mathsf{V}_0 \\ Mv & \text{if } v \in Vars(\varphi) \setminus \mathsf{V}_0, \end{cases} \tag{5}$$

$$M_n v := \begin{cases} M_{n-1} v \cup M_{n-1}\{u \in \mathsf{V}_{n-1} \mid Mu \in Mv\} & \text{if } v \in \mathsf{V}_n \\ M_{n-1} v & \text{if } v \in Vars(\varphi) \setminus \mathsf{V}_n, \end{cases} \tag{6}$$

$$\text{for } n \geqslant 1 \text{ and } v \in Vars(\varphi).$$

As a direct consequence of (5) and (6), the following results can be easily proved by induction:

Lemma 2.2.   (a) *For every $v \in Vars(\varphi)$, we have*

$$Mv \subseteq M_0 v \subseteq \cdots \subseteq M_n v \subseteq \cdots.$$

(b) *For all $v \in Vars(\varphi)$ and $n \in \mathbb{N}$, we have:*

$$M_n v \subseteq Mv \cup \{\mathfrak{s}\} \cup \bigcup_{k=0}^{n-1} M_k \{u \in \mathsf{V}_k \mid Mu \in Mv\}.$$

Lemma 2.2(a) implies that the sequence of assignments $\{M_n\}_{n \in \mathbb{N}}$ is plainly pointwise convergent. As a consequence of the next lemma and corollary, it will follow in fact that $\{M_n\}_{n \in \mathbb{N}}$ converges "uniformly", and it does so in at most $|Vars(\varphi)|$ steps.

Lemma 2.3. *Let $k \in \mathbb{N}$. We have:*

(a) *if $\mathsf{V}_k = \emptyset$ then, for all $n \geqslant k$,*

  (a_1) $\mathsf{V}_n = \emptyset$,

  (a_2) $M_n = M_k$;

(b) if $V_k \neq \emptyset$, then

$$k \leqslant \min\big(|Vars(\varphi)| - 1, \mathrm{rk}(M)\big). \tag{7}$$

Proof. If $V_k = \emptyset$, then $V_{k+1} = \emptyset$ and $M_{k+1} = M_k$ by (4) and (6), respectively. By iterating the same argument, one can easily prove that $V_n = \emptyset$ and $M_n = M_k$, for all $n \in \mathbb{N}$, proving (a).

As for (b), we preliminarily observe that, by (4), for all $v \in Vars(\varphi)$ and $n \geqslant 1$ we have

$$v \in V_n \implies (\exists u \in V_{n-1})Mu \in Mv. \tag{8}$$

Thus, if $V_k \neq \emptyset$, by picking any $v_k \in V_k$ and by repeatedly applying (8), it follows that there exist $v_0, v_1, \ldots, v_{k-1} \in Vars(\varphi)$ such that

$$Mv_0 \in Mv_1 \in \cdots \in Mv_{k-1} \in Mv_k. \tag{9}$$

By the well-foundedness of $\in$, the variables $v_0, v_1, \ldots, v_{k-1}, v_k$ must be pairwise distinct. Hence, $k + 1 \leqslant |Vars(\varphi)|$. In addition, (9) also yields $k \leqslant \mathrm{rk}(Mv_k) \leqslant \mathrm{rk}(M)$. Thus, (7) follows, proving (b). □

The preceding lemma yields immediately the following result.

Corollary 2.4. *For all $h, k > \min\big(|Vars(\varphi)| - 1, \mathrm{rk}(M)\big)$, we have $M_h = M_k$.*

Letting $\overline{n} := |Vars(\varphi)|$, Corollary 2.4 implies that $M_n = M_{\overline{n}}$, for all $n \geqslant \overline{n}$.

Next we prove a number of technical lemmas that will culminate in the proof that

$$M_{\overline{n}} \models \varphi \wedge \bigwedge \mathscr{E}_M^- \wedge \overline{x} \neq \overline{y},$$

where $\overline{x} = \overline{y}$ is the designated equality of $\mathscr{E}$. Thus, we will have that

$$\mathscr{E}_M^- \subsetneq \mathscr{E}_{M_{\overline{n}}}^- \quad \text{and} \quad |\mathscr{E}_{M_{\overline{n}}}^+| < |\mathscr{E}_M^+|,$$

contradicting the minimality of $|\mathscr{E}_M^+|$. Hence, the convexity of MLS will follow, since our initial assumption on φ and $\mathscr{E}$ that conditions (C1) and (C2) hold will be proved to be untenable.

The following lemma provides some useful bounds on the rank of $M_n v$, for $n \in \mathbb{N}$ and $v \in Vars(\varphi)$.

Lemma 2.5. *For all $n \in \mathbb{N}$ and $v \in Vars(\varphi)$, we have*

- $\mathrm{rk}(M_n v) = \mathrm{rk}(\mathfrak{s}) + n + 1$, *if $v \in V_n$,*
- $\mathrm{rk}(M_n v) \leqslant \mathrm{rk}(\mathfrak{s}) + n$, *if $v \notin V_n$.*

Proof. We proceed by induction on n. For $n = 0$ and $v \in V_0$, from (5) we have $M_0 v = Mv \cup \{\mathfrak{s}\}$. Hence, $\mathrm{rk}(M_0 v) = \max\{\mathrm{rk}(Mv), \mathrm{rk}(\{\mathfrak{s}\})\} = \mathrm{rk}(\mathfrak{s}) + 1$, since $\mathrm{rk}(\mathfrak{s}) > \mathrm{rk}(Mv)$. On the other hand, if $v \notin V_0$, then $\mathrm{rk}(M_0 v) = \mathrm{rk}(Mv) < \mathrm{rk}(\mathfrak{s})$.

