

Branching Bisimilarity on Normed BPA Is EXPTIME-complete

Chaodong He Mingzhang Huang

BASICS, Department of Computer Science and Engineering, Shanghai Jiao Tong University

Abstract—We put forward an exponential-time algorithm for deciding branching bisimilarity on normed BPA (Basis Process Algebra) systems. The decidability of branching (or weak) bisimilarity on normed BPA was once a long standing open problem which was closed by Yuxi Fu in [1]. The EXPTIME-hardness is an inference of a slight modification of the reduction presented by Richard Mayr [2]. Our result claims that this problem is EXPTIME-complete.

I. INTRODUCTION

Basic process algebra (BPA) [3] is a fundamental model of infinite state systems, with its famous counterpart in the theory of formal languages: context free grammars in Greibach normal forms, which generate the entire context free languages. In 1987, Baeten, Bergstra and Klop [4] proved a surprising result at the time that strong bisimilarity on normed BPA is decidable. This result is in sharp contrast to the classical fact that language equivalence is undecidable for context free grammar [5]. After this remarkable discovery, decidability and complexity issues of bisimilarity checking on infinite state systems have been intensively investigated. See [6], [7], [8], [9], [10] for a number of surveys.

As regards strong bisimilarity on normed BPA, Hüttel and Stirling [11] improved the result of Baeten, Bergstra and Klop using a more simplified proof by relating the strong bisimilarity of two normed BPA processes to the existence of a successful tableau system. Later, Huynh and Tian [12] showed that the problem is in Σ_2^P , the second level of the polynomial hierarchy. Before long, another significant discovery was made by Hirshfeld, Jerrum and Møller [13] who showed that the problem can even be decided in polynomial time. Improvements on running time was made later in [14], [15], [16].

The decidability of strong bisimilarity on general BPA is affirmed by Christensen, Hüttel and Stirling [17]. 2-EXPTIME is claimed to be an upper bound by Burkart, Caucal and Steffen [18] and is explicitly proven recently by Jančar [19]. As to the lower bound, Kiefer [20] achieves EXPTIME-hardness, which is an improvement of the previous PSPACE-hardness obtained by Srba [21].

In the presence of silent actions, however, the picture is less clear. The decidability for both weak bisimilarity and branching bisimilarity on normed BPA was once long standing open problems. For weak bisimilarity [22], the problem is still open, while for branching bisimilarity [23], [24], a remarkable discovery is made by Fu [1] recently that the problem is decidable. Very recently, using the key property developed in [1], Czerwinski and Jančar shows that there exists an exponentially

large bisimulation base for branching bisimilarity on normed BPA, and by guessing the base, they show that the complexity of this problem is in NEXPTIME [25]. The current best lowerbound for weak bisimilarity is the EXPTIME-hardness established by Mayr [2], whose proof can be slightly modified to show the EXPTIME-hardness for branching bisimilarity as well. As to the general BPA, decidability of branching bisimilarity is still unknown.

In this paper, we confirm that an exponential time algorithm exists for checking branching bisimilarity on normed BPA. Comparing with the known EXPTIME-hardness result, we get the result of EXPTIME-completeness. Thus the complexity class of branching bisimilarity on normed BPA is completely determined.

Basically, we introduce a family of relative bisimilarities parameterized by the reference sets, which can be represented by a decomposition base defined in this paper. The branching bisimilarity is exactly the relative bisimilarity whose reference set is the empty set. We show that this base can be approximated. The approximation procedure starts from an initial base, which is relatively trivial, and is carried on by repeatedly refining the current base. In order to define the approximation procedure and to ensure that the family of relative bisimilarities is achieved at last, a lot of technical difficulties need overcoming. Some of them are listed here:

