



# A new thesis concerning synchronised parallel computing – simplified parallel ASM thesis <sup>☆</sup>



Flavio Ferrarotti <sup>a,\*</sup>, Klaus-Dieter Schewe <sup>a</sup>, Loredana Tec <sup>a</sup>, Qing Wang <sup>b</sup>

<sup>a</sup> Software Competence Center Hagenberg, Austria

<sup>b</sup> Research School of Computer Science, The Australian National University, Australia

## ARTICLE INFO

### Article history:

Received 10 April 2015

Received in revised form 9 August 2016

Accepted 16 August 2016

Available online 24 August 2016

Communicated by D. Sannella

### Keywords:

Parallel algorithm

Abstract state machine

ASM thesis

Behavioural theory

## ABSTRACT

A behavioural theory consists of machine-independent postulates characterizing a particular class of algorithms or systems, an abstract machine model that provably satisfies these postulates, and a rigorous proof that any algorithm or system stipulated by the postulates is captured by the abstract machine model. The class of interest in this article is that of (synchronous) parallel algorithms. For this class a behavioural theory has already been developed by Blass and Gurevich, which unfortunately, though mathematically correct, fails to be convincing, as it is not intuitively clear that the postulates really capture the essence of (synchronous) parallel algorithms.

In this article we present a much simpler (and presumably more convincing) set of four postulates for (synchronous) parallel algorithms, which are rather close to those used in Gurevich's celebrated sequential ASM thesis, i.e. the behavioural theory of sequential algorithms. The key difference is made by an extension of the bounded exploration postulate using multiset comprehension terms instead of ground terms formulated over the signature of the states. In addition, all implicit assumptions are made explicit, which amounts to considering states of a parallel algorithm to be represented by meta-finite first-order structures.

The article first provides the necessary evidence that the axiomatization presented in this article characterizes indeed the whole class of (synchronous) parallel algorithms, then formally proves that parallel algorithms are captured by Abstract State Machines (ASMs). The proof requires some recourse to methods from finite model theory, by means of which it can be shown that if a critical tuple defines an update in some update set, then also every other tuple that is logically indistinguishable defines an update in that update set.

© 2016 Elsevier B.V. All rights reserved.

## 1. Introduction

The starting point for this research was the attempt of Gurevich to characterize algorithms by means of Abstract State Machines (ASMs). The so-called ASM thesis, first proposed in 1985 in a note to the American Mathematical Society [1],

<sup>☆</sup> The research reported in this paper results from the project *Behavioural Theory and Logics for Distributed Adaptive Systems* supported by the **Austrian Science Fund (FWF): [P26452-N15]**. The research has further been supported by the Austrian Ministry for Transport, Innovation and Technology, the Federal Ministry of Science, Research and Economy, and the Province of Upper Austria in the frame of the COMET center SCCH (FFG: [844597]).

\* Corresponding author.

E-mail addresses: [flavio.ferrarotti@scch.at](mailto:flavio.ferrarotti@scch.at) (F. Ferrarotti), [kd.schewe@scch.at](mailto:kd.schewe@scch.at) (K.-D. Schewe), [loredana.tec@scch.at](mailto:loredana.tec@scch.at) (L. Tec), [qing.wang@anu.edu.au](mailto:qing.wang@anu.edu.au) (Q. Wang).

asserts that every algorithm is equivalent, on its natural level of abstraction, to an appropriate abstract state machine. In [2], Gurevich formulated and proved the ASM thesis for sequential algorithms. This consists of three intuitive postulates (sequential time, abstract state, bounded exploration) that are used to define sequential algorithms at any level of abstraction, and a proof that algorithms defined in this way are exactly captured by sequential ASMs. Starting from the sequential ASM thesis, a set of postulates for (synchronous) parallel algorithms has been proposed by Blass and Gurevich in [3,4]. However, these postulates turned up being significantly more complex and less intuitive than the ones for the sequential setting and thus have not fully convinced the ASM community nor others dealing with foundations of computing and rigorous methods.

In this article we formulate and prove an ASM thesis for parallel algorithms which naturally generalizes Gurevich's ASM thesis for sequential algorithms. The aim is to overcome the lack of intuition in the ASM thesis for parallel algorithms of Blass and Gurevich.<sup>1</sup> The key idea is to relax the bounded exploration postulate from the sequential setting by using more general multiset comprehension terms instead of only ground terms. In doing so we present a new parallel ASM thesis for synchronous, parallel algorithms, which consists of: (a) four postulates that capture the fundamental properties of synchronous parallel algorithms (*axiomatization*); (b) a variant of Abstract State Machines (which we call *parallel ASMs*) together with a proof that every parallel ASM satisfies the postulates (*plausibility theorem*); and (c) a proof that every algorithm stipulated by the postulates can be step-by-step simulated by an equivalent parallel ASM (*characterization theorem*).

There are three postulates that are common to the sequential ASM thesis of Gurevich [2] and to the parallel ASM thesis of Blass and Gurevich [4,5]: the *sequential time*, *abstract state* and *background* postulates. While the first two postulates are identical in both cases, the third postulate (although only implicit in the sequential thesis) states the differences between sequential and parallel algorithms w.r.t. the required background of computations. This is because the minimum background required for the computation of parallel algorithms is nonetheless bigger than the minimum background required for sequential algorithms.

The last postulate in the sequential ASM thesis is the *bounded exploration* postulate, which basically says that every sequential algorithm examines only a bounded number of elements in any state, with the number of elements to be examined being bounded uniformly by the algorithm and not by the state. Unfortunately, the three postulates that replace it in the parallel ASM thesis, called the *procket algorithm*, *bounded sequentiality* and *update* postulates, are not as concise and intuitive. They are based on a number of non-trivial concepts such as procket, ken, information flow digraph, etc., and thus difficult to explain in a concise and intuitive manner unless previous knowledge of such concepts is assumed.<sup>2</sup> To gain a better understanding of the properties of parallel algorithms, we propose to replace these three postulates in the parallel ASM thesis by a generalized *bounded exploration* postulate that is tailored to parallel algorithms. This new postulate is based on the observation that only finitely many locations of a state can be changed in one step of a computation, independently of whether the algorithm is sequential or parallel.

By the sequential accessibility principle in [2], the only way in which a sequential algorithm can access an element  $a$  of a state, is by producing a ground term that evaluates to  $a$ . This principle, together with the informal assumption that every algorithm has a finite program, indicates that sequential algorithms can only check agreement between states on a *fixed* finite set of elements denoted by a fixed finite set of ground terms (i.e., the witness set in the bounded exploration postulate for sequential algorithms). Parallel algorithms, however, do not satisfy this principle (see [Example 1.1](#) extracted from [4]).

**Example 1.1.** The following algorithm takes as input an undirected graph and transforms it to its complement. We assume that the vocabulary of the states of this algorithm includes the function symbols  $V$  and  $E$  which are interpreted as the vertex-set and edge-set of the graph, respectively.

```

for all  $x, y$  with  $V(x) \wedge V(y)$  do
  if  $x \neq y$  then  $E(x, y) := \neg(E(x, y))$  endif
end for

```

Clearly, the produced set of updates to the edge set which interprets  $E$  depends on the entire graph while two arbitrary graphs might be very different despite any amount of *fixed* finite agreement between them. Thus, the hypothesis in the bounded exploration postulate for sequential algorithms when applied to this parallel algorithm cannot guarantee any agreement at all between two arbitrary graphs.

Intuitively, in a parallel algorithm many “branches” contribute to the update set produced during a single computation step. Although still finite, the actual number of branches is no longer bounded by the algorithm alone, but also depends on the current state of the algorithm. This number is nevertheless “uniformly” determined by the algorithm. This motivated us to think about an alternative bounded exploration postulate for parallel algorithms based on a more expressive set of terms. The new formulation of the bounded exploration postulate allows us to “capture” in every state  $\mathbf{S}$  of a parallel algorithm  $A$ , the part of  $\mathbf{S}$  that is actually explored by the branches of  $A$ .

<sup>1</sup> In the end it will turn out that both sets of postulates are exactly captured by parallel ASMs, which implies their equivalence.

<sup>2</sup> In fact, different to bounded exploration these concepts are not purely grounded in logic.

### 1.1. Terminology

We would like to stress that by “synchronous parallelism” we mean “parallelism” in exactly the same sense as in the parallel ASM thesis of Blass and Gurevich [4,5]. That is, the amount of work that the algorithm can do in parallel in a computation step depends also on the state. This is sometime referred to as unrestricted parallelism [6] as opposed to the restricted parallelism allowed in the sequential ASM thesis [2], where there is a bound in the amount of work that a sequential algorithm can do in parallel, which is determined for all possible states by the algorithm alone and which does not depend on the state. Bounded parallelism corresponds to the “**par**” rule in the basic single agent ASM model (see Chapter 2.4 in [6] for a formal definition of the basic ASM model) while unrestricted parallelism corresponds to the “**forall**” rule in the same model.

We call them “*synchronous* parallel algorithms” instead of simply “parallel algorithms” to stress the fact that the different parallel branches work in a synchronized way. If we think in terms of multi-agent ASMs, i.e., sets of agents that execute their own ASMs in parallel [6], instead of single agent ASMs as in the parallel ASM thesis of Blass and Gurevich [4,5] and in the present work, then the distinction between synchronous and asynchronous parallelism becomes necessary.

In a synchronous multi-agent ASM each agent executes each step of its own ASM synchronized with the steps of the ASMs of all other agents. Thus, there is an implicit global system clock. Semantically, this is equivalent to all the constituent single agent ASMs working in a synchronized way over global states of the signature formed by the union of the signature of each component. If we consider this implicit global states, then for every synchronous multi-agent ASM there is a behavioural equivalent (see Definition 2.1) single-agent parallel ASM.

On the other hand, (asynchronous) multi-agent ASMs with concurrent runs are not captured by the parallel ASM thesis as studied here. They correspond to the class of concurrent algorithms as per the recently proven concurrent ASM thesis [7]. Concurrent ASMs [7] (a.k.a. distributed ASMs [8]) are multi-agent ASMs, in which agents run together asynchronously, each with its own clock, communicating with each other only through reading/writing values of designated locations.

### 1.2. Related work

The seminal work of Gurevich [8] on Abstract State Machines (ASMs, formerly called “evolving algebras”) aimed to find a precise formal definition of the notion of algorithm. The major discovery was that all computing formalisms are bound to a specific abstraction level, which implies that almost always encodings are required [2,9], so the major breakthrough of ASMs was due to the abstract notion of state, which is defined by general Tarski structures.

The sequential ASM thesis [2] characterizes sequential algorithms in terms of three postulates: sequential time, abstract state and bounded exploration. Moreover, it establishes the characterization theorem for sequential algorithms stating that algorithms defined in this way are exactly captured by sequential ASMs, i.e., a well-defined abstract machine model that relies on the parallel execution of updates on the abstract states, if certain conditions guarding the updates are satisfied. Thus, sequential ASMs also support *bounded* parallelism, where the bound is a priori fixed by the algorithm and does not depend on the state.

Following this work, many other extensions of the sequential ASM thesis to different classes of algorithms have been explored. These include the parallel ASM thesis [4,5] for parallel algorithms, in which the bound on the parallel branches in a computation is dropped. The postulates are significantly more complex, as multisets and multiset operations must be provided explicitly in the background [10] to permit branching and synchronization. While sequential time and abstract state postulates are preserved, the bounded exploration postulate has been replaced by a set of postulates that permit to distinguish between local and global states. There is still a debate in the ASM community, if these postulates can be simplified to obtain an axiomatization for parallel algorithms which is as intuitive as the one for sequential algorithms. A simplified parallel ASM thesis has been conjectured in [11].

The approach used in the sequential ASM thesis has also been successfully adopted in the development of a theory of sequential database transformations [12], where the key problem is to cope with the intrinsic finiteness of databases and the need to capture the constructs and operators that are defined by a data model. This was solved by adopting meta-finite structures [13] for the states, and introducing explicitly background structures that capture the necessary constructs for the data models, e.g. trees, hedges and hedge algebra operations in the case of XML [14]. This has been extended to synchronous, parallel database transformations in [15], which has given hints towards a simplification of the parallel ASM thesis. A conjecture concerning a modified (parallel) bounded exploration postulate was already formulated in [15].

### 1.3. Outline

The remainder of this article is organized as follows. We begin with some preliminaries in Section 2, which include also the first two postulates, which are common for both sequential and parallel settings. Then in Section 3 we highlight implicit assumptions regarding states and the background of a computation. This leads us to consider states as meta-finite structures and to technically distinguish states of an algorithm (as introduced in the abstract state postulate) from states of a computation (that contain many extensions as per the background postulate). The use of meta-finite structures to represent states permits to capture in a natural way the finite components of the states, making explicit their intrinsic finiteness. In

particular, the technicality of assuming that every state includes a finite set of processes or branches (e.g., procllets in [4,5]), is no longer required.

After introducing a bounded exploration postulate for parallel algorithms in Section 4, we discuss in Section 5 the plausibility of an ASM thesis for the class of synchronous parallel algorithms defined by the set of postulates proposed in this work. That is, we define an ASM model that captures the class of algorithms satisfying the sequential time, abstract state, background and (parallel) bounded exploration postulates as defined in Sections 2–4. Our formal ASM model is similar to the ASM model used in the parallel ASM thesis [4,5] modulo some technical details that do not affect the expressiveness of the model. These technical differences are due to the fact that we represent states as meta-finite structures instead of assuming that the states include a finite set of procllets.

In Section 6, we illustrate how the proposed set of postulates characterizes powerful models of parallel computation such as parallel random access machines, circuits and alternating Turing machines. The main result, the characterization theorem stating that for every parallel algorithm there exists an equivalent parallel ASM, is presented in detail in Section 7.

In order to make our results comparable with those in the parallel ASM thesis of Blass and Gurevich, we follow a similar presentation as in [4] and stick to the definitions and concepts from [2–6,16] as much as possible. In particular, the background of computation and meta-finite structures are defined as in [3] and [16], respectively, although the formal use we make of them in the context of the parallel ASM thesis as well as the distinction between states of computation and states of the algorithm is ours. The intuition behind the bounded exploration postulate for parallel algorithms closely mirrors the intuition provided for the bounded exploration postulate for sequential algorithms in [2]. The definition of parallel ASMs in Section 5 is equivalent to the one in [4] and mostly stems from [6]. We complement this definition by the use of meta-finite states and provide an explicit and formal plausibility proof. As expected, the examples studied in Section 6 are defined as in [4]. Further examples can be found in [17]. In this way we can compare both approaches and see that the examples of parallel models of computation captured by the set of postulates in the parallel ASM thesis of Blass and Gurevich, are also captured by our set of postulates. Finally, at a high-level of abstraction our characterization proof follows the same schema as the characterization proof in the sequential ASM thesis. Therefore, some lemmata and the intuitive explanation behind several steps of the proof are adapted from [2] and in particular from the account of the proof of the sequential ASM thesis in [6].

Since we want to make our paper as self-contained as possible, we reuse a considerable amount of text from the work cited in the previous paragraph. To improve the readability much of this text is not paraphrased nor quoted. Given our preceding explanation and the citations in the text, it should nevertheless be sufficiently clear from the context where the credit is due in each case.

## 2. Preliminaries

Following Gurevich's ASM thesis for sequential algorithms [2] and Blass and Gurevich's ASM thesis for parallel algorithms [4,5], our first postulate states that a synchronous parallel algorithm is a sequential algorithm, i.e., that in every possible computation there is an initial state, followed by a second state, followed by a third state and so on, and that the progression from one state to the next is uniquely determined by the algorithm.

**Postulate 1** (*Sequential Time Postulate*). A parallel algorithm  $A$  is associated with a non-empty set  $S_A$  of states, a non-empty subset  $\mathcal{I}_A \subseteq S_A$  of initial states, and a function  $\tau_A : S_A \rightarrow S_A$  called the *one-step transformation* of  $A$ .

A run or a computation of a parallel algorithm  $A$  is a finite or infinite sequence of states  $\mathbf{S}_0, \mathbf{S}_1, \dots$ , where  $\mathbf{S}_0$  is an initial state in  $\mathcal{I}_A$  and  $\mathbf{S}_{i+1} = \tau_A(\mathbf{S}_i)$  holds for every  $i \geq 0$ . A state  $\mathbf{S}$  of  $A$  is called *reachable* if  $\mathbf{S}$  occurs in some run of  $A$ .

We use the following (strong) notion of equivalence among algorithms, which implies that behaviourally equivalent parallel algorithms have the same runs.

**Definition 2.1** (*Behavioural Equivalence*). Algorithms  $A$  and  $B$  are said to be *behaviourally equivalent* if  $S_A = S_B$ ,  $\mathcal{I}_A = \mathcal{I}_B$  and  $\tau_A = \tau_B$  hold.

We follow Gurevich's approach in which states are full instantaneous descriptions of the algorithm that can be conveniently formalized as first-order structures. More formally, we consider states as first-order structures whose *vocabulary* or *signature*  $\Sigma$  is a finite set of function symbols. Each function symbol  $f_i \in \Sigma$  has a fixed *arity*  $r_i \geq 0$ . Function symbols can be marked (by the vocabulary) as *static*. Otherwise, they are *dynamic*. A *first-order structure*  $\mathbf{S}$  of vocabulary  $\Sigma$  is a nonempty set  $S$  called the *base set* of  $\mathbf{S}$  together with an interpretation over  $S$  of every function symbol in  $\Sigma$ . Elements of  $S$  are also called elements of the structure  $\mathbf{S}$ . An *interpretation* of an  $r$ -ary function symbol  $f \in \Sigma$  over  $S$  is a (total) function  $f^{\mathbf{S}}$  from  $S^r$  to  $S$ . Consequently, our second postulate is also unchanged from previous work in the area [2,4,5].

**Postulate 2** (*Abstract State Postulate*). States of a parallel algorithm  $A$  are first-order structures. All states in  $S_A$  have the same vocabulary. The one-step transformation  $\tau_A$  does not change the base set of any state.  $S_A$  and  $\mathcal{I}_A$  are closed under isomorphisms. Any isomorphism between two states  $\mathbf{S}_1$  and  $\mathbf{S}_2$  is also an isomorphism between  $\tau_A(\mathbf{S}_1)$  and  $\tau_A(\mathbf{S}_2)$ .

Apart from defining states of an algorithm as first-order structures of a fixed vocabulary, this postulate ensures that algorithms work at a fixed level of abstraction by requiring the set of states of an algorithm to be closed under isomorphisms and the one-step transformation to preserve those isomorphisms. Recall that two structures  $\mathbf{S}_1$  and  $\mathbf{S}_2$  of a same vocabulary  $\Sigma$  are *isomorphic* (denoted  $\mathbf{S}_1 \simeq \mathbf{S}_2$ ) iff there is a bijection  $\zeta : S_1 \rightarrow S_2$  between the base sets such that  $\zeta(f^{\mathbf{S}_1}(a_1, \dots, a_r)) = f^{\mathbf{S}_2}(\zeta(a_1), \dots, \zeta(a_r))$  holds for all  $r$ -ary function symbols  $f \in \Sigma$  and all  $r$ -tuples  $(a_1, \dots, a_r) \in S_1^r$ .

As usual, we think of a structure that represents a state of an algorithm as a kind of memory that maps locations to values.

**Definition 2.2** (*Locations and Updates*). Let  $\mathbf{S}$  be the state of an algorithm of vocabulary  $\Sigma$ , let  $f \in \Sigma$  be a function symbol of arity  $r$  and let  $\bar{a}$  be an  $r$ -tuple in  $S^r$ . The pair  $(f, \bar{a})$  represents a (memory) *location* in  $\mathbf{S}$ . The *content* of the location  $(f, \bar{a})$  is the value  $f^{\mathbf{S}}(\bar{a})$  in  $S$ . If  $l = (f, \bar{a})$  is a location in a state  $\mathbf{S}$ ,  $f$  is a dynamic function and  $b$  is an element in the base set  $S$ , then the tuple  $(l, b)$  is an *update* of  $\mathbf{S}$ . If  $b = f^{\mathbf{S}}(\bar{a})$ , then the update  $((f, \bar{a}), b)$  is called a *trivial update*.

An update  $(l, b)$  indicates that the content of the location  $l$  in  $\mathbf{S}$  needs to be changed to the value  $b$ . Two updates *clash* if they refer to the same location but are distinct.

**Definition 2.3** (*Consistent Update Set*). A set of updates  $\Delta$  is *consistent* if it has no clashing updates, i.e., if for every pair of updates  $(l_i, b_i)$  and  $(l_j, b_j)$  in  $\Delta$ , we have that  $l_i = l_j$  only if  $b_i = b_j$ .

A consistent set of updates  $\Delta$  is *executed* (or *fired*) by executing all the updates in  $\Delta$  simultaneously.

**Definition 2.4** (*Execution of Updates*). The result of executing (or firing) a consistent update set  $\Delta$  in a state  $\mathbf{S}$  is a new state  $\mathbf{S} + \Delta$  with the same base set as  $\mathbf{S}$  such that for every location  $l_i = (f_i, \bar{a}_i)$  of  $\mathbf{S}$ :

$$f_i^{\mathbf{S}+\Delta}(\bar{a}_i) = \begin{cases} b & \text{if } (l_i, b) \in \Delta; \\ f_i^{\mathbf{S}}(\bar{a}_i) & \text{if there is no } b \text{ with } (l_i, b) \in \Delta. \end{cases}$$

If  $\mathbf{S}_1$  and  $\mathbf{S}_2$  are structures of the same vocabulary and with the same base set, then there is a unique consistent set  $\Delta$  of non-trivial updates of  $\mathbf{S}_1$  such that  $\mathbf{S}_2 = \mathbf{S}_1 + \Delta$ . We use  $\mathbf{S}_2 - \mathbf{S}_1$  to denote this unique consistent set of updates  $\Delta$ .

The following well known lemma is a consequence of the fact that by Postulate 2 the one step transformation function  $\tau_A$  of an algorithm  $A$  is required to preserve isomorphisms.

**Lemma 2.1.** *Suppose that  $\zeta$  is an isomorphism from state  $\mathbf{S}_1$  to state  $\mathbf{S}_2$  of an algorithm  $A$ . We extend  $\zeta$  to locations and update sets of  $\mathbf{S}_1$  as follows:*

- If  $l = (f, (a_1, \dots, a_n))$  is a location in  $\mathbf{S}_1$ , then  $\zeta(l) = (f, (\zeta(a_1), \dots, \zeta(a_n)))$ .
- If  $\Delta$  is an update set for  $\mathbf{S}_1$ , then  $\zeta(\Delta) = \{(\zeta(l), \zeta(v)) \mid (l, v) \in \Delta\}$ .

Then  $\zeta(\tau_A(\mathbf{S}_1) - \mathbf{S}_1) = \tau_A(\mathbf{S}_2) - \mathbf{S}_2$ .

As usual, we assume that a function symbol can be marked (by the vocabulary) as *relational* and that every vocabulary includes the binary function symbol “=” for equality, nullary function symbols *true*, *false* and *undef*, the unary function symbol *Boole*, and the symbols “ $\neg$ ”, “ $\vee$ ”, “ $\wedge$ ” and “ $\rightarrow$ ” corresponding to the usual Boolean operations. With the exception of *undef*, all these *logic symbols* are relational. Furthermore, all of them are marked as static.

We identify a nullary function with its value in the base set of the state. Thus, if  $\mathbf{S}$  is a first-order structure,  $\text{true}^{\mathbf{S}}$ ,  $\text{false}^{\mathbf{S}}$  and  $\text{undef}^{\mathbf{S}}$  are particular elements of  $S$ . We assume that  $\text{true}^{\mathbf{S}}$  is a distinct element from  $\text{false}^{\mathbf{S}}$  and  $\text{undef}^{\mathbf{S}}$ .

An  $r$ -ary relation  $R^{\mathbf{S}} \subseteq S^r$  is *represented* by a relational function  $f_R^{\mathbf{S}}$  from  $S^r$  to  $\{\text{true}^{\mathbf{S}}, \text{false}^{\mathbf{S}}\}$  such that, for every  $\bar{a} \in S^r$ , it holds that  $\bar{a} \in R^{\mathbf{S}}$  iff  $f_R^{\mathbf{S}}(\bar{a}) = \text{true}^{\mathbf{S}}$ . If a relation  $R^{\mathbf{S}}$  is unary, it can be viewed as a (sub)set of elements from the base set of  $\mathbf{S}$ . Thus, in any given structure  $\mathbf{S}$ , *Boole* is interpreted as the set  $\{\text{true}^{\mathbf{S}}, \text{false}^{\mathbf{S}}\}$ . The Boolean operations behave in the usual way on (the interpretation of) *Boole* and produce *false* if at least one of its arguments is not Boolean.

