Automation of aggregate theories:
The cornerstones of equational expressibility[*]

A. Formisano[1], E. G. Omodeo[2], and A. Policriti[3]

[1] Università di Perugia, Dip. di Matematica e Informatica, `formis@dipmat.unipg.it`
[2] Università di L'Aquila, Dipartimento di Informatica, `omodeo@cs.univaq.it`
[3] Università di Udine, Dip. di Matematica e Informatica, `policriti@dimi.uniud.it`

Abstract. The approach to algebraic specifications of set theories proposed by Tarski and Givant inspires current research aimed at taking advantage of the purely equational nature of the resulting formulations for enhanced automation of reasoning on aggregates of various kinds: sets, bags, hypersets, etc. The viability of the said approach rests upon the possibility to form ordered pairs and to decompose them by means of conjugated projections. Ordered pairs can be conceived of in many ways: along with the most classical one, several other pairing functions are examined, which can be preferred to it when either the axiomatic assumptions are too weak to enable pairing formation *à la* Kuratowski, or they are strong enough to make the specification of conjugated projections particularly simple, and their formal properties easy to check within the calculus of dyadic relations.

We also show that a kernel set theory, whose only postulates are the extensionality axiom and single-element adjunction and removal axioms, cannot be expressed in 3 variables (and hence it is not amenable to an algebraic rendering achievable through conjugated projections).

Key words: Weak set theory, Calculus of dyadic relations, Pairing axiom, Aggregates, n-variable expressibility, Pebble games.

Introduction

We will consider some weak theories of sets which result from adopting as axioms some of the sentences in Fig. 1. These sentences are provable within important classical theories of sets, such as full Zermelo-Fraenkel, or within Tarski's theory [21] of finite sets (equipollent to Peano arithmetic, cf. [24]). Actually, *extensionality* (stated as (**E**) in modern terms), and the *pairing axiom* (conjunction of (**N**) with (**P**)) appeared already among Zermelo's original set postulates in 1908 (see [26]; today, however, (**P**) is usually deduced from the *replacement axiom scheme* as shown in [18]). These theories hence retain, in the small, valuable traits. On the other hand, by leaving some of the sentences in Fig. 1 out of our selection of axioms, we can frame our investigation inside less classical but nevertheless

Extensionality	**(E)**	$\forall x \, \forall y \, \big(\forall v \, (v \in x \leftrightarrow v \in y) \; \rightarrow \; x = y \big)$
Null-set existence	**(N)**	$\exists z \, \forall v \, \neg \, v \in z$
Pair	**(P)**	$\forall x \, \forall y \, \exists p \, \forall v \, \big(v \in p \; \leftrightarrow \; (v = x \; \vee \; v = y \,) \big)$
Add an element	**(W)**	$\forall x \, \forall y \, \exists w \, \forall v \, \big(v \in w \; \leftrightarrow \; (v \in x \; \vee \; v = y \,) \big)$
Remove an element	**(L)**	$\forall x \, \forall y \, \exists \ell \, \forall v \, \big(v \in \ell \; \leftrightarrow \; (v \in x \; \wedge \; \neg \, v = y \,) \big)$
Regularity	**(R)**	$\forall x \, \exists r \, \big((r \in x \; \vee \; r = x) \; \wedge \; \neg \exists v \, (v \in r \; \wedge \; v \in x) \big)$
Aciclicity $(n = 0, 1, 2, \dots)$	$(\mathbf{A}^n)$	$\neg \, \exists x_0 \, \cdots \exists x_n \, (\, x_0 \in x_1 \cdots x_{n-1} \in x_n \; \wedge \; x_n \in x_0 \,)$

Fig. 1. Toolkit for assembling weak theories of aggregates

useful variants of set theory: recall that *bags* (also called *multi-sets*, cf. e.g. [7]) do not meet extensionality, **(E)**, and *hypersets* (cf. [1, 2]) meet neither regularity, **(R)**, nor the weaker acyclicity assumption $(\mathbf{A}^n)$.

Tarski and Givant's approach to algebraic formalization of set theories motivates current research in automation of reasoning. The main aim of this research consists in benefiting from the purely equational nature of the resulting specifications to develop enhanced automation of reasoning on aggregates of various kinds: sets, bags, hypersets, etc. Promising results have been obtained in previous works (cf. [12, 13], for instance) which revealed the possibility of exploiting a first-order theorem-prover to experiment with equational rendering of aggregate theories. (As a further contribution to this research, we report on a number of experiments developed with the theorem-prover Otter, cf. Sec.2.)

The viability of this approach relies upon the possibility to form ordered pairs and to decompose them by means of conjugated projections. Since alternative selections of the axioms correspond to different expressive power of the resulting aggregate theory, our ultimate goal consists in identifying those fundamental traits that allow a theory to support a suitable notion of ordered-pair constructor. In doing this we will seek *pairing notions* which are easily amenable to a 3-variable formulation under different (and inequivalent) possible selections of the axioms. The main reason for undertaking this quest, is that any such pairing notion can be used (cf. [23] and [24]) as the keystone of an equational variable-free rendering of the theory under focus, or of any axiomatic extension of it.

We will proceed from two opposite points of view towards the *borderline* of 3-variable (in-)expressibility. As far as the inexpressibility issue is concerned, we provide evidence that some of the possible selections of axioms originate theories that are too weak to support equipollent equational counterparts. This is the case of the theory $(\mathbf{W}) \wedge (\mathbf{L}) \wedge (\mathbf{E})$, which postulates the existence of single-element addition and removal operations only (cf. Sec.4.2). On the 'positive' side of the borderline, we provide automatically verified proofs of the equational equipollence of a number of *weak* theories of aggregates.

1 Weak set-theories, pairing, and Peircean expressibility

In his epochal paper [26], Zermelo calls *axiom of elementary sets* a postulate asserting that:

- there is a set, $\emptyset$, which is devoid of elements;

- a singleton set $\{x\}$ can be formed out of any object x of the domain of discourse; and, more generally,
- an unordered pair $\{x, y\}$ can be formed out of objects x, y whatsoever.

In the original list of postulates for set theory proposed by Zermelo, this postulate occupies the second position, after the *extensionality* axiom stating that distinct sets cannot have precisely the same elements.

Let us place ourselves in the framework of a set theory which does not cater to individuals or proper classes: then extensionality can be stated as simply as

$$\textbf{(E)} \qquad \forall x \, \forall y \, (\, x \neq y \ \rightarrow \ \exists v \, (\, v \in x \leftrightarrow v \notin y \,) \,),$$

and Zermelo's postulate of elementary sets can be decomposed as the conjunction of the following *null-set axiom* and *axiom of unordered pairs*:

$$\textbf{(N)} \ \exists z \, \forall v \, v \notin z, \quad \textbf{(P)} \ \forall x \, \forall y \, \exists p \, \forall v \, (\, v \in p \ \leftrightarrow \ (\, v = x \ \lor \ v = y \,) \,) \, .$$

Several studies (cf., among others, [6, 19, 14]) indicate the number of distinct variables as a significant measure of complexity for sentences. From this angle, one may be led to thinking that **(P)** is somewhat deeper than **(E)**, because it involves 4 variables instead of 3. Alfred Tarski, however, discovered a sentence **(OP)** which involves only 3 variables, is logically equivalent to **(P)**, and explicitly states the existence of *ordered pairs* (cf. [5, pp. 341–343], [23], and [24, p. 129]). An important by-product of having the elementary set postulate recast in 3 variables is that any first-order theory of sets to which **(N)** and **(P)** belong (either as axioms or as theorems) can, through this rendering, be translated into the *arithmetic of (dyadic) relations* (*map calculus*, as we name it). Namely, into the algebraic formalism which developed in the forties (cf. [22, 17, 5]) from the far-reaching studies on logic carried out by Peirce and Schröder in the late 19th and early 20th century. Recently, this approach to the formalization of set theory via relation algebras inspired some research aimed at automating equational set-reasoning (cf. [11, 9, 13]).

Tarski's work shows that the notion of (ordered) pair plays an essential rôle in the process of reformulating first-order theories within map calculus. The availability of pair constructors (together with the corresponding projecting operations) ensures the equipollence of the equational formulation of a theory and its first-order formulation (see [24]). The crucial concept, in this connection, is the one of *conjugated (quasi-)projections*: One names so two functions ℓ, r which are so defined on the universe $\mathcal{V}$ of sets (not necessarily on the whole of it) as to ensure that for any given sets x, y there is at least one set z such that $\ell(z) = x$ and $r(z) = y$. Before proceeding to the definition of ℓ and r, one usually has in mind a specific *pairing operation* $x, y \mapsto p(x, y)$ by which the desired z can be found out of given x, y simply by determining $z = p(x, y)$; notice, however, that z is not required to be unique in general. Whenever one proposes a concrete specification of ℓ and r, one must prove *within map calculus* that ℓ, r are conjugated (quasi-)projections (cf. Sec.2). This will ensure that a fully equipollent axiomatic system of the weak set theory can be obtained via a classical translation from first-order predicate calculus into map calculus.