Next, let $n > 0$ and $v \in V_n$. By (6), we have:

$$\mathrm{rk}(M_n v) = \max\big(\mathrm{rk}(M_{n-1}v), \mathrm{rk}(M_{n-1}\{z \in V_{n-1} \mid Mz \in Mv\})\big). \tag{10}$$

By inductive hypothesis, we readily have

- $\mathrm{rk}(M_{n-1}v) \leqslant \mathrm{rk}(\mathfrak{s}) + n$, and
- $\mathrm{rk}(M_{n-1}\{z \in V_{n-1} \mid Mz \in Mv\}) \leqslant \mathrm{rk}(\mathfrak{s}) + n + 1$.

In addition, since $v \in V_n$, then by (4), $Mu \in Mv$ for some $u \in V_{n-1}$. Hence, again by inductive hypothesis, $\mathrm{rk}(Mu) = \mathrm{rk}(\mathfrak{s}) + n$, and since $u \in \{z \in V_{n-1} \mid Mz \in Mv\}$, we have

$$\mathrm{rk}(M_{n-1}\{z \in V_{n-1} \mid Mz \in Mv\}) = \mathrm{rk}(\mathfrak{s}) + n + 1.$$

Thus, by (10), we get $\mathrm{rk}(M_n v) = \mathrm{rk}(\mathfrak{s}) + n + 1$.

On the other hand, if $v \notin V_n$, then by (6) and by the inductive hypothesis we have $\mathrm{rk}(M_n v) = \mathrm{rk}(M_{n-1}v) \leqslant \mathrm{rk}(\mathfrak{s}) + n$. $\qquad \square$

Next we prove that the set $\mathfrak{s}$ can enter M_n only when $n = 0$.

Lemma 2.6. *For all $n \in \mathbb{N}$ and $v \in Vars(\varphi)$, we have:*

(a) $M_n v \neq \mathfrak{s}$;

(b) $\mathfrak{s} \in M_n x \iff \mathfrak{s} \in M_0 x$.

Proof. Concerning (a), we proceed by induction on n.

For $n = 0$, by (5) we have:

- $\mathrm{rk}(M_0 v) = \mathrm{rk}(\mathfrak{s}) + 1$, if $v \in V_0$ (by Lemma 2.5);
- $\mathrm{rk}(M_0 v) = \mathrm{rk}(Mv) < \mathrm{rk}(\mathfrak{s})$, if $v \notin V_0$.

In both cases, it follows that $M_0 v \neq \mathfrak{s}$.

For the inductive step, let $n > 1$. If $v \in V_n$, then by Lemma 2.5 we have $\mathrm{rk}(M_n v) = \mathrm{rk}(\mathfrak{s}) + n + 1$, and therefore $M_n v \neq \mathfrak{s}$. On the other hand, if $v \notin V_n$, then $M_n v = M_{n-1}v \neq \mathfrak{s}$, by (6) and by the inductive hypothesis.

Next we prove (b) by induction on n.

The base case $n = 0$ is trivial.

For the inductive step, let $n > 0$. If $\mathfrak{s} \in M_0 x$, then Lemma 2.2(a) yields readily $\mathfrak{s} \in M_n x$. Conversely, let $\mathfrak{s} \in M_n x$. If $x \notin V_n$, then by (6) we have $\mathfrak{s} \in M_n x = M_{n-1}x$, and therefore by inductive hypothesis $\mathfrak{s} \in M_0 x$. On the other hand, if $x \in V_n$, then again by (6) we have

$$\mathfrak{s} \in M_n x = M_{n-1}x \cup M_{n-1}\{y \in V_{n-1} \mid My \in Mx\}.$$

In view of (a), the latter formula yields $\mathfrak{s} \in M_{n-1}x$, and therefore $\mathfrak{s} \in M_0 x$ follows again by inductive hypothesis, completing the proof of (b), and in turn of the lemma. $\qquad \square$

The following lemma proves that, at each construction step of the assignments M_n's, only elements of rank at least $\mathrm{rk}(\mathfrak{s})$ can enter into play.

Lemma 2.7. *For every set $\mathfrak{q} \in M_n x$, for some $x \in Vars(\varphi)$ and $n \in \mathbb{N}$, if $\mathrm{rk}(\mathfrak{q}) < \mathrm{rk}(\mathfrak{s})$ then $\mathfrak{q} \in Mx$.*

Proof. Let $x \in Vars(\varphi)$, $n \in \mathbb{N}$, and $\mathfrak{q} \in M_n x$, with $\mathrm{rk}(\mathfrak{q}) < \mathrm{rk}(\mathfrak{s})$. From Lemma 2.2(b), we have

$$M_n x \subseteq Mx \cup \{\mathfrak{s}\} \cup \bigcup_{k=0}^{n-1} M_k \{y \in V_k \mid My \in Mx\}.$$

Since, by Lemma 2.5, the rank of each member of $\{\mathfrak{s}\} \cup \bigcup_{k=0}^{n-1} M_k\{y \in V_k \mid My \in Mx\}$ is greater than or equal to $\mathrm{rk}(\mathfrak{s})$, then necessarily $\mathfrak{q} \in Mx$ $\qquad \square$

All the inequalities $x \neq y$ satisfied by M are satisfied by every M_n, as proved in the following corollary.