- Despite the seeming resemblance, the relative bisimilarities (Section III) defined in this paper is significantly superior to the corresponding concepts in [25]. The relative bisimilarities in this paper is *suffix independent*. This property is extremely crucial for our algorithm. The correctness of definition is characterized in Theorem 2.
- We show that a generalized unique decomposition property holds for the family of relative bisimilarities (Theorem 3). In the decompositions, bisimilarities with different reference sets depend and impact on each other. The notion of decomposition bases (Section V) provides an effective representation of an arbitrary family of process equivalences that satisfies the unique decomposition property.
- In an iteration of refinement operation, a new decomposition base is constructed from the old (Section VI). That is, a new family of equivalences is obtained from the old one. Besides, comparing with all the previous algorithms [26], [15], [27] which take partition refinement approach, our refinement procedure possesses several hallmarks:

- The new base is constructed via a *globally* greedy strategy, which means that all the relevant equivalences with different reference sets are dealt with as a whole.
- The refinement operation in previous works heavily depends on predefined notions of norms and decreasing transitions. These notions can be determined from the normed BPA definition immediately. Such a method does not work at present. Our solution is to define norms in a semantic way (Section IV). Norms, relying on the relevant equivalence relations, together with decreasing transitions, can change dynamically in every iteration. When we start to construct a new base, no information on norms is available. Thus at this time we cannot determine whether a transition is decreasing. Our solution is to incorporate the task of computing norms into the global iteration procedure via the greedy strategy.
- In previous works the order of process constants can be determined in advance. Every time a new base is constructed from the old, the constants are treated in the same order. There is no such predefined order in our algorithm. The treating order is dynamically determined in every iteration.

Equivalence checking on normed BPA is significantly harder than the related problem on *totally* normed BPA. For totally normed BPA, branching bisimilarity is recently shown polynomial-time decidable [27]. What is obtained in this paper is significantly stronger than previous results [28], [29], [27].

II. PRELIMINARIES

A. Normed Basic Process Algebra

A *basic process algebra* (BPA) system Γ is a triple $(\mathbf{C}, \mathcal{A}, \Delta)$, where \mathbf{C} is a finite set of process constants ranged over by X, Y, Z, U, V, W , \mathcal{A} is a finite set of actions, and Δ is a finite set of transition rules. The *processes*, ranged over by $\alpha, \beta, \gamma, \delta, \zeta, \eta$, are generated by the following grammar:

$$\alpha ::= \epsilon \mid X \mid \alpha_1.\alpha_2.$$

The syntactic equality is denoted by $=$. We assume that the sequential composition $\alpha_1.\alpha_2$ is associative up to $=$ and $\epsilon.\alpha = \alpha.\epsilon = \alpha$. Sometimes $\alpha.\beta$ is shortened as $\alpha\beta$. The set of processes is exactly \mathbf{C}^* , the finite strings over \mathbf{C} . There is a special symbol τ in \mathcal{A} for silent transition. ℓ is invariably used to denote an arbitrary action, while a is used to denote a visible (i.e. non-silent) action. The transition rules in Δ are of the form $X \xrightarrow{\ell} \alpha$. The operational semantics of the processes are defined by the following labelled transition rules.

$$\frac{(X \xrightarrow{\ell} \alpha) \in \Delta}{X \xrightarrow{\ell} \alpha} \quad \frac{\alpha \xrightarrow{\ell} \alpha'}{\alpha.\beta \xrightarrow{\ell} \alpha'.\beta}$$

A central dot ‘.’ is often used to indicate an arbitrary process. For example, we write $\alpha \xrightarrow{\ell_1} \cdot \xrightarrow{\ell_2} \beta$, or even $\alpha \xrightarrow{\ell_1} \xrightarrow{\ell_2} \beta$, to mean that there exists some γ such that $\alpha \xrightarrow{\ell_1} \gamma$ and $\gamma \xrightarrow{\ell_2} \beta$.