We assume that all the functions are total and represent partial function as total by using *undef*. Thus the *domain* of a non-relational  $r$ -ary function  $f^{\mathbf{S}}$  of a structure  $\mathbf{S}$  is the set  $\{\bar{a} \in S^r \mid f^{\mathbf{S}}(\bar{a}) \neq \text{undef}^{\mathbf{S}}\}$ . The *range* of  $f^{\mathbf{S}}$  is the set  $\{f^{\mathbf{S}}(\bar{a}) \mid \bar{a} \in S^r \text{ and } f^{\mathbf{S}}(\bar{a}) \neq \text{undef}^{\mathbf{S}}\}$ .

When it is clear from the context, we sometimes use function symbols to denote their interpretations, i.e., we omit the superscripts. We also favour infix notation for certain functions such as the (binary) Boolean operations and equality.

### 3. Background of computation

The background of computation that we need for our work is in essence the same as in Blass and Gurevich's formalization of parallel algorithms [4,5]. However, our formalization is different in two key aspects. First we consider states as meta-finite structures. This makes the intrinsic finiteness of the states of the algorithms explicit, allowing for a natural representation of the finite parts of the states. In particular, the technicality of assuming that every state includes a finite set of processes (i.e., procllets in [4,5]) is no longer needed. Secondly, we make an explicit distinction between “pure” states of the algorithms and *states of the computation* of the algorithms. This latter notion of states includes, apart from the state of the algorithm, the standard background needed for its computation (we formally define them in the following).

#### 3.1. Meta-finiteness of states

States of algorithms are intrinsically finite. However, as pointed out in [3] there is more to a computation than what is just available in the states; this gives rise to the augmentation of states with background structures and to infinite representations of states. In fact, this is the norm in the ASM literature (see [6] among others). Take as an example input to an algorithm composed by a graph and a weight function from the edges of the graph to the natural numbers. There are many ways to represent a state of an algorithm that includes this input as a finite structure. One could for instance replace every edge  $(u, v)$  of weight  $w$  by  $w$  distinct nodes, each being connected to  $u$  and  $v$  but to no other nodes. While the resulting finite structure contains all the information about the original weighted graph, it is very impractical to perform arithmetic operations involving the encoded weights or to perform verification proofs of the relevant algorithm.

On the other hand, if we represent states as arbitrary (possibly infinite) first-order structures, then the intrinsic finiteness of the states of an algorithm can only be captured implicitly, for instance by assuming a background with a variable-free term that evaluates to a finite set such as the term `Procllet` in the background postulate in [4]. A more faithful representation would be to have an auxiliary infinite structure, which in our example could be the set of natural numbers with the usual arithmetic operations. This prompted us to consider states as meta-finite structures as defined in [16].

**Definition 3.1.** A *meta-finite structure*  $\mathbf{I}$  is a triple  $(\mathbf{I}_1, \mathbf{I}_2, F)$  where

- i.  $\mathbf{I}_1$  is a finite first-order structure – the *primary part* of  $\mathbf{I}$ ;
- ii.  $\mathbf{I}_2$  is a possibly infinite first-order structure – the *secondary part* of  $\mathbf{I}$ ;
- iii.  $F$  is a finite set of functions  $f_i : (I_1)^k \rightarrow I_2$  – the *bridge functions* of  $\mathbf{I}$ .

The *vocabulary* of  $\mathbf{I}$  is the triple  $\Sigma_{\mathbf{I}} = (\Sigma_1, \Sigma_2, \Sigma_F)$  where  $\Sigma_1$ ,  $\Sigma_2$  and  $\Sigma_F$  are the (pairwise disjoint) sets of function symbols in  $\mathbf{I}_1$ ,  $\mathbf{I}_2$  and  $F$ , respectively. The *base set*  $I$  of  $\mathbf{I}$  is  $I_1 \cup I_2$ .

**Example 3.1.** Weighted graphs could be represented as meta-finite structures of vocabulary  $\Sigma = (\emptyset, \Sigma_2, \Sigma_F)$ , where  $\Sigma_2$  includes all the (background) function symbols described in Section 2 plus function symbols for the standard arithmetic operations, and  $\Sigma_F$  has two binary function symbols  $f_E$  and  $f_w$  with  $f_E$  marked as relational. For instance, let  $G$  be a digraph with vertex set  $V = \{a, b, c\}$  and edge set  $E = \{(a, b), (b, c), (c, a)\}$ , and  $w : E \rightarrow \mathbb{N}$  be the weight function  $\{(a, b) \mapsto 3, (b, c) \mapsto 5, (c, a) \mapsto 7\}$ . Then  $G$  can be represented by a meta-finite state  $\mathbf{I} = (\mathbf{I}_1, \mathbf{I}_2, F)$  of vocabulary  $\Sigma$  in which  $I_1$  (the base set of  $\mathbf{I}_1$ ) is  $V$ ,  $I_2$  (the base set of  $\mathbf{I}_2$ ) is the set  $\mathbb{N}$  of natural numbers,  $f_E^{\mathbf{I}}(x, y) = \text{true}^{\mathbf{I}}$  iff  $(x, y) \in E$ , and  $f_w^{\mathbf{I}}(x, y) = z$  if  $w(x, y) = z$  or  $f_w^{\mathbf{I}}(x, y) = \text{undef}^{\mathbf{I}}$  otherwise (recall that we assume that all functions are total).

#### 3.2. States of a computation

During a computation, algorithms frequently need to deal with constructions that produce new elements (e.g., tuples or multisets) from old ones (the components of a tuple or the elements of a multiset). Such constructions can be iterated, producing tuples of multisets, multisets of tuples, and so forth. A general approach to this kind of constructions was developed in [3] under the name of “background classes”. These classes formalize the idea of things that can be built on top of a set without introducing any additional structure to the set itself. Formally, background classes are determined by background vocabularies that consist of constructor symbols and function symbols. Different to function symbols of fixed arity, constructor symbols can also be of bounded or even unfixd arity.

**Definition 3.2.** A *background class*  $\mathcal{K}$  of vocabulary  $\Sigma_{\mathcal{K}}$  associates with any set  $U$  a *background structure*  $\mathcal{K}(U)$  constituted by

- the base set  $\text{Base}(\mathcal{K}(U)) = D$ , where  $D$  is the smallest set with  $U \subseteq D$  that satisfies the following properties for each constructor symbol  $\sqcup \in \Sigma_{\mathcal{K}}$ :
  - if  $\sqcup \in \Sigma_{\mathcal{K}}$  has unfixd arity, then  $\sqcup a_1, \dots, a_m \sqcup \in D$  for all  $m \in \mathbb{N}$  and  $a_1, \dots, a_m \in D$ .
  - if  $\sqcup \in \Sigma_{\mathcal{K}}$  has bounded arity  $n$ , then  $\sqcup a_1, \dots, a_m \sqcup \in D$  for all  $m \leq n$  and  $a_1, \dots, a_m \in D$ .
  - if  $\sqcup \in \Sigma_{\mathcal{K}}$  has fixed arity  $n$ , then  $\sqcup a_1, \dots, a_n \sqcup \in D$  for all  $a_1, \dots, a_n \in D$ .

- an interpretation of function symbols in  $\Sigma_{\mathcal{K}}$  over  $\text{Base}(\mathcal{K}(U))$ .

Summing up, a *state of an algorithm*  $A$  can be thought of as a simple meta-finite structure  $\mathbf{I}$ . But, the *initial state of computation* of  $A$  is actually richer, as it should also include the background structure  $\mathcal{K}(I)$  corresponding to the background class  $\mathcal{K}$  of the algorithm  $A$ .

**Definition 3.3** (*State of Computation*). Let  $A$  be an algorithm of vocabulary  $\Sigma_{\mathbf{I}} = (\Sigma_1, \Sigma_2, \Sigma_F)$  with background class  $\mathcal{K}$  of vocabulary  $\Sigma_{\mathcal{K}}$ , where  $\Sigma_{\mathcal{K}}$ ,  $\Sigma_1$ ,  $\Sigma_2$  and  $\Sigma_F$  are pairwise disjoint. Let  $\text{atomic}$  be a unary relation symbol which does not belong to  $\Sigma_{\mathbf{I}} \cup \Sigma_{\mathcal{K}}$ . Let  $\mathbf{I} = (\mathbf{I}_1, \mathbf{I}_2, F)$  be a state of  $A$ , i.e., a meta-finite structure of vocabulary  $\Sigma_{\mathbf{I}}$  that represents a valid state of  $A$ . Let  $\mathbf{S} = (\mathbf{I}_1, \mathbf{B}, F)$  be the meta-finite structure of vocabulary  $\Sigma = (\Sigma_1, \Sigma_2 \cup \Sigma_{\mathcal{K}} \cup \{\text{atomic}\}, \Sigma_F)$ , where  $\mathbf{B}$  is the first-order structure of vocabulary  $\Sigma_2 \cup \{f_i \mid f_i \text{ is a function symbol in } \Sigma_{\mathcal{K}}\} \cup \{\text{atomic}\}$  which satisfies the following conditions:

- The base set  $B$  of  $\mathbf{B}$  is  $\text{Base}(\mathcal{K}(I))$  (recall that  $I$  denotes the base set of  $\mathbf{I}$ ).
- $\text{atomic}^{\mathbf{B}}(x) = \text{true}^{\mathbf{B}}$  iff  $x \in I$  (recall that we assume in Section 2 that every state includes the constants  $\text{true}$ ,  $\text{false}$  and  $\text{undef}$ ).
- For every function symbol  $f_i \in \Sigma_{\mathcal{K}}$  it holds that  $f_i^{\mathbf{B}} = f_i^{\mathcal{K}(I)}$ .
- For every  $f_i \in \Sigma_2$  of arity  $r_i$  and  $\bar{a} \in B^{r_i}$ , it holds that

$$f_i^{\mathbf{B}}(\bar{a}) = \begin{cases} f_i^{\mathbf{I}}(\bar{a}) & \text{if } \bar{a} \in (I_2)^{r_i} \\ \text{false}^{\mathbf{B}} & \text{if } \bar{a} \notin (I_2)^{r_i} \text{ and } f \text{ is marked as relational} \\ \text{undef}^{\mathbf{B}} & \text{otherwise} \end{cases}$$

We say that  $\mathbf{S}_{\mathbf{I}}$  is a *state of computation* of  $A$  that corresponds to the state  $\mathbf{I}$  if it is isomorphic to  $\mathbf{S}$  by an isomorphism  $\zeta$  such that  $\zeta(x) = x$  for all  $x \in I$ .

**Example 3.2.** Let  $\Sigma_{\mathcal{K}}$  be the background vocabulary formed by a constructor symbol for pairing plus unary function symbols  $\text{first}$  and  $\text{second}$  interpreted as the functions mapping pairs to their first and second element, respectively. If the argument is not a pair, then both functions map it to  $\text{undef}$ . A state of computation corresponding to the state  $\mathbf{I}$  of the algorithm described in Example 3.1 is represented by the meta-finite structure  $\mathbf{S}_{\mathbf{I}} = (\mathbf{I}_1, \mathbf{B}, F)$ , where the base set  $B$  of  $\mathbf{B}$  is  $\{a, b, c\} \cup \mathbb{N} \cup \{(a_i, a_j) \mid a_i, a_j \in B\}$ ,  $\{x \mid \text{atomic}^{\mathbf{B}}(x)\} = \{a, b, c\} \cup \mathbb{N}$ ,  $\text{first}^{\mathbf{B}} = \text{first}^{\mathcal{K}(\{a,b,c\} \cup \mathbb{N})}$  and  $\text{second}^{\mathbf{B}} = \text{second}^{\mathcal{K}(\{a,b,c\} \cup \mathbb{N})}$ . The remaining functions in  $\mathbf{B}$ , i.e., the functions corresponding to the standard arithmetic operations and the logic symbols, coincide with their corresponding functions in  $\mathbf{I}_2$  when all their arguments belong to  $\mathbb{N}$  and take otherwise the value  $\text{false}^{\mathbf{B}}$  or  $\text{undef}^{\mathbf{B}}$ , depending on whether the function is relational or not.

Given a state of computation  $\mathbf{S} = (\mathbf{I}, \mathbf{B}, F)$  of an algorithm  $A$ , we call the functions in  $\mathbf{B}$  the *background functions* of  $\mathbf{S}$  and the functions in  $\mathbf{I}$  or  $F$  the *foreground functions* of  $\mathbf{S}$ . Consequently, we call  $\mathbf{B}$  the *background of computation* of  $A$ . As expected, all background functions are assumed to be static with the only exception of the unary function  $\text{reserve}$  defined next.

### 3.3. The reserve

It is justified to assume that the base set of a state does not change during a computation. To realize this, it is convenient to include in every state an infinite supply of *reserve* elements that can be imported by an algorithm, when new elements are needed. The reserve is a “naked set”, i.e., an entirely unstructured part of the base set.

**Definition 3.4.** Let  $A$  be an algorithm of vocabulary  $\Sigma_{\mathbf{I}} = (\Sigma_1, \Sigma_2, \Sigma_F)$ . We assume that  $\Sigma_2$  includes a unary function symbol  $\text{reserve}$  which is marked as relational. We also assume that the interpretation of  $\text{reserve}$  in every state  $\mathbf{I} = (\mathbf{I}_1, \mathbf{I}_2, F)$  of  $A$  satisfies the following conditions:

- $\text{reserve}^{\mathbf{I}_2}(x) = \text{true}^{\mathbf{I}_2}$  iff  $x \notin I_1$  and, for every  $f_i \in \Sigma_2$  of arity  $r_i$  and tuple  $\bar{a}_i \in (I_2)^{r_i}$  which includes  $x$ , it holds that  $f_i^{\mathbf{I}_2}(\bar{a}_i)$  evaluates to  $\text{false}^{\mathbf{I}_2}$  if  $f_i$  is marked as relational or to  $\text{undef}^{\mathbf{I}_2}$  otherwise.
- $R = \{a_i \in I_2 \mid \text{reserve}^{\mathbf{I}_2}(a_i) = \text{true}^{\mathbf{I}_2}\}$  has countably many elements.

We call  $R$ , the *reserve* of the state  $\mathbf{I}$  of  $A$ . We also call  $R$ , the reserve of its corresponding state of computation as per Definition 3.3.

Reserve elements can be imported when, for example, an algorithm needs to add a new vertex to a graph. Importing a new element from the reserve basically involves to take it from the reserve and to add it to the primary (finite) part of the state.

**Definition 3.5.** Let  $A$ ,  $\mathbf{I}$  and  $R$  be as in Definition 3.4. An element  $a_i \in R$  is *imported* from the reserve by simply adding it to the base set  $I_1$  of the primary part of  $\mathbf{I}$  and updating the value of  $\text{reserve}^{I_2}(a_i)$  to  $\text{false}^{I_2}$ .

**Remark 1.** Note that the base set of the primary (finite) part of the state of an algorithm can only grow monotonically during a computation. That is, we can import new elements from the reserve into the base set of the primary part of a state, but we cannot discard elements from it. The base set of the secondary part (i.e., the background of computation) as well as the base set of the whole state, remains the same.

### 3.4. Minimal background requirement

In order to simulate a given parallel algorithm, we need a minimal background, which essentially should contain ordered pairs and multisets. Multiplicities arise naturally in parallel algorithms, mainly from the repetition of tasks in the different parallel branches. For instance, if several branches request to increment the same counter in parallel, then during the synchronization phase the algorithm should take into account the multiplicity of requests concerning the same counter in order to increment it by the correct amount. Multisets are an appropriate tool to collect these multiplicities. In turn, multiset operators are useful for synchronization. In the example of the counter, the synchronization phase would consist in applying a static function “sum” to a multiset to obtain the sum of its members including multiplicities.

Formally, a *multiset*  $M$  can be seen as a function from the underlying set  $M_0$  of elements in  $M$  (the domain of  $M$ ) to the positive integers, such that  $M(x)$  is the multiplicity of  $x$  as an element of  $M$ . We use  $\text{Mult}(x, M)$  to denote the multiplicity  $M(x)$  of an element  $x$  in a multiset  $M$ . If  $x \notin M$  then  $\text{Mult}(x, M) = 0$ . We use double braces  $\{\{ \dots \}\}$  as notation for multisets. We define *binary multiset union*  $M_1 \uplus M_2$  of two multisets  $M_1$  and  $M_2$  by  $\text{Mult}(x, M_1 \uplus M_2) = \text{Mult}(x, M_1) + \text{Mult}(x, M_2)$ . Consequently, we define the *generalized multiset union* of a multiset of multisets  $\mathcal{M}$ , i.e. a multiset  $\mathcal{M}$  whose underlying domain  $\mathcal{M}_0$  is a set which contains only multisets, by  $\text{Mult}(x, \uplus \mathcal{M}) = \sum_{M_i \in \mathcal{M}_0} \text{Mult}(x, M_i) \cdot \text{Mult}(M_i, \mathcal{M})$ .

Our next postulate defines the minimum background. This minimum background is almost the same as the one used in Blass and Gurevich’s work [4,5], except that we no longer need a variable-free term `Proclset` naming a finite set of computation branches. In our work, this finiteness is instead captured by the use of meta-finite structures to represent the states of an algorithm.

**Postulate 3 (Background Postulate).** Let  $A$  be an algorithm of vocabulary  $\Sigma = (\Sigma_1, \Sigma_2, \Sigma_F)$  with background class  $\mathcal{K}$ . The vocabulary  $\Sigma_{\mathcal{K}}$  of  $\mathcal{K}$  includes (at least) a binary *tuple constructor* and a *multiset constructor* of unbounded arity; and the vocabulary  $\Sigma_{\mathbf{B}}$  of the background of the states of computation of  $A$  includes (at least) the following *obligatory* function symbols:

- Nullary function (constants) symbols `true`, `false`, `undef` and  $\emptyset$ .
- Unary function symbols `reserve`, `atomic`, `first`, `second`, `Boole`,  $\neg$ ,  $\{\{ \cdot \}\}$ ,  $\uplus$  and `AsSet`.
- Binary function symbols  $=$ ,  $\wedge$ ,  $\vee$ ,  $\rightarrow$ ,  $\leftrightarrow$ ,  $\uplus$  and  $(, )$ .

All function symbols in  $\Sigma_{\mathbf{B}}$ , with the sole exception of `reserve`, are static. Let  $\mathbf{I} = (I_1, I_2, F)$  be a state of  $A$ . The interpretation of the obligatory function symbols in the vocabulary  $\Sigma_{\mathbf{B}}$  of the secondary part (background) of every state of computation  $\mathbf{S}_1 = (I_1, \mathbf{B}, F)$  corresponding to  $\mathbf{I}$  (see Definition 3.3), satisfies the following conditions:

- $\text{atomic}^{\mathbf{B}}(x) = \text{true}^{\mathbf{B}}$  iff  $x \in I_1$ .
- $\text{reserve}^{\mathbf{B}}(x) = \text{true}^{\mathbf{B}}$  iff  $x \in \text{reserve}^{\mathbf{I}}(x)$ .
- $\text{true}^{\mathbf{B}} = \text{true}^{\mathbf{I}}$ ,  $\text{false}^{\mathbf{B}} = \text{false}^{\mathbf{I}}$  and  $\text{undef}^{\mathbf{B}} = \text{undef}^{\mathbf{I}}$ . Further,  $\text{true}^{\mathbf{B}}$  is a distinct element than  $\text{false}^{\mathbf{B}}$  and  $\text{undef}^{\mathbf{B}}$ .
- $\text{Boole}^{\mathbf{B}}(x) = \text{true}^{\mathbf{B}}$  iff  $x = \text{true}^{\mathbf{B}}$  or  $x = \text{false}^{\mathbf{B}}$ .
- $=^{\mathbf{B}}$  is the identity relation in  $B$ .
- $\neg^{\mathbf{B}}$ ,  $\wedge^{\mathbf{B}}$ ,  $\vee^{\mathbf{B}}$ ,  $\rightarrow^{\mathbf{B}}$  and  $\leftrightarrow^{\mathbf{B}}$  behave in the usual way in  $\{\text{true}^{\mathbf{B}}, \text{false}^{\mathbf{B}}\}$  and produce  $\text{false}^{\mathbf{B}}$  if at least one of its arguments is not Boolean.
- $(x, y)^{\mathbf{B}}$  evaluates to the ordered pair with first element  $x$  and second  $y$ .
- $\text{first}^{\mathbf{B}}(x)$  evaluates to the first element of  $x$  and  $\text{second}^{\mathbf{B}}(x)$  evaluates to the second element of  $x$  if  $x$  is an ordered pair, or to  $\text{undef}^{\mathbf{B}}$  otherwise.
- $\emptyset^{\mathbf{B}}$  is the empty multiset.
- $\{\{x\}\}^{\mathbf{B}}$  evaluates to the singleton multiset whose only element is  $x$ .
- $\text{AsSet}^{\mathbf{B}}(x)$  evaluates to the multiset obtained from  $x$  by setting the multiplicity of every element in  $x$  to 1. If  $x$  is not a multiset, then  $\text{AsSet}^{\mathbf{B}}(x)$  evaluates to  $\text{undef}^{\mathbf{B}}$ .
- $x \uplus y$  evaluates to the binary multiset union of  $x$  and  $y$ . If  $x$  or  $y$  is not a multiset, then  $x \uplus y$  evaluates to  $\text{undef}^{\mathbf{B}}$ .
- $\uplus x$  evaluates to the generalized multiset union of the multisets in  $x$  if  $x$  is a multiset whose elements are all multisets. Otherwise it evaluates to  $\text{undef}^{\mathbf{B}}$ .

#### 4. Bounded exploration for parallel algorithms

We now introduce our fourth and last postulate, namely the bounded exploration postulate for parallel algorithms. This is the key postulate in our work. It replaces the proclat algorithm, bounded sequentiality and update postulates in the parallel ASM thesis of Blass and Gurevich [4,5].

First we define the formal syntax and semantics of the terms that we require to state our postulate. These terms coincide with the terms used by the ASM model for parallel computation considered in this paper. They are built up from variables, functions and a multiset comprehension expression which is similar to the multiset comprehension expression used in the definition of the ASM model in the parallel thesis of Blass and Gurevich.

We follow the standard approach in *meta-finite* model theory [16] assuming that variables range over the domain of the primary part only and considering two different types of basic terms: *point terms* which define functions over the primary part of a meta-finite state, and *bridge terms* which define functions that take arguments in the primary part of a meta-finite state and values in the secondary part. The actual set of terms and its semantics are included in the following definition. If the outermost function symbol of a term  $\varphi$  is relational, we call it a *Boolean-valued term*.

**Definition 4.1.** Let  $\mathbf{S} = (\mathbf{I}, \mathbf{B}, F)$  be a (meta-finite) *state of computation* of an algorithm  $A$  with background class  $\mathcal{K}$ , which includes a multiset constructor (see Definition 3.3). Let  $\Sigma = (\Sigma_{\mathbf{I}}, \Sigma_{\mathbf{B}}, \Sigma_F)$  and  $\Sigma_{\mathcal{K}}$  be the vocabularies of  $\mathbf{S}$  and  $\mathcal{K}$ , respectively. Let  $V = \{x_0, x_1, \dots\}$  be a countable set of variables. The set of terms  $\mathcal{T}_{\Sigma, V}$  over  $\Sigma$  and  $V$  is defined inductively as follows:

- The set of *point terms* is the closure of the set  $V$  of variables under the application of function symbols in  $\Sigma_{\mathbf{I}}$ . Every point term belongs to  $\mathcal{T}_{\Sigma, V}$ .
- If  $t_1, \dots, t_r$  are point terms in  $\mathcal{T}_{\Sigma, V}$  and  $f$  is an  $r$ -ary function symbol in  $\Sigma_F$ , then  $f(t_1, \dots, t_r)$  is a *bridge term* in  $\mathcal{T}_{\Sigma, V}$ .
- If  $F_1, \dots, F_r$  are bridge terms in  $\mathcal{T}_{\Sigma, V}$  and  $f$  is an  $r$ -ary function symbol in  $\Sigma_{\mathbf{B}}$ , then  $f(F_1, \dots, F_r)$  is a *bridge term* in  $\mathcal{T}_{\Sigma, V}$ .
- Let  $\bar{x}$  and  $\bar{y}$  be tuples of variables. If  $t(\bar{x}, \bar{y})$  is a term in  $\mathcal{T}_{\Sigma, V}$  and  $\varphi(\bar{x}, \bar{y})$  is a Boolean valued term also in  $\mathcal{T}_{\Sigma, V}$ , then  $\{\{t(\bar{x}, \bar{y}) \mid \varphi(\bar{x}, \bar{y})\}\}_{\bar{x}}$  is a *multiset comprehension term* in  $\mathcal{T}_{\Sigma, V}$  with free variables  $\bar{y}$ .