Corollary 2.8. *If $Mx \neq My$, for some $x, y \in Vars(\varphi)$, then $M_n x \neq M_n y$, for every $n \in \mathbb{N}$.*

Proof. W.l.o.g., let us assume that $Mx \nsubseteq My$, and let $\mathfrak{q} \in Mx \setminus My$. Also, let $n \in \mathbb{N}$. By Lemma 2.2(a), $\mathfrak{q} \in M_n x$. Plainly, $\mathsf{rk}\,(\mathfrak{q}) < \mathsf{rk}\,(Mx) < \mathsf{rk}\,(\mathfrak{s})$ and $\mathfrak{q} \notin My$. Thus, Lemma 2.7 yields $\mathfrak{q} \notin M_n y$, proving that $M_n x \neq M_n y$. $\square$

To show that every membership $x \in y$ satisfied by M is correctly modeled by $M_{\overline{n}}$, we will need the following result.

Lemma 2.9. *For all $n \in \mathbb{N}$ and $x, y \in Vars(\varphi)$, if $x \in \mathsf{V}_n$ and $Mx \in My$, then $y \in \mathsf{V}_{n+1}$ and $M_n x \in M_{n+1} y$.*

Proof. Let $n \in \mathbb{N}$ and assume that $Mx \in My$, for some $x, y \in Vars(\varphi)$, and that $x \in \mathsf{V}_n$. Then, by (4), $y \in \mathsf{V}_{n+1}$. In addition, from (6), the latter membership relation yields immediately that $M_n x \in M_{n+1} y$. $\square$

We are now ready to prove our main lemma.

Lemma 2.10. *The assignment $M_{\overline{n}}$ satisfies φ.*

Proof. We prove the lemma, by showing that $M_{\overline{n}}$ correctly models all the conjuncts in φ. We recall that, in view of the reduction process outlined in Section 1, our formula φ contains conjuncts of two types only, namely $x \in y$ and $x = y \setminus z$.

Conjuncts of type $x \in y$.   Let $x \in y$ occur in φ, so that $Mx \in My$ holds. If $x \notin \mathsf{V}_n$ for all $n \in \mathbb{N}$, then $M_{\overline{n}} x = Mx \in My \subseteq M_{\overline{n}} y$ (by Lemma 2.2(a)), from which $M_{\overline{n}} x \in M_{\overline{n}} y$ follows.
Conversely, if $x \in \mathsf{V}_n$, for some $n \in \mathbb{N}$, we set $\overline{m} := \max\{n \in \mathbb{N} \mid x \in \mathsf{V}_n\}$. In addition, since $Mx \in My$ and $x \in \mathsf{V}_{\overline{m}}$, Lemma 2.9 implies $y \in \mathsf{V}_{\overline{m}+1}$ and therefore, by Lemma 2.3(b), $\overline{m} + 1 \leqslant |Vars(\varphi)| - 1 \leqslant \overline{n}$. Thus, Lemma 2.9 again together with Lemma 2.2(a) yields $M_{\overline{n}} x = M_{\overline{m}} x \in M_{\overline{m}+1} y \subseteq M_{\overline{n}} y$, from which $M_{\overline{n}} x \in M_{\overline{n}} y$ follows.

Conjuncts of type $x = y \setminus z$.   Let $x = y \setminus z$ occur in φ, so that $Mx = My \setminus Mz$ holds. We will prove that $M_{\overline{n}} \models x = y \setminus z$, by proving that $M_{\overline{n}} x \subseteq M_{\overline{n}} y \setminus M_{\overline{n}} z$ and $M_{\overline{n}} y \setminus M_{\overline{n}} z \subseteq M_{\overline{n}} x$ hold.

Proof of $M_{\overline{n}} x \subseteq M_{\overline{n}} y \setminus M_{\overline{n}} z$.   From Lemma 2.2(b), we have:

$$M_{\overline{n}} x \ \subseteq \ Mx \ \cup \ \{\mathfrak{s}\} \ \cup \ \bigcup_{k=0}^{\overline{n}-1} M_k \{u \in \mathsf{V}_k \mid Mu \in Mx\}.$$

Let $\mathfrak{q} \in M_{\overline{n}} x$. We first consider that case in which $\mathfrak{q} \in Mx$. Then $\mathfrak{q} \in My \setminus Mz$. Hence, by Lemma 2.2(a), $\mathfrak{q} \in M_{\overline{n}} y$. In addition, since $\mathfrak{q} \notin Mz$ and $\mathsf{rk}\,(\mathfrak{q}) < \mathsf{rk}\,(\mathfrak{s})$, Lemma 2.7 yields $\mathfrak{q} \notin M_{\overline{n}} z$. Thus, $\mathfrak{q} \in M_{\overline{n}} y \setminus M_{\overline{n}} z$.
Next, let $\mathfrak{q} = \mathfrak{s}$. Hence, $\mathfrak{s} \in M_0 x$ (by Lemma 2.6(b)), so that $x \in \mathsf{V}_0$ (by (5) and (3)), and therefore $\mathfrak{t} \in \overline{M} x$. Since $\overline{M} x = \overline{M} y \setminus \overline{M} z$, then $\overline{M} x \subseteq \overline{M} y$, and so $\mathfrak{t} \in \overline{M} y$ and $\mathfrak{t} \notin \overline{M} z$; hence, $y \in \mathsf{V}_0$ and $z \notin \mathsf{V}_0$. Therefore $\mathfrak{s} \in M_0 y \subseteq M_{\overline{n}} y$ (by (5) and Lemma 2.2(b)) and $\mathfrak{s} \notin M_0 z$ (by (3)). Thus, by Lemma 2.6(b), $\mathfrak{s} \notin M_{\overline{n}} z$. In conclusion, if $\mathfrak{q} = \mathfrak{s}$ then $\mathfrak{q} \in M_{\overline{n}} y \setminus M_{\overline{n}} z$, as in the preceding case.
Finally, let $\mathfrak{q} = M_k u$, for some $0 \leqslant k < \overline{n}$ and $u \in \mathsf{V}_k$ such that $Mu \in Mx$. Recalling that $Mx = My \setminus Mz$, then $Mu \in My$, so that $M_k u \in M_{k+1} y \subseteq M_{\overline{n}} y$ (by Lemma 2.9). In addition, $Mu \notin Mz$. By Lemma 2.5, $M_k u \notin Mz \cup \{\mathfrak{s}\}$. Since, by Lemma 2.2(b),

