Combining Sets with Integers

Calogero G. Zarba

Stanford University and University of Catania

Abstract. We present a decision procedure for a constraint language combining stratified sets of ur-elements with integers in the presence of a cardinality operator. Our decision procedure is an extension of the Nelson-Oppen combination method specifically tailored to the combination domain of sets, integers, and ur-elements.

1 Introduction

The cardinality of a set is the number of its elements. Thus, in order to reason about set-theoretic formulae involving the cardinality operator, a set-theoretic theorem prover needs the ability to reason about numbers. Such ability can be basically provided in two ways: either by representing numbers directly as sets by means of the set-theoretic identities $0 = \emptyset$ and $n+1 = n \cup \{n\}$, or by employing specialized decision procedures for arithmetic. We argue that, although the former solution is very elegant, the latter is more practical and more amenable to modularization.

In this paper we introduce a constraint language involving the cardinality operator and combining:

1. finite sets of ur-elements;
2. the integers;
3. an arbitrary first order theory T of the ur-elements.

We use a decision procedure for T and a decision procedure for integer linear arithmetic as black boxes to provide in a modular fashion a decision procedure for the satisfiability of constraints in the combined language.

Our decision procedure can be seen as:

- an *augmentation* method which takes a decision procedure for integer linear arithmetic and turns it into a decision procedure for a conservative extension of integer linear arithmetic to a theory of sets with a cardinality operator;
- a *combination* method for the union of an arbitrary theory T of the ur-elements with the theory of finite sets with integers.

Our decision procedure is an extension of the Nelson-Oppen combination method specifically tailored to the combination domain of sets, integers, and ur-elements.

The Nelson-Oppen combination method [5, 6] combines satisfiability checkers for stably infinite[1] first-order theories over disjoint signatures into a single satisfiability checker for the union theory by means of propagating equalities.

It should be noted, however, that although the Nelson-Oppen combination method requires the stable infiniteness of the combined theories, our decision procedure remains correct even if the underlying theory T of the ur-elements is not stably infinite.

1.1 Related work

Several decidability results concerning the cardinality operator have been obtained in computable set theory. In their seminal paper, Ferro, Omodeo and Schwartz [4] prove the decidability of the fragment of set theory known as **MLS** (*multi-level syllogistic*), which contains the basic set theoretic constructs of membership, set equality, union, intersection, and set difference. They also prove the decidability of the extension of **MLS** with the singleton operator and the finite cardinality operator together with arithmetic addition, subtraction and comparison. Cantone and Cutello [1] prove the decidability of the extension of **MLS** with the singleton operator and rank and cardinality comparisons.

It should be noted, however, that the above results deal with pure Zermelo-Fraenkel set theory and do not address the problem of combining in a modular way sets with integers and ur-elements.

The combination of sets with integers and of sets with reals was addressed by Cantone, Cutello and Schwartz [2], who prove the decidability of an unquantified theory of sets of integers and of an unquantified theory of sets of reals, but without the cardinality operator. The combination of sets with ur-elements was addressed by Cantone and Zarba [3], who give a tableau calculus for combining set reasoning with first-order reasoning.

The decision procedure presented in this paper is inspired by the satisfiability procedure presented in [8], where we combine flat lists of ur-elements with integers in the presence of a length function.

1.2 Organization of the paper

The paper is organized as follows. In Section 2 we define the constraint language **F2LSC** (*finite two-level syllogistic with cardinality*) for combining finite sets with integers and ur-elements in the presence of a cardinality operator. In Section 3 we present our decision procedure, and in Section 4 we prove its correctness. Finally, in Section 5 we conclude the paper by pointing at directions for future research.

[1] A first-order theory T is stably infinite if every unquantified formula φ which is satisfiable in T is also satisfiable in an infinite model of T.

2 The constraint language F2LSC

In this section we introduce the constraint language **F2LSC** (*finite two-level syllogistic with cardinality*) for expressing constraints over finite sets, integers, and ur-elements.[2]

2.1 Syntax

The language **F2LSC** is an unquantified many-sorted language with three sorts ur, int and set, plus the following symbols:

- the constants:
  - 0 and 1, both of sort int (*zero* and *one*);
  - $\emptyset$, of sort set (*empty set*);
  - arbitrarily many constants of sort ur;
- the function symbols:
  - $+$ and $-$, both of sort $\mathsf{int} \times \mathsf{int} \to \mathsf{int}$ (*addition* and *subtraction*);
  - $\{\cdot\}$, of sort $\mathsf{ur} \to \mathsf{set}$ (*singleton set*);
  - $\cup, \cap, \setminus$, of sort $\mathsf{set} \times \mathsf{set} \to \mathsf{set}$ (*union, intersection* and *set difference*);
  - $|\cdot|$, of sort $\mathsf{set} \to \mathsf{int}$ (*cardinality*);
  - arbitrarily many function symbols of sort $\underbrace{\mathsf{ur} \times \ldots \times \mathsf{ur}}_{n} \to \mathsf{ur}$, for each $n \geq 1$;
- the predicate symbols:
  - $<$, of sort $\mathsf{int} \times \mathsf{int}$ (*less-than*);
  - $\in$, of sort $\mathsf{ur} \times \mathsf{set}$ (*membership*);
  - arbitrarily many predicate symbols of sort $\underbrace{\mathsf{ur} \times \ldots \times \mathsf{ur}}_{n}$, for each $n \geq 1$;
- an equality symbol $=_\tau$, for each $\tau \in \{\mathsf{ur}, \mathsf{int}, \mathsf{set}\}$;[3]
- variables of sort τ, for each $\tau \in \{\mathsf{ur}, \mathsf{int}, \mathsf{set}\}$.