Let  $\mu$  be a *variable assignment* for  $V$  over the primary part  $\mathbf{I}$  of  $\mathbf{S}$ , i.e., a function which assigns to each variable  $x_i$  in  $V$  a value  $\mu(x_i) \in I$ . Let  $t$  be a term in  $\mathcal{T}_{\Sigma, V}$ . The value  $\text{val}_{\mathbf{S}, \mu}(t)$  of  $t$  in  $\mathbf{S}$  under  $\mu$  is inductively defined as follows:

- If  $t$  is a nullary function symbol in  $\Sigma$ , then  $\text{val}_{\mathbf{S}, \mu}(t) = t^{\mathbf{S}}$ .
- If  $t$  is a variable in  $V$ , then  $\text{val}_{\mathbf{S}, \mu}(t) = \mu(t)$ .
- If  $t$  is a function symbol in  $\Sigma$  of arity  $r \geq 1$  and  $t_1, \dots, t_r$  are terms in  $\mathcal{T}_{\Sigma, X}$ , then  $\text{val}_{\mathbf{S}, \mu}(t(t_1, \dots, t_r)) = t^{\mathbf{S}}(\text{val}_{\mathbf{S}, \mu}(t_1), \dots, \text{val}_{\mathbf{S}, \mu}(t_r))$ .
- Let  $\bar{x} = (x_1, \dots, x_n)$  and  $\bar{y} = (y_1, \dots, y_m)$  for some  $n$  and  $m \geq 0$ . If  $t(\bar{y})$  is a multiset comprehension term of the form  $\{\{s(\bar{x}, \bar{y}) \mid \varphi(\bar{x}, \bar{y})\}\}_{\bar{y}}$ , then  $\text{val}_{\mathbf{S}, \mu[\bar{y} \mapsto \bar{b}]}(t(\bar{x}, \bar{y}))$  is the multiset

$$\{\{\text{val}_{\mathbf{S}, \mu[\bar{x} \mapsto \bar{a}, \bar{y} \mapsto \bar{b}]}(s(\bar{x}, \bar{y})) \mid \text{val}_{\mathbf{S}, \mu[\bar{x} \mapsto \bar{a}, \bar{y} \mapsto \bar{b}]}(\varphi(\bar{x}, \bar{y})) = \text{true}^{\mathbf{S}} \text{ and } \bar{a} \in I^n\}\}$$

If  $t$  is a ground term, we simply use  $\text{val}_{\mathbf{S}}(t)$  to denote its value in  $\mathbf{S}$ . Given a Boolean valued term  $\varphi(x_1, \dots, x_r)$  with free variables among  $\{x_1, \dots, x_r\}$ , we frequently use  $\mathbf{S} \models \varphi(x_1, \dots, x_r)[a_1, \dots, a_r]$  to denote that

$$\text{val}_{\mathbf{S}, \mu[x_1 \mapsto a_1, \dots, x_r \mapsto a_r]}(\varphi(x_1, \dots, x_r)) = \text{true}^{\mathbf{S}}.$$

We use  $\exists x_1 \dots x_r(\varphi(x_1, \dots, x_r))$  and  $\forall x_1 \dots x_r(\varphi(x_1, \dots, x_r))$  to denote that

$$\begin{aligned} &\{\{(x_1, \dots, x_r) \mid \varphi(x_1, \dots, x_r)\}\} \neq \emptyset \text{ and} \\ &\{\{(x_1, \dots, x_r) \mid \neg(\varphi(x_1, \dots, x_r))\}\} = \emptyset, \text{ respectively.} \end{aligned}$$

We refer to the class of multiset comprehension terms of the form

$$\{\{t(x_1, \dots, x_r) \mid \varphi(x_1, \dots, x_r)\}\}$$

which have *no* free-variables and where  $t$  is an ordered pair that represents (using some fixed encoding) a tuple  $(t_0, \dots, t_n)$  of terms with  $\text{free}(t_0) \cup \dots \cup \text{free}(t_n) = \{x_1, \dots, x_r\}$ , as *witness terms*. Consequently, we denote them as  $\{\{(t_1, \dots, t_n) \mid \varphi(x_1, \dots, x_r)\}\}$ .

**Definition 4.2.** Two states of computation  $\mathbf{S}_1$  and  $\mathbf{S}_2$  of a same vocabulary  $\Sigma$  *coincide* over a set  $W$  of witness terms if for every  $\alpha_i \in W$ , we have that  $\text{val}_{\mathbf{S}_1}(\alpha_i) = \text{val}_{\mathbf{S}_2}(\alpha_i)$ .

**Postulate 4 (Bounded Exploration Postulate).** Let  $A$  be a parallel algorithm. Then there is a finite set  $W$  of witness terms (called *bounded exploration witness* of  $A$ ) such that, for every pair of states  $\mathbf{I}_1$  and  $\mathbf{I}_2$  of  $A$ , it holds that  $\tau_A(\mathbf{I}_1) - \mathbf{I}_1 = \tau_A(\mathbf{I}_2) - \mathbf{I}_2$  whenever there are two states of computation  $\mathbf{S}_1$  and  $\mathbf{S}_2$  which correspond to  $\mathbf{I}_1$  and  $\mathbf{I}_2$ , respectively, and coincide over  $W$ .

Same as in the bounded exploration postulate for sequential algorithms, the intuition is that the algorithm  $A$  examines only the part of the state that is given by means of terms in  $W$ . The central difference resides in the fact that in the case of parallel algorithms, the terms in  $W$  are multiset comprehension terms instead of ground terms. In practice, this means that it is also determined by the state, not just by the algorithm, which part of the state is actually relevant for producing the update set.

**Example 4.1.** Let us take the parallel algorithm in [Example 1.1](#) which calculates the complement of a given undirected graph. The (parallel) bounded exploration witness

$$\begin{aligned} & \{ \{ (\neg E(x, y), x, y) \mid x \neq y \wedge V(x) \wedge V(y) \} \}, \\ & \{ \{ (\neg E(x, y), x, y) \mid x \neq y \wedge \neg(V(x) \wedge V(y)) \} \}, \\ & \{ \{ x \neq y \mid V(x) \wedge V(y) \} \}, \{ \{ x \neq y \mid \neg(V(x) \wedge V(y)) \} \}, \{ \{ \text{true} \mid \text{true} \} \} \end{aligned}$$

shows that it satisfies the (parallel) bounded exploration postulate.

We can now formalize the concept of synchronous, parallel algorithm.

**Definition 4.3.** A (synchronous) parallel algorithm satisfies the sequential time, abstract state, background and (parallel) bounded exploration postulates.

## 5. Plausibility theorem

In this section we formally define *parallel ASMs* and show that every parallel ASM defines a parallel algorithm in the sense of [Definition 4.3](#). That is, we show that every parallel ASM satisfies the sequential time, abstract state, background and (parallel) bounded exploration postulates as stated in this work. Our formal ASM model is similar to the ASM model in Blass and Gurevich's thesis [\[4,5\]](#) modulo some technical details which are due to the fact that we use states of computation which are represented as meta-finite structures instead of assuming that the states include a finite set of proclots.

**Definition 5.1 (ASM Rules).** Let  $\mathbf{I}$  be a meta-finite structure of vocabulary  $\Sigma$  and let  $\mathbf{S} = (\mathbf{I}, \mathbf{B}, F)$  of vocabulary  $\Sigma_{\mathbf{S}} = (\Sigma_{\mathbf{I}}, \Sigma_{\mathbf{B}}, \Sigma_F)$  be its corresponding state of computation. Assume that  $\mathbf{S}$  satisfies the background postulate, let  $\mu$  be a variable assignment over the primary part  $\mathbf{I}$  of  $\mathbf{S}$  and let  $\Delta_{\mu}(r, \mathbf{S})$  denote the update set produced by an ASM rule  $r$  in  $\mathbf{S}$  under  $\mu$ . The set  $\mathcal{R}$  of ASM rules over  $\Sigma$  and the interpretation as update set of every rule in  $\mathcal{R}$ , is defined inductively by:

- If  $f \in \Sigma$  is an  $n$ -ary dynamic function symbol and  $t_0, t_1, \dots, t_n$  are terms of vocabulary  $\Sigma_{\mathbf{S}}$ , then  $f(t_1, \dots, t_n) := t_0$  is an assignment rule in  $\mathcal{R}$ , which produces the update set

$$\{ \{ (f, (\text{vals}_{\mathbf{S}, \mu}(t_1), \dots, \text{vals}_{\mathbf{S}, \mu}(t_n))), \text{vals}_{\mathbf{S}, \mu}(t_0) \} \},$$

provided that the following conditions hold:

- if  $f \in \Sigma_{\mathbf{I}}$ , then  $\text{vals}_{\mathbf{S}, \mu}(t_i) \in I$  for every  $0 \leq i \leq n$ ;
- if  $f \in \Sigma_{\mathbf{B}}$ , then  $\text{atomic}^{\mathbf{B}}(\text{vals}_{\mathbf{S}, \mu}(t_i)) = \text{true}^{\mathbf{B}}$  for every  $0 \leq i \leq n$ ;
- if  $f \in \Sigma_F$ , then  $\text{atomic}^{\mathbf{B}}(\text{vals}_{\mathbf{S}, \mu}(t_0)) = \text{true}^{\mathbf{B}}$  and  $\text{vals}_{\mathbf{S}, \mu}(t_i) \in I$  for every  $1 \leq i \leq n$ ;

Otherwise, the update set is undefined.

- If  $r_1, \dots, r_n$  are rules in  $\mathcal{R}$ , then **par**  $r_1 \dots r_n$  **endpar** is a block rule in  $\mathcal{R}$ , which produces the update set  $\Delta_{\mu}(r_1, \mathbf{S}) \cup \dots \cup \Delta_{\mu}(r_n, \mathbf{S})$ , provided all the update sets  $\Delta_{\mu}(r_i, \mathbf{S})$  are defined.
- If  $\varphi$  is a term of vocabulary  $\Sigma_{\mathbf{S}}$  and  $r$  is a rule in  $\mathcal{R}$ , then **if**  $\varphi$  **then**  $r$  **endif** is a conditional rule in  $\mathcal{R}$ , which produces the update set  $\Delta_{\mu}(r, \mathbf{S})$  (if defined) if  $\text{vals}_{\mathbf{S}, \mu}(\varphi) = \text{true}^{\mathbf{B}}$  and the update set  $\emptyset$  if  $\text{vals}_{\mathbf{S}, \mu}(\varphi) \neq \text{true}^{\mathbf{B}}$ .
- If  $\varphi$  is a term of vocabulary  $\Sigma_{\mathbf{S}}$  with  $\text{free}(\varphi) \supseteq \{x_1, \dots, x_k\}$  and  $r$  is a rule in  $\mathcal{R}$ , then **forall**  $x_1, \dots, x_k$  **with**  $\varphi$  **do**  $r$  **enddo** is a forall rule in  $\mathcal{R}$  which produces the update set  $\bigcup_{(a_1, \dots, a_k) \in A} (\Delta_{\mu[x_1 \mapsto a_1, \dots, x_k \mapsto a_k]}(r, \mathbf{S}))$  where  $A = \{(a_1, \dots, a_k) \in I^k \mid \text{vals}_{\mathbf{S}, \mu[x_1 \mapsto a_1, \dots, x_k \mapsto a_k]}(\varphi) = \text{true}^{\mathbf{B}}\}$ , provided all update sets  $\Delta_{\mu[x_1 \mapsto a_1, \dots, x_k \mapsto a_k]}(r, \mathbf{S})$  are defined.

The scope of  $x_i$  ( $1 \leq i \leq k$ ) in **forall**  $x_1, \dots, x_k$  **with**  $\varphi$  **do**  $r$  **enddo** is  $\varphi$  and  $r$ . An occurrence of a variable  $x$  in a transition rule  $r$  is *bound* if it is in the scope of a forall rule or if it is a non free variable in a multiset comprehension term. Otherwise,  $x$  is *free* in  $r$ . A rule  $r$  is *closed* if it has no free variables.

**Definition 5.2 (Parallel ASM).** A parallel abstract state machine  $\mathcal{M}$  of vocabulary  $\Sigma = (\Sigma_1, \Sigma_2, \Sigma_F)$  and background class  $\mathcal{K}$  of vocabulary  $\Sigma_{\mathcal{K}}$  is formed by:

- A set  $\mathcal{S}_{\mathcal{M}}$  of states of vocabulary  $\Sigma$  and a set  $\mathcal{I}_{\mathcal{M}} \subseteq \mathcal{S}_{\mathcal{M}}$  of initial states, both closed under isomorphisms.
- A closed ASM rule  $r_{\mathcal{M}}$  – the main rule of  $\mathcal{M}$  – of vocabulary  $(\Sigma_1, \Sigma_2 \cup \Sigma_{\mathcal{K}} \cup \{\text{atomic}\}, \Sigma_F)$ .
- A transition function  $\tau_{\mathcal{M}}$  over  $\mathcal{S}_{\mathcal{M}}$  such that  $\tau_{\mathcal{M}}(\mathbf{I}) = \mathbf{I} + \Delta(r_{\mathcal{M}}, \mathbf{S})$  for every  $\mathbf{I} \in \mathcal{S}_{\mathcal{M}}$  and every state of computation  $\mathbf{S}$  that corresponds to  $\mathbf{I}$ .

A run or a computation of an ASM  $\mathcal{M}$  is a finite or infinite sequence  $\mathbf{I}_0, \mathbf{I}_1, \dots$ , where  $\mathbf{I}_0$  is an initial state in  $\mathcal{S}_{\mathcal{M}}$  and  $\mathbf{I}_{i+1} = \tau_{\mathcal{M}}(\mathbf{I}_i)$  holds for every  $i \geq 0$ .

Next, we define for every parallel ASM  $\mathcal{M}$ , a finite set  $W_{\mathcal{M}}$  of witness terms which, as shown in [Theorem 5.1](#) below, is a bounded exploration witness for  $\mathcal{M}$ .

**Definition 5.3.** Let  $\mathcal{M}$  be a parallel ASM. For every sub-rule  $r$  of the main rule  $r_{\mathcal{M}}$  of  $\mathcal{M}$ , let  $W_r$  be the set of multiset comprehension terms inductively defined as follows:

- If  $r$  is of the form  $f(t_1, \dots, t_n) := t_0$  and  $\bigcup_{0 \leq i \leq n} \text{free}(t_i) = \{x_1, \dots, x_k\}$ , then  $W_r = \{\{(t_0, t_1, \dots, t_n) \mid \text{true}\}_{x_1, \dots, x_k}\}$ .
- If  $r$  is of the form **par**  $r_1 \dots r_n$  **endpar**, then  $W_r = \bigcup_{1 \leq i \leq n} W_{r_i}$ .
- If  $r$  is of the form **if**  $\varphi$  **then**  $r'$  **endif** and  $\text{free}(r') \cup \text{free}(\varphi) = \{x_1, \dots, x_k\}$ , then

$$W_r = \{\{\{\varphi \mid \text{true}\}_{\text{free}(\varphi)}\} \cup \{\{\{\text{true} \mid \text{true}\}\} \cup \{\{(t_{i0}, \dots, t_{in_i}) \mid \varphi_i \wedge \varphi\}_{x_1, \dots, x_k} \mid \{(t_{i0}, \dots, t_{in_i}) \mid \varphi_i\}_{\text{free}(r')} \in W_{r'}\}\}$$

- If  $r$  is of the form **forall**  $x_1, \dots, x_k$  **with**  $\varphi$  **do**  $r'$  **enddo** and  $(\text{free}(r') \cup \text{free}(\varphi)) \setminus \{x_1, \dots, x_k\} = \{y_1, \dots, y_l\}$ , then

$$W_r = \{\{\{(t_{i0}, \dots, t_{in_i}) \mid \varphi_i \wedge \varphi\}_{y_1, \dots, y_l} \mid \{(t_{i0}, \dots, t_{in_i}) \mid \varphi_i\}_{\text{free}(r')} \in W_{r'}\} \cup \{\{(t_{i0}, \dots, t_{in_i}) \mid \varphi_i \wedge \neg\varphi\}_{y_1, \dots, y_l} \mid \{(t_{i0}, \dots, t_{in_i}) \mid \varphi_i\}_{\text{free}(r')} \in W_{r'}\}\}$$

It is easy to see that if  $r$  is a closed rule, then the multiset comprehension terms in  $W_r$  have no free variables. Thus, we can define the bounded exploration witness for  $\mathcal{M}$  as the set of witness terms (i.e., multiset comprehension terms without free variables)  $W_{r_{\mathcal{M}}}$  corresponding to the main (closed) rule  $r_{\mathcal{M}}$  of  $\mathcal{M}$ .

**Example 5.1.** The main ASM rule in [Example 1.1](#) has the following sub-rules:

$$r_1 = E(x, y) := \neg E(x, y)$$

$$r_2 = \text{if } x \neq y \text{ then } r_1 \text{ endif}$$

$$r_3 = \text{forall } x, y \text{ with } V(x) \wedge V(y) \text{ do } r_2 \text{ enddo}$$

Their corresponding sets of witness terms as determined by the inductive construction in [Definition 5.3](#) are:

$$W_{r_1} = \{\{\{\neg E(x, y), x, y \mid \text{true}\}_{x, y}\}$$

$$W_{r_2} = \{\{\{\neg E(x, y), x, y \mid \text{true} \wedge x \neq y\}_{x, y}, \{\{x \neq y \mid \text{true}\}_{x, y}, \{\{\text{true} \mid \text{true}\}\}$$

$$W_{r_3} = \{\{\{\neg E(x, y), x, y \mid \text{true} \wedge x \neq y \wedge V(x) \wedge V(y)\}, \{\{x \neq y \mid \text{true} \wedge V(x) \wedge V(y)\}, \{\{\text{true} \mid \text{true} \wedge V(x) \wedge V(y)\}\}, \{\{\neg E(x, y), x, y \mid \text{true} \wedge x \neq y \wedge \neg(V(x) \wedge V(y))\}, \{\{x \neq y \mid \text{true} \wedge \neg(V(x) \wedge V(y))\}, \{\{\text{true} \mid \text{true} \wedge \neg(V(x) \wedge V(y))\}\}\}$$

Of course,  $W_{r_3}$  can be reduced (see [Example 4.1](#)). The objective here is however to illustrate the construction that we actually use in the proof of our next theorem, rather than to construct a minimal bounded exploration witness.

**Theorem 5.1 (Plausibility).** Every parallel ASM  $\mathcal{M}$  defines a parallel algorithm with the same vocabulary and background as  $\mathcal{M}$ .

**Proof.** Let  $\mathcal{M}$  be a parallel ASM. We have to show that the four postulates (sequential time, abstract state, background and parallel bounded exploration postulates) are satisfied. The sequential time and background postulates are already built into the definition of an ASM. The same holds for the abstract state postulate, and the preservation of isomorphisms is straightforward.

In what follows, we prove that  $\mathcal{M}$  satisfies also the bounded exploration postulate. Let  $r$  be a well formed ASM rule of vocabulary  $\Sigma$ . Let  $W_r$  be the set of multiset comprehension terms corresponding to  $r$  as per [Definition 5.3](#). Let  $\mathbf{S}_1$  and  $\mathbf{S}_2$  be states of computation of vocabulary  $\Sigma$ . Let  $\mu_1$  and  $\mu_2$  be variable assignments over the primary part  $\mathbf{I}_1$  of  $\mathbf{S}_1$  and  $\mathbf{I}_2$  of  $\mathbf{S}_2$ , respectively. We show that:

If  $\text{vals}_{\mathbf{S}_1, \mu_1}(\alpha_i) = \text{vals}_{\mathbf{S}_2, \mu_2}(\alpha_i)$  for every  $\alpha_i \in W_r$ , then  $\Delta_{\mu_1}(r, \mathbf{S}_1) = \Delta_{\mu_2}(r, \mathbf{S}_2)$ .

We proceed by induction on the set of ASM rules over  $\Sigma$ .

- If  $r$  is a rule of the form  $f(t_1, \dots, t_n) := t_0$  and  $\bigcup_{0 \leq i \leq n} \text{free}(t_i) = \{x_1, \dots, x_k\}$  then by definition  $W_r = \{\{(t_0, t_1, \dots, t_n) \mid \text{true}\}_{x_1, \dots, x_k}\}$ . Let  $\alpha = \{(t_0, t_1, \dots, t_n) \mid \text{true}\}_{x_1, \dots, x_k}$ . Since by [Definition 4.1](#)

$$\text{vals}_{\mathbf{S}_1, \mu_1}(\alpha) = \{(\text{vals}_{\mathbf{S}_1, \mu_1}(t_0), \text{vals}_{\mathbf{S}_1, \mu_1}(t_1), \dots, \text{vals}_{\mathbf{S}_1, \mu_1}(t_n))\} \text{ and}$$

$$\text{vals}_{\mathbf{S}_2, \mu_2}(\alpha) = \{(\text{vals}_{\mathbf{S}_2, \mu_2}(t_0), \text{vals}_{\mathbf{S}_2, \mu_2}(t_1), \dots, \text{vals}_{\mathbf{S}_2, \mu_2}(t_n))\},$$

by our assumption  $\text{vals}_{\mathbf{S}_1, \mu_1}(\alpha) = \text{vals}_{\mathbf{S}_2, \mu_2}(\alpha)$  and by [Definition 5.1](#)

$$\Delta_{\mu_1}(r, \mathbf{S}_1) = \{((f, (\text{vals}_{\mathbf{S}_1, \mu_1}(t_1), \dots, \text{vals}_{\mathbf{S}_1, \mu_1}(t_n))), \text{vals}_{\mathbf{S}_1, \mu_1}(t_0))\} \text{ and}$$

$$\Delta_{\mu_2}(r, \mathbf{S}_2) = \{((f, (\text{vals}_{\mathbf{S}_2, \mu_2}(t_1), \dots, \text{vals}_{\mathbf{S}_2, \mu_2}(t_n))), \text{vals}_{\mathbf{S}_2, \mu_2}(t_0))\},$$

we get that  $\Delta_{\mu_1}(r, \mathbf{S}_1) = \Delta_{\mu_2}(r, \mathbf{S}_2)$ .

- If  $r$  is a rule of the form **par**  $r_1 \dots r_n$  **endpar** then by definition  $W_r = W_{r_1} \cup \dots \cup W_{r_n}$ . Since  $\text{vals}_{\mathbf{S}_1, \mu_1}(\alpha_i) = \text{vals}_{\mathbf{S}_2, \mu_2}(\alpha_i)$  for every  $\alpha_i \in W_r$  and  $W_{r_j} \subseteq W_r$  for every  $1 \leq j \leq n$ , we know that  $\text{vals}_{\mathbf{S}_1, \mu_1}(\alpha_i) = \text{vals}_{\mathbf{S}_2, \mu_2}(\alpha_i)$  for every  $\alpha_i \in W_{r_j}$ . Then it follows by the induction hypothesis that  $\Delta_{\mu_1}(r_j, \mathbf{S}_1) = \Delta_{\mu_2}(r_j, \mathbf{S}_2)$  for every  $1 \leq j \leq n$ . By [Definition 5.1](#),  $\Delta_{\mu_1}(r, \mathbf{S}_1) = \Delta_{\mu_1}(r_1, \mathbf{S}_1) \cup \dots \cup \Delta_{\mu_1}(r_n, \mathbf{S}_1)$  and  $\Delta_{\mu_2}(r, \mathbf{S}_2) = \Delta_{\mu_2}(r_1, \mathbf{S}_2) \cup \dots \cup \Delta_{\mu_2}(r_n, \mathbf{S}_2)$ . Hence  $\Delta_{\mu_1}(r, \mathbf{S}_1) = \Delta_{\mu_2}(r, \mathbf{S}_2)$ .
- If  $r$  is of the form **if**  $\varphi$  **then**  $r'$  **endif** and  $\text{free}(r') \cup \text{free}(\varphi) = \{x_1, \dots, x_k\}$ , then by definition

$$W_r = \{\{\varphi \mid \text{true}\}_{\text{free}(\varphi)}\} \cup \{\{\text{true} \mid \text{true}\}\} \cup$$

$$\{\{(t_{i_0}, \dots, t_{i_n}) \mid \varphi_i \wedge \varphi\}_{x_1, \dots, x_k} \mid \{(t_{i_0}, \dots, t_{i_n}) \mid \varphi_i\}_{\text{free}(r')} \in W_{r'}\}.$$

Since  $\{\{\text{true} \mid \text{true}\}\} \in W_r$  and  $\{\{\varphi \mid \text{true}\}_{\text{free}(\varphi)}\} \in W_r$ , we know (by our assumption that  $\text{vals}_{\mathbf{S}_1, \mu_1}(\alpha_i) = \text{vals}_{\mathbf{S}_2, \mu_2}(\alpha_i)$  for all  $\alpha_i \in W_r$ ) that  $\text{true}^{\mathbf{S}_1} = \text{true}^{\mathbf{S}_2}$  and  $\text{vals}_{\mathbf{S}_1, \mu_1}(\varphi) = \text{vals}_{\mathbf{S}_2, \mu_2}(\varphi)$ . Hence  $\text{vals}_{\mathbf{S}_1, \mu_1}(\varphi) = \text{true}^{\mathbf{S}_1}$  iff  $\text{vals}_{\mathbf{S}_2, \mu_2}(\varphi) = \text{true}^{\mathbf{S}_2}$ . Let  $\text{vals}_{\mathbf{S}_1, \mu_1}(\varphi) = \text{true}^{\mathbf{S}_1}$  and  $\text{vals}_{\mathbf{S}_2, \mu_2}(\varphi) = \text{true}^{\mathbf{S}_2}$ . It follows by definition of  $W_r$  that  $\text{vals}_{\mathbf{S}_1, \mu_1}(\alpha'_i) = \text{vals}_{\mathbf{S}_2, \mu_2}(\alpha'_i)$  for all  $\alpha'_i \in W_{r'}$ . By the induction hypothesis we then have that  $\Delta_{\mu_1}(r', \mathbf{S}_1) = \Delta_{\mu_2}(r', \mathbf{S}_2)$ . From [Definition 5.1](#) and the fact that  $\text{vals}_{\mathbf{S}_1, \mu_1}(\varphi) = \text{true}^{\mathbf{S}_1}$  and  $\text{vals}_{\mathbf{S}_2, \mu_2}(\varphi) = \text{true}^{\mathbf{S}_2}$ , we get that  $\Delta_{\mu_1}(r, \mathbf{S}_1) = \Delta_{\mu_1}(r', \mathbf{S}_1)$  and that  $\Delta_{\mu_2}(r, \mathbf{S}_2) = \Delta_{\mu_2}(r', \mathbf{S}_2)$ . Hence  $\Delta_{\mu_1}(r, \mathbf{S}_1) = \Delta_{\mu_2}(r, \mathbf{S}_2)$ .