$$M_{\overline{n}} z \ \subseteq \ Mz \ \cup \ \{\mathfrak{s}\} \ \cup \ \bigcup_{k=0}^{\overline{n}-1} M_k \{v \in \mathsf{V}_k \mid Mv \in Mz\}, \tag{11}$$

to prove that $M_k u \notin M_{\overline{n}} z$, it is sufficient to show that $M_k u \notin \bigcup_{h=0}^{\overline{n}-1} M_h \{v \in V_h \mid Mv \in Mz\}$. By way of contradiction, let us assume that $M_k u = M_h v$, for some $0 \leqslant h < \overline{n}$ and $v \in V_h$ such that $Mv \in Mz$. By Lemma 2.5, and since $u \in V_k$, we must have $h = k$. Since $Mu \notin Mz$ while $Mv \in Mz$, we plainly have $Mu \neq Mv$. Hence, by Corollary 2.8, $M_h u \neq M_h v = M_k u$, which contradicts our preceding assumption $M_k u = M_h v$. Thus, $M_k u \notin \bigcup_{h=0}^{\overline{n}-1} M_h \{v \in V_h \mid Mv \in Mz\}$ holds. In view of $M_k u \notin Mz \cup \{\mathfrak{s}\}$ and (11), the latter equation implies $M_k u \notin M_{\overline{n}} z$, proving that $\mathfrak{q} \in M_{\overline{n}} y \setminus M_{\overline{n}} z$ even in the case in which $\mathfrak{q} \in \bigcup_{k=0}^{\overline{n}-1} M_k \{u \in V_k \mid Mu \in Mz\}$.

From the arbitrariness of $\mathfrak{q} \in M_{\overline{n}} x$, we conclude that $M_{\overline{n}} x \subseteq M_{\overline{n}} y \setminus M_{\overline{n}} z$ holds.

Proof of $M_{\overline{n}} y \setminus M_{\overline{n}} z \subseteq M_{\overline{n}} x$.   Let us assume now that $\mathfrak{q} \in M_{\overline{n}} y \setminus M_{\overline{n}} z$, so that $\mathfrak{q} \in M_{\overline{n}} y$. Again from Lemma 2.2(b), we have:

$$M_{\overline{n}} y \ \subseteq \ My \cup \{\mathfrak{s}\} \cup \bigcup_{k=0}^{\overline{n}-1} M_k \{v \in V_k \mid Mv \in My\}.$$

First we consider the case in which $\mathfrak{q} \in My$, so that $\mathrm{rk}\,(\mathfrak{q}) < \mathrm{rk}\,(\mathfrak{s})$. Since $\mathfrak{q} \notin M_{\overline{n}} z$, then by Lemma 2.2(a) $\mathfrak{q} \notin Mz$, and therefore $\mathfrak{q} \in My \setminus Mz = Mx \subseteq M_{\overline{n}} x$. Thus, $\mathfrak{q} \in M_{\overline{n}} x$.

Next, if $\mathfrak{q} = \mathfrak{s}$, then $\mathfrak{s} \in M_{\overline{n}} y \setminus M_{\overline{n}} z$. Thus, $\mathfrak{s} \in M_0 y$ and $\mathfrak{s} \notin M_0 z$ by Lemmas 2.6(b) and 2.2(a), respectively. Hence, by (5), $y \in V_0$ and $z \notin V_0$, so that $\mathfrak{t} \in \overline{M} y \setminus \overline{M} z = \overline{M} x$ (since $\overline{M} \models \varphi$). In view of (3), the latter membership relation yields $x \in V_0$. Thus $\mathfrak{q} = \mathfrak{s} \in M_0 x \subseteq M_{\overline{n}} x$, which readily implies $\mathfrak{q} \in M_{\overline{n}} x$.

Finally, let us assume that $\mathfrak{q} = M_k v$, for some $0 \leqslant k < \overline{n}$ such that $v \in V_k$ and $Mv \in My$. Plainly, $Mv \notin Mz$, otherwise by Lemma 2.9 we should have $\mathfrak{q} = M_k v \in M_{k+1} z \subseteq M_{\overline{n}} z$, contradicting $\mathfrak{q} \in M_{\overline{n}} y \setminus M_{\overline{n}} z$. Thus, $Mv \in My \setminus Mz = Mx$, so that $Mv \in Mx$. But then, by Lemma 2.9 again, we get $\mathfrak{q} = M_k v \in M_{k+1} x \subseteq M_{\overline{n}} x$, from which $\mathfrak{q} \in M_{\overline{n}} x$ follows even in the last case.