Definition 1. **F2LSC**-*terms (resp.* **F2LSC**-*formulae) are well sorted terms (resp. formulae) constructed using the symbols of the language* **F2LSC**.

Definition 2. *A* set-*term*[4] *is* PURE *if all symbols in it are* ur-*variables or* set-*variables, or one of* $\emptyset, \{\cdot\}, \cup, \cap, \setminus$. *Pure* ur-*terms and pure* int-*terms are defined similarly.*

A PURE set-PREDICATE *is a predicate of the form* $u \in t$ *or* $s = t$, *where* u *is an* ur-*variable and* s, t *are pure* set-*terms. Similarly one can define pure* ur-*predicates, pure* int-*predicates and, in general, pure* τ-*formulae, for* $\tau \in \{\mathsf{ur}, \mathsf{int}, \mathsf{set}\}$.

[2] Ur-elements (also known as *atoms* or *individuals*) are objects which contain no elements but are distinct from the empty set. "Ur" is a German prefix meaning "primitive" or "original".

[3] We will write $=$ in place of $=_\tau$ when τ is clear from the context.

[4] For a sort τ, a τ-term is a term of sort τ.

2.2 Semantics

Definition 3. *An* INTERPRETATION $\mathcal{A}$ *of* **F2LSC** *is a many-sorted interpretation of the sorts, variables and symbols in the language* **F2LSC** *satisfying the following conditions:*

- *each sort* $\tau \in \{\mathsf{ur}, \mathsf{int}, \mathsf{set}\}$ *is mapped to a non-empty set* A_τ *such that:*
  - A_{ur} *is a non-empty set;*
  - A_{int} *is the set of all integers* $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$*;*
  - $A_{\mathsf{set}} = \{a \in 2^{A_{\mathsf{ur}}} : a \text{ is finite}\}$*;*
- *for each sort* τ*, each variable* x *of sort* τ *is mapped to an element* $x^{\mathcal{A}}$ *in* A_τ*;*
- *the symbols* 0*,* 1*,* $\emptyset$*,* $+$*,* $-$*,* $\{\cdot\}$*,* $\cap$*,* $\cup$*,* $\setminus$*,* $<$*,* $\in$ *are interpreted as in their intuitive meaning;*
- $=_\tau$ *is interpreted as the identity in* A_τ*, for* $\tau \in \{\mathsf{ur}, \mathsf{int}, \mathsf{set}\}$*.*

In the rest of the paper the calligraphic letters $\mathcal{A}$, $\mathcal{B}$, ... will denote interpretations, and the corresponding Roman letters, properly subscripted, will denote the domains of the interpretations.

Definition 4. *A* **F2LSC***-formula* φ *is*

- VALID*, if it evaluates to true in all interpretations;*
- SATISFIABLE*, if it evaluates to true in some interpretation;*
- UNSATISFIABLE*, if it evaluates to false in all interpretations.*

2.3 Theories

In **F2LSC** the elements of sort ur can be modeled by means of ur*-theories.*

Definition 5. *An* ur*-theory is any collection of universally quantified pure* ur*-formulae.*

Given an ur-theory T, a T-interpretation is an interpretation of **F2LSC** in which all formulae in T evaluate to true.

Definition 6. *Given an* ur*-theory* T*, a* **F2LSC** *formula* φ *is*

- T-VALID*, if it evaluates to true in all* T*-interpretations;*
- T-SATISFIABLE*, if it evaluates to true in some* T*-interpretation;*
- T-UNSATISFIABLE*, if it evaluates to false in all* T*-interpretations.*

2.4 Venn diagrams and places

Venn diagrams [7] are a visual representations of relationships among sets using overlapping ovals that divide the plane into regions. Some basic set-theoretic identities like

$$(x \cup y) \cup z = x \cup (y \cup z)$$

or

$$x \setminus (y \cap z) = (x \setminus y) \cup (x \setminus z)$$

can be nicely shown on a blackboard using Venn diagrams. For more complex identities, however, writing on a blackboard is not anymore a feasible way to proceed: we need the help of digital computers. Indeed, using computers we can conveniently represent the Venn regions in a Venn diagram by means of *places*.

Places are one of the most important and successful tool of computable set theory. The following is a formal definition.

Definition 7. *Let V be a collection of* set*-variables. A* PLACE *of V is a map $\pi : V \to \{0,1\}$ such that $\pi(x) = 1$, for at least one variable $x \in V$. Given an interpretation $\mathcal{M}$ of* **F2LSC** *and a place π of V, the notation $venn_{\mathcal{M}}(\pi)$ stands for the set $\bigcap_{\pi(x)=1} x^{\mathcal{M}} \setminus \bigcup_{\pi(y)=0} y^{\mathcal{M}}$.*

It should be noted, however, that places were not invented to represent just *any* Venn region. The real intuition is that places are meant to represent the *non-empty* Venn regions.

In the computable set theory literature, the idea of places as syntactic place holders of non-empty Venn regions is permeated in all proofs which use places as a device for proving decidability results for extensions of **MLS**. In particular, this idea is at the base of the decision procedure described in the next section.

3 A decision procedure for F2LSC

Let T be an ur-theory for which a decision procedure for unquantified pure ur-formulae is available. We now describe a decision procedure for checking the T-satisfiability of any unquantified **F2LSC**-formula φ. Note that, by converting φ into a disjunctive normal form, without loss of generality we may restrict ourselves to consider only conjunctions of **F2LSC**-literals.