To better understand Tarski's idea on how to specify **(P)** in three variables, one should bear in mind the encoding of ordered pairs in the form

$$(x, y) \ =_{\mathrm{Def}} \big\{ \{ x, y \}, \{ x \} \big\}$$

devised by Kazimierz Kuratowski in 1921, and accept also the set $\big\{ \{ x, y \}, \{ x \}, \emptyset \big\}$ as a legitimate—though redundant—encoding for the same ordered pair. By way of first approximation, **(OP)** can be formulated as follows:

$$\textbf{(OP)} \quad \forall x \, \forall y \, \exists q \, (\, q \, \pi_0 \, x \ \wedge \ q \, \pi_1 \, y \,),$$

where the abbreviating relators π_0 and π_1 designate conjugated projections associated with ordered pairs of the above kind and are defined as follows:

$$q \, \sigma \, x \ \leftrightarrow_{\mathrm{Def}} \exists s \, \big(\, x \in s \, \wedge \, s \in q \, \wedge \, \neg \exists u \, (\, u \in s \, \wedge \, u \neq x \,) \big),$$

$$\text{viz., there is a singleton } s \text{ in } q \text{ to which } x \text{ belongs;}$$

$$q \, \pi_0 \, x \ \leftrightarrow_{\mathrm{Def}} q \, \sigma \, x \, \wedge \, \neg \exists v \, (\, q \, \sigma \, v \, \wedge \, v \neq x \,),$$

$$\text{viz., there is a unique singleton } s \text{ in } q, \text{ and } x \text{ belongs to } s;$$

$$q \, \pi_1 \, y \ \leftrightarrow_{\mathrm{Def}} \exists w \, \big(\, y \in w \, \wedge \, w \in q \, \big) \, \wedge \, \neg \exists z \, \big(\exists t \, (\, z \in t \, \wedge \, t \in q \,) \, \wedge \, \neg q \, \pi_0 \, z \, \wedge \, z \neq y \, \big),$$

$$\text{viz., } q \text{ has either the form } \{\{x,y\},\{x\}\} \text{ or the form } \{\{x,y\},\{x\},\emptyset\}, \text{ for some } x.$$

Then, by unfolding π_0 and π_1 within **(OP)** and by judiciously renaming bound variables, one can bring no variables other than x, y, and q into play.

Even though **(OP)** and **(P)** can be shown to be logically equivalent to each other, the intuitive meaning of **(OP)** differs from the one of **(P)**. Notice, however, that if **(OP)** (which is readily seen to logically follow from **(P)**) is assumed, then, in view of the single-valuedness of π_b for $b = 0, 1$ (to wit, $\forall q \, \forall u \, \forall v \big(\, (\, q \pi_b u \, \wedge \, q \pi_b v \,) \, \rightarrow \, u = v \, \big)$), the following becomes an intuitively acceptable 3-variable rendering of **(P)**:

$$\forall q \Big(\, \big((\exists v \, q \, \pi_0 \, v) \wedge (\exists v \, q \, \pi_1 \, v) \big) \, \rightarrow \, \exists p \, \forall v \, \big(v \in p \ \leftrightarrow \ (\, q \, \pi_0 \, v \ \vee \ q \, \pi_1 \, v \,) \big) \Big).$$

Under the assumption **(OP)** one could, with equal ease, get 3-variable formulations of **(W)** and **(L)**; e.g., **(W)** could be stated as follows:

$$\forall q \big((\, \exists v \, q \, \pi_0 \, v \,) \, \rightarrow \, \exists p \, \forall v \, \big(v \in p \ \leftrightarrow \ (\, q \, \pi_1 \, v \ \vee \ \exists p (\, q \, \pi_0 \, p \wedge v \in p) \,) \big) \big).$$

On the other hand, notice that $\ \forall q \, \exists p \, \forall v \, \big(v \in p \ \leftrightarrow \ (\, q \, \pi_0 \, v \ \vee \ q \, \pi_1 \, v \,) \big)$ would *not* be an acceptable rendering of **(P)**; in fact, should there be a q devoid of both π_0-image and π_1-image, then the set p corresponding to such a q as here specified would be null.

In this frame of mind, we will consider different alternative weak theories. Since we will provide automated validations of our claims (cf. Sec.3). Next section introduces the basics of map calculus and its deductive machinery.

2   Deduction in the arithmetic of dyadic relations

We will slightly adapt here the notions developed in [24] as an evolution of the algebraic approach to logic first proposed by Augustus De Morgan, Charles Sanders Peirce, and Ernst Schröder.

In the arithmetic of dyadic relations one can state, and infer, properties of relations—*maps*—over an unspecified, yet fixed, domain $\mathcal{U}$ of discourse. The signature of the ground language $\mathcal{L}^\times$ underlying map calculus consists of constant symbols (i.e., $:\!\emptyset$, $\mathbb{1}$, and ι); a single map letter, $\in$ (of arity 0, like constants, but freely interpretable); primitive Boolean map operators, $\cap$ and $\triangle$ (both dyadic), and Peircean map operators $\circ$ (dyadic) and $\smile$ (monadic), in terms of which

$$P \cap Q = Q \cap P \qquad\qquad\qquad \iota \circ P = P$$
$$P \cap (Q \triangle R) \triangle P \cap Q = P \cap R \qquad\qquad P^{\smile\smile} = P$$
$$(P \star_1 Q) \star_1 R = P \star_1 (Q \star_1 R) \qquad (P \star_2 Q)^{\smile} = Q^{\smile} \star_2 P^{\smile}$$
$$P^{\smile} \circ (R \cap (P \circ Q \triangle R)) \cap Q = \mathbb{0} \qquad\qquad \mathbb{1} \cap P = P$$
$$((P \triangle Q) \triangle P \cap Q) \circ R = (Q \circ R \triangle P \circ R) \triangle Q \circ R \cap P \circ R$$
$$\star_1 \in \{\triangle, \cap, \circ\} \text{ and } \star_2 \in \{\cap, \circ\}$$

Fig. 2. Logical axioms of map algebra

other constructs such as $\cup$ and $\setminus$ (dyadic), and $^{-}$ (monadic complementation) can be expressed.[4]

Semantics can be assigned to the terms of this signature simply by fixing a nonempty domain $\mathcal{U}$, by choosing a subset $\in^{\Im}$ of the Cartesian square $\mathcal{U} \times \mathcal{U}$ as interpretation of the map letter $\in$, and by then interpreting in the usual manner the basic constants and constructs:

$$\mathbb{0}^{\Im} =_{\mathrm{Def}} \emptyset, \qquad \mathbb{1}^{\Im} =_{\mathrm{Def}} \mathcal{U} \times \mathcal{U}, \qquad \iota^{\Im} =_{\mathrm{Def}} \{(a,a) \mid a \text{ in } \mathcal{U}\};$$
$$(Q \cap R)^{\Im} =_{\mathrm{Def}} \{(a,b) \in Q^{\Im} \mid (a,b) \in R^{\Im}\};$$
$$(Q \triangle R)^{\Im} =_{\mathrm{Def}} \{(a,b) \in Q^{\Im} \mid (a,b) \notin R^{\Im}\} \cup \{(a,b) \in R^{\Im} \mid (a,b) \notin Q^{\Im}\};$$
$$(Q \circ R)^{\Im} =_{\mathrm{Def}} \{(a,b) \in \mathbb{1}^{\Im} \mid \text{there are pairs } (a,c) \in Q^{\Im} \text{ such that } (c,b) \in R^{\Im}\};$$
$$(Q^{\smile})^{\Im} =_{\mathrm{Def}} \{(b,a) \mid (a,b) \in Q^{\Im}\}.$$

The intended domain $\mathcal{U}$ of discourse, in this paper, is the universe $\mathcal{V}$ of all sets. Properties of maps can be stated through *map equalities* $Q = R$ whose sides Q, R are map expressions. The language $\mathcal{L}^{\times}$ can be extended profitably with many derived operators (in addition to $\cup, \setminus, ^{-}$) and with a number of shorthand pieces of notation for equalities, as illustrated below:[5]

$$P \subseteq Q \leftrightarrow_{\mathrm{Def}} P \setminus Q = \mathbb{0}$$
$$\mathsf{RUniq}(P) \leftrightarrow_{\mathrm{Def}} P^{\smile} \circ P \subseteq \iota \qquad\qquad \mathsf{LUniq}(P) \leftrightarrow_{\mathrm{Def}} \mathsf{RUniq}(P^{\smile})$$
$$\mathsf{funcPart}(P) =_{\mathrm{Def}} P \setminus P \circ \overline{\iota} \qquad\qquad \mathsf{valve}(P,Q) =_{\mathrm{Def}} P \setminus \iota \circ (P \setminus Q)$$
$$\mathsf{syq}(P,Q) =_{\mathrm{Def}} \overline{P^{\smile} \circ \overline{Q}} \cap \overline{\overline{P}^{\smile} \circ Q} \qquad\qquad \mathsf{noy}(P) =_{\mathrm{Def}} \mathsf{syq}(P,P)$$

In order to characterize the behavior of the map constructs, a number of axioms are imposed. Fig. 2 shows an axiomatization involving the primitive map constructs. The choice of such *logical* axioms is a preparatory step for the development of an inference machinery for map-reasoning—and, subordinately, for set-reasoning.

The problem of translating first-order sentences or entire first-order theories into map calculus has been treated, among others, in [4, 13]. In particular, the (re-)formulation of the Zermelo-Fraenkel theory ZF within map calculus amounts to introducing, in addition the logical axioms, a number of *proper* axioms to restrain the possible interpretations of the primitive map $\in$. Fig. 3 shows translated versions of **(E)**, **(N)**, **(OP)**, **(R)**, and **($\mathbf{A}^n$)** in this ground equational formalism, where the steps in the formalization of **(OP)** reflect the ideas discussed in Sec.1.