Thus, in all cases we have $\mathfrak{q} \in M_{\overline{n}} x$. By the arbitrariness if $\mathfrak{q}$ in $M_{\overline{n}} y \setminus M_{\overline{n}} z$, we therefore obtain $M_{\overline{n}} y \setminus M_{\overline{n}} z \subseteq M_{\overline{n}} x$.

In view of the reverse inclusion $M_{\overline{n}} x \subseteq M_{\overline{n}} y \setminus M_{\overline{n}} z$ established earlier, the latter inclusion yields $M_{\overline{n}} x = M_{\overline{n}} y \setminus M_{\overline{n}} z$, namely $M_{\overline{n}} \models x = y \setminus z$.

Summing up, we have proved that the assignment $M_{\overline{n}}$ satisfies all the conjuncts of φ, and therefore $M_{\overline{n}}$ satisfies φ. $\qquad\square$

Together with Corollary 2.8, the preceding lemma implies

$$M_{\overline{n}} \ \models \ \varphi \ \wedge \ \bigwedge \mathscr{E}_M^-.$$

To find a contradiction, it only remains to prove that $M_{\overline{n}} \models \overline{x} \neq \overline{y}$, where $\overline{x} = \overline{y}$ is the designated equality of $\mathscr{E}_M^+$, which we do next.

Lemma 2.11. *The assignment $M_{\overline{n}}$ models the inequality $\overline{x} \neq \overline{y}$ correctly.*

Proof. We know that $\mathfrak{t} \in \overline{M} \overline{x} \setminus \overline{M} \overline{y}$, therefore $\overline{x} \in V_0$ and $\overline{y} \notin V_0$, $\mathfrak{s} \in M_0 \overline{x} \setminus M_0 \overline{y}$. Hence, from Lemma 2.6(b) it follows that $\mathfrak{s} \in M_{\overline{n}} \overline{x} \setminus M_{\overline{n}} \overline{y}$, proving that $M_{\overline{n}} \models \overline{x} \neq \overline{y}$. $\qquad\square$

From Lemmas 2.10 and 2.11 and Corollary 2.8, we have:

$$M_{\overline{n}} \ \models \ \varphi \ \wedge \ \bigwedge \mathscr{E}_M^- \ \wedge \ \overline{x} \neq \overline{y}.$$

Setting $\mathscr{E}_{M_{\overline{\pi}}}^{+} := \{\ell \in \mathscr{E} \mid M_{\overline{n}} \models \ell\}$ and $\mathscr{E}_{M_{\overline{\pi}}}^{-} := \{\neg\ell \mid \ell \in \mathscr{E} \setminus \mathscr{E}_{M_{\overline{\pi}}}^{+}\}$, we have $\mathscr{E}_M^{-} \subsetneq \mathscr{E}_{M_{\overline{\pi}}}^{-}$ and so $|\mathscr{E}_{M_{\overline{\pi}}}^{+}| < |\mathscr{E}_M^{+}|$, contradicting the minimality of $|\mathscr{E}_M^{+}|$ among all the set assignments that satisfy φ. Thus, our initial hypothesis that MLS were not convex is inadmissible, and therefore we can conclude that:

Theorem 2.12. *The theory* MLS *is convex.*

We expect that the proof of convexity of MLS can be suitably generalized to show that also the extension MLSI of MLS with literals of the form $x = \bigcap y$ is convex too, where $\bigcap$ is the *general intersection operator*.[3] We recall that the intended semantics of $x = \bigcap y$ is the following: for a given set assignment M, we have $M(x = \bigcap y) = \mathsf{true}$ if and only if $My \neq \emptyset$ and $Mx = \bigcap My$, namely $Mx = \bigcap_{\mathfrak{y} \in My} \mathfrak{y}$.

Several fragments of MLS admit polynomial-time decision procedures, so they are very appealing in the context of combination of decision procedures *à la* Nelson-Oppen. We briefly review them next.

2.1 Polynomial fragments of MLS

Convexity of MLS is plainly inherited by all of its fragments. In [8] and [10], we recently investigated them with the goal of spotting the polynomial ones, namely the fragments of MLS endowed with polynomial-time satisfiability tests. Specifically, we examined all the sublanguages of the theories

$$\mathbb{BST} := \mathsf{BST}(\cup, \cap, \setminus, =\emptyset, \neq\emptyset, \mathsf{Disj}, \neg\mathsf{Disj}, \subseteq, \nsubseteq, =, \neq) \qquad \text{and} \qquad \mathbb{MST} := \mathsf{MST}(\cup, \cap, \setminus, \in, \notin),$$

where:

- $\mathbb{BST}$ (acronym for Boolean Set Theory) is the collection of all the conjunctions of literals of the types

$$\begin{array}{llll} s = \emptyset, & \mathsf{Disj}(s,t), & s \subseteq t, & s = t, \\ s \neq \emptyset, & \neg\mathsf{Disj}(s,t), & s \nsubseteq t, & s \neq t, \end{array}$$

  with s and t terms involving set variables and the Boolean operators $\cup$, $\cap$, and $\setminus$, and where $\mathsf{Disj}(s,t)$ stands for $s \cap t = \emptyset$;

- $\mathbb{MST}$ (acronym for Membership Set Theory) is the collection of all the conjunctions of literals of the two types $s \in t$ and $s \notin t$, with, as above, s and t terms involving set variables and the Boolean operators $\cup$, $\cap$, and $\setminus$.