The decision procedure consists of four phases, which we systematically describe in the next four subsections.

3.1 First phase: variable abstraction

The first phase of our decision procedure takes as input a conjunction φ of mixed **F2LSC**-literals, and converts it into a conjunction of pure **F2LSC**-literals. More specifically, the output of the variable abstraction phase is a pair $\langle \varphi', \varphi'' \rangle$ of conjunctions of **F2LSC**-literals with the following properties:

(a) $\varphi' \cup \varphi''$ is T-satisfiable if and only if so is φ;
(b) each literal in φ' is pure;
(c) each pure set-literal in φ' is of the form $x = y, x \neq y, x = \{u\}$, $x = y \cup z$, $x = y \cap z$, or $x = y \setminus z$, where x, y, z are set-variables and u is an ur-variable;
(d) each literal in φ'' is of the form $v = |x|$, where v is an int-variable and x is a set-variable.

In order to ensure properties (a), (b) and (d), we first let $\varphi' := \varphi$ and $\varphi'' := \emptyset$, and then we repeatedly apply the following transformations until nothing more can be done:

1. pick a literal of the form $s \in t$ (resp. $s \notin t$) in φ' where s is not an ur-variable, replace it with the literal $u_s \in t$ (resp. $u_s \notin t$), where u_s is a newly generated ur-variable, and add the literal $u_s = s$ to φ';
2. pick a term of the form $\{t\}$ in φ' where t is not an ur-variable, replace it with $\{u_t\}$, where u_t is a newly generated ur-variable, and add the literal $u_t = t$ to φ';
3. pick a term of the form $|t|$ in φ', and replace it with a newly generated int-variable v_t; in addition:
   - if t is a set-variable, add the literal $v_t = |t|$ to φ'';
   - if t is not a set-variable, generate a new set-variable x_t, and add the literals $x_t = t$ and $v_t = |x_t|$ to φ' and φ'', respectively.

It can be seen by standard ranking arguments that the above process eventually terminates, and that at its end properties (a), (b) and (d) hold. In order to enforce also property (c), we then repeatedly apply to φ' the following additional transformations until nothing more can be done:

1' replace each literal of the form $u \in t$ (resp. $u \notin t$) with the literal $t = t \cup \{u\}$ (resp. $t \neq t \cup \{u\}$);
2' replace every occurrence of the symbol $\emptyset$ with a newly generated set-variable w, and add the literal $w = w \setminus w$ to φ';
3' pick a term of the form $\{u\}$, where u is an ur-variable, replace every occurrence of it with a newly introduced set-variable w; and add the literal $w = \{u\}$ to φ';
4' pick a term of the form $x \cup y$ (resp. $x \cap y$, $x \setminus y$) where x, y are set-variables; replace every occurrence of it with a newly introduced set-variable z; and add the literal $z = x \cup y$ to φ' (resp. $z = x \cap y$, $z = x \setminus y$).

Note however that, in order to ensure termination, transformations 3' and 4' must be applied using the restriction that any given term cannot be picked more than once.

3.2 Second phase: partition

In the second phase we partition $\varphi' \cup \varphi''$ into four disjoint sets of literals $\varphi_{\mathsf{ur}}, \varphi_{\mathsf{int}}$, φ_{set}, and φ_{size} where

- φ_{ur} contains all pure ur-literals in φ';
- φ_{int} contains all pure int-literals in φ';
- φ_{set} contains all pure set-literals in φ';
- $\varphi_{\mathsf{size}} = \varphi''$.

We call $\varphi_{\mathsf{ur}} \cup \varphi_{\mathsf{int}} \cup \varphi_{\mathsf{set}} \cup \varphi_{\mathsf{size}}$ a conjunction of **F2LSC**-literals in *separate* form. Moreover, in the rest of the paper we will denote with U_φ the collection of ur-variables occurring in both φ_{ur} and φ_{set}, and with V_φ the collection of set-variables occurring in $\varphi_{\mathsf{set}} \cup \varphi_{\mathsf{size}}$.

3.3 Third phase: decomposition

Let $\varphi = \varphi_{\mathsf{ur}} \cup \varphi_{\mathsf{int}} \cup \varphi_{\mathsf{set}} \cup \varphi_{\mathsf{size}}$ be a conjunction of **F2LSC**-literals in separate form. In the third phase of our decision procedure we nondeterministically guess an *arrangement* of φ. Intuitively, an arrangement of φ specifies:

- which ur-variables in U_φ are to be modeled as equals and which not;
- which Venn regions in the Venn diagram relative to V_φ are empty and which are not;
- for each ur-variable u, which Venn region should contain u.

More formally, we have the following definition.

Definition 8. *Let $\varphi = \varphi_{\mathsf{ur}} \cup \varphi_{\mathsf{int}} \cup \varphi_{\mathsf{set}} \cup \varphi_{\mathsf{size}}$ be a conjunction of* **F2LSC***-literals in separate form. An* ARRANGEMENT *of φ is a triple $\langle R, \Pi, at \rangle$ where:*

- *$R \subseteq U_\varphi \times U_\varphi$ is an equivalence relation;*
- *Π is a (finite) collection of places of V_φ;*
- *at is a map from U_φ into Π.*

Note that guessing an arrangement $\rho = \langle R, \Pi, at \rangle$ of φ is equivalent to guess that φ is satisfied by a T-interpretation $\mathcal{M}$ of **F2LSC** such that:

- if uRv then $u^{\mathcal{M}} = v^{\mathcal{M}}$, and if not uRv then $u^{\mathcal{M}} \neq v^{\mathcal{M}}$;
- if $\pi \in \Pi$ then $venn_{\mathcal{M}}(\pi) \neq \emptyset$, and if $\pi \notin \Pi$ then $venn_{\mathcal{M}}(\pi) = \emptyset$;
- if $at(u) = \pi$ then $u \in venn_{\mathcal{M}}(\pi)$.