If \asymp is an equivalence relation on processes, then we will use $\alpha \xrightarrow{\tau} \alpha'$ to denote the fact $\alpha \xrightarrow{\tau} \alpha'$ and $\alpha \asymp \alpha'$, and use $\alpha \xrightarrow{\neq} \alpha'$ to denote the fact $\alpha \xrightarrow{\tau} \alpha'$ and $\alpha \not\asymp \alpha'$. We write \Longrightarrow for the reflexive transitive closure of $\xrightarrow{\tau}$, and \Longleftarrow for the symmetric closure of \Longrightarrow (i.e. $\Longleftarrow \stackrel{\text{def}}{=} \Longrightarrow \cup \Longrightarrow^{-1}$). Accordingly, \Longleftrightarrow is understood as the reflexive transitive closure of $\xrightarrow{\neq}$. That is, $\alpha \Longleftrightarrow \alpha'$ if and only if $\alpha \xrightarrow{\neq} \dots \xrightarrow{\neq} \alpha'$.

Remark 1. $\alpha \Longleftrightarrow \alpha'$ is slightly different from $\alpha \Longrightarrow \alpha' \asymp \alpha$. If Computation Lemma (Lemma 1) holds for \asymp , then $\alpha \Longleftrightarrow \alpha'$ if and only if $\alpha \Longrightarrow \alpha' \asymp \alpha$.

A process α is *normed* if $\alpha \xrightarrow{\ell_1} \dots \xrightarrow{\ell_n} \epsilon$ for some ℓ_1, \dots, ℓ_n . A BPA system $\Gamma = (\mathbf{C}, \mathcal{A}, \Delta)$ is normed if all the processes defined in Γ are normed. In other words, Γ is normed if X is normed for every $X \in \mathbf{C}$. In the rest of the paper, we will invariably use $\Gamma = (\mathbf{C}, \mathcal{A}, \Delta)$ to indicate the concerned normed BPA system. A BPA system Γ is called *realtime* if for every $(X \xrightarrow{\ell} \alpha) \in \Delta$, we have $\ell \neq \tau$.

A process α is called a *ground* process if $\alpha \Longrightarrow \epsilon$. The set of ground constants is denoted by \mathbf{C}_G . Apparently $\mathbf{C}_G \subseteq \mathbf{C}$ and α is ground if and only if $\alpha \in \mathbf{C}_G^*$.

Remark 2. A BPA system $\Gamma = (\mathbf{C}, \mathcal{A}, \Delta)$ is *totally normed* if and only if rules of the form $X \xrightarrow{\tau} \epsilon$ are forbidden. $\Gamma = (\mathbf{C}, \mathcal{A}, \Delta)$ is totally normed if and only if $\mathbf{C}_G = \emptyset$.

B. Bisimulation and Bisimilarity

In the presence of silent actions, branching bisimilarity of van Glabbeek and Weijland [23], [24] is well-known.

Definition 1. Let \asymp be an equivalence relation on processes. \asymp is called a *branching bisimulation*, if the following *bisimulation property* hold: whenever $\alpha \asymp \beta$,

- If $\alpha \xrightarrow{a} \alpha'$, then $\beta \Longleftrightarrow \cdot \xrightarrow{a} \beta'$ for some β' such that $\alpha' \asymp \beta'$.
- If $\alpha \xrightarrow{\neq} \alpha'$, then $\beta \Longleftrightarrow \cdot \xrightarrow{\neq} \beta'$ for some β' such that $\alpha' \asymp \beta'$.

The *branching bisimilarity* \simeq is the largest branching bisimulation.

Remark 3. In this paper, branching bisimulations in Definition 1 and other bisimulation-like relations in later chapters are forced to be equivalence relations. This technical convention does not affect the notion of branching bisimilarity.

The branching bisimilarity is a congruence relation, and it satisfies the following famous lemma.

Lemma 1 (Computation Lemma [23]). If $\alpha \Longrightarrow \alpha' \Longrightarrow \alpha'' \simeq \alpha$, then $\alpha' \simeq \alpha$.