More generally, we denote by $\mathsf{BST}(\mathsf{op}_1, \dots, \mathsf{pred}_1, \dots)$ (resp., $\mathsf{MST}(\mathsf{op}_1, \dots, \mathsf{pred}_1, \dots)$) the subtheory of $\mathbb{BST}$ (resp., $\mathbb{MST}$) involving only the set operators $\mathsf{op}_1, \dots$ drawn from the collection $\{\cup, \cap, \setminus\}$ and the predicate symbols $\mathsf{pred}_1, \dots$ drawn from $\{=\emptyset, \neq\emptyset, \mathsf{Disj}, \neg\mathsf{Disj}, \subseteq, \nsubseteq, =, \neq\}$ (resp., $\{\in, \notin\}$).

We figured out that the maximal polynomial fragments of $\mathbb{BST}$ and $\mathbb{MST}$ (namely the polynomial fragments of $\mathbb{BST}$ and $\mathbb{MST}$ that are not strictly contained in any polynomial fragment of $\mathbb{BST}$ and $\mathbb{MST}$, respectively) are:

- $\mathsf{BST}(\cup, =\emptyset, \neq\emptyset, \mathsf{Disj}, \neg\mathsf{Disj}, \nsubseteq, \neq)$,

- $\mathsf{BST}(\cup, =\emptyset, \neq\emptyset, \neg\mathsf{Disj}, \subseteq, \nsubseteq, =, \neq)$,

- $\mathsf{BST}(\cap, =\emptyset, \neq\emptyset, \mathsf{Disj}, \neg\mathsf{Disj}, \subseteq, \nsubseteq, =, \neq)$
  (all of which admitting a cubic-time satisfiability test) and

---

[3] The decision problem for MLSI has been solved in [7].

- MST$(\cup, \in, \not\in)$ (admitting a linear-time satisfiability test),
- MST$(\cap, \in, \not\in)$ (admitting a quadratic-time satisfiability test).

In addition, we further spotted the following non-maximal polynomial fragments of $\mathbb{BST}$ admitting sub-cubic satisfiability tests:

- BST$(\cup, =\varnothing, \neq\varnothing, \mathsf{Disj}, \not\subseteq, \neq)$ (admitting a linear-time satisfiability test),
- BST$(\cup, \mathsf{Disj}, \neg\mathsf{Disj})$ (admitting a quadratic-time satisfiability test),
- BST$(\cap, =\varnothing, \neq\varnothing, \mathsf{Disj}, \neg\mathsf{Disj}, \neq)$ (admitting a quadratic-time satisfiability test).

As already observed, all of the above fragments plainly inherit convexity from MLS, so that, their decision procedures can be efficiently combined with the decision procedures of other convex theories with disjoint signatures within a Nelson-Oppen framework.

In the following section, we review various non-convex extensions of MLS.

3 Non-convex extensions of MLS

To prove that some extensions of MLS are non-convex, we rely on the following property.

Lemma 3.1. *Let* T *be any extension of* MLS *containing a conjunction* φ *with a designated variable* $\bar{x}$ *such that, for some integer* $k \geqslant 2$, *we have:*

- $\models \varphi \longrightarrow |\bar{x}| \leqslant k$,
- $\varphi \wedge |\bar{x}| = k$ *is satisfiable,*

where $|\bar{x}|$ *stands for the cardinality of* $\bar{x}$. *Then* T *is not convex.*

Proof sketch. Given φ, $\bar{x}$, and k as in the hypotheses, it is enough to set $\Phi := \varphi \wedge \bigwedge_{i=1}^{k+1} x_i \in \bar{x}$, where $x_1, \ldots, x_{k+1}$ are pairwise distinct variables not occurring in φ. Then, we have:

$$\models \Phi \longrightarrow \bigvee_{1 \leqslant i < j \leqslant k+1} x_i = x_j.$$

In addition, each conjunction $\Phi \wedge x_i \neq x_j$, with $1 \leqslant i < j \leqslant k+1$, is satisfiable. Hence, none of the statements

$$\models \Phi \longrightarrow x_i = x_j$$

can hold, for $1 \leqslant i < j \leqslant k+1$. Thus, the theory T is not convex. $\qquad \square$

Using Lemma 3.1, we show next that the following extensions of MLS are non-convex:

- MLSS $=$ MLS $+$ '$\{\cdot\}$': MLS extended with the singleton operator $x = \{y\}$ (see [14]),
- MLSP $=$ MLS $+$ '$\mathscr{P}(\cdot)$': MLS extended with the powerset operator (see [6]),
- MLSU $=$ MLS $+$ '$\bigcup \cdot$': MLS extended with the general union operator (see [5]),
- MLS$\times$ $=$ MLS $+$ '$\times$': MLS extended with the Cartesian product operator.[4]

Concerning the theory MLSS, let us consider the conjunction

$$\varphi := x = \{y\} \wedge x' = \{y'\} \wedge \bar{x} = x \cup x'.$$

Then,

---

[4]The decision problem for MLS$\times$ is still open.