As already said, the crucial concept in obtaining relational counterpart of given theories, is the one of conjugated projections. Formalized within $\mathcal{L}^{\times}$, the

---

[4] We assume that the priorities of these operators are decreasing w.r.t. the ordering
$^{-}, \smile, \circ, \cap, \triangle, \cup, \setminus$.

[5] The noy operator was introduced by Jacques Riguet in 1948.

$$
\begin{array}{|c|c|}
\hline
\ni =_{\mathrm{Def}} \in^{\smile} & \ni\ni =_{\mathrm{Def}} \ni \circ \ni \\
\in\in =_{\mathrm{Def}} \in \circ \in & \notni\in =_{\mathrm{Def}} \overline{\in} \circ \in \\
\sigma =_{\mathrm{Def}} \ni \circ (\ni \setminus \ni \circ \bar{\iota}) & \mathsf{mix} =_{\mathrm{Def}} \in\in \cap \notni\in \\
\hline
\end{array}
$$

$$
\begin{array}{|ll|ll|}
\hline
\multicolumn{2}{|l|}{\boldsymbol{\pi_0} =_{\mathrm{Def}} \boldsymbol{\sigma} \setminus \boldsymbol{\sigma} \circ \bar{\iota}} & \multicolumn{2}{l|}{\boldsymbol{\pi_1} =_{\mathrm{Def}} \ni\ni \setminus (\ni\ni \setminus \pi_0) \circ \bar{\iota}} \\
\textbf{(E)} & \iota = \mathsf{noy}(\in) & \textbf{(N)} & \mathbb{1} = \overline{\mathbb{1} \circ \in} \circ \mathbb{1} \\
\textbf{(OP)} & \mathbb{1} = \pi_0^{\smile} \circ \pi_1 & \textbf{(R)} & \mathbb{1} \circ \in = \mathbb{1} \circ (\in \setminus \ni \circ \in) \\
\textbf{(A}^n\textbf{)} & \emptyset = \underbrace{\in \circ \cdots \circ \in}_{n+1 \text{ factors}} \cap\, \iota & & \\
\hline
\end{array}
$$

Fig. 3. Shorthand notation and a Peircean specification of a very weak set theory

$$
\begin{array}{|r|l||r|l|}
\hline
i. & \mathsf{LUniq}(P), \mathsf{LUniq}(Q) \vdash^{\times} \mathsf{LUniq}(P{\circ}Q) & iv. & Q \circ Q \cap \iota = \emptyset \vdash^{\times} \mathsf{RUniq}\big(P \setminus P \circ (\bar{\iota}\setminus Q)\big) \\
ii. & \mathsf{LUniq}(Q) \vdash^{\times} \mathsf{LUniq}\big(\mathsf{valve}(P,Q)\big) & v. & \vdash^{\times} \mathsf{RUniq}\big(\mathsf{funcPart}(P)\big) \\
iii. & \textbf{(E)} \vdash^{\times} \mathsf{RUniq}\big(\mathsf{syq}(\mathsf{P},\in)\big) & vi. & (\mathbf{A}^{2\cdot n+1}) \vdash^{\times} \mathsf{RUniq}(\boldsymbol{\gamma}_{n+1}) \\
\hline
\end{array}
$$

where $\boldsymbol{\gamma}_n =_{\mathrm{Def}} \ni \setminus \ni \circ (\bar{\iota} \setminus \underbrace{\in \circ \cdots \circ \in}_{n \text{ factors}})$

Fig. 4. Basic lemmas proved with Otter in map calculus

conditions for two maps to be conjugated (quasi-)projections are:
$$\ell^{\smile} \circ r = \mathbb{1}, \qquad \mathsf{RUniq}(\ell), \qquad \mathsf{RUniq}(r).$$
Notice that $\ell^{\smile} \circ r = \mathbb{1}$ directly reflects into the equational formulation of **(OP)**.

General translation techniques can be designed, by which one can translate any first-order formula of the set-theoretic language whose only primitive predicate symbols are $=$ and $\in$ into map calculus, when conjugated projections are available. Any equation of map calculus can easily be translated, in its turn, into a 3-variable first-order sentence (cf., e.g., [24, Chap.4] and [11]). Of course the same reduction to 3-variable sentences can be performed under axioms different from those in Fig. 3, provided such axioms enable one to identify a pair of conjugated projections.

As mentioned, previous research shown the possibility of automating equational reasoning based on relational specifications of the kind given in Figures 2 and 3 (cf. [12, 13], for instance). The first aim of this activity consisted in proving a collection of general algebraic laws mainly related to functionality of maps (cf. Fig. 4). This task prepares a solid ground for the development of further experimentation on the set-theoretical notions of ordered pair.

Some of the proved laws are of particular interest on their own. For instance, consider law *iii* of Fig. 4. Otter was able to prove both this law and its converse (cf. [3]) This result certifies that the map equality $\mathsf{RUniq}(\mathsf{syq}(P,\in))$ constitutes an alternative formulation of the extensionality axiom **(E)**.

A crucial law among those in Fig. 4 is *iv*. Let us now briefly sketch the proof of this law as generated with Otter. After introduced the definition:
$$\mathsf{protoFuncPart}(P,Q) =_{\mathrm{Def}} P \setminus (P \circ Q),$$
the leading derivation steps yielding the desired proof of *iv* are:

- $\mathsf{funcPart}(P) = \mathsf{protoFuncPart}(P, \bar{\iota})$
- $\mathsf{protoFuncPart}(P,Q) \cap \mathsf{protoFuncPart}(P,Q) \circ Q = \emptyset$
- $\mathsf{protoFuncPart}(P,Q)^{\smile} \circ \mathsf{protoFuncPart}(P,Q) \subseteq \overline{Q}$

- $\mathsf{protoFuncPart}(P,Q)^{\smile} \circ \mathsf{protoFuncPart}(P,Q) \subseteq \overline{Q} \cap \overline{Q}^{\smile}$
- $Q \circ Q \subseteq \bar{\iota} \; \vdash^{\times} \; \mathsf{RUniq}(\mathsf{protoFuncPart}(P, \bar{\iota} \cap \overline{Q}))$
- $Q \circ Q \cap \iota = \emptyset \; \vdash^{\times} \; \mathsf{RUniq}(\mathsf{protoFuncPart}(P, \bar{\iota} \setminus Q))$

Each of the above proof steps has been derived by using the axioms (cf. Fig. 2) and a collection of lemmas on map constructs (cf. [12, 13]).[6]

As corollaries of *iv*, Otter easily obtained the proofs of *v* (timing: 0.01 sec., length: 3) and of several instances of the scheme *vi* of Fig. 4 (for instance, in the case $n = 3$, the length of the generated proof is 4 and it was obtained in 0.75 sec). This is an excerpt of the laws (mainly related to functionality of maps) that have been obtained with Otter:

law	length (steps)/time (sec.)	generated/kept clauses
$\mathsf{RUniq}(\emptyset)$	1/0.06	917/109
$\mathsf{RUniq}(\iota)$	1/0.06	917/109
$\mathsf{RUniq}(P) \vdash^{\times} \mathsf{RUniq}(P \cap Q)$	7/1.86	26575/4371
$\mathsf{RUniq}(P), \mathsf{RUniq}(Q) \vdash^{\times} \mathsf{RUniq}(P \circ Q)$	6/0.05	926/217
$\mathsf{valve}(P,Q) \subseteq P$	2/1.11	11435/6041
$\mathsf{valve}(P,Q) \subseteq \overline{\bar{\iota} \circ (P \cap \overline{Q})}$	5/1.10	12334/5893
$R \circ \mathsf{valve}(P,Q) \subseteq R \circ \overline{\bar{\iota} \circ (P \cap \overline{Q})}$	4/0.94	19114/2324
$\mathsf{valve}(P,Q) \cap R \subseteq P \cap R$	5/0.20	3791/670
$P \subseteq Q \vdash^{\times} \mathsf{valve}(P,Q) = P$	5/0.90	11600/4079
$\mathsf{LUniq}(Q) \vdash^{\times} \mathsf{LUniq}(\mathsf{valve}(P,Q))$	12/66.27	253318/15441

3 Expressibility in 3-variables

In this section we consider three alternative weak aggregate theories and introduce suitable notions of ordered pair. For all these pairing notions a couple of relations will be defined and proved to meet the conditions to be a pair conjugated quasi-projections. These results certify the equipollence of the equational formulations of our theories and their first-order formulations.