If Γ is realtime, the branching bisimilarity is the same as the *strong bisimilarity*. In this paper, branching bisimilarity will be abbreviated as *bisimilarity*. For realtime systems, the term bisimilarity will also be used to indicate strong bisimilarity.

III. RELATIVIZED BISIMILARITIES ON NORMED BPA

A. Retrospection

In [1], Yuxi Fu creates the notion of redundant processes, and discover the following Proposition 3, which is crucial to

the proof of decidability of bisimilarity for normed BPA.

Definition 2. A process α is a \simeq -redundant over γ if $\alpha\gamma \simeq \gamma$.

We use $\text{Rd}(\gamma) = \{X \mid X\gamma \simeq \gamma\}$ to indicate the set of all constants that is \simeq -redundant over γ . Clearly, $\text{Rd}(\gamma) \subseteq \mathbf{C}_G$.

The following lemma confirms that the redundant processes over γ are completely determined by the redundant constants.

Lemma 2. $\alpha\gamma \simeq \gamma$ if and only if $\alpha \in (\text{Rd}(\gamma))^*$.

The crucial observation in [1] is the following fact.

Proposition 3. Assume that $\text{Rd}(\gamma_1) = \text{Rd}(\gamma_2)$, then $\alpha\gamma_1 \simeq \beta\gamma_1$ if and only if $\alpha\gamma_2 \simeq \beta\gamma_2$.

Proposition 3 inspires us to define a relativized version of bisimilarity \simeq_R for a given suitable *reference set* R , which will satisfy the following theorem.

Theorem 1. Let γ be a process satisfying $\text{Rd}(\gamma) = R$. Then $\alpha \simeq_R \beta$ if and only if $\alpha\gamma \simeq \beta\gamma$.

Proposition 3 confirms that \simeq_R does not depend on the special choice of γ under the assumption of the existence of γ such that $R = \text{Rd}(\gamma)$. However, it is much wiser not to take Theorem 1 as the definition of \simeq_R from a computational point of view. Here are the reasons.

- We cannot tell beforehand (except when we can decide \simeq) whether, for a given R , there exists γ such that $R = \text{Rd}(\gamma)$, nor can we tell whether $R = \text{Rd}(\gamma)$ even if both R and γ are given.
- The algorithm developed in this paper takes the refinement approach. Imagine that \asymp is an approximation of \simeq , we can define, for example, the \asymp -redundant constants $\text{Rd}^\asymp(\gamma)$ accordingly. It is quite possible to run into the situation where, for a specific R , there is no δ such that $R = \text{Rd}^\asymp(\delta)$ even if $R = \text{Rd}(\gamma)$ for some γ .

Therefore it is advisable to make \simeq_R well-defined for every R satisfying $R \subseteq \mathbf{C}_G$. Importantly, \simeq_R should be defined without the knowledge of the existence of γ .

Remark 4. In [25], Czerwiński and Jančar also define a relativized version of bisimilarities. The difference is that they directly take Theorem 1 as the definition. After that, they establish a *weaker* version of unique decomposition property. In [25], \simeq_R is defined only for those R 's such that $R = \text{Rd}(\gamma)$ for some γ . Using Theorem 1, a property of \simeq_R can be proved by a translation of a property of \simeq . Though seemingly similar, the properties which will be developed in this section are much stronger than those properties in [25].

B. Definition of R -Bisimilarities

Now we elaborate on the definition of \simeq_R . Some auxiliary notations are introduced to make things clear.

Definition 3. Let $R \subseteq \mathbf{C}_G$. Two processes α and β are R -equal, denoted by $\alpha =_R \beta$ if there exist ζ, α', β' such that $\alpha = \zeta\alpha'$, $\beta = \zeta\beta'$, and $\alpha', \beta' \in R^*$.

Two processes are R -equal if they differ only in suffixes in R^* . R -equality is an equivalence relation. Eliminating a suffix in R^* from a process does not change the $=_R$ -class.