- for every model M for φ, we have $M\bar{x} = \{My, My'\}$, so that $|M\bar{x}| \leqslant 2$ holds;

- letting $\overline{M}$ be the set assignment for φ such that

$$\overline{M}y = \emptyset, \qquad \overline{M}y' = \overline{M}x = \{\emptyset\}, \qquad \overline{M}x' = \{\{\emptyset\}\}, \qquad \overline{M}\bar{x} = \{\emptyset, \{\emptyset\}\},$$

then $\overline{M}$ satisfies φ and $|\overline{M}\bar{x}| = 2$.

Thus, by Lemma 3.1, MLSS is non-convex.

Next, as for the theory MLSP, let us consider the conjunction

$$\varphi := \ x = \emptyset \ \wedge \ y = \mathscr{P}(x) \ \wedge \ \bar{x} = \mathscr{P}(y).$$

Then, φ is plainly satisfiable and, for every set assignment M satisfying φ, we have $M\bar{x} = \{\emptyset, \{\emptyset\}\}$, so that $|M\bar{x}| = 2$. Thus, by Lemma 3.1, MLSP is non-convex.

Concerning the fragment MLSU, let us consider the conjunction

$$\varphi := \ x = \emptyset \ \wedge \ \bigcup y = x \ \wedge \ \bigcup \bar{x} = y.$$

Then,

- for every set assignment M satisfying φ, we have $M\bar{x} \subseteq \{\emptyset, \{\emptyset\}\}$ so that $|M\bar{x}| \leqslant 2$ holds;

- letting $\overline{M}$ be the set assignment over $Vars(\varphi)$ such that

$$\overline{M}x = \emptyset, \qquad \overline{M}y = \{\emptyset\}, \qquad \overline{M}\bar{x} = \{\emptyset, \{\emptyset\}\},$$

we readily have that $\overline{M}$ satisfies φ and $|\overline{M}\bar{x}| = 2$.

Hence, by Lemma 3.1, MLSU is non-convex.

Since MLSSP is an extension of non-convex theories, namely MLSS and MLSP, it follows immediately that MLSSP is non-convex as well.

Regarding the extension MLS$\times$ of MLS with the Cartesian product, we have

$$\models x \times y = \emptyset \ \longrightarrow \ (x = \emptyset \ \vee \ y = \emptyset). \tag{12}$$

Since the two conjunctions $x \times y = \emptyset \ \wedge x \neq \emptyset$ and $x \times y = \emptyset \ \wedge y \neq \emptyset$ are clearly satisfiable, then

$$\not\models x \times y = \emptyset \ \longrightarrow \ x = \emptyset \qquad \text{and} \qquad \not\models x \times y = \emptyset \ \longrightarrow \ y = \emptyset.$$

Together with (12), the latter statements imply that MLS$\times$ is non-convex.

By replacing in the above proof the Cartesian product $\times$ by the unordered Cartesian product $\otimes$, one can readily show that the extension MLS$\otimes$ of MLS with the unordered Cartesian product $\otimes$ is non-convex too.

Finally, notice that the membership relator did not play any role in the above proof of non-convexity of MLS$\times$ and MLS$\otimes$. Therefore, by exactly the same argument as the above, one can show that the extensions BST$\times$ and BST$\otimes$ of BST with the Cartesian product and the unordered Cartesian product are non-convex.

Summarizing, we have proved:

Lemma 3.2. *The theories* MLSS, MLSP, MLSSP, MLSU, MLS$\times$, MLS$\otimes$, BST$\times$, *and* BST$\otimes$ *are all non-convex.*

4   Conclusions

In this paper, we have shown that the fragment of Zermelo-Fraenkel set theory called Multi-Level Syllogistic is convex. We also proved that most common extensions of MLS studied within the field of computable set theory are non-convex. Two possible exceptions are MLSI, namely the extension of MLS with the general intersection operator ⋂, and the extension of MLS with a finiteness predicate and some cardinality constraints. In fact, we conjecture that both extensions are convex, and we plan to prove it in the near future.

Although the decision problem for MLS is NP-complete, several of its fragments are endowed with polynomial decision procedures. Due to the fact that convexity is inherited by all the fragments of MLS, the ones with polynomial-time decision procedures are particularly interesting in view of their integration with other convex, stably infinite decidable theories with disjoint signatures (such as the theory of lists, linear arithmetic, etc.) within a Nelson-Oppen context.

We therefore intend to continue our investigation of sublanguages of MLS that admit a polynomial satisfiability procedure, with the ultimate goal of obtaining a complete taxonomy for the decision problem for MLS subtheories.

We also plan to explore extensions to the basic Nelson-Oppen procedure that overcome the restriction of stable infiniteness and/or of signature disjointness (such as, for instance, the politeness property [17], or the Noetherian property [15]) that are particularly suited for combinations of decision procedures for fragments of set theory.

Finally, we intend to generalize to decidable fragments of pure set theory some combination results present in literature (such as the ones with integers and cardinals—see [19, 21, 20]), which are currently limited to *flat* sets of urelements only.

Acknowledgements

References

[1] K. Bansal, C. W. Barrett, A. Reynolds & C. Tinelli (2018): *Reasoning with Finite Sets and Cardinality Constraints in SMT*. Logical Methods in Computer Science 14(4), pp. 1–31, doi:10.23638/LMCS-14(4:12)2018.

[2] C. Barrett, A. Stump & C. Tinelli (2010): *The Satisfiability Modulo Theories Library*. Available at http://www.smtlib.org.