If on the other hand  $\text{vals}_{\mathbf{S}_1, \mu_1}(\varphi) \neq \text{true}^{\mathbf{S}_1}$  and  $\text{vals}_{\mathbf{S}_2, \mu_2}(\varphi) \neq \text{true}^{\mathbf{S}_2}$  then, by [Definition 5.1](#),  $\Delta_{\mu_1}(r, \mathbf{S}_1) = \Delta_{\mu_2}(r, \mathbf{S}_2) = \emptyset$ .

- If  $r$  is a rule of the form **forall**  $x_1, \dots, x_k$  **with**  $\varphi$  **do**  $r'$  **and**

$$(\text{free}(r') \cup \text{free}(\varphi)) \setminus \{x_1, \dots, x_k\} = \{y_1, \dots, y_l\}$$

then by definition

$$W_r = \{\{(t_{i_0}, \dots, t_{i_n}) \mid \varphi_i \wedge \varphi\}_{y_1, \dots, y_l} \mid \{(t_{i_0}, \dots, t_{i_n}) \mid \varphi_i\}_{\text{free}(r')} \in W_{r'}\} \cup$$

$$\{\{(t_{i_0}, \dots, t_{i_n}) \mid \varphi_i \wedge \neg\varphi\}_{y_1, \dots, y_l} \mid \{(t_{i_0}, \dots, t_{i_n}) \mid \varphi_i\}_{\text{free}(r')} \in W_{r'}\}.$$

Let  $\alpha'_i = \{(t_{i_0}, \dots, t_{i_n}) \mid \varphi_i\}_{\text{free}(r')} \in W_{r'}$  and

$$A_{\alpha'_i} = \{(a_1, \dots, a_k) \in (I_1)^k \mid \text{vals}_{\mathbf{S}_1, \mu_1[x_1 \mapsto a_1, \dots, x_k \mapsto a_k]}(\varphi_i) = \text{true}^{\mathbf{S}_1} \wedge \\ \text{vals}_{\mathbf{S}_1, \mu_1[x_1 \mapsto a_1, \dots, x_k \mapsto a_k]}(\varphi) = \text{true}^{\mathbf{S}_1}\}$$

$$B_{\alpha'_i} = \{(a_1, \dots, a_k) \in (I_2)^k \mid \text{vals}_{\mathbf{S}_2, \mu_2[x_1 \mapsto a_1, \dots, x_k \mapsto a_k]}(\varphi_i) = \text{true}^{\mathbf{S}_2} \wedge \\ \text{vals}_{\mathbf{S}_2, \mu_2[x_1 \mapsto a_1, \dots, x_k \mapsto a_k]}(\varphi) = \text{true}^{\mathbf{S}_2}\}$$

$$A_{\alpha'_i}^- = \{(a_1, \dots, a_k) \in (I_1)^k \mid \text{vals}_{\mathbf{S}_1, \mu_1[x_1 \mapsto a_1, \dots, x_k \mapsto a_k]}(\varphi_i) = \text{true}^{\mathbf{S}_1} \wedge \\ \text{vals}_{\mathbf{S}_1, \mu_1[x_1 \mapsto a_1, \dots, x_k \mapsto a_k]}(\varphi) \neq \text{true}^{\mathbf{S}_1}\}$$

$$B_{\alpha'_i}^- = \{(a_1, \dots, a_k) \in (I_2)^k \mid \text{vals}_{\mathbf{S}_2, \mu_2[x_1 \mapsto a_1, \dots, x_k \mapsto a_k]}(\varphi_i) = \text{true}^{\mathbf{S}_2} \wedge \\ \text{vals}_{\mathbf{S}_2, \mu_2[x_1 \mapsto a_1, \dots, x_k \mapsto a_k]}(\varphi) \neq \text{true}^{\mathbf{S}_2}\}$$

Since for  $\alpha_i = \{(t_{i0}, \dots, t_{in_i}) \mid \varphi_i \wedge \varphi\}_{y_1, \dots, y_l}$  we have assumed that  $\text{vals}_{\mathbf{S}_1, \mu_1}(\alpha_i) = \text{vals}_{\mathbf{S}_2, \mu_2}(\alpha_i)$ , then there is a bijection  $\zeta$  from  $A_{\alpha_i}$  to  $B_{\alpha_i}$  such that for all  $(a_1, \dots, a_k) \in A_{\alpha_i}$  and corresponding  $\zeta((a_1, \dots, a_k)) = (b_1, \dots, b_k) \in B_{\alpha_i}$ ,

$$\text{vals}_{\mathbf{S}_1, \mu_1[x_1 \mapsto a_1, \dots, x_k \mapsto a_k]}((t_{i0}, \dots, t_{in_i})) = \text{vals}_{\mathbf{S}_2, \mu_2[x_1 \mapsto b_1, \dots, x_k \mapsto b_k]}((t_{i0}, \dots, t_{in_i}))$$

Likewise, since for  $\alpha_i^- = \{(t_{i0}, \dots, t_{in_i}) \mid \varphi_i \wedge \neg\varphi\}_{y_1, \dots, y_l}$  we have assumed that  $\text{vals}_{\mathbf{S}_1, \mu_1}(\alpha_i^-) = \text{vals}_{\mathbf{S}_2, \mu_2}(\alpha_i^-)$ , then there is a bijection  $\zeta'$  from  $A_{\alpha_i}^-$  to  $B_{\alpha_i}^-$  such that for all  $(a_1, \dots, a_k) \in A_{\alpha_i}^-$  and corresponding  $\zeta'((a_1, \dots, a_k)) = (b_1, \dots, b_k) \in B_{\alpha_i}^-$ ,

$$\text{vals}_{\mathbf{S}_1, \mu_1[x_1 \mapsto a_1, \dots, x_k \mapsto a_k]}((t_{i0}, \dots, t_{in_i})) = \text{vals}_{\mathbf{S}_2, \mu_2[x_1 \mapsto b_1, \dots, x_k \mapsto b_k]}((t_{i0}, \dots, t_{in_i}))$$

Since  $A_{\alpha_i} \cap A_{\alpha_i}^- = \emptyset$  and  $B_{\alpha_i} \cap B_{\alpha_i}^- = \emptyset$ , we get that  $\zeta'' = \zeta \cup \zeta'$  is a bijection from  $A_{\alpha_i} \cup A_{\alpha_i}^-$  to  $B_{\alpha_i} \cup B_{\alpha_i}^-$  which preserves

$$\text{vals}_{\mathbf{S}_1, \mu_1[x_1 \mapsto a_1, \dots, x_k \mapsto a_k]}((t_{i0}, \dots, t_{in_i})) = \text{vals}_{\mathbf{S}_2, \mu_2[x_1 \mapsto b_1, \dots, x_k \mapsto b_k]}((t_{i0}, \dots, t_{in_i}))$$

for all  $(a_1, \dots, a_k) \in A_{\alpha_i} \cup A_{\alpha_i}^-$  and corresponding  $\zeta''((a_1, \dots, a_k)) = (b_1, \dots, b_k) \in B_{\alpha_i} \cup B_{\alpha_i}^-$ .

Hence, for every  $\alpha'_i \in W_r$  we get that  $\text{vals}_{\mathbf{S}_1, \mu_1}(\alpha'_i) = \text{vals}_{\mathbf{S}_2, \mu_2}(\alpha'_i)$  and, by the inductive hypothesis, that  $\Delta_{\mu_1}(r', \mathbf{S}_1) = \Delta_{\mu_2}(r', \mathbf{S}_2)$ . Since this holds for every pair of variable assignments  $\mu_1$  and  $\mu_2$  on  $\mathbf{I}_1$  and  $\mathbf{I}_2$ , respectively, which satisfies our assumption that  $\text{vals}_{\mathbf{S}_1, \mu_1}(\alpha_i) = \text{vals}_{\mathbf{S}_2, \mu_2}(\alpha_i)$  for every  $\alpha_i \in W_r$ , then it also holds in particular for every pair of variable assignments  $\mu'_1 = \mu_1[x_1 \mapsto a_1, \dots, x_k \mapsto a_k]$  with  $(a_1, \dots, a_k) \in (I_1)^k$  and  $\mu'_2 = \mu_2[x_1 \mapsto b_1, \dots, x_k \mapsto b_k]$  with  $(b_1, \dots, b_k) \in (I_2)^k$  such that  $\text{vals}_{\mathbf{S}_1, \mu'_1}(\varphi) = \text{true}^{\mathbf{S}_1}$  and  $\text{vals}_{\mathbf{S}_2, \mu'_2}(\varphi) = \text{true}^{\mathbf{S}_2}$ . Thus, it follows from Definition 5.1 that  $\Delta_{\mu_1}(r, \mathbf{S}_1) = \Delta_{\mu_2}(r, \mathbf{S}_2)$  holds.  $\square$

## 6. Examples

In this section we provide evidence that the general axiomatic description of parallel algorithms in Definition 4.3 captures the notion of deterministic, parallel algorithm that works synchronously on a fixed level of abstraction. We discuss some familiar approaches to parallelism in a way that is analogous to the discussion in the ASM thesis for parallel algorithms of Blass and Gurevich [4,5], showing that they fit our (simplified) axiomatic characterization.

### 6.1. Circuits

A popular model for parallel computing, which was shown to satisfy the postulates in the original ASM thesis for parallel algorithms [4], is provided by the class of unbounded fan-in combinational Boolean circuit (see for instance [18]). We show next that this kind of circuits also fit the new axiomatization proposed in this work.

A *Boolean circuit of unbounded fan-in* with  $n$  inputs  $x_1, \dots, x_n$  is a labeled acyclic digraph with a set of nodes  $V$  (usually called gates), a set of edges  $E$  and a labeling function  $\lambda$  from  $V$  to  $\{x_1, \dots, x_n\} \cup \{\wedge, \vee, \neg\}$  such that:  $\lambda(v) \in \{x_1, \dots, x_n\}$  implies that  $v$  has in-degree 0 and  $\lambda(v) = \neg$  implies that  $v$  has in-degree 1. The in-degree of a node is called *fan-in*. The fan-in is unbounded for nodes labeled with  $\wedge$  or  $\vee$ .

We consider the states of computation of the algorithm to include, apart from the requirements of the background postulate, the following functions:

- A static bridge function  $f_V$  which evaluates to `true` if its argument is a node in  $V$  and to `false` otherwise.
- A static bridge function  $f_E$  such that  $f_E(v_1, v_2)$  evaluates to `true` if there is an edge from  $v_1$  to  $v_2$  in  $E$ .
- A static function  $f_\lambda$  in the primary part of the state such that  $f_\lambda(v) = \lambda(v)$  if  $v \in V$  and  $f_\lambda(v) = \text{undef}$  otherwise.
- A dynamic bridge function `val` which assigns to each node  $v \in V$  with  $\lambda(v) = x_i$  for some  $x_i$  in  $\{x_1, \dots, x_n\}$  the input value given to  $x_i$ , and to each node  $v$  with  $\lambda(v) \notin \{x_1, \dots, x_n\}$  the value it computes (which is `undef` in the initial state and updated exactly once during the computation).

---

#### Algorithm 1 Boolean circuits of unbounded fan-in.

---

```

for all  $x$  with  $f_V(x)$  do
  if  $\forall y (f_E(y, x) \rightarrow \text{val}(y) \neq \text{undef}) \wedge \text{val}(x) = \text{undef}$  then
    par
      if  $f_\lambda(x) = \neg$  then  $\text{val}(x) := \{\{y \mid f_E(y, x) \wedge \text{val}(y) = \text{true}\}\} = \emptyset$  endif
      if  $f_\lambda(x) = \vee$  then  $\text{val}(x) := \{\{y \mid f_E(y, x) \wedge \text{val}(y) = \text{true}\}\} \neq \emptyset$  endif
      if  $f_\lambda(x) = \wedge$  then  $\text{val}(x) := \{\{y \mid f_E(y, x) \wedge \text{val}(y) = \text{false}\}\} = \emptyset$  endif
    endpar
  end if
end for

```

---

It is easy to see that the transition function described by Algorithm 1, together with the states described above, define a parallel algorithm that satisfies the sequential time, abstract state, and background postulates and computes the boolean

function that corresponds to the input Boolean circuit. The following witness terms show that it also satisfies the bounded exploration postulate.

$$\begin{aligned}
\alpha_1 &= \{ \{ \{ y \mid f_E(y, x) \wedge \text{val}(y) = \text{true} \} = \emptyset, x \mid f_V(x) \wedge \\
&\quad \forall y (f_E(y, x) \rightarrow \text{val}(y) \neq \text{undef}) \wedge \text{val}(x) = \text{undef} \wedge f_\lambda(x) = \neg \} \} \\
\alpha_2 &= \{ \{ \{ y \mid f_E(y, x) \wedge \text{val}(y) = \text{true} \} \neq \emptyset, x \mid f_V(x) \wedge \\
&\quad \forall y (f_E(y, x) \rightarrow \text{val}(y) \neq \text{undef}) \wedge \text{val}(x) = \text{undef} \wedge f_\lambda(x) = \vee \} \} \\
\alpha_3 &= \{ \{ \{ y \mid f_E(y, x) \wedge \text{val}(y) = \text{false} \} = \emptyset, x \mid f_V(x) \wedge \\
&\quad \forall y (f_E(y, x) \rightarrow \text{val}(y) \neq \text{undef}) \wedge \text{val}(x) = \text{undef} \wedge f_\lambda(x) = \wedge \} \} \\
\alpha_4 &= \{ \{ f_\lambda(x) = \neg \mid \forall y (f_E(y, x) \rightarrow \text{val}(y) \neq \text{undef}) \wedge \text{val}(x) = \text{undef} \wedge f_V(x) \} \} \\
\alpha_5 &= \{ \{ f_\lambda(x) = \vee \mid \forall y (f_E(y, x) \rightarrow \text{val}(y) \neq \text{undef}) \wedge \text{val}(x) = \text{undef} \wedge f_V(x) \} \} \\
\alpha_6 &= \{ \{ f_\lambda(x) = \wedge \mid \forall y (f_E(y, x) \rightarrow \text{val}(y) \neq \text{undef}) \wedge \text{val}(x) = \text{undef} \wedge f_V(x) \} \} \\
\alpha_7 &= \{ \{ \forall y (f_E(y, x) \rightarrow \text{val}(y) \neq \text{undef}) \wedge \text{val}(x) = \text{undef} \mid f_V(x) \} \} \\
\alpha_8 &= \{ \{ \text{true} \mid \text{true} \} \}
\end{aligned}$$

The set of witness terms additionally includes the terms obtained by replacing  $f_V(x)$  with its negation in each of the witness terms  $\alpha_1, \dots, \alpha_7$ . To simplify our presentation, we omit them here.

As a final consideration regarding this example, we would like to note that the model of Boolean circuit of unbounded fan-in is rather limited in the sense that it only computes Boolean functions from  $\{\text{true}, \text{false}\}^n$  to  $\{\text{true}, \text{false}\}$  for a fixed  $n$ . That is, the model can only represent a finite number ( $2^{2^n}$ ) of finite Boolean functions. This is analogous to consider propositional calculus as a parallel computation model. On the other hand, a *uniform family* of Boolean circuits (without restrictions in the algorithm which ensures the uniformity) is a more interested model since, as long as the size and depth of the circuits is not bounded, it exactly captures the class of computable functions. Furthermore, when these parameters are restricted to the classes NC and AC, the model provides a prime example for parallel computation of functions. It is not difficult to extend the work in this section to see that this model also satisfies our postulates. Due to space restrictions, we leave it as an exercise for the reader.

## 6.2. Parallel random access machine

The parallel random access machine (PRAM) model is a most idealized and powerful model of parallel computation. Following [19], we define a PRAM program as a sequence of random access machines (RAM) programs,  $P = (\Pi_1, \Pi_2, \dots, \Pi_q)$  one for each of  $q$  RAMs. In turn, each RAM  $i$  ( $1 \leq i \leq q$ ) is a finite sequence  $(\pi_{i1}, \pi_{i2}, \dots, \pi_{im_i})$  of instructions of the kinds shown in Figure 2.6 in [19] (i.e., READ, STORE, LOAD, JUMP, etc), with arguments standing for the contents of registers (memory locations). Register  $i$  is the accumulator of the RAM  $i$ , where the result of the current operation is stored. All registers, including the accumulators, are shared. That is, every RAM can both read and write all registers. Every RAM  $i$  executes its own program  $\Pi_i$ . At each step, the RAM  $i$  executes the instruction pointed by the program counter  $\kappa_i$ , reading and writing integer values on the registers as required by the instruction. There is also a set of input registers  $I = (i_1, \dots, i_m)$ . The HALT instruction stops the computation by setting the program counter to 0. Every semantically wrong instruction is considered as a HALT instruction. We assume that, apart from the requirements of the background postulate, the states of computation include the following functions:

- A unary bridge function  $P$  which is Boolean and static, and evaluates to `true` only for the RAM programs  $(1, \dots, p)$ .
- A unary static function  $I$  in the secondary part. If  $j$  is an input register,  $I(j)$  evaluates to its value. Otherwise, it evaluates to `undef`.
- Binary bridge functions  $\text{Inst}$ ,  $\text{OpType}$  and  $\text{OpVal}$  in the primary part which are static and map each program  $i$  and line  $l$  of  $i$  to the instruction, the type of operand (either  $j$ ,  $\uparrow j$  or  $=j$ ) and the operand value (an integer), respectively, that appears in the line  $l$  of the program  $i$ . If  $i$  is not a program or  $l$  is not a line of  $i$ , then  $\text{Inst}$ ,  $\text{OpType}$  and  $\text{OpVal}$  evaluate to `undef`.
- A unary dynamic function  $R$  from the set of positive integers to the set of integers which belongs to the secondary part and maps each register to its current value.
- A unary dynamic function  $\kappa$  which belongs to the primary part and maps each program to the current value of its program counter.
- A unary bridge function  $W$  which is dynamic and maps processors to pairs of the form (register, value). This is an auxiliary function which is used to collect the processors requests to update registers. It allows our ASM to detect whether more than one processor try to update the same register. In such cases, we use the convention that the processor with the smallest index prevails and has its value written in the register.

- A nullary bridge function `mode` which is interpreted by the values 0 or 1 depending on whether our ASM needs to execute a PRAM step or update the registers, respectively.

---

**Algorithm 2** Parallel random access machine.<sup>3</sup>


---

```

if mode = 0 then
for all  $i$  with  $P(i)$  do
  if  $\kappa(i) \neq 0$  then
    if  $\text{Inst}(i, \kappa(i)) = \text{READ}$  then
       $\kappa(i) := \kappa(i) + 1$ 
      if  $\text{OpType}(i, \kappa(i)) = j$  then  $W(i) := (i, I(\text{OpVal}(i, \kappa(i))))$  end if
      if  $\text{OpType}(i, \kappa(i)) = \uparrow j$  then
         $W(i) := (i, I(R(\text{OpVal}(i, \kappa(i)))))$  end if
      end if
    if  $\text{Inst}(i, \kappa(i)) = \text{STORE}$  then
       $\kappa(i) := \kappa(i) + 1$ 
      if  $\text{OpType}(i, \kappa(i)) = j$  then  $W(i) := (\text{OpVal}(i, \kappa(i)), R(i))$  end if
      if  $\text{OpType}(i, \kappa(i)) = \uparrow j$  then
         $W(i) := (R(\text{OpVal}(i, \kappa(i))), R(i))$  end if
      end if
    end if
    :
    :
    if  $\text{Inst}(i, \kappa(i)) = \text{HALT}$  then
       $\kappa(i) := 0$ 
    end if
  end if
end for
mode := 1
end if
if mode = 1 then
for all  $i$  with  $W(i) \neq \text{undef}$  do
  if  $\{\{x \mid \text{first}(W(x)) = \text{first}(W(i)) \wedge x < i\} = \emptyset\}$  then
     $R(\text{first}(W(i))) := \text{second}(W(i))$ 
  end if
   $W(i) := \text{undef}$ 
end for
mode := 0
end if

```

---

The base set of the (finite) primary part of each state of our algorithm includes: a finite totally ordered set of RAM programs, a finite set of instructions, three operands, a finite set of operand values (integers which appear in the programs) and a finite totally ordered set of line numbers. We assume that the primary part also includes a successor function “+1” defined on the set of line numbers, a constant “0” which does not belong to the set of line numbers, the relation “<” defined in the set of RAM programs and constants “ $j$ ”, “ $\uparrow j$ ” and “ $=j$ ” for the operands. The secondary part includes (in addition to the elements in the primary part) the set of integers. Also we assume that the secondary part includes functions for the standard arithmetic operations and relations among integers. In every initial state, if  $i$  is a program,  $\kappa(i)$  evaluates to the first line of  $i$  and  $W(i)$  evaluates to `undef`, and  $R(j)$  evaluates to 0 if  $j$  is a register (i.e., a positive integer) and to `undef` otherwise.

To simplify and shorten the exposition we assume that every instruction is semantically correct. That is, we assume that the programs do not contain semantically wrong instructions such as one that addresses Register  $-14$ . For the very same reason, in [Algorithm 2](#) we only show the cases corresponding to the `READ`, `STORE` and `HALT` instructions.