3.1 Expressibility of (E) ∧ (N) ∧ (W) ∧ (L) in 3 variables

In our own formalization of the axiom of elementary sets, very much like in Tarski's one, the notion of ordered pair will be the hinge of the formulation in three variables. The pairs we have here in mind are as follows:
$$\langle x, y \rangle \;=_{\mathrm{Def}}\; \big\{ \{ y \} \,\mathsf{less}\, x \,,\, \{ y \} \,\mathsf{with}\, x \big\}$$
where the binary functions less and with, and the constant $\emptyset$, result from the Skolemization of **(L)**, **(W)**, and **(N)**, respectively, and
$$\{ v, w \} =_{\mathrm{Def}} (\emptyset \,\mathsf{with}\, v) \,\mathsf{with}\, w \,, \qquad \{ v \} =_{\mathrm{Def}} \{ v, v \} \,.$$
Although the structure of such pairs only marginally departs from the Kuratowski's pair notion, we need to assume the extensionality axiom, **(E)**, which is

---

not necessary with the traditional approach. By proceeding in a way similar (but much simpler) to the way **(P)** got restated as **(OP)**, we achieve the following restatement of **(N)** $\wedge$ **(W)** $\wedge$ **(L)**:

(D) $\quad \forall x \, \forall y \, \exists d \left(y \in d \,\wedge\, \forall v \big(\exists w (v \in w \,\wedge\, w \in d) \,\wedge\, \exists \ell (v \notin \ell \,\wedge\, \ell \in d) \,\leftrightarrow\, v = x \big) \right),$

which under the renaming $v \mapsto y$, $w \mapsto x$, $\ell \mapsto x$ of bound variables becomes a 3-variable sentence. This **(D)** says that one can build the set $\big\{ y \text{ less } x, \, y \text{ with } x \big\}$ out of sets x, y whatsoever. Only indirectly, it enables one to form singletons, the null set $\emptyset$, and ordered pairs of the form $\langle x, y \rangle$. By bringing **(D)** into Skolemized form we get:[7]

(D′) $\quad Y \in (Y \, \mathbf{❂} \, X) \,\wedge\, \forall v \big(\exists w (v \in w \,\wedge\, w \in Y \, \mathbf{❂} \, X) \,\wedge\, \exists \ell (v \notin \ell \,\wedge\, \ell \in Y \, \mathbf{❂} \, X) \,\leftrightarrow\, v = X \big),$

which is equivalent to the conjunction of **(N)**, **(W)**, and **(L)**, in this sense:

- under **(N)**, **(W)**, and **(L)**, one can define $X \, \mathbf{❂} \, Y =_{\mathrm{Def}} \{ X \text{ less } Y, \, X \text{ with } Y \}$ and then derive **(D′)**;

- under **(E)** and **(D′)**, one can prove that
  (W′) $\exists w \in Y \, \mathbf{❂} \, X \, \forall v (v \in w \,\leftrightarrow\, v \in Y \,\vee\, v = X)$,
  (L′) $\exists \ell \in Y \, \mathbf{❂} \, X \, \forall v (v \in \ell \,\leftrightarrow\, v \in Y \,\wedge\, v \neq X)$,
  (N′) $\exists s \in (Y \, \mathbf{❂} \, X) \, \mathbf{❂} \, Y \, \exists e \in s \, \exists z \in e \, \mathbf{❂} \, s \, \forall v \, v \notin z$,
  whence **(W)**, **(L)**, and **(N)** readily follow.

By introducing a suitable pair of map-expressions:
$$\boldsymbol{\lambda} =_{\mathrm{Def}} \mathsf{valve}(\mathsf{mix}, \emptyset) \qquad \boldsymbol{\varrho} =_{\mathrm{Def}} \mathsf{valve}(\in \in, \boldsymbol{\lambda})$$
the following comes out to be an immediate translation of **(D)** into the arithmetic of relations:
$$\textbf{(D)} \qquad \mathbb{1} = \boldsymbol{\lambda} \circ \ni,$$
while the relations $\boldsymbol{\lambda}^{\smile}$ and $\boldsymbol{\varrho}^{\smile}$ constitute a pair of conjugated projections corresponding to our notion $\langle x, y \rangle$ of ordered pair very much like the expressions $\boldsymbol{\pi}_0, \boldsymbol{\pi}_1$ in Fig. 3 designate projections associated with Kuratowski's pair notion. In the arithmetic of relations it can easily be proved that $\mathsf{LUniq}(\boldsymbol{\lambda})$ and $\mathsf{LUniq}(\boldsymbol{\varrho})$ both hold (viz., $\boldsymbol{\lambda}^{\smile}, \boldsymbol{\varrho}^{\smile}$ designate partial functions). These laws can be easily proved from law *ii* of Fig. 4 and the simple lemma $\mathsf{LUniq}(\emptyset)$. Otter was able to prove $\mathsf{LUniq}(\boldsymbol{\lambda})$ in 0.01 seconds by producing a proof of length 3. Then, a proof of length 3 of $\mathsf{LUniq}(\boldsymbol{\varrho})$ has been obtained as an immediate corollary.

We also succeeded in deriving the analogue $\mathbb{1} = \boldsymbol{\lambda} \circ \boldsymbol{\varrho}^{\smile}$ of **(OP)** from **(D)** and **(N)** (cf. [3]); on the other hand, we have been unable to obtain this unless by assuming **(N)**. Nevertheless, we can be sure that **(N)** follows from **(D)** in the arithmetic of relations, because if we put $\boldsymbol{\rho} =_{\mathrm{Def}} \boldsymbol{\lambda} \circ \big(\in \cap \ni \circ \overline{\boldsymbol{\iota} \circ \mathsf{mix}} \big)$ then (much more easily than for $\boldsymbol{\varrho}$) one can prove that $\mathbb{1} = \boldsymbol{\lambda} \circ \boldsymbol{\rho}^{\smile}$, and one can easily derive $\mathsf{LUniq}(\boldsymbol{\rho})$ from **(E)**. In defining this new $\boldsymbol{\rho}$, we have in mind a second variant of Kuratowski's pair, which is
$$[x, y] =_{\mathrm{Def}} (x \, \mathbf{❂} \, y) \, \mathbf{❂} \, x.$$
Otter's proof of $\mathbb{1} = \boldsymbol{\lambda} \circ \boldsymbol{\rho}^{\smile}$ relies on the following lemmas:

---

[7] From now on, we will adopt the convention that uppercase variables are meant to be universally bound.

law	length/time (sec.)	gener./kept clauses
$P \circ Q = \mathbb{1} \vdash^{\times} \ P \circ (Q \cap Q^{\smile} \circ P^{\smile}) = \mathbb{1}$	3/0.03	169/51
$P \circ R^{\smile} \cap S \subseteq P \circ (R^{\smile} \cap P^{\smile} \circ S)$	2/0.25	4499/305
$P \subseteq Q \vdash^{\times} \ P \circ (R \cap P^{\smile} \circ S) \subseteq P \circ (R \cap Q^{\smile} \circ S)$	4/3.45	16941/5070

From them, these proof steps yielded the proof of our thesis:

- **(D)** $\vdash^{\times} (\in \cap \boldsymbol{\lambda} \circ \ni) \circ \boldsymbol{\lambda}^{\smile} = \mathbb{1}$ length:3; time:0.03
- $\in \cap \boldsymbol{\lambda} \circ \ni \ \subseteq \ \boldsymbol{\lambda} \circ (\ni \cap (\overline{\boldsymbol{\iota} \circ \mathsf{mix}})^{\smile} \circ \in)$ length:4; time:0.11
- $\mathbb{1} = (\in \cap \boldsymbol{\lambda} \circ \ni) \circ \boldsymbol{\lambda}^{\smile} \ \subseteq \ (\boldsymbol{\lambda} \circ (\ni \cap (\overline{\boldsymbol{\iota} \circ \mathsf{mix}})^{\smile} \circ \in)) \circ \boldsymbol{\lambda}^{\smile}$ length:7; time:4.11
- $\mathbb{1} = (\boldsymbol{\lambda} \circ (\ni \cap (\overline{\boldsymbol{\iota} \circ \mathsf{mix}})^{\smile} \circ \in)) \circ \boldsymbol{\lambda}^{\smile}$ length:5; time:0.25

To prove $\mathsf{LUniq}(\boldsymbol{\rho})$ from **(E)**, the following auxiliary lemma had to be proved:

$$(\textbf{E}) \vdash^{\times} \mathsf{LUniq}\left(\in \cap \ni \circ \overline{\boldsymbol{\iota} \circ \mathsf{mix}}\right). \tag{1}$$

Here is the trace of the proof generated with Otter. Notice that it was necessary to prove a number of auxiliary lemmas.

- $\overline{\overline{P} \circ Q} \circ Q^{\smile} \subseteq P$
- $(W \cap R \circ Q) \circ T \subseteq \boldsymbol{\iota} \vdash^{\times} R \cap W \circ (Q^{\smile} \cap T \circ P) = \emptyset$
- $\overline{P} \cap R \circ S^{\smile} \circ (Q^{\smile} \cap T \circ P) = \emptyset \vdash^{\times} (Q \cap P^{\smile} \circ T^{\smile}) \circ S \cap \overline{P}^{\smile} \circ R = \emptyset$
- $P \circ R^{\smile} \cap S = \emptyset \vdash^{\times} (P \circ R \cap Q)^{\smile} \cap S = \emptyset$
- $(R \circ S^{\smile} \cap \overline{P} \circ Q) \circ T \subseteq \boldsymbol{\iota} \vdash^{\times} (Q \cap P^{\smile} \circ T^{\smile}) \circ S \cap \overline{P}^{\smile} \circ R = \emptyset$
- $(P \circ P \cap \overline{P} \circ P) \circ \overline{\boldsymbol{\iota} \circ (P \circ P \cap \overline{P} \circ P)}^{\smile} \subseteq \boldsymbol{\iota} \vdash^{\times} (P \cap P^{\smile} \circ \overline{\boldsymbol{\iota} \circ (P \circ P \cap \overline{P} \circ P)}) \circ P^{\smile} \cap \overline{P}^{\smile} \circ P = \emptyset$
- $(P \cap P^{\smile} \circ \overline{\boldsymbol{\iota} \circ (P \circ P \cap \overline{P} \circ P)}) \circ P^{\smile} \cap \overline{P}^{\smile} \circ P = \emptyset$
- $(P \cap P^{\smile} \circ \overline{\boldsymbol{\iota} \circ (P \circ P \cap \overline{P} \circ P)}) \circ (P \cap P^{\smile} \circ \overline{\boldsymbol{\iota} \circ (P \circ P \cap \overline{P} \circ P)})^{\smile} \cap \overline{P}^{\smile} \circ P = \emptyset$
- $(P \cap P^{\smile} \circ \overline{\boldsymbol{\iota} \circ (P \circ P \cap \overline{P} \circ P)}) \circ (P \cap P^{\smile} \circ \overline{\boldsymbol{\iota} \circ (P \circ P \cap \overline{P} \circ P)})^{\smile} \cap \overline{P}^{\smile} \circ \overline{P} = \emptyset$
- $(\in \cap \ni \circ \overline{\boldsymbol{\iota} \circ (\in \circ \in \cap \not\ni \circ \in)}) \circ (\in \cap \ni \circ \overline{\boldsymbol{\iota} \circ (\in \circ \in \cap \not\ni \circ \in)})^{\smile} \cap (\not\ni \circ \in \cup \ni \circ \not\in) = \emptyset$

The overall time spent in proving these laws was 15.62 seconds. The longest and most time-consuming proof was the one of the last law: length 8 in 6.52 seconds. From the last of the above laws, by the definition of noy and mix, and by assuming **(E)** we can conclude the proof of (1).