For an arrangement $\rho = \langle R, \Pi, at \rangle$ we define the following collection of literals:

$$\begin{aligned} res_{\mathsf{ur}}(\rho) = &\{u = v : u, v \in U_\varphi \text{ and } uRv\} \cup \\ &\{u \neq v : u, v \in U_\varphi \text{ and not } uRv\} \end{aligned}$$

and

$$\begin{aligned} res_{\mathsf{int}}(\rho) = &\{0 < v_\pi : \pi \in \Pi\} \cup \\ &\{v_\pi = 1 : \pi \in range(at)\} \cup \\ &\{v = \sum_{\pi(x)=1} v_\pi : \text{ the literal } v = |x| \text{ is in } \varphi_{\mathsf{size}}\} \end{aligned}$$

where, for each place $\pi \in \Pi$, v_π is a newly generated variable whose intuitive meaning is the cardinality of the Venn region $\bigcap_{\pi(x)=1} x \setminus \bigcup_{\pi(y)=0} y$.

In order to better understand the intuitive meaning of $res_{\mathsf{ur}}(\rho)$ and $res_{\mathsf{int}}(\rho)$, assume that there exists a T-interpretation $\mathcal{M}$ of **F2LSC** satisfying φ and such that:

- $u^{\mathcal{M}} = v^{\mathcal{M}}$ iff uRv, for each ur-variable $u, v \in U_\varphi$;
- $venn_{\mathcal{M}}(\pi) \neq \emptyset$, for each $\pi \in \Pi$;
- if $at(u) = \pi$ then $u^{\mathcal{M}} \in venn_{\mathcal{M}}(\pi)$, for each $u \in U_\varphi$ and for each $\pi \in \Pi$.

– $v_\pi^{\mathcal{M}} = |venn_{\mathcal{M}}(\pi)|$, for each $\pi \in \Pi$.

Then, the following must be true.

– $u^{\mathcal{M}} = v^{\mathcal{M}}$ if and only if uRv.
– If $\pi \in \Pi$ then $venn_{\mathcal{M}}(\pi) \neq \emptyset$ and therefore $v_\pi^{\mathcal{M}} > 0$.
– If $\pi \in range(at)$ then there exists an ur-variable u such that $at(u) = \pi$. But then a literal of the form $x = \{u\}$ must occur in φ_{set}. Since $u^{\mathcal{M}} \in venn_{\mathcal{M}}(\pi)$, we have that $venn_{\mathcal{M}}(\pi) \cap x^{\mathcal{M}} \neq \emptyset$, and therefore $v_\pi^{\mathcal{M}} = 1$.
– If the literal $v = |x|$ is in V_{size} then the cardinality of $x^{\mathcal{M}}$ is the sum of the cardinality of the Venn regions contained in $x^{\mathcal{M}}$.

Before describing the fourth and last phase of our decision procedure, we need to introduce the notation $|\mathsf{ur}| \geq n$, which intuitively stands for stands for a formula forcing the domain of ur-elements to have cardinality at least n. Formally, we use the notation $\psi \cup \{|\mathsf{ur}| \geq n\}$, for every conjunction ψ of pure ur-literals and every $n > 0$, to denote a conjunction of literals obtained by using the following process:

– generate n new ur-variables $u_1, \ldots, u_n$ not occurring in ψ;
– let $|\mathsf{ur}| \geq n$ be the conjunction $\bigwedge_{i<j} u_i \neq u_j$.

3.4 Fourth phase: check

Let $\varphi = \varphi_{\mathsf{ur}} \cup \varphi_{\mathsf{int}} \cup \varphi_{\mathsf{set}} \cup \varphi_{\mathsf{size}}$ be a conjunction of **F2LSC**-literals in separate form, and let $\rho = \langle R, \Pi, at \rangle$ be an arrangement of φ.

The fourth phase of our decision procedure consists of three steps.

Step 1: Check that ρ satisfies the following conditions:

(C1) $at(u) = at(v)$ if and only if uRv, for each two ur-variables $u, v \in U_\varphi$;
(C2) if $x = y$ is in φ_{set} then $\pi(x) = \pi(y)$, for each place $\pi \in \Pi$;
(C3) if $x \neq y$ is in φ_{set} then $\pi(x) \neq \pi(y)$, for some place $\pi \in \Pi$;
(C4) if $x = \{u\}$ is in φ_{set} then $\pi(x) = 1$ if and only if $at(u) = \pi$, for each place $\pi \in \Pi$;
(C5) if $x = y \cup z$ is in φ_{set} then $\pi(x) = 1$ if and only if $\pi(y) = 1$ or $\pi(z) = 1$, for each place $\pi \in \Pi$;
(C6) if $x = y \cap z$ is in φ_{set} then $\pi(x) = 1$ if and only if $\pi(y) = 1$ and $\pi(z) = 1$, for each place $\pi \in \Pi$;
(C7) if $x = y \setminus z$ is in φ_{set} then $\pi(x) = 1$ if and only if $\pi(y) = 1$ and $\pi(z) = 0$, for each place $\pi \in \Pi$.

If the arrangement ρ does not satisfy conditions (C1)–(C7) output `fail`, otherwise proceed to step 2.