The transition function described by the ASM in [Algorithm 2](#) together with the states described above and the following witness terms show that the PRAM model of parallel computation satisfies the sequential time, abstract state, background and bounded exploration postulates for parallel algorithms.

$$\alpha_1 = \{\{(\kappa(i) + 1, i) \mid \text{mode} = 0 \wedge P(i) \wedge \kappa(i) \neq 0 \wedge \text{Inst}(i, \kappa(i)) = \text{READ}\}\}$$

$$\alpha_2 = \{\{((i, I(\text{OpVal}(i, \kappa(i))))), i) \mid \text{mode} = 0 \wedge P(i) \wedge \kappa(i) \neq 0 \wedge \text{Inst}(i, \kappa(i)) = \text{READ} \wedge \text{OpType}(i, \kappa(i)) = j\}\}$$

$$\alpha_3 = \{\{((i, I(R(\text{OpVal}(i, \kappa(i))))), i) \mid \text{mode} = 0 \wedge P(i) \wedge \kappa(i) \neq 0 \wedge \text{Inst}(i, \kappa(i)) = \text{READ} \wedge \text{OpType}(i, \kappa(i)) = \uparrow j\}\}$$

$$\alpha_4 = \{\{(\kappa(i) + 1, i) \mid \text{mode} = 0 \wedge P(i) \wedge \kappa(i) \neq 0 \wedge \text{Inst}(i, \kappa(i)) = \text{STORE}\}\}$$

---

<sup>3</sup> We have intentionally omitted the par blocks so that the algorithm fits in one page. Sequences of instructions at a same level are implicitly assumed to be executed in parallel.

$$\begin{aligned}
\alpha_5 &= \{ \{ ((\text{OpVal}(i, \kappa(i)), R(i)), i) \mid \text{mode} = 0 \wedge P(i) \wedge \kappa(i) \neq 0 \wedge \\
&\quad \text{Inst}(i, \kappa(i)) = \text{STORE} \wedge \text{OpType}(i, \kappa(i)) = j \} \} \\
\alpha_6 &= \{ \{ ((R(\text{OpVal}(i, \kappa(i))), R(i)), i) \mid \text{mode} = 0 \wedge P(i) \wedge \kappa(i) \neq 0 \wedge \\
&\quad \text{Inst}(i, \kappa(i)) = \text{STORE} \wedge \text{OpType}(i, \kappa(i)) = \uparrow j \} \} \\
\alpha_7 &= \{ \{ \text{Inst}(i, \kappa(i)) = \text{READ} \mid \text{mode} = 0 \wedge P(i) \wedge \kappa(i) \neq 0 \} \} \\
\alpha_8 &= \{ \{ \text{Inst}(i, \kappa(i)) = \text{STORE} \mid \text{mode} = 0 \wedge P(i) \wedge \kappa(i) \neq 0 \} \} \\
\alpha_9 &= \{ \{ \kappa(i) \neq 0 \mid P(i) \wedge \kappa(i) \neq 0 \} \} \\
&\quad \vdots \\
\alpha_n &= \{ \{ (0, i) \mid \text{mode} = 0 \wedge P(i) \wedge \kappa(i) \neq 0 \wedge \text{Inst}(i, \kappa(i)) = \text{HALT} \} \} \\
\alpha_{n+1} &= \{ \{ \text{Inst}(i, \kappa(i)) = \text{HALT} \mid \text{mode} = 0 \wedge P(i) \wedge \kappa(i) \neq 0 \} \} \\
\alpha_{n+2} &= \{ \{ 1 \mid \text{mode} = 0 \} \} \\
\alpha_{n+3} &= \{ \{ \text{mode} = 0 \mid \text{true} \} \} \\
\alpha_{n+4} &= \{ \{ (\text{second}(W(i)), \text{first}(W(i))) \mid \text{mode} = 1 \wedge W(i) \neq \text{undef} \wedge \\
&\quad \{ \{ x \mid \text{first}(W(x)) = \text{first}(W(i)) \wedge x < i \} = \emptyset \} \} \} \\
\alpha_{n+5} &= \{ \{ (\text{undef}, i) \mid \text{mode} = 1 \wedge W(i) \neq \text{undef} \} \} \\
\alpha_{n+6} &= \{ \{ \{ \{ x \mid \text{first}(W(x)) = \text{first}(W(i)) \wedge x < i \} = \emptyset \mid \text{mode} = 1 \wedge W(i) \neq \text{undef} \} \} \} \\
\alpha_{n+7} &= \{ \{ 0 \mid \text{mode} = 1 \} \} \\
\alpha_{n+8} &= \{ \{ \text{mode} = 1 \mid \text{true} \} \} \\
\alpha_{n+9} &= \{ \{ \text{true} \mid \text{true} \} \}
\end{aligned}$$

The set of witness terms additionally includes the terms obtained by replacing  $P(i)$  by its negation in each of the witness terms  $\alpha_1, \dots, \alpha_{n+1}$  and also the terms obtained by replacing  $W(i) \neq \text{undef}$  by its negation in each of the witness terms  $\alpha_{n+4}, \dots, \alpha_{n+6}$ .

### 6.3. Alternating Turing machines

An *alternating Turing machine* is a variation of the nondeterministic Turing machine whose set of control states  $Q$  is divided into four classes  $Q_{\exists}$ ,  $Q_{\forall}$ ,  $Q_{acc}$  and  $Q_{rej}$ . Thus there are existential, universal, accepting and rejecting states. The notion of acceptance is defined by induction on the computation tree. The alternating Turing machine in a given configuration  $c$  *accepts* iff  $c$  is in a final accepting state, or  $c$  is in an existential state and at least one of its children in the computation tree accepts, or  $c$  is in a universal state, it has at least one child in the computation tree, and all its children in the computation tree accept. Note that an alternating machine all of whose non-final control states are existential, is essentially a nondeterministic Turing machine.

We begin our description of alternating Turing machines as a parallel algorithm which satisfies our postulates, by describing the states of computation of the algorithm. They include, in addition to the requirements of the background postulate, the following:

- Unary bridge functions  $\Gamma$ ,  $Q_{\exists}$ ,  $Q_{\forall}$ ,  $Q_{acc}$  and  $Q_{rej}$  which are Boolean valued and evaluate to `true` only for those elements that are symbols in the tape alphabet (which includes a symbol “\_” for blank) and control states in the classes of existential, universal, accepting and rejecting states, respectively.
- A unary bridge function `config` which maps nodes in the computation tree to configurations. Elements that do not correspond to nodes in the computation tree are mapped to `undef`. A *configuration* is a string in  $\Gamma^* \cdot Q \cdot \Gamma^*$  that specifies the content of the tape, the state, and the position of the head as follows. Let the tape contain symbols  $w_n, w_{n+1}, \dots, w_{m-1}, w_m$  where  $w_i \in \Gamma$  is the symbol on the  $i$ -th position of the tape and  $n < m$ . Assume that the read/write head is in position  $n \leq j \leq m$  and  $n$  and  $m$  are such that for all  $n' < n$ , and  $m' > m$ ,  $w_n = w_m = \_$  (the blank symbol). If the machine is in control state  $q$ , we denote this configuration by  $w_n \dots w_{j-1}, q, w_j \dots w_m$ .
- A unary bridge function `active` which evaluates to `true` for an element  $v$  if `config(v) ≠ undef` (i.e.  $v$  is a node of the computation tree) and  $v$  is computing (i.e., has not spawned sub-computations yet), to `undef` if `config(v) = undef`, and to `false` otherwise.

- A unary bridge function `value` which evaluates to `true` for an element  $v$  if  $v$  is an accepting node in the computation tree, to `false` if  $v$  is a rejecting node, and to `undef` if the value of  $v$  has not been established (by the algorithm) yet or  $v$  is not a node.
- A bridge function  $\delta$  that represents the transition relation  $\delta \subseteq Q \times \Gamma \times Q \times \Gamma \times \{L, R\}$  of the alternating Turing Machine.
- A binary, Boolean valued function `parent`( $x, y$ ) which belongs to the primary (finite) part and evaluates to `true` iff  $x$  is the parent node of  $y$  in the computation tree.
- Unary functions `state` and `read` which belong to the secondary part and map each configuration to the current state and symbol (in the position of the read/write head), respectively.
- A function `nextConf` of arity 4 in the secondary part which maps a given configuration  $c$ , state  $q$ , symbol  $a$  and movement  $m$  to the configuration obtained by replacing the state in  $c$  by  $q$ , the symbol in the current position of the read/write head by  $a$ , and updating the position of the head one cell to the left ( $m = L$ ) or to the right ( $m = R$ ).

---

**Algorithm 3** Alternating Turing machines.<sup>4</sup>


---

```

for all  $x$  with config( $x$ )  $\neq$  undef do
  if active( $x$ ) then
    if  $Q_{acc}(\text{state}(\text{config}(x))) \wedge \text{value}(x) = \text{undef}$  then
      value( $x$ ) := true endif
    if  $Q_{rej}(\text{state}(\text{config}(x))) \wedge \text{value}(x) = \text{undef}$  then
      value( $x$ ) := false endif
    if  $Q_{\exists}(\text{state}(\text{config}(x))) \vee Q_{\forall}(\text{state}(\text{config}(x)))$  then
      for all  $q, a, m$  with  $\delta(\text{state}(\text{config}(x)), \text{read}(\text{config}(x)), q, a, m)$  do
        import  $c$  do
          active( $c$ ) := true
          config( $c$ ) := nextConfig( $x, q, a, m$ )
          value( $c$ ) := undef
          parent( $x, c$ ) := true
        enddo
      end for
      active( $x$ ) := false
    end if
  end if
  if  $\neg \text{active}(x)$  then
    if  $Q_{\exists}(\text{state}(\text{config}(x)))$  then
      if  $\exists y(\text{parent}(x, y) \wedge \text{value}(y) = \text{true})$  then value( $x$ ) := true endif
      if  $\forall y(\text{parent}(x, y) \wedge \text{value}(y) = \text{false})$  then value( $x$ ) := false endif
    end if
    if  $Q_{\forall}(\text{state}(\text{config}(x)))$  then
      if  $\exists y(\text{parent}(x, y) \wedge \forall y(\text{parent}(x, y) \wedge \text{value}(y) = \text{true}))$  then
        value( $x$ ) := true endif
      if  $\exists y(\text{parent}(x, y) \wedge \text{value}(y) = \text{false})$  then value( $x$ ) := false endif
    end if
  end if
end for

```

---

The base set of the (finite) primary part of each meta-finite state includes a finite set of control states  $Q = Q_{\exists} \cup Q_{\forall} \cup Q_{acc} \cup Q_{rej}$ , a finite set of tape symbols  $\Gamma$ , a finite set of nodes of the computation tree and two distinguished elements  $L$  and  $R$ . The secondary part includes (in addition to the elements in the primary part) all possible configurations (finite strings) in  $\Gamma^* \cdot Q \cdot \Gamma^*$ . The initial states are those in which the computation tree is just a single node  $v$  which is mapped via `config` to an initial configuration, `value`( $v$ ) is undefined and `active`( $v$ ) is true. An initial configuration is represented by a string  $q_0 \cdot s$  where  $s \in (\Gamma - \{\_ \})^*$ , that is, the control state is  $q_0$ , the read/write head points to the first position of  $s$ , and the tape contains  $s$  preceded and followed by countably many blank cells. Apart from `active`, `config`, `value`, `parent` and `reserve` (see the background postulate) which are dynamic functions, all the others are static.

The transition function is defined by Algorithm 3. Note that, during each step of the computation of an alternating Turing machine, new nodes are added to the computation tree. We handle this situation by importing new elements from the reserve following the schema in Section 3.3 and using the construct “**import**  $x$  **do**  $P$ ”. By extending the language with this construct, reserve elements will be chosen for all combinations of the values  $x$  such that  $x$  is in the scope of any rule having import as a sub-rule. This construct with the corresponding semantics will be made explicit and addressed in full details elsewhere. In this example we simply assume that every state of computation has a function `import` which uniformly

---

<sup>4</sup> We have intentionally omitted the par blocks so that the algorithm fits in one page. Sequences of instructions at a same level are implicitly assumed to be executed in parallel.

(through all possible states of computation) maps tuples of values to reserve elements. Thus, the bounded exploration witness is formed by the following witness terms:

$$\begin{aligned}
\alpha_1 &= \{ \{ (\text{true}, x) \mid \text{config}(x) \neq \text{undef} \wedge \text{active}(x) \wedge \\
&\quad Q_{acc}(\text{state}(\text{config}(x))) \wedge \text{value}(x) = \text{undef} \} \} \\
\alpha_2 &= \{ \{ (\text{false}, x) \mid \text{config}(x) \neq \text{undef} \wedge \text{active}(x) \wedge \\
&\quad Q_{rej}(\text{state}(\text{config}(x))) \wedge \text{value}(x) = \text{undef} \} \} \\
\alpha_3 &= \{ \{ (\text{true}, \text{import}((x, q, a, m))) \mid \text{config}(x) \neq \text{undef} \wedge \text{active}(x) \wedge \\
&\quad (Q_{\exists}(\text{state}(\text{config}(x))) \vee Q_{\forall}(\text{state}(\text{config}(x)))) \wedge \\
&\quad \delta(\text{state}(\text{config}(x)), \text{read}(\text{config}(x)), q, a, m) \} \} \\
\alpha_4 &= \{ \{ (\text{nextConfig}(x, q, a, m), \text{import}((x, q, a, m))) \mid \text{config}(x) \neq \text{undef} \wedge \\
&\quad \text{active}(x) \wedge (Q_{\exists}(\text{state}(\text{config}(x))) \vee Q_{\forall}(\text{state}(\text{config}(x)))) \wedge \\
&\quad \delta(\text{state}(\text{config}(x)), \text{read}(\text{config}(x)), q, a, m) \} \} \\
\alpha_5 &= \{ \{ (\text{undef}, \text{import}((x, q, a, m))) \mid \text{config}(x) \neq \text{undef} \wedge \text{active}(x) \wedge \\
&\quad (Q_{\exists}(\text{state}(\text{config}(x))) \vee Q_{\forall}(\text{state}(\text{config}(x)))) \wedge \\
&\quad \delta(\text{state}(\text{config}(x)), \text{read}(\text{config}(x)), q, a, m) \} \} \\
\alpha_6 &= \{ \{ (\text{true}, x, \text{import}((x, q, a, m))) \mid \text{config}(x) \neq \text{undef} \wedge \text{active}(x) \wedge \\
&\quad (Q_{\exists}(\text{state}(\text{config}(x))) \vee Q_{\forall}(\text{state}(\text{config}(x)))) \wedge \\
&\quad \delta(\text{state}(\text{config}(x)), \text{read}(\text{config}(x)), q, a, m) \} \} \\
\alpha_7 &= \{ \{ (\text{false}, x) \mid \text{config}(x) \neq \text{undef} \wedge \text{active}(x) \wedge \\
&\quad (Q_{\exists}(\text{state}(\text{config}(x))) \vee Q_{\forall}(\text{state}(\text{config}(x)))) \} \} \\
\alpha_8 &= \{ \{ (\text{true}, x) \mid \text{config}(x) \neq \text{undef} \wedge \neg \text{active}(x) \wedge \\
&\quad Q_{\exists}(\text{state}(\text{config}(x))) \wedge \exists y(\text{parent}(x, y) \wedge \text{value}(y) = \text{true}) \} \} \\
\alpha_9 &= \{ \{ (\text{false}, x) \mid \text{config}(x) \neq \text{undef} \wedge \neg \text{active}(x) \wedge \\
&\quad Q_{\exists}(\text{state}(\text{config}(x))) \wedge \forall y(\text{parent}(x, y) \wedge \text{value}(y) = \text{false}) \} \} \\
\alpha_{10} &= \{ \{ (\text{true}, x) \mid \text{config}(x) \neq \text{undef} \wedge \neg \text{active}(x) \wedge \\
&\quad Q_{\forall}(\text{state}(\text{config}(x))) \wedge \exists y(\text{parent}(x, y)) \wedge \\
&\quad \forall y(\text{parent}(x, y) \wedge \text{value}(y) = \text{true}) \} \} \\
\alpha_{11} &= \{ \{ (\text{false}, x) \mid \text{config}(x) \neq \text{undef} \wedge \neg \text{active}(x) \wedge \\
&\quad Q_{\forall}(\text{state}(\text{config}(x))) \wedge \exists y(\text{parent}(x, y) \wedge \text{value}(y) = \text{false}) \} \} \\
\alpha_{12} &= \{ \{ \text{active}(x) \mid \text{config}(x) \neq \text{undef} \} \} \\
\alpha_{13} &= \{ \{ \text{true} \mid \text{active}(x) \wedge \text{config}(x) \neq \text{undef} \} \} \\
\alpha_{14} &= \{ \{ Q_{acc}(\text{state}(\text{config}(x))) \wedge \text{value}(x) = \text{undef} \mid \text{active}(x) \wedge \\
&\quad \text{config}(x) \neq \text{undef} \} \} \\
\alpha_{15} &= \{ \{ Q_{rej}(\text{state}(\text{config}(x))) \wedge \text{value}(x) = \text{undef} \mid \text{active}(x) \wedge \\
&\quad \text{config}(x) \neq \text{undef} \} \} \\
\alpha_{16} &= \{ \{ (Q_{\exists}(\text{state}(\text{config}(x))) \vee Q_{\forall}(\text{state}(\text{config}(x)))) \mid \text{active}(x) \wedge \\
&\quad \text{config}(x) \neq \text{undef} \} \} \\
\alpha_{17} &= \{ \{ \neg \text{active}(x) \mid \text{config}(x) \neq \text{undef} \} \} \\
\alpha_{18} &= \{ \{ Q_{\exists}(\text{state}(\text{config}(x))) \mid \neg \text{active}(x) \wedge \text{config}(x) \neq \text{undef} \} \} \\
\alpha_{19} &= \{ \{ Q_{\forall}(\text{state}(\text{config}(x))) \mid \neg \text{active}(x) \wedge \text{config}(x) \neq \text{undef} \} \}
\end{aligned}$$

$$\alpha_{20} = \{\{\exists y(\text{parent}(x, y) \wedge \text{value}(y) = \text{true}) \mid Q_{\exists}(\text{state}(\text{config}(x)) \wedge \neg \text{active}(x) \wedge \text{config}(x) \neq \text{undef})\}$$

$$\alpha_{21} = \{\{\forall y(\text{parent}(x, y) \wedge \text{value}(y) = \text{false}) \mid Q_{\exists}(\text{state}(\text{config}(x)) \wedge \neg \text{active}(x) \wedge \text{config}(x) \neq \text{undef})\}$$

$$\alpha_{22} = \{\{\exists y(\text{parent}(x, y) \wedge \forall y(\text{parent}(x, y) \wedge \text{value}(y) = \text{true}) \mid Q_{\forall}(\text{state}(\text{config}(x)) \wedge \neg \text{active}(x) \wedge \text{config}(x) \neq \text{undef})\}$$

$$\alpha_{23} = \{\{\exists y(\text{parent}(x, y) \wedge \text{value}(y) = \text{false}) \mid Q_{\forall}(\text{state}(\text{config}(x)) \wedge \neg \text{active}(x) \wedge \text{config}(x) \neq \text{undef})\}$$

$$\alpha_{24} = \{\{\text{true} \mid \text{true}\}$$

The set of witness terms additionally includes the terms  $\alpha'_3 - \alpha'_6$  obtained by replacing  $\delta(\text{state}(\text{config}(x)), \text{read}(\text{config}(x)), q, a, m)$  by its negation in  $\alpha_3 - \alpha_6$  and also terms obtained by replacing  $\text{config}(x) \neq \text{undef}$  in each of the witness terms  $\alpha_1, \dots, \alpha_{23}$  and  $\alpha'_3 - \alpha'_6$ .

## 7. The characterization theorem

This section is devoted to prove the key characterization theorem of our parallel ASM thesis, which states that for every parallel algorithm there is a behaviourally equivalent parallel ASM. We start by defining the necessary concepts and proving the central lemmata. Our proof follows the same schema as the proof of the characterization theorem for sequential algorithms in [2]. Of course, from a technical perspective the proof is considerably more challenging since we have to deal with witness sets formed by multiset comprehension terms instead of simple ground terms.

Throughout this section we fix a bounded exploration witness  $W$  for a parallel algorithm  $A$ , and without loss of generality we assume that  $W$  is closed under subterms in the following sense: if  $\{\{t \mid \varphi\} \in W$ , then also  $\{\{t' \mid \exists x_1, \dots, x_k \varphi\} \in W$ , where  $t'$  is a subterm of  $t$  and  $\{x_1, \dots, x_k\} = \text{free}(\varphi) - (t')$ .

The proof strategy is as follows. We first define (in Subsection 7.1) the concept of critical structure. The intuition is that the *critical structure*  $\mathbf{S}|_W$  is the finite part of the state of computation  $\mathbf{S}$  which can be accessed with the set  $W$  of witness terms. The arguments of locations that have to be updated by  $A$  in  $\mathbf{S}$  as well as their new content are all elements of  $\mathbf{S}_W$ . We call these elements *critical values*. The purpose of the critical structure is to capture the interrelationships in  $\mathbf{S}$  among critical values.

At this point the proof requires some recourse to methods from finite model theory. More precisely, we use the model theoretical concept of *type of a tuple* to show that if a *critical tuple*  $\bar{a}$  defines an update in the update set  $\Delta$  yielded by  $A$  in  $\mathbf{S}$ , then every other tuple which has the same type as  $\bar{a}$  in the critical structure  $\mathbf{S}_W$ , also defines an update in  $\Delta$ . Intuitively this means that the algorithm  $A$  cannot distinguish among critical tuples  $\bar{a}$  and  $\bar{b}$  if they have the same type in  $\mathbf{S}_W$ , and thus it cannot produce an update corresponding to the tuple  $\bar{a}$  without also producing the update corresponding to the tuple  $\bar{b}$  and vice versa. The model theoretical fundamentals and lemmata required for this part of the characterization proof are presented in Subsections 7.2 and 7.3. The technical details in these subsections are relatively complex and use advanced concepts and techniques from finite model theory. If the reader is not familiar with the area, we recommend to skip them during a first reading of the proof. The key Lemma 7.5 regarding indistinguishable updates is presented in Subsection 7.4.

In Section 7.5 we again use methods from finite model theory to show that for every critical tuple  $\bar{a}$  in  $\mathbf{S}$  we can write a Boolean term  $t_{\chi}^{\bar{a}}$  which isolates the type of  $\bar{a}$  in the sense that every tuple  $\bar{b}$  which satisfies  $t_{\chi}^{\bar{a}}$  has exactly the same type as  $\bar{a}$ , and thus it is indistinguishable from  $\bar{a}$  by the algorithm  $A$ .

The characterization proof is finalized in Subsection 7.6. From this point on, we follow closely the strategy of the characterization proof of the sequential ASM thesis. We first use the Boolean terms of the form  $t_{\chi}^{\bar{a}}$  to produce for each tuple  $\bar{a} \in \Delta$  a corresponding parallel ASM rule of the form:

**forall**  $x_0, x_1, \dots, x_r$  **with**  $t_{\chi}^{\bar{a}}(x_0, x_1, \dots, x_r)$  **do**  $f(x_1, \dots, x_r) := x_0$  **enddo**

The rule  $r_{A,W}^{\mathbf{S}}$  obtained by taking the parallel composition of this finite set of rules yields on  $\mathbf{S}$  the same update set  $\Delta$  as the algorithm  $A$ . The following lemmas are devoted to show that if an state  $\mathbf{S}'$  is  $W$ -similar to  $\mathbf{S}$  in the precise sense of Definition 7.9, then the rule  $r_{A,W}^{\mathbf{S}}$ , when evaluated in  $\mathbf{S}'$ , produces the correct (according to the algorithm  $A$ ) set of updates. The fact that there is a finite number of classes of  $W$ -similar structures together with the  $r_{A,W}^{\mathbf{S}}$  rules give us the key for proving the main characterization theorem, i.e., we can show that there is a finite parallel ASM rule which corresponds to the transition function  $\tau_A$  of  $A$ .

### 7.1. Critical structures

A first consequence of the postulates, more specifically of the bounded exploration postulate, is that the values that appear in the updates that have to be made to a state  $\mathbf{I}$  in order to obtain the successor state  $\tau_A(\mathbf{I})$ , are restricted to those values which can be accessed through witness terms.

**Definition 7.1** (*Critical Values*). Let  $W$  be a bounded exploration witness set for a parallel algorithm  $A$  and let  $\mathbf{S}$  be a state of computation of  $A$ . We define the set  $V_{\mathbf{S},W}$  of *critical values* of  $\mathbf{S}$  w.r.t.  $W$  as  $\bigcup_{\alpha_i \in W} V_{\mathbf{S},\alpha_i}$  where

$$V_{\mathbf{S},\alpha_i} = \{a_i \mid \bar{a} \in \text{vals}(\alpha_i) \text{ and } a_i \text{ occurs in } \bar{a}\}.$$

A *critical tuple* is a tuple  $(a_0, \dots, a_r)$ , where each  $a_i$  is a critical value.

**Lemma 7.1.** Let  $\mathbf{I}$  be a state of a parallel algorithm  $A$  and let  $\mathbf{S}$  be a corresponding state of computation. If  $(f, (a_1, \dots, a_r), a_0)$  is an update in  $\tau_A(\mathbf{I}) - \mathbf{I}$  and  $W$  is a parallel exploration witness for  $A$ , then  $(a_0, a_1, \dots, a_r)$  is a critical tuple in  $(V_{\mathbf{S},W})^{r+1}$ .

**Proof.** Assume that  $(a_0, a_1, \dots, a_r) \notin (V_{\mathbf{S},W})^{r+1}$ . Then, for some  $1 \leq i \leq r$ , we have that  $a_i \notin V_{\mathbf{S},W}$ . Let  $\mathbf{S}'$  be the state of computation isomorphic to  $\mathbf{S}$  obtained by replacing  $a_i$  in  $\mathbf{S}$  by a fresh element  $b \notin S$  and let  $\mathbf{I}'$  be the state of  $A$  isomorphic to  $\mathbf{I}$  obtained by replacing  $a_i$  in  $\mathbf{I}$  by  $b$ . By the abstract state postulate, it is clear that  $\mathbf{I}'$  is a state of  $A$ . Further,  $\mathbf{S}'$  is a state of computation that corresponds to  $\mathbf{I}'$ . By our assumption that  $a_i \notin V_{\mathbf{S},W}$  and by construction of  $\mathbf{S}'$ , we have that  $\text{vals}_{\mathbf{S}'}(\alpha_j) = \text{vals}_{\mathbf{S}}(\alpha_j)$  for every witness term  $\alpha_j \in W$ . Thus  $\mathbf{S}$  and  $\mathbf{S}'$  coincide over  $W$  and, by the parallel bounded exploration postulate, the update sets  $\tau_A(\mathbf{I}') - \mathbf{I}'$  and  $\tau_A(\mathbf{I}) - \mathbf{I}$  also coincide. Then  $(f(a_1, \dots, a_r), a_0)$  is in  $\tau_A(\mathbf{I}') - \mathbf{I}'$  as well. But  $a_i$  is not in  $\mathbf{I}'$ , and by the (inalterable base set part of) the abstract state postulate,  $a_i$  is not in the base set of  $\tau_A(\mathbf{I}')$  either. Thus it cannot occur in  $\tau_A(\mathbf{I}') - \mathbf{I}'$ , which gives us the desired contradiction.  $\square$

We define next a purely relational and finite structure  $\mathbf{S}|_W$ , which captures the part of a state of computation  $\mathbf{S}$  which can be accessed with a set  $W$  of witness terms.