Lemma 4. 1) $\alpha =_R \alpha\gamma$ if and only if $\gamma \in R^*$.

2) $\alpha =_R \epsilon$ if and only if $\alpha \in R^*$.

Definition 4. Let $R \subseteq \mathbf{C}_G$. α is in R -normal-form (R -nf) if

- 1) either $\alpha = \epsilon$,
- 2) or there exist α' and X such that $\alpha = \alpha'X$ and $X \notin R$.

If $\alpha =_R \alpha'$ and α' is in R -nf, then α' is called an R -nf of α . The (unique) R -nf of α is denoted by α_R .

From Definition 4, taking the R -nf of α is nothing but removing any suffix of α in R . R -equality is the syntactic equality on R -nf's. In particular, \emptyset -equality is exactly the ordinary syntactic equality.

Lemma 5. $\alpha =_R \beta$ if and only if $\alpha_R = \beta_R$. In particular, $\alpha =_\emptyset \beta$ if and only if $\alpha = \beta$.

The transition relations can be relativized as follows.

Definition 5. The R -transition relations between R -nf's are defined as follows: We write $\zeta \xrightarrow{\ell}_R \eta$ if there exists α and β such that $\zeta = \alpha_R$, $\eta = \beta_R$, and $\alpha \xrightarrow{\ell} \beta$.

According to Definition 5, the relation $\xrightarrow{\ell}_R$ is defined only on the set of processes in R -nf. When we write $\alpha \xrightarrow{\ell}_R \beta$, α and β are implicitly supposed to be R -nf's.

Lemma 6. $\alpha_R \xrightarrow{\ell}_R \beta_R$ if and only if $\alpha =_R \cdot \xrightarrow{\ell} \cdot =_R \beta$.

Let $\alpha \xrightarrow{\ell}_R \beta$. Intuitively, if $\alpha \neq \epsilon$, then $\alpha \xrightarrow{\ell}_R \beta$ is induced by α ; if $\alpha = \epsilon$, then $\alpha \xrightarrow{\ell}_R \beta$ is induced by one of the constants in R . This important fact is formalized in the following lemma.

Lemma 7. $\alpha_R \xrightarrow{\ell}_R \beta_R$ if and only if

- 1) either $\alpha_R = \epsilon$ and $X \xrightarrow{\ell} \beta'$ for some β' and $X \in R$ such that $\beta' =_R \beta$.
- 2) or $\alpha_R \neq \epsilon$ and $\alpha \xrightarrow{\ell} \beta'$ for some β' such that $\beta' =_R \beta$.

As usual, we write \Longrightarrow_R for the reflexive transitive closure of $\xrightarrow{\tau}_R$, and \Longleftarrow_R for the symmetric closure of \Longrightarrow_R (i.e. $\Longleftarrow_R \stackrel{\text{def}}{=} \Longrightarrow_R \cup \Longrightarrow_R^{-1}$). Accordingly, $\alpha \xrightarrow{\tau}_R \alpha'$ is understood as $\alpha \xrightarrow{\tau}_R \alpha' \asymp \alpha$, and \Longrightarrow_R is the reflexive transitive closure of $\xrightarrow{\tau}_R$.

The ground processes are robust under relativization.

Lemma 8. $\alpha \Longrightarrow \epsilon$ if and only if $\alpha_R \Longrightarrow_R \epsilon$.

Now it is time for defining R -bisimilarity.

Definition 6. Let $R \subseteq \mathbf{C}_G$ and let \asymp be an equivalence relation such that $=_R \subseteq \asymp$. We say \asymp is an R -bisimulation, if the following conditions are satisfied whenever $\alpha \asymp \beta$:

- 1) *ground preservation*: If $\alpha \Longrightarrow \epsilon$, then $\beta \Longrightarrow \epsilon$.
- 2) If $\alpha \xrightarrow{*} \alpha'$, then $\beta_R \Longrightarrow_R \cdot \xrightarrow{*}_R \beta'$ for some β' such that $\alpha' \asymp \beta'$.