Step 2: If $\varphi_{\mathsf{int}} \cup res_{\mathsf{int}}(\rho)$ is unsatisfiable (in $\mathbb{Z}$) output `fail`; otherwise compute the minimal value of $\sum_{\pi \in \Pi} v_\pi$ in a solution of $\varphi_{\mathsf{int}} \cup res_{\mathsf{int}}(\rho)$. Note that this can be effectively done in a naïve way by opportunely iterating over all possible assignments over the variables in $\varphi_{\mathsf{int}} \cup res_{\mathsf{int}}(\rho)$. Denote with $minsol(\varphi, \rho)$ this value, and proceed to step 3.

Step 3: If $\varphi_{\mathsf{ur}} \cup res_{\mathsf{ur}}(\rho) \cup \{|\mathsf{ur}| \geq minsol(\varphi, \rho)\}$ is T-unsatisfiable output `fail`; otherwise output `succeed`.

Note that all the above steps can be effectively executed. In particular, Step 2 can be performed by using any decision procedure for integer linear arithmetic (since integer linear arithmetic is a decidable and complete theory), whereas Step 3 can be performed by using the available decision procedure for T.

3.5 An example

As an example of how our decision procedure works, let us consider the following T-valid **F2LSC**-formula, where T is the empty ur-theory:

$$x = \{u\} \cup x \;\rightarrow\; |x \cup \{u\}| < |x| + |\{u\}|\,. \tag{1}$$

Clearly, in order to prove that (1) is T-valid, it suffices to prove that the following conjunction

$$\varphi = \left\{ \begin{array}{l} x = \{u\} \cup x\,, \\ \neg\,(|x \cup \{u\}| < |x| + |\{u\}|) \end{array} \right\}$$

is T-unsatisfiable. After applying the variable abstraction phase we obtain the following conjunction $\varphi' \cup \varphi''$:

$$\varphi' = \left\{ \begin{array}{l} x = y \cup x\,, \\ y = \{u\}\,, \\ z = x \cup y\,, \\ \neg(v_1 < v_2 + v_3) \end{array} \right\}\,, \qquad \varphi'' = \left\{ \begin{array}{l} v_1 = |z|\,, \\ v_2 = |x|\,, \\ v_3 = |y| \end{array} \right\}\,,$$

which is partitioned in:

$$\varphi_{\mathsf{ur}} = \emptyset\,, \qquad \varphi_{\mathsf{int}} = \{\neg(v_1 < v_2 + v_3)\}\,,$$

$$\varphi_{\mathsf{set}} = \left\{ \begin{array}{l} x = y \cup x\,, \\ y = \{u\}\,, \\ z = x \cup y \end{array} \right\}\,, \qquad \varphi_{\mathsf{size}} = \left\{ \begin{array}{l} v_1 = |z|\,, \\ v_2 = |x|\,, \\ v_3 = |y| \end{array} \right\}\,.$$

We now need to guess an arrangement $\rho = \langle R, \Pi, at \rangle$. Since $U_\varphi = \emptyset$, the only possible choice for R is $R = \emptyset$. On the other hand, since $V_\varphi = \{x, y, z\}$, there are 2^{2^3-1} possible choices for Π, and for each of them there are many choices for at. Nevertheless, there are only two arrangements, depicted in Figures 1 and 2, which satisfy all properties (C1)–(C7).

Let us consider the arrangement $\rho = \langle R, \Pi, at \rangle$ depicted in Figure 1 and formally defined by:

$$\begin{array}{ll} R = \emptyset\,, & \pi_1(x) = \pi_1(y) = \pi_1(z) = 1\,, \\ \Pi = \{\pi_1, \pi_2\}\,, & \pi_2(x) = \pi_2(z) = 1\,, \\ at(u) = \pi_1\,, & \pi_2(y) = 0\,. \end{array}$$

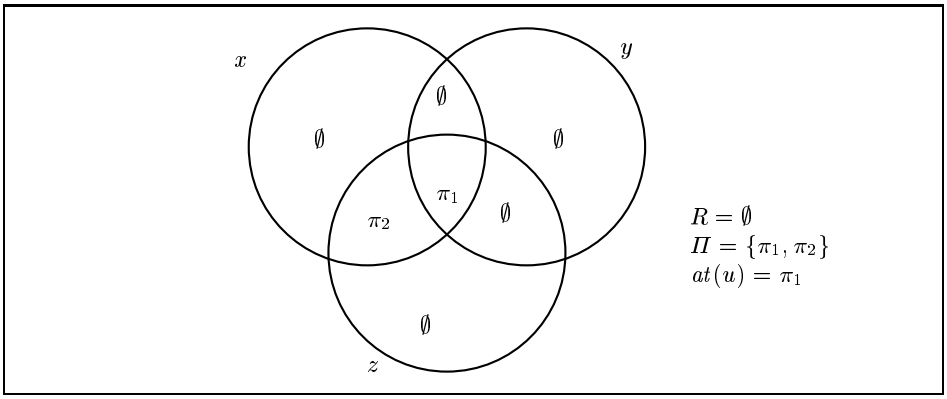

Fig. 1: An arrangement.