**Definition 7.2** (*Critical Structure*). Let  $A$  be a parallel algorithm, let  $\mathbf{I}$  be a state of  $A$ , let  $\mathbf{S}$  be a state of computation that corresponds to  $\mathbf{I}$  and let  $W = \{\alpha_1, \dots, \alpha_m\}$  be a set of witness terms. We define a purely relational and finite structure  $\mathbf{S}|_W$  (which we call *critical (sub) structure* of  $\mathbf{S}$ ) of vocabulary  $\Sigma_W = \{R_{\alpha_1}, \dots, R_{\alpha_m}\}$  where for  $1 \leq i \leq m$  and  $\alpha_i = \{(t_0, \dots, t_n) \mid \varphi_i(x_1, \dots, x_r)\}$ , the relation symbol  $R_{\alpha_i}$  has arity  $n+2$  and the following interpretation:

$$\begin{aligned} R_{\alpha_i}^{\mathbf{S}|_W} &= \{(b_0, \dots, b_n, i \cdot b_0 \cdots b_n \cdot a_1 \cdots a_r) \mid (a_1, \dots, a_r) \in I^{r_i}, \\ &\quad \mathbf{S} \models \varphi_i(x_1, \dots, x_r)[a_1, \dots, a_r] \text{ and} \\ &\quad \text{vals}_{\mathbf{S}, \mu[x_1 \mapsto a_1, \dots, x_r \mapsto a_r]}(t_0) = b_0, \dots, \text{vals}_{\mathbf{S}, \mu[x_1 \mapsto a_1, \dots, x_r \mapsto a_r]}(t_n) = b_n\}, \end{aligned}$$

where  $i \cdot b_0 \cdots b_n \cdot a_1 \cdots a_r$  denotes the string obtained by concatenating  $i, b_0, \dots, b_n, a_1, \dots, a_r$ . An element  $a_i$  belongs to the domain  $\mathbf{S}|_W$  of  $\mathbf{S}|_W$  iff for some  $\alpha_i \in W$  there is a  $\bar{a} \in R_{\alpha_i}^{\mathbf{S}|_W}(\bar{a})$  such that  $a_i$  appears in  $\bar{a}$ .

In the case of critical structures, we do *not* assume the existence of an equality relation since we do not want to include anything outside of what is prescribed by the witness set. The strings of the form  $i \cdot b_0 \cdots b_n \cdot a_1 \cdots a_r$  have the sole purpose of encoding the multiplicities of the elements in the multiset resulting from the evaluation of  $\alpha_i$  in  $\mathbf{S}$ , again without including anything outside of what is prescribed by the witness set.

### 7.2. Types

We can now restrict ourselves to consider the properties of tuples which are definable in a given logic over *finite relational structures*. For this, we use the model-theoretic concept of type.

**Definition 7.3.** Let  $\mathcal{L}$  be a logic, let  $\mathbf{A}$  be a relational structure of vocabulary  $\Sigma$ , and let  $\bar{a} = (a_1, \dots, a_k)$  be a  $k$ -tuple over  $\mathbf{A}$ . The  $\mathcal{L}$ -type of  $\bar{a}$  in  $\mathbf{A}$ , denoted as  $tp_{\mathbf{A}}^{\mathcal{L}}(\bar{a})$ , is the set  $\mathcal{L}[\Sigma]$  of formulas in  $\mathcal{L}$  of vocabulary  $\Sigma$  with free variables among  $\{x_1, \dots, x_k\}$  which are satisfied in  $\mathbf{A}$  by any variable assignments assigning for  $1 \leq i \leq k$  the  $i$ -th component of  $\bar{a}$  to the variable  $x_i$ , i.e.

$$tp_{\mathbf{A}}^{\mathcal{L}}(\bar{a}) = \{\varphi \in \mathcal{L}[\Sigma] : \text{free}(\varphi) \subseteq \{x_1, \dots, x_k\} \text{ and } \mathbf{A} \models \varphi[a_1, \dots, a_k]\}.$$

Note that, the  $\mathcal{L}$ -type of a given tuple  $\bar{a}$  over a relational structure  $\mathbf{A}$ , includes not only the properties of all sub-tuples of  $\bar{a}$ , but also the set of all sentences in  $\mathcal{L}$  which are true when evaluated on  $\mathbf{A}$ .

In particular, we are interested in the properties of tuples which are definable in first-order logic with and without equality (denoted FO and FO<sub>wo=</sub>, respectively), i.e., we are interested in FO-types and FO<sub>wo=</sub>-types, respectively. FO-types are also known as isomorphism types since every tuple can be characterized up to isomorphism by its FO-type. FO<sub>wo=</sub>-types correspond to a (weaker) type of equivalence relation among tuples (see [20]). Instead of the partial isomorphism condition used in the Ehrenfeucht–Fraïssé characterization of FO equivalence, the Ehrenfeucht–Fraïssé characterization of FO<sub>wo=</sub> equivalence involves the following condition.

**Definition 7.4.** Let **A** and **B** be relational structures of some vocabulary  $\Sigma$ . A relation  $p \subseteq A \times B$  is a *partial relativeness correspondence* iff for every  $n$ -ary relation symbol  $R \in \Sigma$  and every  $(a_1, b_1), \dots, (a_n, b_n) \in p$ ,

$$(a_1, \dots, a_n) \in R^{\mathbf{A}} \quad \text{iff} \quad (b_1, \dots, b_n) \in R^{\mathbf{B}}.$$

**Definition 7.5.** Let **A** and **B** be relational structures of the same vocabulary. **A** and **B** are *m-finitely relative* via  $(I_k)_{k \leq m}$  (denoted as  $(I_k)_{k \leq m} : \mathbf{A} \sim_m \mathbf{B}$ ) iff the following holds:

- i. Every  $I_k$  is a nonempty set of partial relativeness correspondences.
- ii. For any  $k+1 \leq m$ , any  $p \in I_{k+1}$  and any  $a \in A$ , there are  $b \in B$  and  $q \in I_k$  such that  $q \supseteq p$  and  $(a, b) \in q$  (forth condition).
- iii. For any  $k+1 \leq m$ , any  $p \in I_{k+1}$  and any  $b \in B$ , there are  $a \in A$  and  $q \in I_k$  such that  $q \supseteq p$  and  $(a, b) \in q$  (back condition).

The following result is an immediate consequence of [20, Prop. 4.5 and Thm. 4.6].

**Theorem 7.2.** Let **A** and **B** be relational structures of some vocabulary  $\Sigma$ . For every  $r \geq 0$ ,  $r$ -tuples  $\bar{a} = (a_1, \dots, a_r) \in A^r$  and  $\bar{b} = (b_1, \dots, b_r) \in B^r$ , and  $p = \{(a_1, b_1), \dots, (a_r, b_r)\}$ , the following holds:

- i. There is a sequence  $(I_k)_{k \leq m}$  such that  $(I_k)_{k \leq m} : \mathbf{A} \sim_m \mathbf{B}$  and  $p \in I_m$  iff for every equality-free formula  $\varphi$  of quantifier rank up to  $m$  with at most  $r$  distinct free variables,  $\mathbf{B} \models \varphi[\bar{b}]$  just in case  $\mathbf{A} \models \varphi[\bar{a}]$ .
- ii. For every  $m \geq 0$  there is a sequence  $(I_k)_{k \leq m}$  such that  $(I_k)_{k \leq m} : \mathbf{A} \sim_m \mathbf{B}$  and  $p \in I_m$  iff for every equality-free formula  $\varphi$  with at most  $r$  distinct free variables,  $\mathbf{B} \models \varphi[\bar{b}]$  just in case  $\mathbf{A} \models \varphi[\bar{a}]$ .

### 7.3. Indistinguishable updates

We want to show that if  $\bar{a}$  is a critical tuple that defines an update  $((f, (a_1, \dots, a_r)), a_0)$  in some update set of the parallel algorithm  $A$  and  $\bar{b}$  has the same  $\mathcal{L}$ -type over the critical structure of  $A$ , then also  $\bar{b}$  is a critical tuple that defines an update  $((f, (b_1, \dots, b_r)), b_0)$  in the same update set. This will lead to our Lemma 7.5. For the proof it will turn out to be convenient, if there exists an isomorphism that takes  $\bar{a}$  to  $\bar{b}$ . However, this cannot always be guaranteed. Therefore, in this subsection we will show how the general case can be reduced to the specific case assuming such an isomorphism, and the latter case will be handled in the next subsection.

Thus, for every parallel algorithm  $A$  we define next a modified parallel algorithm  $A^*$  by means of a bijection from the states of  $A$  to the states of  $A^*$ . Then we prove that this modified version  $A^*$  of  $A$  satisfies the properties that are required for the proof of Lemma 7.5 – the key lemma in the characterization proof.

**Definition 7.6.** For each state  $I_i$  of a parallel algorithm  $A$ , let  $I_i^*$  denote a corresponding state of vocabulary  $\Sigma^* = \{g_i \mid f_i \in \Sigma\} \cup \{h\}$  such that:

- The base set of  $I_i^*$  is the disjoint union of  $I_i$  with the positive natural numbers  $\mathbb{N}^+$ .
- $h^{I_i^*}$  is a static function that is a bijection from  $I_i$  to  $\mathbb{N}^+$ .
- For every  $r$ -ary function  $g_j \in \Sigma^*$  and every  $(n+1)$ -ary tuple  $(c_0, c_1, \dots, c_n)$  in  $(I_i^*)^{n+1}$ ,

$$g_j^{I_i^*}(c_1, \dots, c_n) = \begin{cases} c_0 & \text{if there is a } (d_0, d_1, \dots, d_n) \in (I_i)^{n+1} \\ & \text{such that } f_j^{I_i}(d_1, \dots, d_n) = d_0 \text{ and} \\ & c_i = \text{prime}(i+1)^{h(d_i)} \text{ for } 0 \leq i \leq n; \\ \text{false} & \text{if the previous condition does not hold and} \\ & f \text{ is marked as relational;} \\ \text{undef} & \text{otherwise.} \end{cases}$$

Here,  $\text{prime}(i)$  denotes the  $i$ -th prime number in the sequence of primes.

We define  $A^*$  as the parallel algorithm with set of states  $\mathcal{S}_{A^*} = \{I_i^* \mid I_i \in \mathcal{S}_A\}$ , set of initial states  $\mathcal{I}_{A^*} = \{I_i^* \mid I_i \in \mathcal{I}_A\}$  and transition function  $\tau_{A^*}$  such that for every  $I_i^*, I_j^* \in \mathcal{S}_{A^*}$  it holds that:

- i. If the base sets of  $\mathbf{I}_i^*$  and  $\mathbf{I}_j^*$  coincide, then  $h^{\mathbf{I}_i^*} = h^{\mathbf{I}_j^*}$ .
- ii.  $\tau_{A^*}(\mathbf{I}_i^*) = \mathbf{I}_j^*$  iff  $\tau_A(\mathbf{I}_i) = \mathbf{I}_j$ .

**Definition 7.7.** Let  $t$  be a term of vocabulary  $\Sigma$ . We define  $t^*$  as the term of vocabulary  $\Sigma^*$  obtained from  $t$  as follows:

- If  $t$  is a nullary function symbol  $f_i \in \Sigma$ , then  $t^*$  is  $g_i$ .
- If  $t$  is a variable  $x_i \in V$ , then  $t^*$  is  $2^{h(x_i)}$ .
- If  $t$  is of the form  $f_i(t_1, \dots, t_r)$  where  $f_i \in \Sigma$ ,  $\text{arity}(f_i) = r$  and  $t_1, \dots, t_r$  are terms, then  $t^*$  is  $g_i(\text{prime}(2)^{\log_2(t_1^*)}, \dots, \text{prime}(r+1)^{\log_2(t_r^*)})$ .
- If  $t(\bar{y})$  is a multiset comprehension term of the form  $\{\{s(\bar{x}, \bar{y}) \mid \varphi(\bar{x}, \bar{y})\}\}_{\bar{y}}$ , then  $t^*$  is  $2^{h(\|\{h^{-1}(\log_2(s^*(\bar{x}, \bar{y}))\})\|_{h^{-1}(\log_2(\varphi^*(\bar{x}, \bar{y}))\})\}_{\bar{y}}})$ .

**Lemma 7.3.** Let  $\mathbf{S}$  be a state of computation of vocabulary  $\Sigma$ , let  $\alpha$  be a term of vocabulary  $\Sigma$ , let  $\alpha^*$  be the corresponding term of vocabulary  $\Sigma^*$  as per Definition 7.7 and let  $\mu$  be a variable assignment over the primary part of  $\mathbf{S}$ . We have that  $\text{vals}_{\mathbf{S}, \mu}(\alpha) = a$  iff  $\text{vals}_{\mathbf{S}^*, \mu}(\alpha^*) = 2^{h(a)}$ .

**Proof.** We proceed by induction on  $\alpha$ .

- If  $\alpha$  is a nullary function symbol  $f_i \in \Sigma$ , then  $\text{vals}_{\mathbf{S}, \mu}(f_i) = f_i^{\mathbf{S}}$  and  $\text{vals}_{\mathbf{S}^*, \mu}(\alpha^*) = g_i^{\mathbf{S}^*}$ , and by Definition 7.6,  $f_i^{\mathbf{S}} = a$  iff  $g_i^{\mathbf{S}^*} = 2^{h(a)}$ .
- If  $\alpha$  is a variable  $x_i$ , then  $\text{vals}_{\mathbf{S}, \mu}(x_i) = \mu(x_i)$  and  $\text{vals}_{\mathbf{S}^*, \mu}(\alpha^*) = 2^{h(\mu(x_i))}$ , and clearly,  $\mu(x_i) = a$  iff  $2^{h(\mu(x_i))} = 2^{h(a)}$ .
- If  $\alpha$  is of the form  $f_i(t_1, \dots, t_r)$  where  $f_i$  is an  $r$ -ary function symbol in  $\Sigma$  and  $t_1, \dots, t_r$  are terms of vocabulary  $\Sigma$ , then by induction hypothesis  $\text{vals}_{\mathbf{S}, \mu}(t_i) = a_i$  iff  $\text{vals}_{\mathbf{S}^*, \mu}(t_i^*) = 2^{h(a_i)}$  for every  $1 \leq i \leq r$ . Thus, by Definition 7.7 and Definition 7.6, we get that  $\text{vals}_{\mathbf{S}, \mu}(\alpha) = f_i^{\mathbf{S}}(a_1, \dots, a_r) = a$  iff  $\text{vals}_{\mathbf{S}^*, \mu}(\alpha^*) = g_i^{\mathbf{S}^*}(\text{prime}(2)^{\log_2(2^{h(a_1)})}, \dots, \text{prime}(r+1)^{\log_2(2^{h(a_r)})}) = 2^{h(a)}$ .
- If  $\alpha$  is of the form  $\{\{s(\bar{x}, \bar{y}) \mid \varphi(\bar{x}, \bar{y})\}\}_{\bar{y}}$  where  $\bar{x} = (x_1, \dots, x_n)$  and  $\bar{y} = (y_1, \dots, y_m)$ , then for every  $\bar{b} \in S^n$  it holds by induction hypothesis that  $\text{val}_{\mathbf{S}, \mu[\bar{x} \mapsto \bar{b}]}(s(\bar{x}, \bar{y})) = a_i$  and  $\text{val}_{\mathbf{S}, \mu[\bar{x} \mapsto \bar{b}]}(\varphi(\bar{x}, \bar{y})) = a_j$  iff  $\text{val}_{\mathbf{S}^*, \mu[\bar{x} \mapsto \bar{b}]}(s^*(\bar{x}, \bar{y})) = 2^{h(a_i)}$  and  $\text{val}_{\mathbf{S}^*, \mu[\bar{x} \mapsto \bar{b}]}(\varphi^*(\bar{x}, \bar{y})) = 2^{h(a_j)}$ . Thus  $\text{vals}_{\mathbf{S}, \mu}(\alpha) = a$  iff  $\text{vals}_{\mathbf{S}^*, \mu}(\{\{h^{-1}(\log_2(s^*(\bar{x}, \bar{y}))) \mid h^{-1}(\log_2(\varphi^*(\bar{x}, \bar{y})))\}\}_{\bar{y}}) = a$  iff  $\text{vals}_{\mathbf{S}^*, \mu}(\alpha^*) = 2^{h(a)}$ .  $\square$

**Lemma 7.4.** Let  $A$  be a parallel algorithm and  $W$  be a bounded exploration witness for  $A$ . The following holds:

- i. For every  $\mathbf{I}_i \in S_A$  and every  $f_i \in \Sigma$ ,

$$(f_i, (d_1, \dots, d_n), d_0) \in \tau_A(\mathbf{I}_i) - \mathbf{I}_i \quad \text{iff}$$

$$(g_i, (\text{prime}(2)^{h(d_1)}, \dots, \text{prime}(n+1)^{h(d_n)}), \text{prime}(1)^{h(d_0)}) \in \tau_{A^*}(\mathbf{I}_i^*) - \mathbf{I}_i^*.$$

- ii. The set  $W^* = \{\alpha_i^* \mid \alpha_i \in W\}$  of witness terms is a bounded exploration witness for the modified parallel algorithm  $A^*$ .

**Proof.** Let  $\tau_A(\mathbf{I}_i) = \mathbf{I}_j$ . Since  $(f_i, (d_1, \dots, d_n), d_0) \in \tau_A(\mathbf{I}_i) - \mathbf{I}_i$ , we know that  $f_i^{1j}(d_1, \dots, d_n) = d_0$  and  $f_i^{1i}(d_1, \dots, d_n) \neq d_0$ . Then, by Definition 7.6 we get that  $g_i^{1j}(\text{prime}(2)^{h(d_1)}, \dots, \text{prime}(n+1)^{h(d_n)}) = \text{prime}(1)^{h(d_0)}$  and that  $g_i^{1i}(\text{prime}(2)^{h(d_1)}, \dots, \text{prime}(n+1)^{h(d_n)}) \neq \text{prime}(1)^{h(d_0)}$ . It follows that,  $(g_i, (\text{prime}(2)^{h(d_1)}, \dots, \text{prime}(n+1)^{h(d_n)}), \text{prime}(1)^{h(d_0)}) \in \tau_{A^*}(\mathbf{I}_i^*) - \mathbf{I}_i^*$ . The same argument can be used to prove the other direction of (i).

Regarding (ii.), we proceed by contradiction. Assume that  $\mathbf{I}_1^*$  and  $\mathbf{I}_2^*$  are states of  $A^*$  and that  $\mathbf{S}_1^*$  and  $\mathbf{S}_2^*$  are states of computation corresponding to  $\mathbf{I}_1^*$  and  $\mathbf{I}_2^*$ , respectively, such that  $\mathbf{S}_1^*$  and  $\mathbf{S}_2^*$  coincide on  $W^*$  and  $\tau_{A^*}(\mathbf{I}_1^*) - \mathbf{I}_1^* \neq \tau_{A^*}(\mathbf{I}_2^*) - \mathbf{I}_2^*$ . Since  $\mathbf{S}_1^*$  and  $\mathbf{S}_2^*$  coincide on  $W^*$ , it follows from Lemma 7.3 and the construction of  $W^*$  from  $W$  that  $\mathbf{S}_1$  and  $\mathbf{S}_2$  coincide on  $W$ . Given that  $W$  is a bounded exploration witness for  $A$ , it follows from the bounded exploration postulate that  $\tau_A(\mathbf{I}_1) - \mathbf{I}_1 = \tau_A(\mathbf{I}_2) - \mathbf{I}_2$ . But then, by condition (ii) in Definition 7.6, we get that also  $\tau_{A^*}(\mathbf{I}_1^*) - \mathbf{I}_1^* = \tau_{A^*}(\mathbf{I}_2^*) - \mathbf{I}_2^*$  which contradicts our assumption.  $\square$

#### 7.4. A key lemma

The following key lemma shows that updates composed by tuples of elements that share a same  $\text{FO}_{w_0=}$ -type (in a critical structure) are indistinguishable (by the algorithm) from one another. This implies that if the corresponding tuples of elements in two different updates to a same dynamic function share the same  $\text{FO}_{w_0=}$ -type, then either both updates belong to the update set or neither of them does.

**Lemma 7.5.** Let  $A$  be a parallel algorithm, let  $\mathbf{I}$  be a state of  $A$ , let  $\mathbf{S}$  be a corresponding state of computation, let  $(f, (a_1, \dots, a_r), a_0) \in \tau_A(\mathbf{I}) - \mathbf{I}$ , let  $\bar{a} = (a_0, \dots, a_r)$  and let  $W$  be a parallel bounded exploration witness for  $A$ . For every  $(r + 1)$ -tuple of critical values  $\bar{b} = (b_0, \dots, b_r) \in (Vs, W)^{r+1}$ , if  $tp_{\mathbf{S}|W}^{\text{FOwo}}(\bar{b}) = tp_{\mathbf{S}|W}^{\text{FOwo}}(\bar{a})$  then  $(f, (b_1, \dots, b_r), b_0)$  also belongs to  $\tau_A(\mathbf{I}) - \mathbf{I}$ .

**Proof.** By contradiction. Assume that  $(f, (b_1, \dots, b_r), b_0) \notin \tau_A(\mathbf{I}) - \mathbf{I}$ . Let  $\mathbf{I}^*$  be the state of the modified parallel algorithm  $A^*$  which corresponds to the state  $\mathbf{I}$  of  $A$  (see Definition 7.6). Let  $\mathbf{J}^*$  be the state isomorphic to  $\mathbf{I}^*$  induced by the automorphism  $\zeta$  of  $\mathbf{I}^*$  such that  $\zeta(x) = \text{prime}(i + 1)^{h(b_i)}$  if  $x$  is  $\text{prime}(i + 1)^{h(a_i)}$  for some  $0 \leq i \leq r$ ,  $\zeta(x) = \text{prime}(i + 1)^{h(a_i)}$  if  $x$  is  $\text{prime}(i + 1)^{h(b_i)}$  for some  $0 \leq i \leq r$ , and  $\zeta(x) = x$  otherwise.

By the abstract state postulate,  $\mathbf{J}^*$  is also a state of  $A^*$ . Since by part (i) of Lemma 7.4

$$(g, (\text{prime}(2)^{h(a_1)}, \dots, \text{prime}(r + 1)^{h(a_r)}), \text{prime}(1)^{h(a_0)}) \in \tau_{A^*}(\mathbf{I}^*) - \mathbf{I}^*,$$

we get by the isomorphism  $\zeta$  that

$$(g, (\text{prime}(2)^{h(b_1)}, \dots, \text{prime}(r + 1)^{h(b_r)}), \text{prime}(1)^{h(b_0)}) \in \tau_{A^*}(\mathbf{J}^*) - \mathbf{J}^*.$$

Let  $\mathbf{S}_{\mathbf{I}^*}$  and  $\mathbf{S}_{\mathbf{J}^*}$  be states of computation of  $A^*$  corresponding to  $\mathbf{I}^*$  and  $\mathbf{J}^*$ , respectively. We claim that  $\mathbf{S}_{\mathbf{I}^*}$  and  $\mathbf{S}_{\mathbf{J}^*}$  coincide on  $W^*$ , i.e., that  $\text{vals}_{\mathbf{S}_{\mathbf{I}^*}}(\alpha_i) = \text{vals}_{\mathbf{S}_{\mathbf{J}^*}}(\alpha_i)$  for every  $\alpha_i \in W^*$ . Then, by part (ii) of Lemma 7.4 and the parallel bounded exploration postulate, we get that  $\tau_{A^*}(\mathbf{I}^*) - \mathbf{I}^* = \tau_{A^*}(\mathbf{J}^*) - \mathbf{J}^*$ . But then also

$$(f, (\text{prime}(2)^{h(b_1)}, \dots, \text{prime}(r + 1)^{h(b_r)}), \text{prime}(1)^{h(b_0)}) \in \tau_{A^*}(\mathbf{I}^*) - \mathbf{I}^*.$$

Consequently,  $(f, (b_1, \dots, b_r), b_0) \in \tau_A(\mathbf{I}) - \mathbf{I}$  (by the other direction of part (i) of Lemma 7.4) which gives us the desired contradiction.