[3] M.P. Bonacina, S. Ghilardi, E. Nicolini, S. Ranise & D. Zucchelli (2006): *Decidability and undecidability results for Nelson-Oppen and rewrite-based decision procedures*. In U. Furbach & N. Shankar, editors: *Automated Reasoning. IJCAR 2006*, Lecture Notes in Computer Science 4130, pp. 513–527, doi:10.1007/11814771_42.

[4] Aaron R. Bradley & Zohar Manna (2007): *The calculus of computation - decision procedures with applications to verification*. Springer, doi:10.1007/978-3-540-74113-8.

[5] D. Cantone, A. Ferro & J.T. Schwartz: *Decision procedures for elementary sublanguages of set theory. V: Multilevel syllogistic extended by the general union operator*. Journal of Computer and System Sciences (1), pp. 1–18, doi:10.1016/0022-0000(87)90001-8.

[6] D. Cantone, J. T. Schwartz & A. Ferro: *Decision procedures for elementary sublanguages of set theory. VI. Multi-level syllogistic extended by the powerset operator*. Communications on Pure and Applied Mathematics (5), pp. 549–571, doi:10.1002/cpa.3160380507.

[7] Domenico Cantone & Vincenzo Cutello (1989): *Decision procedures for elementary sublanguages of Set Theory. XVI. Multilevel syllogistic extended by singleton, rank comparison and unary intersection*. Bulletin of EATCS 39, pp. 139–148.

[8] Domenico Cantone, Andrea De Domenico, Pietro Maugeri & Eugenio G. Omodeo (2021): *Complexity Assessments for Decidable Fragments of Set Theory. I: A Taxonomy for the Boolean Case*. Fundamenta Informaticae 181, pp. 37–69, doi:10.3233/fi-2021-2050.

[9] Domenico Cantone, Alfredo Ferro & Eugenio G. Omodeo (1989): *Computable set theory*. International Series of Monographs on Computer Science, Oxford Science Publications 6, Clarendon Press, Oxford, UK, doi:10.2307/2275351.

[10] Domenico Cantone, Pietro Maugeri & Eugenio G. Omodeo: *Complexity assessments for decidable fragments of set theory. II: A taxonomy for 'small' languages involving membership*. Theoretical Computer Science, pp. 28–46, doi:10.1016/j.tcs.2020.08.023.

[11] Domenico Cantone, Eugenio G. Omodeo & Alberto Policriti (1990): *The Automation of Syllogistic. II: Optimization and Complexity Issues*. J. Autom. Reasoning 6(2), pp. 173–187, doi:10.1007/BF00245817.

[12] Domenico Cantone, Eugenio G. Omodeo & Alberto Policriti (2001): *Set theory for computing - From decision procedures to declarative programming with sets*. Monographs in Computer Science, Springer-Verlag, New York, doi:10.1007/978-1-4757-3452-2.

[13] Domenico Cantone & Pietro Ursino (2018): *An Introduction to the Technique of Formative Processes in Set Theory*. Springer International Publishing, doi:10.1007/978-3-319-74778-1.

[14] Alfredo Ferro, Eugenio G. Omodeo & Jacob T. Schwartz (1980): *Decision Procedures for Elementary Sublanguages of Set Theory. I: Multilevel Syllogistic and Some Extensions*. Comm. Pure Appl. Math. 33, pp. 599–608, doi:10.1002/cpa.3160330503.

[15] S. Ghilardi, E. Nicolini & D. Zucchelli (2005): *A Comprehensive Framework for Combined Decision Procedures*. In B. Gramlich, editor: *Frontiers of Combining Systems (FroCoS 2005), Lecture Notes in Computer Science* 3717, Springer, Berlin, Heidelberg, pp. 1–30, doi:10.1007/11559306_1.

[16] G. Nelson & D.C. Oppen (1979): *Simplification by cooperating decision procedures*. ACM Transactions on Programming Languages and Systems 1(2), pp. 245–257, doi:10.1145/357073.357079.

[17] S. Ranise, C. Ringeissen & C.G. Zarba (2005): *Combining Data Structures with Nonstably Infinite Theories Using Many-Sorted Logic*. In B. Gramlich, editor: *Frontiers of Combining Systems (FroCoS 2005), Lecture Notes in Computer Science* 3717, Springer, Berlin, Heidelberg, pp. 48–64, doi:10.1007/11559306_3.

[18] Jacob T. Schwartz, Domenico Cantone & Eugenio G. Omodeo (2011): *Computational logic and set theory: Applying formalized logic to analysis*. Springer-Verlag, doi:10.1007/978-0-85729-808-9. Foreword by M. Davis.

[19] Calogero G. Zarba: *Combining Multisets with Integers*. In Andrei Voronkov, editor: *Automated Deduction - CADE-18, 18th International Conference on Automated Deduction, Copenhagen, Denmark, July 27-30, 2002, Proceedings*, Lecture Notes in Computer Science, Springer, pp. 363–376, doi:10.1007/3-540-45620-1_30.

[20] Calogero G. Zarba: *Combining Sets with Cardinals*. J. Autom. Reason. (1), pp. 1–29, doi:10.1007/s10817-005-3075-8.

[21] Calogero G. Zarba: *Combining Sets with Integers*. In Alessandro Armando, editor: *Frontiers of Combining Systems, 4th International Workshop, FroCoS 2002, Santa Margherita Ligure, Italy, April 8-10, 2002, Proceedings*, Lecture Notes in Computer Science, Springer, pp. 103–116, doi:10.1007/3-540-45988-X_9.