- 3) If $\alpha \xrightarrow{a} \alpha'$, then $\beta_R \xRightarrow{\sim}_R \cdot \xrightarrow{a}_R \beta'$ for some β' such that $\alpha' \asymp \beta'$.

The R -bisimilarity \simeq_R is the largest R -bisimulation.

Remark 5. R -bisimilarity \simeq_R is well-defined, based on the following observations:

- $=_R$ is an R -bisimulation.
- If \asymp_1 and \asymp_2 are both R -bisimulations, then $(\asymp_1 \cup \asymp_2)^*$ is an R -bisimulation.

If $R = \emptyset$, then \simeq_\emptyset is exactly the ordinary bisimilarity \simeq .

R -bisimulations can actually be understood as the bisimulations on R -nf's under R -transitions, as is stated below.

Proposition 9. Let $R \subseteq \mathbf{C}_G$ and let \asymp be an equivalence relation such that $=_R \subseteq \asymp$. Then \asymp is an R -bisimulation if and only if whenever $\alpha \asymp \beta$,

- 1) if $\alpha_R \Rightarrow_R \epsilon$, then $\beta_R \Rightarrow_R \epsilon$;
- 2) if $\alpha_R \xrightarrow{*}_R \alpha'_R$, then $\beta_R \xRightarrow{\sim}_R \cdot \xrightarrow{*}_R \beta'_R$ for some β' such that $\alpha' \asymp \beta'$;
- 3) if $\alpha_R \xrightarrow{a}_R \alpha'_R$, then $\beta_R \xRightarrow{\sim}_R \cdot \xrightarrow{a}_R \beta'_R$ for some β' such that $\alpha' \asymp \beta'$.

Comparing with the definition of bisimulation (Definition 1), Definition 6 and Proposition 9 contains an extra *ground preservation* condition which guarantees that a ground process cannot be related to a non-ground process in an R -bisimulation. In the definition of bisimulation, this condition is also satisfied, for it can be derived from other bisimulation conditions. As to R -bisimulation, this is not always the case, as is illustrated in the following example.

Example 1. Consider the following normed BPA $(\mathbf{C}, \mathcal{A}, \Delta)$:

- $\mathbf{C} = \{A_0, A_1\}$;
- $\mathcal{A} = \{a, \tau\}$;
- Δ is the set containing the following rules:

$$A_0 \xrightarrow{a} A_1, \quad A_1 \xrightarrow{a} A_1, \quad A_1 \xrightarrow{\tau} \epsilon$$

Let $R = \{A_1\}$, and let \asymp be the equivalence relation which relates every processes defined in Γ to ϵ . Clearly $A_0 \not\Rightarrow_R \epsilon$. However, we can show that (A_0, ϵ) satisfies R -bisimulation conditions except for the ground preserving condition:

Considering that the R -transitions of ϵ can be trivially matched by A_0 , it remains to show that ϵ can match the R -transitions of A_0 . The unique R -transition of A_0 is $A_0 \xrightarrow{a}_R \epsilon$, which can be matched by $\epsilon \xrightarrow{a}_R \epsilon$ since $A_1 \xrightarrow{a} A_1$ and $(A_1)_R = \epsilon$.

The relative bisimilarity \simeq_R is not a congruence in general. For example, we may not have $\alpha\gamma \simeq_R \beta\gamma$ even if $\alpha \simeq_R \beta$. However, we have the following result.

Lemma 10. If $\gamma \simeq_R \delta$ and $\alpha \simeq \beta$, then $\alpha\gamma \simeq_R \beta\delta$. In particular, If $\gamma \simeq_R \delta$, then $\alpha\gamma \simeq_R \alpha\delta$.