To finalize the proof, we need to show that our claim holds, i.e., that  $\mathbf{S}_{\mathbf{I}^*}$  and  $\mathbf{S}_{\mathbf{J}^*}$  coincide on  $W^*$ .

From the characterization in Theorem 7.2 and the fact that  $tp_{\mathbf{S}|W}^{\text{FOwo}}(\bar{b}) = tp_{\mathbf{S}|W}^{\text{FOwo}}(\bar{a})$ , we get that for every  $m \geq 0$ , there is a sequence of partial relativeness correspondences  $(I_k)_{k \leq m} : \mathbf{S}|_W \sim_m \mathbf{S}|_W$  with  $\{(a_0, b_0), \dots, (a_r, b_r)\} \in I_m$ . Thus for every  $k \leq m$ , every  $p_i \in I_k$ , every  $n$ -ary relation symbol  $R$  in the relational vocabulary of  $\mathbf{S}|_W$  and every  $(c_1, d_1), \dots, (c_n, d_n) \in p_i$ , it holds that  $(c_1, \dots, c_n) \in R^{\mathbf{S}|_W}$  iff  $(d_1, \dots, d_n) \in R^{\mathbf{S}|_W}$ . By construction of  $\mathbf{S}_{\mathbf{I}^*}|_{W^*}$  from  $\mathbf{S}_{\mathbf{I}^*}$  and by part (i) of Lemma 7.4, this implies that there is an  $x$  such that for every  $y$  the following equation (1) holds.

$$\begin{aligned} (\text{prime}(1)^{h(c_1)}, \dots, \text{prime}(n - 1)^{h(c_{n-1})}, x) \in R^{\mathbf{S}_{\mathbf{I}^*}|_{W^*}} \\ \text{iff} \\ (\text{prime}(1)^{h(d_1)}, \dots, \text{prime}(n - 1)^{h(d_{n-1})}, y) \in R^{\mathbf{S}_{\mathbf{I}^*}|_{W^*}}. \end{aligned} \tag{1}$$

For the same reason, we also have that there is a  $y$  such that for every  $x$  equation (1) again holds. Also by construction of  $\mathbf{S}_{\mathbf{I}^*}|_{W^*}$ , for every  $c'$  and  $d'$  such that

$$\begin{aligned} (\text{prime}(1)^{h(c_1)}, \dots, \text{prime}(n - 1)^{h(c_{n-1})}, c') \in R^{\mathbf{S}_{\mathbf{I}^*}|_{W^*}} \text{ and} \\ (\text{prime}(1)^{h(d_1)}, \dots, \text{prime}(n - 1)^{h(d_{n-1})}, d') \in R^{\mathbf{S}_{\mathbf{I}^*}|_{W^*}}, \end{aligned}$$

we have that

$$\{(\text{prime}(1)^{h(c_1)}, \text{prime}(1)^{h(d_1)}), \dots, (\text{prime}(n)^{h(c_n)}, \text{prime}(n)^{h(d_n)}), (c', d')\}$$

is a partial function which defines a partial automorphism on  $\mathbf{S}_{\mathbf{I}^*}|_{W^*}$ . Clearly, this means that for every  $(I_k)_{k \leq m} : \mathbf{S}|_W \sim_m \mathbf{S}|_W$  with  $\{(a_0, b_0), \dots, (a_r, b_r)\} \in I_m$  and  $m \geq 0$  we can build a sequence  $I_0^*, \dots, I_m^*$  of partial automorphisms on  $\mathbf{S}_{\mathbf{I}^*}|_{W^*}$  which have the back and forth properties and such that

$$\{(\text{prime}(1)^{h(a_0)}, \text{prime}(1)^{h(b_0)}), \dots, (\text{prime}(r + 1)^{h(a_r)}, \text{prime}(r + 1)^{h(b_r)})\} \in I_m^*.$$

Thus by the classical characterization of first-order logic in terms of sequences of partial isomorphisms, we get that  $tp_{\mathbf{S}_{\mathbf{I}^*}|_{W^*}}^{\text{FO}}(\bar{b}^*) = tp_{\mathbf{S}_{\mathbf{I}^*}|_{W^*}}^{\text{FO}}(\bar{a}^*)$  for  $\bar{b}^* = (\text{prime}(1)^{h(b_0)}, \dots, \text{prime}(r + 1)^{h(b_r)})$  and  $\bar{a}^* = (\text{prime}(1)^{h(a_0)}, \dots, \text{prime}(r + 1)^{h(a_r)})$ .

Now, we proceed by contradiction. Let us assume that there is an

$$\alpha_i = \{(t_0, \dots, t_n) \mid \varphi(x_1, \dots, x_m)\} \in W^* \text{ such that } \text{vals}_{\mathbf{S}_{\mathbf{I}^*}}(\alpha_i) \neq \text{vals}_{\mathbf{S}_{\mathbf{J}^*}}(\alpha_i).$$

Then there is a tuple  $\bar{c} = (c_0, \dots, c_n) \in (S_{\mathbf{I}^*})^{n+1}$  (and therefore also in  $(S_{\mathbf{J}^*})^{n+1}$ ) such that either

$$\text{Mult}(\bar{c}, \text{vals}_{\mathbf{S}_{\mathbf{I}^*}}(\alpha_i)) > \text{Mult}(\bar{c}, \text{vals}_{\mathbf{S}_{\mathbf{J}^*}}(\alpha_i)) \text{ or}$$

$$\text{Mult}(\bar{c}, \text{vals}_{\mathbf{S}_{\mathbf{I}^*}}(\alpha_i)) < \text{Mult}(\bar{c}, \text{vals}_{\mathbf{S}_{\mathbf{J}^*}}(\alpha_i)).$$

Let us assume that  $\text{Mult}(\bar{c}, \text{vals}_{\mathbf{S}_{\mathbf{I}^*}}(\alpha_i)) > \text{Mult}(\bar{c}, \text{vals}_{\mathbf{S}_{\mathbf{J}^*}}(\alpha_i))$  and define:

$$\begin{aligned}
A = & \{(d_1, \dots, d_m) \in (\mathbf{S}_{\mathbf{I}^*})^m \mid \mathbf{S}_{\mathbf{I}^*} \models \varphi(x_1, \dots, x_m)[d_1, \dots, d_m] \text{ and} \\
& \text{vals}_{\mathbf{S}_{\mathbf{I}^*}, \mu[x_1 \mapsto d_1, \dots, x_m \mapsto d_m]}(t_0) = c_0, \dots, \text{vals}_{\mathbf{S}_{\mathbf{I}^*}, \mu[x_1 \mapsto d_1, \dots, x_m \mapsto d_m]}(t_n) = c_n\}. \\
B = & \{(d_1, \dots, d_m) \in (\mathbf{S}_{\mathbf{J}^*})^m \mid \mathbf{S}_{\mathbf{J}^*} \models \varphi(x_1, \dots, x_m)[d_1, \dots, d_m] \text{ and} \\
& \text{vals}_{\mathbf{S}_{\mathbf{J}^*}, \mu[x_1 \mapsto d_1, \dots, x_m \mapsto d_m]}(t_0) = c_0, \dots, \text{vals}_{\mathbf{S}_{\mathbf{J}^*}, \mu[x_1 \mapsto d_1, \dots, x_m \mapsto d_m]}(t_n) = c_n\}.
\end{aligned}$$

Since  $|A| > |B|$  and  $\mathbf{S}_{\mathbf{I}^*} \simeq \mathbf{S}_{\mathbf{J}^*}$ , there must be some tuple  $(d_1, \dots, d_m) \in A$  such that  $(\zeta(d_1), \dots, \zeta(d_m)) \notin B$ . Furthermore, since

$$\mathbf{S}_{\mathbf{I}^*} \models \varphi(x_1, \dots, x_m)[d_1, \dots, d_m] \text{ iff } \mathbf{S}_{\mathbf{J}^*} \models \varphi(x_1, \dots, x_m)[\zeta(d_1), \dots, \zeta(d_m)],$$

it must hold that

$$\begin{aligned}
& (\text{vals}_{\mathbf{S}_{\mathbf{I}^*}, \mu[x_1 \mapsto d_1, \dots, x_m \mapsto d_m]}(t_0), \dots, \text{vals}_{\mathbf{S}_{\mathbf{I}^*}, \mu[x_1 \mapsto d_1, \dots, x_m \mapsto d_m]}(t_n)) = \bar{c} \neq \zeta(\bar{c}) = \\
& (\text{vals}_{\mathbf{S}_{\mathbf{J}^*}, \mu[x_1 \mapsto \zeta(d_1), \dots, x_m \mapsto \zeta(d_m)]}(t_0), \dots, \text{vals}_{\mathbf{S}_{\mathbf{J}^*}, \mu[x_1 \mapsto \zeta(d_1), \dots, x_m \mapsto \zeta(d_m)]}(t_n)).
\end{aligned}$$

Then, since  $\zeta$  is the identity function on the set of elements which do not appear in  $\bar{a}^*$  or  $\bar{b}^*$ , we know that there is at least one  $c_i$  that appears in  $\bar{a}^*$  or  $\bar{b}^*$  and such that  $\zeta(c_i) \neq c_i$ . Let us assume, again w.l.o.g., that this is the case for exactly one  $c_i$  and that  $c_i = c_0 = a_0^* = \text{prime}(1)^{h(a_0)}$ . Also let

$$\begin{aligned}
\psi(y_0, \dots, y_n) \equiv & \exists \bar{z}_1 \dots \bar{z}_{|A|} \left( \bigwedge_{1 \leq j < k \leq |A|} \bar{z}_j \neq \bar{z}_k \wedge \right. \\
& \bigwedge_{1 \leq j \leq |A|} (\varphi[\bar{z}_j] \wedge t_0[\bar{z}_j] = y_0 \wedge \dots \wedge t_n[\bar{z}_j] = y_n) \wedge \\
& \left. \neg \exists \bar{z}' \left( \bigwedge_{1 \leq j \leq |A|} \bar{z}' \neq \bar{z}_j \wedge \varphi[\bar{z}'] \wedge t_0[\bar{z}'] = y_0 \wedge \dots \wedge t_n[\bar{z}'] = y_n \right) \right),
\end{aligned}$$

where for  $z_j = (z_{j1}, \dots, z_{jm})$  we use  $\varphi[\bar{z}_j]$  and  $t_0[\bar{z}_j], \dots, t_n[\bar{z}_j]$  to denote the formula and the terms obtained by replacing in  $\varphi$  and  $t_0, \dots, t_n$ , respectively, every occurrence of a variable  $x_i \in \{x_1, \dots, x_m\}$  by  $z_{ji}$ . Likewise, we use  $\bar{z}_j \neq \bar{z}_k$  to denote the formula  $\neg(z_{j1} = z_{k1} \wedge \dots \wedge z_{jm} = z_{km})$ .

It follows that

$$\mathbf{S}_{\mathbf{I}^*} \models \psi(y_0, \dots, y_n)[a_0^*, c_1, \dots, c_n] \text{ and } \mathbf{S}_{\mathbf{J}^*} \not\models \psi(y_0, \dots, y_n)[a_0^*, c_1, \dots, c_n],$$

and since  $\zeta^{-1}(a_0^*) = b_0^* = \text{prime}(1)^{h(b_0)}$ , we get that

$$\mathbf{S}_{\mathbf{I}^*} \not\models \psi(y_0, \dots, y_n)[b_0^*, \zeta^{-1}(c_1), \dots, \zeta^{-1}(c_n)].$$

But then, for

$$\begin{aligned}
\psi'(y_0, \dots, y_n) \equiv & \exists z_1 \dots z_{|A|} \left( \bigwedge_{1 \leq j < k \leq |A|} z_j \neq z_k \wedge \bigwedge_{1 \leq j \leq |A|} R_{\alpha_i}(y_0, \dots, y_n, z_j) \wedge \right. \\
& \left. \neg \exists z' \left( \bigwedge_{1 \leq j \leq |A|} z' \neq z_j \wedge R_{\alpha_i}(y_0, \dots, y_n, z') \right) \right),
\end{aligned}$$

we get that

$$\begin{aligned}
\mathbf{S}_{\mathbf{I}^*} \upharpoonright_{W^*} \models & \psi'(y_0, \dots, y_n)[a_0^*, c_1, \dots, c_n] \text{ and} \\
\mathbf{S}_{\mathbf{I}^*} \upharpoonright_{W^*} \not\models & \psi'(y_0, \dots, y_n)[b_0^*, \zeta^{-1}(c_1), \dots, \zeta^{-1}(c_n)].
\end{aligned}$$

This contradicts the fact that  $tp_{\mathbf{S}_{\mathbf{I}^*} \upharpoonright_{W^*}}^{\text{FO}}(\bar{b}^*) = tp_{\mathbf{S}_{\mathbf{I}^*} \upharpoonright_{W^*}}^{\text{FO}}(\bar{a}^*)$ . The same contradiction is obtained if we assume that  $\text{Mult}(\bar{c}, \text{vals}_{\mathbf{S}_{\mathbf{I}^*}}(\alpha_i)) < \text{Mult}(\bar{c}, \text{vals}_{\mathbf{S}_{\mathbf{J}^*}}(\alpha_i))$ . Thus we have that  $\text{Mult}(\bar{c}, \text{vals}_{\mathbf{S}_{\mathbf{I}^*}}(\alpha_i)) = \text{Mult}(\bar{c}, \text{vals}_{\mathbf{S}_{\mathbf{J}^*}}(\alpha_i))$  which contradicts our assumption that there is an  $\alpha_i \in W$  such that  $\text{vals}_{\mathbf{S}_{\mathbf{I}^*}}(\alpha_i) \neq \text{vals}_{\mathbf{S}_{\mathbf{J}^*}}(\alpha_i)$ .  $\square$

### 7.5. Isolating formulae

Although types are infinite sets of formulae, a single  $\text{FO}_{w_0=}$ -formula is equivalent to the  $\text{FO}_{w_0=}$ -type of a tuple over a given finite relational structure. The equivalence holds for all finite relational structures of the same schema.

**Lemma 7.6 (Isolating Formulae).** *For every relational vocabulary  $\Sigma$  with no constants, for every finite structure  $\mathbf{A}$  of vocabulary  $\Sigma$ , for every  $r \geq 0$ , and for every  $r$ -tuple  $\bar{a}$  over  $\mathbf{A}$ , there is a formula  $\chi \in tp_{\mathbf{A}}^{\text{FO}_{w_0=}}(\bar{a})$  such that for any finite relational structure  $\mathbf{B}$  of vocabulary  $\Sigma$  and for every  $r$ -tuple  $\bar{b}$  over  $\mathbf{B}$ ,  $\mathbf{B} \models \chi[\bar{b}]$  iff  $tp_{\mathbf{A}}^{\text{FO}_{w_0=}}(\bar{a}) = tp_{\mathbf{B}}^{\text{FO}_{w_0=}}(\bar{b})$ .*

**Proof.** We define for every  $m \in \mathbb{N}$ , a formula  $\varphi_a^m$  with free variables  $\bar{x} = (x_1, \dots, x_r)$  and such that  $\mathbf{A} \models \varphi_a^m[\bar{a}]$ , which characterizes  $\bar{a}$  completely up to equivalence on  $\text{FO}_{\text{wo}=\}$  formulae with quantifier rank  $\leq m$ . The  $\varphi_a^m$  are defined by induction as follows:

$$\varphi_a^0(\bar{x}) \equiv \bigwedge \{ \varphi(\bar{x}) \mid \varphi \text{ is an equality free atomic or negated atomic formula such that } \mathbf{A} \models \varphi[\bar{a}] \}$$

$$\varphi_a^{m+1}(\bar{x}) \equiv \bigwedge_{a \in A} \exists x_{r+1} (\varphi_{aa}^m(\bar{x}, x_{r+1})) \wedge \tag{2}$$

$$\forall x_{r+1} \left( \bigvee_{a \in A} \varphi_{aa}^m(\bar{x}, x_{r+1}) \right). \tag{3}$$

We prove first that

$$\mathbf{B} \models \varphi_a^m[\bar{b}] \text{ iff there is a sequence } (I_k)_{k \leq m} \text{ such that} \tag{4}$$

$$(I_k)_{k \leq m} : \mathbf{A} \sim_m \mathbf{B} \text{ and } p = \{(a_1, b_1), \dots, (a_r, b_r)\} \in I_m.$$

The existence of  $(I_k)_{k \leq m} : \mathbf{A} \sim_m \mathbf{B}$  with  $p \in I_m$  implies by part (i) of [Theorem 7.2](#) that, for every equality-free formula  $\varphi$  of quantifier rank  $\leq m$ ,  $\mathbf{B} \models \varphi[b_1, \dots, b_r]$  iff  $\mathbf{A} \models \varphi[a_1, \dots, a_r]$ . Since the quantifier rank of  $\varphi_a^m$  is  $m$  and  $\mathbf{A} \models \varphi_a^m[\bar{a}]$  (by construction), we get that  $\mathbf{B} \models \varphi_a^m[\bar{b}]$ .

The converse can be proven by induction on  $m$  as follows:

- Basis ( $m = 0$ ): Since  $\mathbf{B} \models \varphi_a^0[b_1, \dots, b_r]$ ,  $p = \{(a_1, b_1), \dots, (a_r, b_r)\}$  is a partial reliveness correspondence. Thus  $I_0 = \{p\}$  is a nonempty set of partial reliveness correspondences, even if  $\bar{a} = ()$  (which means that  $p$  is the empty relation since  $\Sigma$  has no constants).

- Induction step ( $m + 1$ ):

Since  $\mathbf{B} \models \varphi_a^{m+1}[\bar{b}]$ , we know the following:

- For every  $a \in A$ , there is a  $b \in B$  such that  $\mathbf{B} \models \varphi_{aa}^m[\bar{b}b]$  (by part (2) in the definition of  $\varphi_a^{m+1}$ ).
- For every  $b \in B$ , there is an  $a \in A$  such that  $\mathbf{B} \models \varphi_{aa}^m[\bar{b}b]$  (by part (3) in the definition of  $\varphi_a^{m+1}$ ).

Let  $I_{m+1} = \{p\}$ . Thus by the induction hypothesis, the following holds:

- For every  $a \in A$ , there is a  $b \in B$  and a sequence  $(I_k^{\bar{a}a})_{k \leq m}$  such that  $(I_k^{\bar{a}a})_{k \leq m} : \mathbf{A} \sim_m \mathbf{B}$  and  $p \cup \{(a, b)\} \in I_m^{\bar{a}a}$ .
- For every  $b \in B$ , there is an  $a \in A$  and a sequence  $(I_k^{\bar{b}b})_{k \leq m}$  such that  $(I_k^{\bar{b}b})_{k \leq m} : \mathbf{A} \sim_m \mathbf{B}$  and  $p \cup \{(a, b)\} \in I_m^{\bar{b}b}$ .

Let  $I_j = \bigcup_{a \in A} I_j^{\bar{a}a} \cup \bigcup_{b \in B} I_j^{\bar{b}b}$  (for  $0 \leq j \leq m$ ). Note that, in general,  $m$ -finite reliveness is preserved under this type of element-wise union. Thus we only need to check that the back and forth conditions hold for  $I_{m+1}$  and  $I_m$ , i.e., we need to check the following:

- For every  $a \in A$  there are  $b \in B$  and  $q \in I_m$  such that  $q \supseteq p$  and  $(a, b) \in q$  (forth condition).
- For every  $b \in B$  there are  $a \in A$  and  $q \in I_m$  such that  $q \supseteq p$  and  $(a, b) \in q$  (back condition).

These properties follow from parts (2) and (3) in the definition of  $\varphi_a^{m+1}$ , respectively.

Let  $\bar{c} \in A^n$  for some  $n \geq 0$ . Let  $X_c^m = \{\bar{d} \in A^n \mid \mathbf{A} \models \varphi_c^m[\bar{d}]\}$ . Since  $X_c^m \supseteq X_c^{m+1}$  for every  $m \geq 0$  and  $\mathbf{A}$  is a finite structure, then there must be an  $m^{\bar{c}}$  such that  $X_c^{m^{\bar{c}}} = X_c^m$  for every  $m > m^{\bar{c}}$ . Let  $m^*$  be the maximum  $m^{\bar{c}}$  in  $\{m^{\bar{c}} \mid \bar{c} \in A^{\leq |\mathcal{P}(A \times A)|}\}$  (here  $A^{\leq |\mathcal{P}(A \times A)|}$  denotes the set of tuples of length  $\leq |\mathcal{P}(A \times A)|$ ). Note that there is at most  $|\mathcal{P}(A \times A)|$  partial reliveness correspondences on  $\mathbf{A}$ , which implies that we do not need to consider tuples of length  $> |\mathcal{P}(A \times A)|$  since any extension of a tuple of length  $|\mathcal{P}(A \times A)|$  would correspond to a partial reliveness correspondence already covered by some tuple of length  $|\mathcal{P}(A \times A)|$ . Assume w.l.g. that the length of  $\bar{a}$  is  $\leq |\mathcal{P}(A \times A)|$ . We define the formula  $\chi$  as follows:

$$\chi(\bar{x}) \equiv \varphi_a^{m^*}(\bar{x}) \wedge \bigwedge_{\bar{c} \in A^{\leq |\mathcal{P}(A \times A)|}} \forall \bar{y} (\varphi_c^{m^*}(\bar{y}) \rightarrow \varphi_c^{m^*+1}(\bar{y})) \tag{5}$$

In the previous formula we clearly abuse the notation since  $\bar{y}$  does not have a fixed length. We assume that, for each  $\bar{c} \in A^{\leq |\mathcal{P}(A \times A)|}$ , the length of  $\bar{y}$  in the corresponding conjunct is equal to the length of  $\bar{c}$ .

Finally, we show the following:

$$\mathbf{B} \models \chi[\bar{b}] \text{ iff } tp_{\mathbf{A}}^{\text{FO}_{\text{wo}=\}}(\bar{a}) = tp_{\mathbf{B}}^{\text{FO}_{\text{wo}=\}}(\bar{b}).$$

We need to check that if  $\mathbf{B} \models \chi[\bar{b}]$  then  $tp_{\mathbf{A}}^{\text{FO}_{\text{wo}=\}}(\bar{a}) = tp_{\mathbf{B}}^{\text{FO}_{\text{wo}=\}}(\bar{b})$ . The other direction is immediate.

$$\text{Let } R = \{ \{(c_1, d_1), \dots, (c_l, d_l)\} \mid (c_1, \dots, c_l) \in A^{\leq |\mathcal{P}(A \times B)|}, \\ (d_1, \dots, d_l) \in B^{\leq |\mathcal{P}(A \times B)|} \}$$

$$\mathbf{B} \models \varphi_{c_1 \dots c_l}^{m^*+1} [d_1, \dots, d_l]$$

Since  $\mathbf{B} \models \chi[\bar{b}]$  and  $\bar{a} \in A^{\leq |\mathcal{P}(A \times B)|}$ , we have that  $\mathbf{B} \models \varphi_{\bar{a}}^{m^*+1}[\bar{b}]$  and thus that the set  $R$  is not empty. It follows from (4) that for each  $f \in R$ , there is a sequence  $(I_k^f)_{k \leq m^*+1}$  such that  $(I_k^f)_{k \leq m^*+1} : \mathbf{A} \sim_{m^*+1} \mathbf{B}$  and  $f \in I_{m^*+1}^f$ .

Let  $(I_k)_{k \leq m^*+n}$  ( $n \geq 1$ ) be the sequence where  $I_k = \bigcup_{f \in R} I_k^f$  for  $k \leq m^*+1$  and  $I_k = I_{m^*+1}$  for  $k > m^*+1$ . We claim that, for every  $n \geq 1$ , it holds that  $(I_k)_{k \leq m^*+n} : \mathbf{A} \sim_{m^*+n} \mathbf{B}$  and  $p \in I_{m^*+n}$ . We prove it for  $n=2$ , the rest then follows.

By definition we know that  $p \in I_{m^*+2}$  and that every  $I_k$  is a nonempty set of partial relativeness correspondences. We show that the back and forth conditions hold for  $I_{m^*+2}$  and  $I_{m^*+1}$ . The rest then follows.

Regarding the forth condition, consider any  $f \in I_{m^*+2}$  and any  $c \in A$ . By definition  $f \in I_{m^*+1}$ . Since  $(I_k)_{k \leq m^*+1} : \mathbf{A} \sim_{m^*+1} \mathbf{B}$ , there is a  $g \in I_{m^*}$  such that  $f \subseteq g$  and  $c \in \text{dom}(g)$ . Let  $g = \{(c_1, d_1), \dots, (c_l, d_l)\}$ . Then, by the other direction of (4),  $\mathbf{B} \models \varphi_{c_1 \dots c_l}^{m^*} [d_1, \dots, d_l]$ . Therefore, by the implication in (5),  $\mathbf{B} \models \varphi_{c_1 \dots c_l}^{m^*+1} [d_1, \dots, d_l]$  and so  $g \in R$ . Since  $g \in I_{m^*+1}^g$ , it follows that  $g \in I_{m^*+1}$ , which proves that the forth condition is met. The same argument can be used to prove that the back condition also holds.