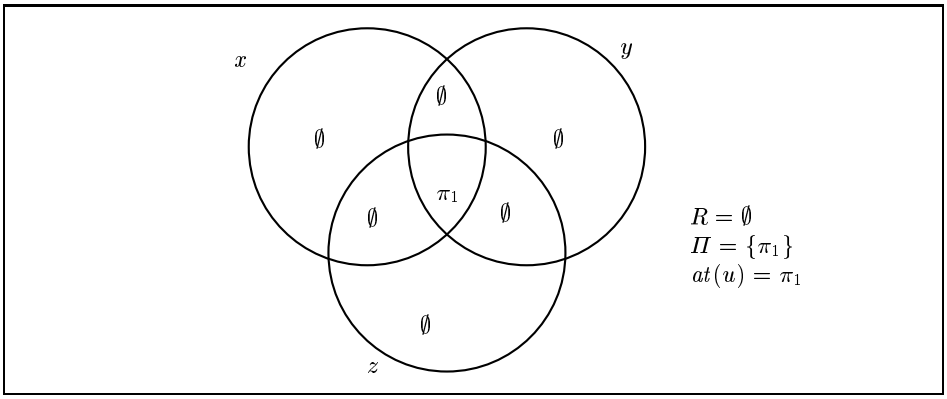

Fig. 2: An arrangement.

We have

$$res_{\mathsf{int}}(\rho) = \left\{ \begin{array}{l} v_{\pi_1} = 1\,, \\ 0 < v_{\pi_2}\,, \\ v_1 = v_{\pi_1} + v_{\pi_2}\,, \\ v_2 = v_{\pi_1}\,, \\ v_3 = v_{\pi_1} + v_{\pi_2} \end{array} \right\}\,,$$

and therefore Step 2 of the check phase fails, since $\varphi_{\mathsf{int}} \cup res_{\mathsf{int}}(\rho)$ is unsatisfiable (in $\mathbb{Z}$).

Similarly, it can be verified that Step 2 of the check phase also fails with the arrangement depicted in Figure 2. Thus, the check phase fails with all possible arrangements, and therefore we conclude that φ is T-unsatisfiable, and consequently that (1) is T-valid.

4 Soundness, completeness and decidability

In this section we prove that our decision procedure is sound and complete for the T-satisfiability of conjunctions of **F2LSC**-literals. Let us start with soundness.

Theorem 1 (soundness). *Let $\varphi = \varphi_{\mathsf{ur}} \cup \varphi_{\mathsf{int}} \cup \varphi_{\mathsf{set}} \cup \varphi_{\mathsf{size}}$ be a conjunction of* **F2LSC***-literals in separate form, and let T be an* ur*-theory. Assume that there exists an arrangement $\rho = \langle R, \Pi, at \rangle$ of φ such that:*

(i) ρ satisfies conditions (C1)–(C7) of page 8;
(ii) $\varphi_{\mathsf{int}} \cup res_{\mathsf{int}}(\rho)$ is satisfiable (in $\mathbb{Z}$);
(iii) $\varphi_{\mathsf{ur}} \cup res_{\mathsf{ur}}(\rho) \cup \{|\mathsf{ur}| \geq minsol(\varphi, \rho)\}$ is T-satisfiable.

Then φ is T-satisfiable.

Proof. Let $\mathcal{A}$ be a T-interpretation satisfying $\varphi_{\mathsf{ur}} \cup res_{\mathsf{ur}}(\varphi)$, and let $\mathcal{B}$ be a solution of $\varphi_{\mathsf{int}} \cup res_{\mathsf{int}}(\varphi)$ such that $\sum_{\pi \in \Pi} v_\pi^{\mathcal{B}} = minsol(\varphi, \rho)$.

We now start to define an interpretation $\mathcal{M}$. First, we specify the domains by putting $M_{\mathsf{ur}} = A_{\mathsf{ur}}$, $M_{\mathsf{int}} = \mathbb{Z}$, and $M_{\mathsf{set}} = \{a \in 2^{A_{\mathsf{ur}}} : a \text{ is finite}\}$. Then, we put $u^{\mathcal{M}} = u^{\mathcal{A}}$, for every ur-variable u, and $v^{\mathcal{M}} = u^{\mathcal{B}}$, for every int-variable v.

In order to define $\mathcal{M}$ over the set-variables, we first define $\mathcal{M}$ over the places in Π by means of the following construction:

- If $\pi \in range(at)$ then there exists an ur-variable $u \in U_\varphi$ such that $at(u) = \pi$, and we put $\pi^{\mathcal{M}} = \{u^{\mathcal{M}}\}$. Note that this definition is sound. In fact, if there are two ur-variables $u, v \in U_\varphi$ such that $at(u) = \pi$ and $at(v) = \pi$ then, by property (C1), uRv follows, and therefore the literal $u = v$ is in $res_{\mathsf{ur}}(\rho)$, which implies that $u^{\mathcal{M}} = v^{\mathcal{M}}$.
- If instead $\pi \notin range(at)$ then we pick $v_\pi^{\mathcal{B}}$ elements in A_{ur} and we put $\pi^{\mathcal{M}}$ to be the set of such picked elements.

It is important that the above construction satisfy the property that the sets $\pi^{\mathcal{M}}$'s be pairwise disjoint, that is, $\pi_0^{\mathcal{M}} \cap \pi_1^{\mathcal{M}} = \emptyset$, for every two distinct places $\pi_0, \pi_1 \in \Pi$. This property can certainly be forced, provided that A_{ur} contains at least $\sum_{\pi \in \Pi} v_\pi^{\mathcal{B}}$ elements. Indeed, $\sum_{\pi \in \Pi} v_\pi^{\mathcal{B}} = minsol(\varphi, \rho)$ and A_{ur} has at least $minsol(\varphi, \rho)$ elements.

We can now define $\mathcal{M}$ over the set-variables, by putting $x^{\mathcal{M}} = \bigcup_{\pi(x)=1} \pi^{\mathcal{M}}$, for every set-variable x.