The computation lemma also holds for \simeq_R .

Lemma 11 (Computation Lemma for \simeq_R). If $\alpha \Rightarrow_R \alpha' \Rightarrow_R \alpha'' \simeq_R \alpha$ then $\alpha' \simeq_R \alpha$.

C. R -identities and Admissible Reference Sets

Clearly, R -bisimilarity has the following basic property.

Lemma 12. Let $R \subseteq \mathbf{C}_G$. If $X \in R$, then $X \simeq_R \epsilon$.

Be aware that the converse of Lemma 12 does not hold in general. That is, if $X \simeq_R \epsilon$, there is no guarantee that $X \in R$. This basic observation leads to further discussion.

Definition 7. Let $R \subseteq \mathbf{C}_G$. A process α is called a \simeq_R -identity if $\alpha \simeq_R \epsilon$. We use Id_R to denote $\{X \mid X \simeq_R \epsilon\}$.

By Lemma 12 and Definition 6, $R \subseteq \text{Id}_R \subseteq \mathbf{C}_G$. Moreover,

Lemma 13. $\alpha \simeq_R \epsilon$ if and only if $\alpha \in (\text{Id}_R)^*$.

Below we will demonstrate that, as a reference set, Id_R plays an important role. At first we state a useful proposition for relative bisimilarities. It says that \simeq_R is monotone.

Proposition 14. Let $R_1 \subseteq R_2 \subseteq \mathbf{C}_G$. If $\alpha \simeq_{R_1} \beta$, then $\alpha \simeq_{R_2} \beta$.

Corollary 15. Let $R_1 \subseteq R_2 \subseteq \mathbf{C}_G$. Then, $\text{Id}_{R_1} \subseteq \text{Id}_{R_2}$.

Intuitively, \simeq_R is the relative bisimilarity which is induced by regarding the constants in R as ϵ purposely. It is reasonable to expect that $X \simeq_{\text{Id}_R} \epsilon$ if and only if $X \in \text{Id}_R$. This intuition is confirmed by Proposition 16 and its corollaries.

Proposition 16. $\alpha \simeq_R \beta$ if and only if $\alpha \simeq_{\text{Id}_R} \beta$.

Corollary 17. Let $R_1 \subseteq \mathbf{C}_G$ and $R_2 \subseteq \mathbf{C}_G$. If $\text{Id}_{R_1} = \text{Id}_{R_2}$, then $\alpha \simeq_{R_1} \beta$ if and only if $\alpha \simeq_{R_2} \beta$.

Corollary 18. Let $R, S \subseteq \mathbf{C}_G$ such that $R \subseteq S \subseteq \text{Id}_R$, then $\text{Id}_S = \text{Id}_R$.

A direct inference of Corollary 18 is the following fact.

Lemma 19. $X \simeq_{\text{Id}_R} \epsilon$ if and only if $X \in \text{Id}_R$. In other words, $\text{Id}_{\text{Id}_R} = \text{Id}_R$.

The above discussions lead to the following definition.

Definition 8. An $R \subseteq \mathbf{C}_G$ is called *admissible* if $R = \text{Id}_R$.

The significance of Proposition 14, Proposition 16, and their corollaries is the revelation of the following fact: The set $\{\simeq_R\}_{R \subseteq \mathbf{C}_G}$ of all relative bisimilarities is completely determined by those \simeq_R 's in which R is admissible.

Lemma 20. For every $R \subseteq \mathbf{C}_G$, Id_R is admissible. Id_R is the smallest admissible set which contains R .

D. R -redundant Constants

The properties of \simeq -redundant processes (Definition 2 and Proposition 3) in Section III-A can now be generalized for the relative bisimilarity \simeq_R .

Definition 9. Let $R \subseteq \mathbf{C}_G$. A process α is \simeq_R -redundant over γ if $\alpha\gamma \simeq_R \gamma$. We use $\text{Rd}_R(\gamma)$ to denote $\{X \mid X\gamma \simeq_R \gamma\}$.