The fact that  $(I_k)_{k \leq m^*+n} : \mathbf{A} \sim_{m^*+n} \mathbf{B}$  and  $p \in I_{m^*+n}$  for every  $n \geq 1$ , together with part (ii) of Theorem 7.2, allow us to conclude that  $tp_{\mathbf{A}}^{\text{FO}_{w_0=}}(\bar{a}) = tp_{\mathbf{B}}^{\text{FO}_{w_0=}}(\bar{b})$ .  $\square$

We say that the formula  $\chi$  in Lemma 7.6 isolates the  $tp_{\mathbf{A}}^{\text{FO}_{w_0=}}(\bar{a})$ .

Let  $\mathbf{A}$  be a finite structure. It is not difficult to see that if  $X_{\bar{a}_i}^m = X_{\bar{a}_i}^{m+1}$  for every  $\bar{a}_i \in A^{|\mathcal{P}(A \times A)|}$ , then  $X_{\bar{a}_i}^m = X_{\bar{a}_i}^{m+1}$  for every tuple  $\bar{a}_i$  of elements from  $A$ . Since the relation  $\bar{a}_j \in X_{\bar{a}_i}^m$  is an equivalence relation on tuples, the sets  $X_{\bar{a}_i}^m$  determine a partition of tuples of a given length. Given that there are  $|A|^{|\mathcal{P}(A \times A)|}$  tuples of length  $|\mathcal{P}(A \times A)|$ , we can derive the bound  $m^* \leq |A|^{|\mathcal{P}(A \times A)|}$ .

Given a formula  $\chi$  which isolates the  $\text{FO}_{w_0=}$ -type of a critical tuple  $\bar{a}$  in a critical structure  $\mathbf{S}|_W$ , we can write an equivalent term  $t_\chi$  which evaluates to true in  $\mathbf{S}$  only for those tuples which have the same  $\text{FO}_{w_0=}$ -type as  $\bar{a}$  in  $\mathbf{S}|_W$ .

**Lemma 7.7 (Isolating Terms).** *Let  $S$  be a state of computation of a parallel algorithm  $A$  of vocabulary  $\Sigma$ , let  $W$  be a bounded exploration witness for  $A$ , let  $\bar{a}$  be an  $r$ -tuple in  $(\mathbf{S}|_W)^r$  and let  $\chi$  be an isolating formula for the  $\text{FO}_{w_0=}$ -type of  $\bar{a}$  in  $\mathbf{S}|_W$ . Then there is a term  $t_\chi$  of vocabulary  $\Sigma$  such that, for every  $\bar{b} \in (V_{\mathbf{S}, W})^r$ , it holds that:*

$$\text{val}_{\mathbf{S}, \mu[\bar{x} \mapsto \bar{b}]}(t_\chi) = \text{true}^{\mathbf{S}} \quad \text{iff} \quad \mathbf{S}|_W \models \chi[\bar{b}].$$

**Proof.** We define for every  $\text{FO}_{w_0=}$ -formula  $\varphi$  of vocabulary  $\Sigma_W$ , a corresponding term  $t_\varphi$ .

- If  $\varphi(x_1, \dots, x_r, y)$  is an atomic formula of the form  $R_\alpha(x_1, \dots, x_r, y)$  where  $\alpha = \{(t_1, \dots, t_r) \mid \psi(y_1, \dots, y_k)\}$ , then  $t_\varphi(x_1, \dots, x_r, y_1, \dots, y_k)$  is  $t_1 = x_1 \wedge \dots \wedge t_r = x_r \wedge \psi(y_1, \dots, y_k)$ .
- If  $\varphi$  is a formula of the form  $\neg\psi$  or  $\psi \wedge \beta$ , then  $t_\varphi$  is  $\neg t_\psi$  or  $t_\psi \wedge t_\beta$ , respectively.
- If  $\varphi$  is a formula of the form  $\exists x(\psi(x))$  or  $\forall x(\psi(x))$ , then  $t_\varphi$  is the term  $\{(z_1, \dots, z_m) \mid t_{\text{dom}(z_1)} \wedge \dots \wedge t_{\text{dom}(z_m)} \wedge t_\psi(z_1, \dots, z_m)\} \neq \emptyset$  or  $\{(z_1, \dots, z_m) \mid \neg(t_{\text{dom}(z_1)} \wedge \dots \wedge t_{\text{dom}(z_m)}) \rightarrow t_\psi(z_1, \dots, z_m)\} = \emptyset$ , respectively, where  $z_1, \dots, z_m$  denote the free variables in  $t_\psi$  that correspond to  $x$  and

$$t_{\text{dom}(z_i)} \equiv \bigvee_{\{(t_1, \dots, t_r) \mid \psi(x_1, \dots, x_k)\} \in W} \left( \begin{array}{l} \{(x_1, \dots, x_k, y_1, \dots, y_r) \mid \\ \psi(x_1, \dots, x_k) \wedge t_1 = y_1 \wedge \\ \dots \wedge t_r = y_r \wedge (z_i = x_1 \vee \\ \dots \vee z_i = x_k \vee z_i = y_1 \vee \\ \dots \vee z_i = y_r)\}_{z_i} \neq \emptyset \end{array} \right).$$

It is an easy exercise to show by induction on  $\varphi$  that for every tuple  $\bar{b}$  of critical elements from  $V_{\mathbf{S}, W}$ ,  $\mathbf{S}|_W \models \varphi[\bar{b}]$  iff  $\text{val}_{\mathbf{S}, \mu[\bar{x} \mapsto \bar{b}]}(t_\varphi) = \text{true}^{\mathbf{S}}$ . The isolating formula  $\chi$  is just an instance of an  $\text{FO}_{w_0=}$ -formula of vocabulary  $\Sigma_W$ .  $\square$

## 7.6. Characterization

With these tools, we can now show that every update set produced by a parallel algorithm can be programmed by a transition rule of a parallel ASM.

**Definition 7.8.** For  $(f, (a_1, \dots, a_r), a_0) \in \tau_A(\mathbf{I}) - \mathbf{I}$ ,  $\mathbf{S}$  a state of computation corresponding to  $\mathbf{I}$  and  $W$  a parallel bounded exploration witness for  $A$ , let  $\chi^{\bar{a}}(x_0, x_1, \dots, x_r)$  be the isolating formula (in Lemma 7.6) for the  $\text{FO}_{w_0=}$ -type of the critical tuple  $\bar{a} = (a_0, a_1, \dots, a_r)$  in the critical structure  $\mathbf{S}|_{C_W}$  and let  $t_\chi^{\bar{a}}(x_0, x_1, \dots, x_r)$  be its corresponding isolating term (in Lemma 7.7). We define  $r_{A, W}^{\mathbf{S}}$  as the parallel combination of the following set of update rules:

$$P_A^S = \{\text{forall } x_0, x_1, \dots, x_r \text{ with } t_{\chi}^{\bar{a}}(x_0, x_1, \dots, x_r) \text{ do } f(x_1, \dots, x_r) := x_0 \mid \\ \bar{a} = (a_0, a_1, \dots, a_r) \in (S|_W)^{r+1} \text{ and } (f, (a_1, \dots, a_r), a_0) \in \tau_A(\mathbf{I}) - \mathbf{I}\}$$

**Corollary 7.8.** *If  $\mathbf{S}$  is a state of computation that corresponds to a state  $\mathbf{I}$  of a parallel algorithm  $A$  and  $W$  is a witness set for  $A$ , then  $\Delta(r_{A,W}^S, \mathbf{S}) = \tau_A(\mathbf{I}) - \mathbf{I}$ .*

**Proof.** Since  $\mathbf{S}|_W$  is finite and the vocabulary of  $\mathbf{S}$  has a finite number of function symbols of fixed arity, we get that the set  $P_A^S$  is finite too. By Lemma 7.1, we clearly have that  $\tau_A(\mathbf{I}) - \mathbf{I} \subseteq \Delta(r_{A,W}^S, \mathbf{S})$ . On the other hand, by the semantics of the assignment rule in Definition 5.1, we have that  $((f, (a_1, \dots, a_r)), a_0) \in \Delta(r_{A,W}^S, \mathbf{S})$  only if  $(a_0, a_1, \dots, a_r) \in I'$ . Thus by Lemma 7.5 we also have that  $\Delta(r_{A,W}^S, \mathbf{S}) \subseteq \tau_A(\mathbf{I}) - \mathbf{I}$ .  $\square$

Note that the rule  $r_{A,W}^S$  in Corollary 7.8 only involves critical terms that appear in the chosen bounded exploration witness  $W$ . This also implies that the rule is by no means uniquely determined.

For two different states  $\mathbf{S}$  and  $\mathbf{S}'$  of a parallel algorithm  $A$  with bounded exploration witness  $W$ , the rules  $r_{A,W}^S$  and  $r_{A,W}^{S'}$  can of course be quite different. Nevertheless, if  $\mathbf{S}$  and  $\mathbf{S}'$  coincide on  $W$ , then  $r_{A,W}^S$  and  $r_{A,W}^{S'}$  coincide.

**Lemma 7.9.** *Let  $\mathbf{I}$  and  $\mathbf{I}'$  be states of a parallel algorithm  $A$ , let  $W$  be a bounded exploration witness for  $A$  and let  $\mathbf{S}$  and  $\mathbf{S}'$  be states of computation of  $A$  that coincide on  $W$  and correspond to  $\mathbf{I}$  and  $\mathbf{I}'$ , respectively. Then  $\Delta(r_{A,W}^S, \mathbf{S}') = \tau_A(\mathbf{I}') - \mathbf{I}'$ .*

**Proof.** By Corollary 7.8, we get  $\Delta(r_{A,W}^{S'}, \mathbf{S}') = \tau_A(\mathbf{I}') - \mathbf{I}'$ . Since  $\mathbf{S}$  and  $\mathbf{S}'$  coincide on  $W$ , it follows that  $\tau_A(\mathbf{I}) - \mathbf{I} = \tau_A(\mathbf{I}') - \mathbf{I}'$  (by the bounded exploration postulate), and that  $\mathbf{S}|_W$  and  $\mathbf{S}'|_W$  are isomorphic by an isomorphism  $\zeta$  such that  $\zeta(a) = a$  for every critical value  $a \in V_{\mathbf{S}|_W} = V_{\mathbf{S}'|_W}$ . Hence, for every  $(f, (a_1, \dots, a_r), a_0) \in \tau_A(\mathbf{I}) - \mathbf{I}$ ,  $tp_{\mathbf{S}|_W}^{\text{FOwo}}((a_0, a_1, \dots, a_r)) = tp_{\mathbf{S}'|_W}^{\text{FOwo}}((a_0, a_1, \dots, a_r))$ . Thus,  $r_{A,W}^S = r_{A,W}^{S'}$  (by construction) and consequently  $\Delta(r_{A,W}^S, \mathbf{S}') = \Delta(r_{A,W}^{S'}, \mathbf{S}') = \tau_A(\mathbf{I}') - \mathbf{I}'$ .  $\square$

**Lemma 7.10.** *Let  $\mathbf{I}$ ,  $\mathbf{I}'$ , and  $\mathbf{I}''$  be states of a parallel algorithm  $A$ , let  $W$  be a bounded exploration witness for  $A$  and let  $\mathbf{S}$ ,  $\mathbf{S}'$ , and  $\mathbf{S}''$  be states of computation of  $A$  that correspond to  $\mathbf{I}$ ,  $\mathbf{I}'$ , and  $\mathbf{I}''$ , respectively. If  $\mathbf{S}' \simeq \mathbf{S}''$  and  $\Delta(r_{A,W}^S, \mathbf{S}'') = \tau_A(\mathbf{I}'') - \mathbf{I}''$ , then  $\Delta(r_{A,W}^S, \mathbf{S}') = \tau_A(\mathbf{I}') - \mathbf{I}'$ .*

**Proof.** Let  $\zeta$  be an isomorphism from  $\mathbf{S}'$  to  $\mathbf{S}''$ . Extend it to locations and updates. Then, by Lemma 2.1, we have that  $\tau_A(\mathbf{I}'') - \mathbf{I}'' = \zeta(\tau_A(\mathbf{I}') - \mathbf{I}')$  and that  $\Delta(r_{A,W}^S, \mathbf{S}'') = \zeta(\Delta(r_{A,W}^S, \mathbf{S}'))$ . Since by assumption  $\Delta(r_{A,W}^S, \mathbf{S}'') = \tau_A(\mathbf{I}'') - \mathbf{I}''$ , we get  $\zeta(\Delta(r_{A,W}^S, \mathbf{S}')) = \zeta(\tau_A(\mathbf{I}') - \mathbf{I}')$  and hence  $\Delta(r_{A,W}^S, \mathbf{S}') = \tau_A(\mathbf{I}') - \mathbf{I}'$  as  $\zeta$  is an isomorphism.  $\square$

In our last lemma, we show that if  $\mathbf{S}$  and  $\mathbf{S}'$  are similar in the sense of the following definition, then the rule  $r_{A,W}^S$ , when evaluated in  $\mathbf{S}'$ , produces the correct (according to the algorithm  $A$ ) set of updates.

**Definition 7.9.** Let  $W$  be a bounded exploration witness for a parallel algorithm  $A$ , we say that two states  $\mathbf{S}$  and  $\mathbf{S}'$  of computation of  $A$  are  $W$ -similar if for all  $\alpha_i, \alpha_j \in W$ , it holds that  $\text{val}_{\mathbf{S}}(\alpha_i) = \text{val}_{\mathbf{S}'}(\alpha_j)$  iff  $\text{val}_{\mathbf{S}}(\alpha_i) = \text{val}_{\mathbf{S}'}(\alpha_j)$ .

**Lemma 7.11.** *Let  $\mathbf{I}$  and  $\mathbf{I}'$  be states of a parallel algorithm  $A$ . Let  $W$  be a bounded exploration witness for  $A$ . Let  $\mathbf{S}$  and  $\mathbf{S}'$  be states of computation of  $A$  which correspond to  $\mathbf{I}$  and  $\mathbf{I}'$ , respectively. If  $\mathbf{S}$  and  $\mathbf{S}'$  are  $W$ -similar, then  $\Delta(r_{A,W}^S, \mathbf{S}') = \tau_A(\mathbf{I}') - \mathbf{I}'$ .*

**Proof.** W.l.o.g. we assume that the base sets of  $\mathbf{I}$  and  $\mathbf{I}'$  are disjoint. Otherwise we can always take an isomorphic copy of  $\mathbf{I}'$  with no elements from  $\mathbf{I}$ . Consequently the base set of  $\mathbf{S}$  is disjoint from the base set of  $\mathbf{S}'$ . Let  $\zeta$  be a function that replaces in the base set of  $\mathbf{S}'$ , the values of each witness terms in  $W$  with its corresponding value in  $\mathbf{S}$ , i.e.,  $\zeta(\text{val}_{\mathbf{S}'}(\alpha_i)) = \text{val}_{\mathbf{S}}(\alpha_i)$  for every  $\alpha_i \in W$ , and  $\zeta(a) = a$  if  $a$  is not the value of a witness term in  $W$ . Since  $\mathbf{S}$  and  $\mathbf{S}'$  are disjoint and  $W$ -similar,  $\zeta$  is a well defined function and a bijection. Let  $\mathbf{S}''$  be the isomorphic image of  $\mathbf{S}'$  under  $\zeta$ . Since  $\zeta(a) = a$  for all  $a \in \mathbf{I}'$  and  $\mathbf{S}'' \simeq \mathbf{S}'$ , we have that  $\mathbf{S}''$  is also a state of computation of  $\mathbf{I}'$ . Clearly,  $\mathbf{S}$  and  $\mathbf{S}''$  coincide on  $W$ . By Lemma 7.9 we get that  $\Delta(r_{A,W}^S, \mathbf{S}'') = \tau_A(\mathbf{I}') - \mathbf{I}'$ . Finally, by Lemma 7.10 we obtain  $\Delta(r_{A,W}^S, \mathbf{S}') = \tau_A(\mathbf{I}') - \mathbf{I}'$  as claimed.  $\square$

We can now prove our main characterization theorem.

**Theorem 7.12.** *For every parallel algorithm there is a behaviourally equivalent parallel ASM.*

**Proof.** Let  $A$  be a parallel algorithm, let  $W$  be a witness set for  $A$ , let  $\mathbf{I}$  be a state of  $A$  and let  $\mathbf{S}$  be a state of computation that corresponds to  $\mathbf{I}$ . Let  $\varphi_{\mathbf{S}}$  denote the term which characterizes the similarity type of  $\mathbf{S}$  in the sense that for every state of computation  $\mathbf{S}'$  of  $A$ ,  $\text{val}_{\mathbf{S}}(\varphi_{\mathbf{S}}) = \text{true}^{\mathbf{S}'}$  holds iff  $\mathbf{S}$  and  $\mathbf{S}'$  are  $W$ -similar, i.e., let

$$\varphi_S \equiv \bigwedge_{\substack{\alpha_i, \alpha_j \in W \\ \text{vals}(\alpha_i) = \text{vals}(\alpha_j)}} \alpha_i = \alpha_j \wedge \bigwedge_{\substack{\alpha_i, \alpha_j \in W \\ \text{vals}(\alpha_i) \neq \text{vals}(\alpha_j)}} \neg(\alpha_i = \alpha_j)$$

Since  $W$  is finite, there is a finite set  $S = \{S_1, \dots, S_n\}$  of states of computation of  $A$  such that the following holds:

- For every state of computation  $S'$  of  $A$ , there is a state of computation  $S_i \in S$  which is  $W$ -similar to  $S'$ .
- For every  $S_i, S_j \in S$ ,  $\text{vals}_{S_i}(\varphi_{S_i}) = \text{false}^{S_i}$  and  $\text{vals}_{S_j}(\varphi_{S_j}) = \text{false}^{S_j}$ .

The ASM rule that corresponds to the transition function  $\tau_A$  of  $A$  can then be defined as the parallel combination of the following rules:

**if**  $\varphi_{S_1}$  **then**  $r_{A,W}^{S_1}$  **endif**  
 $\vdots$   
**if**  $\varphi_{S_n}$  **then**  $r_{A,W}^{S_n}$  **endif**

If  $I'$  is a state of  $A$  and  $S'$  a state of computation of  $A$  which corresponds to  $I'$ , then there is exactly one state of computation  $S_i \in S$  such that  $S_i$  and  $S'$  are  $W$ -similar. Hence,  $\text{vals}_{S'}(\varphi_{S_i}) = \text{true}^{S'}$  and by Lemma 7.11,  $\Delta(r_{A,W}^{S_i}, S') = \tau_A(I') - I'$ .  $\square$

## 8. Conclusions

In this article we revisited the problem of the “parallel ASM thesis” (see [4]), i.e., to provide a machine-independent definition of parallel algorithms and a proof that these algorithms are faithfully captured by Abstract State Machines. The main motivation is the often uttered conviction that although the mathematical proof is correct, the definition of parallel algorithms given by Blass and Gurevich in [4] is not convincing, as the postulates reside too much on the technical side and do not provide the same level of intuitive clarity as the postulates for sequential algorithms. Our intention was thus to prove the conjecture in [11], according to which four simplified postulates suffice to justify ASMs as a general model for parallel computation, i.e. to provide a more intuitive set of postulates and to formally prove that parallel algorithms as stipulated by these new postulates are indeed captured by ASMs.

As a matter of fact, postulates are always debatable, so we open the debate, whether the goal to provide an intuitively clear and acceptable characterization of synchronous parallel algorithms has now been reached. Technically, the new set of postulates is equivalent to the one given by Blass and Gurevich, as both are captured exactly by ASMs.

The set of postulates for synchronous parallel algorithms presented in this article is rather close to the one used for sequential algorithms [2], which has been widely accepted by the scientific community. There are two main differences. The first one is the addition of a background postulate analogous to the background postulate in [4]. In a sense, this postulate makes all assumptions about the background of a computation explicit. It is only necessary, as there is a need to exploit tuples and multisets, which are not required in sequential algorithms. In a strict formal sense there is also a background for sequential algorithms, but the assumptions have been left implicit. The second one is the extension of the bounded exploration postulate, which still claims a finite set of exploration witness terms that determine update sets, but instead of simple ground terms now multiset comprehension terms are needed. By means of these, the varying parallel branches in a parallel computation which depend not only on the algorithm but also on the state are captured and there is no need for a separate concept of “prolet”.

With the new parallel ASM thesis at hand we will now proceed further towards a thesis for concurrent ASMs capturing asynchronous parallel algorithms. The work in [7] contains a first attempt in this direction, which so far is restricted to families of sequential algorithms. We believe that with the result in this article we can achieve an easy generalization to families of parallel algorithms.

## Acknowledgement

We would like to express our gratitude to Prof. José María Turull Torres who thoroughly read a preliminary version of this paper, provided us with valuable feedback and suggestions, and pointed out some gaps in the characterization proof which were corrected in this final version.

## References

- [1] Y. Gurevich, A new thesis, in: Abstract 85T-68-203, in: Amer. Math. Soc. Abstracts, vol. 6, 1985, p. 317.
- [2] Y. Gurevich, Sequential abstract-state machines capture sequential algorithms, ACM Trans. Comput. Log. 1 (1) (2000) 77–111.
- [3] A. Blass, Y. Gurevich, Background, reserve, and Gandy machines, in: P. Clote, H. Schwichtenberg (Eds.), CSL, in: Lecture Notes in Computer Science, vol. 1862, Springer, 2000, pp. 1–17.
- [4] A. Blass, Y. Gurevich, Abstract state machines capture parallel algorithms, ACM Trans. Comput. Log. 4 (4) (2003) 578–651.
- [5] A. Blass, Y. Gurevich, Abstract state machines capture parallel algorithms: correction and extension, ACM Trans. Comput. Log. 9 (3).

- [6] E. Börger, R.F. Stärk, *Abstract State Machines. A Method for High-Level System Design and Analysis*, Springer, 2003.
- [7] E. Börger, K.-D. Schewe, Concurrent abstract state machines, *Acta Inform.* 53 (5) (2016) 469–492.
- [8] Y. Gurevich, Evolving algebra 1993 – Lipari guide, in: *Specification and Validation Methods*, Oxford University Press, 1995, pp. 9–36.
- [9] Y. Gurevich, Foundational analyses of computation, in: S.B. Cooper, A. Dawar, B. Löwe (Eds.), *How the World Computes – Turing Centenary Conference and 8th Conference on Computability in Europe (CiE 2012)*, in: LNCS, vol. 7318, Springer, 2012, pp. 264–275.
- [10] A. Blass, Y. Gurevich, D. Rosenzweig, B. Rossman, Interactive small-step algorithms I – axiomatization, *Log. Methods Comput. Sci.* 3 (4) (2007), paper 3.
- [11] K.-D. Schewe, Q. Wang, A simplified parallel ASM thesis, in: J. Derrick, et al. (Eds.), *Abstract State Machines, Alloy, B, VDM, and Z – Third International Conference (ABZ 2012)*, in: LNCS, vol. 7316, Springer, 2012, pp. 341–344.
- [12] K.-D. Schewe, Q. Wang, A customised ASM thesis for database transformations, *Acta Cybernet.* 19 (4) (2010) 765–805.
- [13] E. Grädel, Y. Gurevich, Metafinite model theory, *Inform. and Comput.* 140 (1) (1998) 26–81.
- [14] K.-D. Schewe, Q. Wang, XML database transformations, *J.UCS* 16 (20) (2010) 3043–3072.
- [15] K.-D. Schewe, Q. Wang, Synchronous parallel database transformations, in: T. Lukasiewicz, A. Sali (Eds.), *Foundations of Information and Knowledge Bases (FolKS 2012)*, in: LNCS, vol. 7153, Springer, 2012, pp. 371–384.
- [16] E. Grädel, Y. Gurevich, Metafinite model theory, *Inform. and Comput.* 140 (1) (1998) 26–81.
- [17] F. Ferrarotti, K. Schewe, L. Tec, Q. Wang, A new thesis concerning synchronised parallel computing – simplified parallel ASM thesis, CoRR abs/1504.06203. URL <http://arxiv.org/abs/1504.06203>.
- [18] R.M. Karp, V. Ramachandran, Parallel algorithms for shared-memory machines, in: *Handbook of Theoretical Computer Science, Volume A: Algorithms and Complexity*, 1990, pp. 869–942.
- [19] C.H. Papadimitriou, Computational complexity, in: *Encyclopedia of Computer Science*, John Wiley and Sons Ltd., Chichester, UK, 2003, pp. 260–265.
- [20] E. Casanovas, P. Dellunde, R. Jansana, On elementary equivalence for equality-free logic, *Notre Dame J. Form. Log.* 37 (3) (1996) 506–522.