We claim that $\mathcal{M}$ is a T-interpretation satisfying φ. Clearly, $\mathcal{M}$ satisfies $T \cup \varphi_{\mathsf{ur}} \cup \varphi_{\mathsf{int}}$. Moreover, it is easy to verify that, in virtue of properties (C2)–(C7), $\mathcal{M}$ also satisfies all the literals in φ_{set}. Finally, consider a literal of the form $v = |x|$ in φ_{size}. We have $|x^{\mathcal{M}}| = \left|\bigcup_{\pi(x)=1} \pi^{\mathcal{M}}\right| = \sum_{\pi(x)=1} |\pi^{\mathcal{M}}| = \sum_{\pi(x)=1} v_\pi^{\mathcal{B}}$, and since the literal $\sum_{\pi(x)=1} v_\pi = v$ is in $res_{\mathsf{int}}(\rho)$, we infer that $|x^{\mathcal{M}}| = v^{\mathcal{B}} = v^{\mathcal{M}}$. This concludes the proof. □

Our decision procedure is also complete, as proved by the following theorem.

Theorem 2 (completeness). *Let $\varphi = \varphi_{\mathsf{ur}} \cup \varphi_{\mathsf{int}} \cup \varphi_{\mathsf{set}} \cup \varphi_{\mathsf{size}}$ be a T-satisfiable conjunction of* **F2LSC***-literals in separate form.*

Then there exists an arrangement $\rho = \langle R, \Pi, at \rangle$ of φ such that:

(a) ρ satisfies conditions (C1)–(C7) of page 8;
(b) $\varphi_{\mathsf{int}} \cup res_{\mathsf{int}}(\rho)$ is satisfiable (in $\mathbb{Z}$);
(c) $\varphi_{\mathsf{ur}} \cup res_{\mathsf{ur}}(\rho) \cup \{|\mathsf{ur}| \geq minsol(\varphi, \rho)\}$ is T-satisfiable.

Proof. Let $\mathcal{M}$ be a T-interpretation satisfying φ. Let us define an arrangement $\rho = \langle R, \Pi, at \rangle$ of φ as follows:

- for each two variables $u, v \in U_\varphi$, we let uRv if and only if $u^{\mathcal{M}} = v^{\mathcal{M}}$;
- $\Pi = \{\pi : venn_{\mathcal{M}}(\pi) \neq \emptyset\}$;
- for each $u \in U_\varphi$, we let $at(u)$ be the unique place π such that $venn_{\mathcal{M}}(\pi) = \{u\}$.[5]

Note that, by construction, we have that

(i) $\pi(x) = 1$ if and only if $venn_{\mathcal{M}}(\pi) \subseteq x^{\mathcal{M}}$, for each $\pi \in \Pi$ and $x \in V_\varphi$;
(ii) $x^{\mathcal{M}} = \bigcup_{\pi(x)=1} venn_{\mathcal{M}}(\pi)$.

We can now verify that ρ satisfies conditions (C1)–(C7) of page 8.

(C1) By construction.
(C2) Let the literal $x = y$ be in φ_{set} and assume, for a contradiction, that $\pi(x) \neq \pi(y)$, for some place $\pi \in \Pi$. Without loss of generality, let $\pi(x) = 1$ and $\pi(y) = 0$. Since $x^{\mathcal{M}} = y^{\mathcal{M}}$, we have that $venn_{\mathcal{M}}(\pi) \subseteq x^{\mathcal{M}}$ and $venn_{\mathcal{M}}(\pi) \not\subseteq y^{\mathcal{M}} = x^{\mathcal{M}}$, a contradiction.
(C3) Let the literal $x \neq y$ be in φ_{set}. Then $x^{\mathcal{M}} \neq y^{\mathcal{M}}$. If it were $\pi(x) = \pi(y)$, for each place $\pi \in \Pi$, then by (ii) above we would have $x^{\mathcal{M}} = y^{\mathcal{M}}$, a contradiction.
(C4) Let the literal $x = \{u\}$ be in φ_{set}. Then $at(u) = \pi$ iff $venn_{\mathcal{M}}(\pi) = \{u^{\mathcal{M}}\}$ iff $venn_{\mathcal{M}}(\pi) \subseteq \{u^{\mathcal{M}}\}$ iff $venn_{\mathcal{M}} \subseteq x^{\mathcal{M}}$ iff $\pi(x) = 1$.
(C5) Let the literal $x = y \cup z$ be in φ_{set}. Then $\pi(x) = 1$ iff $venn_{\mathcal{M}}(\pi) \subseteq x^{\mathcal{M}}$ iff $venn_{\mathcal{M}}(\pi) \subseteq y^{\mathcal{M}} \cup z^{\mathcal{M}}$ iff $venn_{\mathcal{M}}(\pi) \subseteq y^{\mathcal{M}} \vee venn_{\mathcal{M}}(\pi) \subseteq z^{\mathcal{M}}$ iff $\pi(y) = 1 \vee \pi(z) = 1$.
(C6) Analogously to condition (C5).
(C7) Analogously to condition (C5).

Next, in order to verify property (b), notice that by assumption $\mathcal{M}$ satisfies φ_{int}. In addition, since the variables v_π's do not occur in φ, we can safely extend $\mathcal{M}$ by letting $v_\pi^{\mathcal{M}} = |venn_{\mathcal{M}}(\pi)|$, for each place $\pi \in \Pi$. We claim that now $\mathcal{M}$ also satisfies $res_{\mathsf{int}}(\rho)$. In fact:

- Let the literal $v_\pi > 0$ be in $res_{\mathsf{int}}(\rho)$. Since $venn_{\mathcal{M}}(\pi) \neq \emptyset$ it follows that $v_\pi^{\mathcal{M}} > 0$.