At this point, $\mathsf{LUniq}(\boldsymbol{\rho})$ could be derived readily by means of law i in Fig. 4.

3.2 Expressibility of $(\textbf{E}) \wedge (\textbf{A}^n) \wedge (\textbf{W}) \wedge (\textbf{L})$ in 3 variables

In this section we show that under **(E)**, one can drop the null-set axiom **(N)**, provided that acyclicity of sets is assumed (by means of $(\textbf{A}^n)$). In this case, in fact, **(W)** and **(L)** suffice to support suitable notions of ordered pair. The ordered pair we deal with in this section is

$$\lfloor X, Y \rfloor \ =_{\mathrm{Def}} \ X \,\mathsf{with}(Y \,\mathsf{with}(Y \,\mathsf{with} X)).$$

Corresponding to this pair we introduce the following pair of relations:

$$\boldsymbol{\alpha} \ =_{\mathrm{Def}} \ \mathsf{syq}(\in \cap \in \circ \in \circ \circ \in \circ \in, \ \in), \ \text{ and } \ \boldsymbol{\beta} \ =_{\mathrm{Def}} \ \boldsymbol{\gamma}_3 \circ \mathsf{syq}(\in \cap \in \circ \in, \ \in),$$

to be meant as left and right projections, respectively.

Consider that both **(E)** and $(\textbf{A}^n)$ have already been expressed within the map calculus (cf. Fig. 3). Moreover, by $(\textbf{A}^5)$, we immediately obtain $\mathsf{RUniq}(\boldsymbol{\alpha})$ and $\mathsf{RUniq}(\boldsymbol{\beta})$ —Otter generated the proofs of these facts in 0.01 (length 2) and 0.06 (length 6) seconds, respectively, by using the laws in Fig. 4. As a consequence of these results, an easy manner to express $(\textbf{E}) \wedge (\textbf{A}^n) \wedge (\textbf{W}) \wedge (\textbf{L})$

in 3 variables consists in explicitly asserting a further *pairing* axiom:
$$(\mathbf{OP}_1) \qquad \alpha^{\smile} \circ \beta = \mathbb{1}.$$
This ensures that α and β are a pair of conjugated projections. Notice that this law follows from $(\mathbf{E}) \wedge (\mathbf{A}^5) \wedge (\mathbf{W}) \wedge (\mathbf{L})$ within the predicate calculus. At this point, by means of the pair of conjugated projections α and β, we can express both $(\mathbf{W})$ and $(\mathbf{L})$ in three variables, in order to complete the equational rendering of $(\mathbf{E}) \wedge (\mathbf{A}^n) \wedge (\mathbf{W}) \wedge (\mathbf{L})$.

3.3 Expressibility of $(\mathbf{R}) \wedge (\mathbf{N}) \wedge (\mathbf{W}) \wedge (\mathbf{L})$ in 3 variables

Unlike the pair notions analyzed so far, the one to be examined in this section will not benefit from the extensionality axiom $(\mathbf{E})$. Each one of the two pairing functions considered in Sections 3.1 and 3.2 has some advantage over Kuratowski's pairing: one leads, in fact, to very simple specifications of the projections and, consequently, to a terse formulation of the conjunction $(\mathbf{N}) \wedge (\mathbf{W}) \wedge (\mathbf{L})$ (provided $(\mathbf{E})$ is assumed); the other one, even though more cumbersome, can be exploited in certain contexts where Kuratowski's pairing is not viable, because there is no guarantee that the operation $X \mapsto \{X\}$ can be performed.

Here we are assuming $(\mathbf{N}) \wedge (\mathbf{W})$—which yield $(\mathbf{P})$; Kuratowski's pairing would hence be viable, but we propose a notion of pair which relies on the axioms $(\mathbf{L})$ and $(\mathbf{R})$ too. Save for the fact that the associated projections car and cdr are total (which is a rather marginal virtue), we make no claim that these projections are any better than the projections π_0, π_1 discussed in Sec.1 (see also π_0 and π_1 in Fig. 3). However, since proving that car and cdr meet the formal properties of conjugated projections requires some labour in first-order logic, a labour which we have already afforded with Otter, we can take this as a benchmark from which to start comparing the performances of an automatic theorem-prover confronted with full first-order reasoning on the one hand, and with purely equational reasoning on the other, in carrying out the same task. Currently, we have not provided yet a full equational proof that car and cdr are conjugated projections, and leave this as future work. The notion of pair we adopt here is:
$$\lceil X, Y \rceil \ =_{\mathrm{Def}} \Big\{ \{X\}, \big\{\{X\}, \{Y, \{Y\}\}\big\} \Big\}.$$
Consequently, a pair of conjugated projections car and cdr can be so defined:

$$\mathsf{arb} =_{\mathrm{Def}} \mathsf{funcPart}(\ni \setminus \ni \in), \qquad \mathsf{car} =_{\mathrm{Def}} \mathsf{arb} \circ \mathsf{arb},$$

$$\mathsf{arb\_lessArb} =_{\mathrm{Def}} \mathsf{syq}(\in\setminus\mathsf{arb}^{\smile}, \in) \circ \mathsf{arb}, \qquad \mathsf{cdr} =_{\mathrm{Def}} \mathsf{syq}(\in \circ \mathsf{arb\_lessArb}^{\smile} \setminus \mathsf{arb}^{\smile}, \in) \circ \mathsf{car}.$$

Clearly, functionality of arb and of car directly follows from laws in Fig. 4. However, we have been unable till now to obtain Otter-proofs of $\mathsf{RUniq}(\mathsf{cdr})$ and of $\mathsf{car}^{\smile} \circ \mathsf{cdr} = \mathbb{1}$ within map calculus. Obtaining a proof of $\mathsf{RUniq}(\mathsf{cdr})$ will be our next task in this work. After obtaining such a proof we could, at worst, complete our weak theory by adopting $\mathsf{car}^{\smile} \circ \mathsf{cdr} = \mathbb{1}$ as one of our axioms, analogously to the way we have proceeded in the previous case.

4   Inexpressibility in 3-variables

In Sections 4.1 and 4.2 we will prove that the axiom **(W)**, neither considered in isolation nor taken together with **(L)**, can be expressed with only three variables. To show this, we will rely on a model-theoretic method introduced in [16]. This method centers around so-called *pebble games*, which are two-player processes closely akin to the older Ehrenfeucht-Fraïssé games (cf. [8, 15]). We will proceed by first singling out two structures which disagree on the truth-values of **(W)** and **(L)** but agree w.r.t. **(E)**; games will then be the essential tool for proving that these structures are indistinguishable by formulas in three variables. Our aim will be to suggest the winning strategy to the player, named Duplicator, in favor of which our inexpressibility analysis will be inclined.

The way in which we will carry out this 2-stage investigation, will turn out to be somewhat more 'semantic' than, for example, the application of games in establishing the inexpressibility of the density property in structures of propositional linear time logic (see [16, 25]). *Localization*, the approach which underlies inductive constructions of the winning strategies for exploitations of pebble games in the realm of temporal structures (either linear or not), does not appear adequate to behave well in our framework. The reason is that models of weak set theory are very poor in structure compared to models of time, which are either lines or trees. In our framework, in order to suggest the winning strategy to Duplicator, it will be necessary to provide a deeper insight in the peculiarities of the structures than is necessary for temporal structures. As a matter of fact, to set the ground for the desired strategy we will be forced to impose somewhat artificial orderings on the domains of the structures.

The proofs of all the results we present in this section can be found in [10].

4.1   Inexpressibility of (W) in 3 variables

Preliminary to the stronger result to be discussed in Sec.4.2, we show that **(W)** is not expressible in 3 variables, closing the question addressed in [20] and [24]. We proceed by exhibiting a *'rich'* structure, $\mathfrak{R}$, and a *'poor'* structure, $\mathfrak{P}$, which model **(W)** and ¬**(W)**, respectively. The inexpressibility of **(W)** in 3 variables will be proved by showing that these structures satisfy the same collection of sentences in (at most) 3 variables. In turn, the equivalence of $\mathfrak{R}$ and $\mathfrak{P}$ relative to sentences in 3 variables will be proved, as already announced, by the technique based on pebble games. In our case the players, named *Duplicator* and *Spoiler*, own three pebbles each (the number of pebbles clearly corresponds to the number of variables which we regard as the critical threshold).