[5] Such place exists because for each $u \in U_\varphi$ there must be a literal of the form $x = \{u\}$ in φ_{set}.

– Let the literal $v_\pi = 1$ be in $res_{\mathsf{int}}(\rho)$, for some $\pi \in range(at)$. Then $at(u) = x$, for some variable $u \in U_\varphi$. It follows that $venn_{\mathcal{M}}(\pi) = \{u^{\mathcal{M}}\}$ which implies $v_\pi^{\mathcal{M}} = 1$.
– Let the literal $v = \sum_{\pi(x)=1} v_\pi$ be in $res_{\mathsf{int}}(\rho)$. Then the literal $v = |x|$ is in φ_{size}, and therefore $v^{\mathcal{M}} = |x^{\mathcal{M}}|$. By property (ii) we have $v^{\mathcal{M}} = |x^{\mathcal{M}}| = \sum_{\pi(x)=1} |venn_{\mathcal{M}}(\pi)| = \sum_{\pi(x)=1} v_\pi^{\mathcal{M}}$.

It remains to verify that property (c) also holds. To do this, note that by assumption $\mathcal{M}$ satisfies φ_{ur}, and that by construction $\mathcal{M}$ satisfies $res_{\mathsf{ur}}(\rho)$. In addition, we claim that M_{ur} has at least $minsol(\varphi, \rho)$ elements. In fact M_{ur} as at least $\sum_{\pi \in \Pi} v_\pi^{\mathcal{M}}$ elements and $\sum_{\pi \in \Pi} v_\pi^{\mathcal{M}} \geq minsol(\varphi, \rho)$. Therefore $\mathcal{M}$ satisfies $|\mathsf{ur}| \geq n$, which completes the proof. □

Combining Theorems 1 and 2 with the observation that there is only a finite number of arrangements of any collection φ of **F2LSC**-literals in separate form, we obtain the following decidability result.

Theorem 3 (decidability). *Let T be an* ur*-theory for which a decision procedure for unquantified pure* ur*-formulae is available. Then the T-satisfiability problem of unquantified formulae in the language* **F2LSC** *is decidable.*

5 Conclusion

We defined the constraint language **F2LSC** for combining finite sets with integers and ur-elements in the presence of a cardinality operator. We then presented a decision procedure for **F2LSC** and we proved its correctness. In particular, our decision procedure remains correct even if the underlying theory T of the ur-elements is not stably infinite.

Although not shown in this paper, it is easy to verify that our decision procedure can be easily adapted to the case of sets of integers, thus allowing the expression of constraints of the form $|x| \in x$, which are forbidden by the syntax of **F2LSC**.

Regarding future research, we plan to develop smart heuristics for exploring the space of all possible arrangements. We also plan to extend the results of this paper to the general case in which sets may be infinite.

Acknowledgments

Henny B. Sipma gave useful comments on an earlier draft. Bernd Finkbeiner explained me the meaning of the German prefix "ur". Three anonymous referees gave very helpful comments and suggested several improvements.

This research was supported in part by NSF(ITR) grant CCR-01-21403, by NSF grant CCR-99-00984-001, by ARO grant DAAD19-01-1-0723, and by ARPA/AF contracts F33615-00-C-1693 and F33615-99-C-3014.

References

1. Domenico Cantone and Vincenzo Cutello. A decision procedure for set-theoretic formulae involving rank and cardinality comparison. In A. Bertoni, C. Böhm, and P. Miglioli, editors, *Proceedings of the 3rd Italian Conference on Theoretical Computer Science*, pages 150–163. World Scientific, 1989.
2. Domenico Cantone, Vincenzo Cutello, and Jacob T. Schwartz. Decision problems for Tarski's and Presburger arithmetics extended with sets. In *Proceedings of the fourth Computer Science Logic Workshop*, volume 533 of *Lecture Notes in Computer Science*, pages 95–109. Springer, 1990.
3. Domenico Cantone and Calogero G. Zarba. A tableau calculus for integrating first-order reasoning with elementary set theory reasoning. In Roy Dyckhoff, editor, *Automated Reasoning with Analytic Tableaux and Related Methods*, volume 1847 of *Lecture Notes in Artificial Intelligence*, pages 143–159. Springer, 2000.
4. Alfredo Ferro, Eugenio G. Omodeo, and Jacob T. Scwhartz. Decision procedures for elementary sublanguages of set theory. I. Multi-level syllogistic and some extensions. *Communications on Pure and Applied Mathematics*, 33(5):599–608, 1980.
5. Greg Nelson and Derek C. Oppen. Simplification by cooperating decision procedures. *ACM Transactions on Programming Languages and Systems*, 1(2):245–257, 1979.
6. Cesare Tinelli and Mehdi T. Harandi. A new correctness proof of the Nelson-Oppen combination procedure. In Franz Baader and Klaus U. Schulz, editors, *Frontiers of Combining Systems*, volume 3 of *Applied Logic Series*, pages 103–120. Kluwer Academic Publishers, 1996.
7. John Venn. On the diagrammatic and mechanical representation of propositions and reasonings. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 9(59):1–18, 1880.
8. Calogero G. Zarba. Combining lists with integers. In Rajeev Gorè, Alexander Leitsch, and Tobias Nipkow, editors, *International Joint Conference on Automated Reasoning (Short Papers)*, Technical Report DII 11/01, pages 170–179. University of Siena, Italy, 2001.