This section well illustrates the valuable insight provided by pebble games in expressibility analysis. Notice, however, that a simpler conceptual tool already present in [20] would have sufficed to treat the case at hand. On the other hand, the next case before us, to be treated in Sec.4.2, seems to lie beyond the power of Kwatinetz' approach.

Definition 1. *Let* $\mathbb{N} = \{0, 1, 2, \dots\}$, $\mathbb{Z} = \mathbb{N} \cup \{-i \mid i \in \mathbb{N}\}$, *and let* $|X|$ *designate the* cardinality *of any set* X. *A subset* A *of* $\mathbb{Z}$ *is said to be* REPRESENTABLE *if*

it meets the condition $0 \notin A \ \wedge \ |A \setminus \mathbb{N}| < \aleph_0 \ \wedge \ |\mathbb{N} \setminus A| < \aleph_0$. *For* $i, j \in \mathbb{Z}$ *and* $X \subseteq \mathbb{Z}$, *we define* interval, left endpoints, radius, *and* footprint *as follows:*

$$[i,j] =_{Def} \{ h \in \mathbb{Z} \mid i \leqslant h \ \wedge \ h \leqslant j \}, \qquad lend(X) =_{Def} \{ i \in X \mid i - 1 \notin X \},$$
$$rad(X) =_{Def} \min\{ i \in \mathbb{N} \mid lend(X) \subseteq [-i,i] \}, \quad foot(X) =_{Def} X \cap [-rad(X), \max(lend(X))].$$
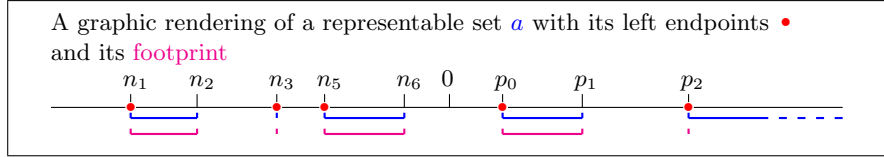$$\square$$

By little reflection, one sees that any representable set A can be uniquely decomposed in the form of a disjoint union

$$A = \bigcup_{i=1}^{\nu}[n_{2 \cdot i - 1}, n_{2 \cdot i}] \ \cup \ \bigcup_{j=0}^{\pi-1}[p_{2 \cdot j}, p_{2 \cdot j+1}] \ \cup \ \{ k \in \mathbb{Z} \mid k \geqslant p_{2 \cdot \pi} \},$$

of non-void intervals some of which may be singletons, one of which is infinite, and whose (left and right) endpoints form the set

$$lend(A) \ \cup \ \{ i \in A \mid i + 1 \notin A \} = \{ n_1, \ldots, n_{2 \cdot \nu} \} \ \cup \ \{ p_0, \ldots, p_{2 \cdot \pi} \},$$

where the n's are negative integers, the p's are positive integers, and $\nu, \pi \in \mathbb{N}$. The footprint $foot(A)$ of such an A is a set which, despite having finite cardinality, fully characterizes A. Notice that $rad(A) = rad(foot(A))$ holds for any representable set A; moreover, a finite set $X \subseteq \mathbb{Z}$ equals $foot(A)$ for some representable set A if and only if $0 \notin X \neq \emptyset$ holds.

Example 1. Let $n_0 < \cdots < n_3 = n_4 < \cdots < n_6 < 0 < p_0 < \cdots < p_2$ be integer numbers and consider the representable set so defined: $a = [n_1, n_2] \cup \{n_3\} \cup [n_5, n_6] \cup [p_0, p_1] \cup \{k \in \mathbb{N} \mid k \geqslant p_2\}$. This set of integers can be graphically represented as follows:

A graphic rendering of a representable set a with its left endpoints $\bullet$ and its footprint

Let $\mathbb{Z}' = \mathbb{Z} \setminus \{0\}$. The respective domains of $\mathfrak{R}$ and $\mathfrak{P}$ are defined as follows:
$$\mathfrak{R} =_{Def} \mathbb{Z}' \cup \big\{ A \subseteq \mathbb{Z} \mid A \text{ is representable} \big\},$$
$$\mathfrak{P} =_{Def} \mathbb{Z}' \cup \big\{ B \subseteq \mathbb{Z} \mid B \in \mathfrak{R} \ \wedge \ |foot(B)| \text{ is even} \big\},$$

The interpretation $\in^{\mathfrak{R}}$ of the membership relator in $\mathfrak{R}$ is defined as:
$$a_1 \in^{\mathfrak{R}} a_2 \quad \leftrightarrow_{Def} \ \big(a_2 \in \mathfrak{R} \setminus \mathbb{Z}' \ \rightarrow \ a_1 \in a_2 \cup (\mathfrak{R} \setminus \mathbb{Z}') \big),$$

with $a_1, a_2 \in \mathfrak{R}$. While the interpretation $\in^{\mathfrak{P}}$ simply is the restriction of $\in^{\mathfrak{R}}$ to $\mathfrak{P}$. The following result can be easily proved:

Lemma 1. *Both* $\mathfrak{R} \models (\mathbf{W})$ *and* $\mathfrak{P} \models \neg(\mathbf{W})$ *hold.*

Prop.1, below, states the result sought for. Its proof is based on the main result on pebble games (cf. [16, Thm.C.1] or [8, Thm.2.3.2]). Namely, "Duplicator has a winning strategy in any 3-pebble-game played on the two structures $\mathfrak{R}, \mathfrak{P}$, if and only if $\mathfrak{R}$ and $\mathfrak{P}$ model the same sentences in (at most) 3 variables."

Proposition 1. Duplicator *has a winning strategy in any 3-pebble-game played on the two structures* $\mathfrak{R}, \mathfrak{P}$. *Thus,* $(\mathbf{W})$ *cannot be expressed in 3 variables.*

4.2 Inexpressibility of $(\mathbf{E}) \wedge (\mathbf{W}) \wedge (\mathbf{L})$ in 3 variables

Now, we will show that the conjunction $(\mathbf{E}) \wedge (\mathbf{W}) \wedge (\mathbf{L})$ cannot be stated by means of a 3-variable sentence. We will see that the difficult moves for Dupli-

cator will be the ones in which Spoiler chooses in $\mathfrak{R} = \left(\mathfrak{R}, \in^{\mathfrak{R}} \right)$ and Duplicator must answer in $\mathfrak{P} = \left(\mathfrak{P}, \in^{\mathfrak{P}} \right)$, two structures satisfying **(E)** and such that **(W)** and **(L)** are true in $\mathfrak{R}$ and false in $\mathfrak{P}$. In order to devise the strategy in those cases, we will perform a *'spiral'* construction of an embedding of $\mathfrak{R}$ into $\mathfrak{P}$. Representable subsets of $\mathbb{Z}$, together with all pertaining notation ($rad, foot$, etc.), will again enter into this spiral construction. We start by putting

$$\mathfrak{R} =_{\mathrm{Def}} \left\{ A \subseteq \mathbb{Z} \mid A \text{ is representable } \right\},$$
$$\mathfrak{P} =_{\mathrm{Def}} \left\{ X \in \mathfrak{R} \mid |X \cap [0, rad(X)]| \geqslant |lend(X \setminus \mathbb{N})| \right\},$$

and, preliminary to defining the interpretations $\in^{\mathfrak{R}}, \in^{\mathfrak{P}}$ of the membership relator in the two structures, we observe that a dyadic relation $\prec$ on $\mathfrak{R}$ exists such that $\prec$ is a total ordering, and the following conditions are met, for all $X, Y \in \mathfrak{R}$ (It can be proved that such an ordering exists, cf. [10, pp.7–8]):

1) $rad(X) < rad(Y)$ implies $X \prec Y$;
2) there are infinitely many $\ell \in \mathbb{N}$ such that a representable set $V \in \mathfrak{P}$ with $foot(V) = \{-\ell\} \cup foot(X)$ is the smallest among all representable sets W with $rad(W) = \ell$;
3) if X is the smallest among all representable sets W satisfying $rad(W) = rad(X) = \ell$, then $-\ell \in X \in \mathfrak{P}$.

Next, in terms of $\prec$, we define two bijective functions

$$\mathfrak{I}_{\mathfrak{R}} : \mathfrak{R} \longrightarrow \mathbb{Z} \setminus \{0\}, \qquad \mathfrak{I}_{\mathfrak{P}} : \mathfrak{P} \longrightarrow \mathbb{Z} \setminus \{0\},$$

which associate integer *indices* with representable sets. Here are $\mathfrak{I}_{\mathfrak{R}}$ and $\mathfrak{I}_{\mathfrak{P}}$:

$$\mathfrak{I}_{\mathfrak{R}}(X) =_{\mathrm{Def}} \min \left(X \setminus \left\{ \mathfrak{I}_{\mathfrak{R}}(Y) \mid Y \in \mathfrak{R} \ \wedge \ Y \prec X \right\} \right);$$
$$\mathfrak{I}_{\mathfrak{P}}(X) =_{\mathrm{Def}} \min \left(X \setminus \left\{ \mathfrak{I}_{\mathfrak{P}}(Y) \mid Y \in \mathfrak{P} \ \wedge \ Y \prec X \right\} \right).$$

These definitions clearly make sense and ensure the injectivity of $\mathfrak{I}_{\mathfrak{R}}$ and $\mathfrak{I}_{\mathfrak{P}}$. Then, for each X (processing all representable sets according to the ordering $\prec$), we are choosing as index $\mathfrak{I}_{\mathfrak{R}}(X)$ the least number j in X which has not been chosen as index $\mathfrak{I}_{\mathfrak{R}}(Y)$ for any $Y \prec X$—and analogously with $\mathfrak{I}_{\mathfrak{P}}$.

Membership is then interpreted in terms of $\mathfrak{I}_{\mathfrak{R}}$ in $\mathfrak{R}$, and in terms of $\mathfrak{I}_{\mathfrak{P}}$ in $\mathfrak{P}$:

$$X \in^{\mathfrak{R}} Y \text{ iff } \mathfrak{I}_{\mathfrak{R}}(X) \in Y, \qquad V \in^{\mathfrak{P}} Y \text{ iff } \mathfrak{I}_{\mathfrak{P}}(V) \in Y,$$

where $X \in \mathfrak{R}$, $V \in \mathfrak{P}$, and $Y \subseteq \mathbb{Z}$. The verification that both $\mathfrak{R}$ and $\mathfrak{P}$ satisfy **(E)** while **(W)** and **(L)** are true in $\mathfrak{R}$ and false in $\mathfrak{P}$ are left to the reader. Notice also that $X \in^{\mathfrak{R}} X$ and $Y \in^{\mathfrak{P}} Y$ hold for all $X \in \mathfrak{R}$ and $Y \in \mathfrak{P}$.

Our next proposition asserts, among other things, that $\mathfrak{I}_{\mathfrak{R}}$ and $\mathfrak{I}_{\mathfrak{P}}$ are surjective on $\mathbb{Z} \setminus \{0\}$ (as we have announced before):

Lemma 2. *For all $\ell \in \mathbb{N} \setminus \{0, 1, 2\}$, there are representable sets a, b, b', with $b, b' \in \mathfrak{P}$, such that $\mathfrak{I}_{\mathfrak{R}}(b') = \mathfrak{I}_{\mathfrak{P}}(b') = -\ell$, $\mathfrak{I}_{\mathfrak{R}}(a) = \mathfrak{I}_{\mathfrak{P}}(b) = \ell$, $rad(b') = \ell$, and $rad(a) = rad(b) < \ell$. Similar statements, with $rad(a) = rad(b) = \ell$, hold when $\ell = 2, 1$.*

As a direct consequence we have the following

Corollary 1. *Either $\mathfrak{I}_{\mathfrak{R}}(a) = -rad(a)$, or $\mathfrak{I}_{\mathfrak{R}}(a) \geqslant rad(a)$ —in particular, $\mathfrak{I}_{\mathfrak{R}}(a) > rad(a)$ if $rad(a) > 2$— holds, for each set $a \in \mathfrak{R}$. The situation with $\mathfrak{I}_{\mathfrak{P}}(b)$, $b \in \mathfrak{P}$, is entirely analogous.* $\square$

The following notion will play a crucial role in the proof that $\mathfrak{R}$ and $\mathfrak{P}$ are indistinguishable by means of a 3-pebble game:

Definition 2. *An* EMBEDDING *of* $\mathfrak{R}$ *into* $\mathfrak{P}$ *is an injective function* $\kappa : \mathfrak{R} \longrightarrow \mathfrak{P}$ *such that, for all* $a', a'' \in \mathfrak{R}$ *and* $b \in \mathfrak{P}$, *the following conditions hold:*

$$a' \in^{\mathfrak{R}} a'' \leftrightarrow \kappa(a') \in^{\mathfrak{P}} \kappa(a''),$$
$$b \in^{\mathfrak{P}} \kappa(a') \ \wedge \ b \notin^{\mathfrak{P}} \kappa(a'') \rightarrow \exists a \in \mathfrak{R} \ \ b = \kappa(a).$$

$\square$

The reader may benefit from the following, equivalent, way of expressing the requirements in the definition of embedding in terms of symmetric set-difference:

$$\kappa(a'') \supseteq \{\mathfrak{I}_{\mathfrak{P}}(\kappa(a')) \mid a' \in^{\mathfrak{R}} a''\} \ \wedge \ \kappa(a'') \cap \{\mathfrak{I}_{\mathfrak{P}}(\kappa(a')) \mid a' \notin^{\mathfrak{R}} a''\} = \emptyset,$$
$$\kappa(a') \triangle \kappa(a'') \ = \ \{\mathfrak{I}_{\mathfrak{P}}(\kappa(a)) \mid a \in^{\mathfrak{R}} a' \triangle a''\},$$

where $a', a'' \in \mathfrak{R}$.

A main step in our treatment consists in proving that an embedding of $\mathfrak{R}$ into $\mathfrak{P}$ exists. An important intermediate result is the following

Corollary 2. *Let* $a, a'a'' \in \mathfrak{R}$. *If* $a'' \prec a$ *and* $a' \in^{\mathfrak{R}} a'' \triangle a$, *then either* $a' \prec a$, *or* $a' = a$ *and* $\mathfrak{I}_{\mathfrak{R}}(a) = -rad(a)$.

The following pseudo-algorithm, which exploits the enumeration $a_0, a_1, \ldots$ of $\mathfrak{R}$ associated with $\prec$, will guarantee the existence of an embedding from $\mathfrak{R}$ into $\mathfrak{P}$. Lemma 3 states correctness of the procedure.

$\kappa := \emptyset$; -- *initialization of embedding*
for $i := 0, 1, 2, \ldots$ *(ad inf.)* **loop**
$\quad$ **let** a_i **be** the next element of $\mathfrak{R}$ w.r.t. $\prec$;
$\quad$ **pick** b_i in $\mathfrak{P}$ **so that**, for all $j < i$, $\kappa(a_j) \neq b_i$ and the following
$\quad$ conditions are met:
$\qquad$ *i.* $\ a_j \in^{\mathfrak{R}} a_i \ \leftrightarrow \ \kappa(a_j) \in^{\mathfrak{P}} b_i,$
$\qquad$ *ii.* $\ \mathfrak{I}_{\mathfrak{R}}(a_i) > 0 \ \leftrightarrow \ b_i \in^{\mathfrak{P}} \kappa(a_j),$
$\qquad$ *iii.* $\ \kappa(a_j) \triangle b_i = \{\mathfrak{I}_{\mathfrak{P}}(\kappa(a')) \mid a' \neq a_i \wedge (a' \in^{\mathfrak{R}} a_j \ \leftrightarrow \ a' \notin^{\mathfrak{R}} a_i)\}$
$\qquad\qquad\qquad\quad \cup \ (\textbf{if} \ a_i \notin^{\mathfrak{R}} a_j \ \textbf{then} \ \{\mathfrak{I}_{\mathfrak{R}}(b_i)\} \ \textbf{else} \ \emptyset \ \textbf{end if});$
$\quad$ $\kappa(a_i) := b_i$;
end loop.

Lemma 3. *The above procedure does not terminate and defines a function* κ *which is an embedding of* $\mathfrak{R}$ *in* $\mathfrak{P}$.

Remark 1. Notice that one could initialize κ at the beginning of the embedding procedure as *any* finite partial function from $\mathfrak{R}$ to $\mathfrak{P}$. Then, replacing the **let**-statement by:

$\quad$ **let** a_i **be** the next element of $\mathfrak{R}$ w.r.t. $\prec$, whose $\kappa(a_i)$ is still undefined;

the thesis of Lemma 3 continues to hold as long as the indices of the $\kappa(a)$s in the range of the initializing partial function are chosen *cum grano salis*: their value must guarantee that the b_is to be defined later will belong to $\mathfrak{P}$. In particular, this will be the case whenever the initializing partial function is an initial segment of a given embedding. $\square$

Our next task consists in proving the impossibility to distinguish the 'rich' structure $\mathfrak{R}$ from the 'poor' structure $\mathfrak{P}$ by means of sentences involving only

three variables. Before doing so, we need to introduce some definitions characterizing a sort of *partial* embedding that will be used when we must update the embedding suggesting the strategy to *Duplicator*.

Definition 3. *We will call Δ-closure of a set $X \subseteq \mathfrak{R}$ the minimum fixed point defined as follows:*[8]

$$\Delta X =_{Def} (\mu Y \supseteq X)(a, b \in Y \rightarrow a \triangle b \subseteq Y).\qquad\qquad\square$$

Notice that the Δ-closure is defined as being a fixpoint of the monotone non-decreasing function $X \mapsto X \cup \bigcup\{a\triangle b \: : \: a, b \in X\}$ $(= X \cup \{c \in \mathfrak{R} \mid (\exists a, b \in X)(c \in^{\mathfrak{R}} a\triangle b)\})$. Let $\prec X$ denote the set $\{y \mid (\exists x \in X)(y \preccurlyeq x)\}$. By Corollary 2, we have that $\Delta X \subseteq \prec X$; hence ΔX is finite when X is a finite set, because obviously $\prec X$ is finite in this case.

From now on, *let a (resp. b)*, with or without subscripts or superscripts, *indicate a generic element of $\mathfrak{R}$ (resp. $\mathfrak{P}$)*, and let $\hat{a} = a_1, \ldots, a_i$ and $\hat{b} = b_1, \ldots, b_i$.

Definition 4. *We say that $\Delta\{\hat{a}\}$ and $\Delta\{\hat{b}\}$ are ISOMORPHIC, $\Delta\{\hat{a}\} \simeq \Delta\{\hat{b}\}$, if there exists an $\in$-isomorphism from the former into the latter sending a_j to b_j for $j \in \{1, \ldots, i\}$.* $\qquad\qquad\square$

An isomorphism between Δ-closures is a sort of partial embedding. The following lemma proves the possibility of extending partial embeddings.

Lemma 4. *If $\Delta\{\hat{a}\} \simeq \Delta\{\hat{b}\}$, then $(\forall b \notin \Delta\{\hat{b}\})(\exists a)\big(\Delta\{\hat{a}, a\} \simeq \Delta\{\hat{b}, b\}\big)$. Moreover, if $\mathfrak{I}_{\mathfrak{P}}(b) > 0$ then $\mathfrak{I}_{\mathfrak{R}}(a) > 0$, and if $\mathfrak{I}_{\mathfrak{P}}(b) < 0$, then $\mathfrak{I}_{\mathfrak{R}}(a) < 0$ and infinitely many such a are available.*

By virtue of Lemma 4, Thm.1 gives the result sought for. In its proof (cf. [10]) we resort to pebble games and prove that there exists a winning strategy for Duplicator in any 3-pebble game played on $\mathfrak{R}$ and $\mathfrak{P}$.

Theorem 1. *The structures $\mathfrak{R}$ and $\mathfrak{P}$ cannot be distinguished using a 3-pebble game. Then, $(\mathbf{E}) \wedge (\mathbf{W}) \wedge (\mathbf{L})$ cannot be expressed in 3 variables.*

5 Conclusions

The table below summarizes the 'positive' results contained in this paper, obtained with the assistance of Otter as described in Sec.3. Moreover, its row where dashes occur is meant to indicate that a pairing notion is missing under specific, relatively weak axiomatic assumptions: this recalls the negative result discussed in Sec.4. These results identify a sharp borderline to be crossed for an 'algebraization' of Set Theory. In fact, they clearly indicate that 3-variable expressibility intimately depends on reasonable restraints imposed on the structure of the universe and on precise properties of membership. Studies of this kind contribute to the rather fine classification, undertaken by Tarski and Givant [24,

---

[8] We will sometimes abuse notation, as here, by applying certain relations (e.g. $\supseteq$ or $=$) or operations (e.g., $\triangle, \cup$, or $\cap$) to sets whose elements should be 'de-referenced' as common-sense will suggest, by applying either $\mathfrak{I}_{\mathfrak{P}}$ or $\mathfrak{I}_{\mathfrak{R}}$.

Sect.4.6], of the conditions enabling an aggregate theory (even a very weak one) to be formulated within the algebra of (dyadic) relations.

Axiomatic assumptions	Pairing construct	Short	Projections
$(\mathbf{P})$	$\big\{\{x,y\},\{x\}\big\}$	(x,y)	$\boldsymbol{\pi}_0,\ \boldsymbol{\pi}_1$
$(\mathbf{W})\wedge(\mathbf{L})\wedge(\mathbf{N})$	$\big\{\{x,y\},\{x\}\big\}$	(x,y)	$\boldsymbol{\pi}_0,\ \boldsymbol{\pi}_1$
$(\mathbf{E})\wedge(\mathbf{W})\wedge(\mathbf{L})$	$-$	$-$	$-$
$(\mathbf{E})\wedge(\mathbf{W})\wedge(\mathbf{L})\wedge(\mathbf{N})$	$\big\{\{x\ \text{less}\ y,\ x\ \text{with}\ y\}\ \text{less}\ x,\ \{x\ \text{less}\ y,\ x\ \text{with}\ y\}\ \text{with}\ x\big\}$	$[x,y]$	$\boldsymbol{\lambda}^{\smile},\ \boldsymbol{\rho}^{\smile}$
$(\mathbf{E})\wedge(\mathbf{W})\wedge(\mathbf{L})\wedge(\mathbf{N})$	$\big\{\{y\}\ \text{less}\ x,\ \{y\}\ \text{with}\ x\big\}$	$\langle x,y\rangle$	$\boldsymbol{\lambda}^{\smile},\ \boldsymbol{\varrho}^{\smile}$
$(\mathbf{E})\wedge(\mathbf{W})\wedge(\mathbf{L})\wedge(\mathbf{A}^5)$	$x\ \text{with}\ \big(y\ \text{with}\ (y\ \text{with}\ x)\big)$	$\lfloor x,y\rfloor$	$\boldsymbol{\alpha},\ \boldsymbol{\beta}$
$(\mathbf{R})\wedge(\mathbf{W})\wedge(\mathbf{L})\wedge(\mathbf{N})$	$\Big\{\{x\},\big\{\{x\},\{y,\{y\}\}\big\}\Big\}$	$\lceil x,y\rceil$	$\text{car},\ \text{cdr}$

References

[1] P. Aczel. *Non-Well-Founded Sets*. CSLI Lecture Notes, vol. 14, Stanford, 1988.

[2] J. Barwise and L. Moss. *Vicious Circles*. CSLI Pub. Notes, vol. 60, Stanford, 1996.

[3] A. Chiacchiaretta, A. Formisano, and E. G. Omodeo. Benchmark #1 for equational set theory. In *Giornata "Analisi Sperimentale di Algoritmi per l'Intelligenza Artificiale"*. AI*IA, 1999.

[4] D. Cantone, A. Formisano, E. G. Omodeo, and C. G. Zarba. Compiling dyadic first-order specifications into map algebra. *TCS*, 303, 2002. To appear.

[5] L. H. Chin and A. Tarski. Distributive and modular laws in relation algebras. *University of California Publications in Mathematics*, 1(9):341–384, 1951.

[6] A. Dawar. Finite models and finitely many variables. *Banach Center Publications*, 46, 1999.

[7] N. Dershowitz and Z. Manna. Proving termination with multiset ordering. *Communications of the ACM*, 22(8):465–476, 1979.

[8] H.-D. Ebbinghaus and J. Flum. *Finite Model Theory*. Perspectives in Mathematical Logic. Springer-Verlag, 1995.

[9] A. Formisano and E. Omodeo. An equational re-engineering of set theories. In R. Caferra and G. Salzer, eds. *Automated Deduction in Classical and Non-Classical Logics*, LNCS 1761 (LNAI). Springer-Verlag, pp. 175–190. 2000.

[10] A. Formisano, E. G. Omodeo, and A. Policriti. The axiom of elementary sets. II: The edge of Peircean expressibility. Tech. Rep. 20/02, Dip. di Matematica e Informatica, Univ. di Perugia, 2002.

[11] A. Formisano, E. G. Omodeo, and M. Temperini. Goals and benchmarks for automated map reasoning. *J. of Symbolic Computation*, 29(2), 2000. Special issue. M.-P. Bonacina and U. Furbach, eds.

[12] A. Formisano, E. G. Omodeo, and M. Temperini. Layered map reasoning: An experimental approach put to trial on sets. In A. Dovier, M.-C. Meo, and A. Omicini, eds. *Electronic Notes in Theoretical Computer Science*, 48, Elsevier. 2001.

[13] A. Formisano, E. G. Omodeo, and M. Temperini. Instructing equational set-reasoning with Otter. In R. Gore, A. Leitsch, and T. Nipkow, eds. *Automated Reasoning*, LNCS 2083 (LNAI). Springer-Verlag, pp. 152–167. 2001.

[14] I. Hodkinson. Finite variable logics. *Bulletin of the European Association for TCS*, 51:111–140, 1993. Columns: Logic in Computer Science.

[15] N. Immerman and D. Kozen. Definability with bounded number of bound variables. *Information and Computation*, 83(2):121–139, 1989.

[16] N. Immerman. Upper and lower bounds for first order expressibility. *J. of Computer and System Sciences*, 25(1):76–98, 1982.

[17] B. Jónsson and A. Tarski. Representation problems for relation algebras. *Bull. Amer. Math. Soc.*, 54:80,1192, 1948.

[18] J. L. Krivine. *Introduction to axiomatic set theory*. Reidel, Dordrecht. Holland, 1971.

[19] P. G. Kolaitis and M. Y. Vardi. On the expressive power of variable-confined logics. In *Proceedings, 11*th *Annual IEEE Symposium on Logic in Computer Science*, pp. 348–359, New Brunswick, New Jersey, 1996. IEEE Computer Society Press.

[20] M. K. Kwatinetz. *Problems of expressibility in finite languages*. PhD thesis, University of California, Berkeley, 1981.

[21] A. Tarski. Sur les ensembles fini. *Fundamenta Mathematicae*, VI:45–95, 1924.

[22] A. Tarski. On the calculus of relations. *J. of Symbolic Logic*, 6(3):73–89, 1941.

[23] A. Tarski. Some metalogical results concerning the calculus of relations. *J. of Symbolic Logic*, 18:188–189, 1953.

[24] A. Tarski and S. Givant. *A formalization of Set Theory without variables*, vol. 41 of *Colloquium Publications*. American Mathematical Society, 1987.

[25] W. Thomas. Languages, automata and logic. In G. Rozenberg and Salomaa A., eds, *Handbook of formal languages, Vol. III*, pp. 389–455. Springer, 1997.

[26] E. Zermelo. Untersuchungen über die Grundlagen der Mengenlehre I. (1908.) English translation in J. van Heijenoort, ed. *From Frege to Gödel - A source book in mathematical logic, 1879–1931*. pp. 199–215. Harvard University Press, 3rd edition, 1977.