Note that $\text{Rd}(\gamma)$ defined in Section III-A is exactly $\text{Rd}_\emptyset(\gamma)$. Also note that Id_R is the same as $\text{Rd}_R(\epsilon)$.

Lemma 21. If $\gamma \simeq_R \delta$, then $\text{Rd}_R(\gamma) = \text{Rd}_R(\delta)$.

Lemma 22. 1) $\alpha \simeq_R \epsilon$ if and only if $\alpha \in (\text{Id}_R)^*$.

2) $\alpha\gamma \simeq_R \gamma$ if and only if $\alpha \in (\text{Rd}_R(\gamma))^*$.

Lemma 21 is a direct inference of Lemma 10. Lemma 22 is the strengthened version of Lemma 2.

Now we can state the fundamental theorem for \simeq_R .

Theorem 2. Let $R' = \text{Rd}_R(\gamma)$, then $\alpha \simeq_{R'} \beta$ if and only if $\alpha\gamma \simeq_R \beta\gamma$.

Proposition 23. Assume that $\text{Rd}_R(\gamma_1) = \text{Rd}_R(\gamma_2)$, then $\alpha\gamma_1 \simeq_R \beta\gamma_1$ if and only if $\alpha\gamma_2 \simeq_R \beta\gamma_2$.

Proposition 24. Suppose that $\gamma \simeq_R \delta$ and let $R' = \text{Rd}_R(\gamma) = \text{Rd}_R(\delta)$. Then $\alpha\gamma \simeq_R \beta\delta$ if and only if $\alpha \simeq_{R'} \beta$.

Theorem 2 and Proposition 23 are the strengthened versions of Theorem 1 and Proposition 3. Proposition 24 is an inference of Lemma 10 and Theorem 2. Theorem 2 and Proposition 24 act as the relativized version of the congruence property and the cancellation law.

The following lemma is an inference of Theorem 2.

Lemma 25. $\text{Rd}_{\text{Rd}_R(\delta)}(\gamma) = \text{Rd}_R(\gamma\delta)$.

In the following we discuss the significance of the admissible reference sets. First it is easy to see the following fact according to Proposition 16.

Lemma 26. $\text{Rd}_R(\gamma) = \text{Rd}_{\text{Id}_R}(\gamma)$ for every γ and R .

The following lemma ensures that the admissible set is preserved under the ‘redundant’ operation.

Lemma 27. If $R = \text{Rd}_{R'}(\gamma)$ for some γ , then R is admissible.

Remark 6. Even if R is admissible, it is not guaranteed that $R = \text{Rd}_{R'}(\gamma)$ for some γ and R' . This fact indicates that, even if \simeq_R is only attractive for only admissible R ’s, our notion of R -bisimilarities strictly generalizes the ones in [25].

E. Unique Decomposition Property for R -bisimilarities

When Γ is realtime, the set \mathbf{C} of process constants can be divided into two disjoint sets: *primes* Pr and *composites* Cm . Every process α is bisimilar to a sequential composition of prime constants $P_1 \dots P_r$, and moreover, the prime decomposition is unique (up to bisimilarity). That is, if $P_1 \dots P_r \simeq Q_1 \dots Q_s$, then $r = s$ and $P_i \simeq Q_i$ for every $1 \leq i \leq r$. This property is called *unique decomposition property*, which is first established by Hirshfeld *et al.* in [13]. When Γ is totally normed, the unique decomposition property still holds [27].

If Γ is not totally normed, the unique decomposition property in the above sense does not hold due to the existence of redundant processes. However, we expound that, apart from the existence of redundant constants, the relative bisimilarities $\{\simeq_R\}$ enjoys a ‘weakened’ version of unique decomposition property (Theorem 3), which is still called *unique decomposition property* in this paper.

Definition 10. Let $R \subseteq \mathbf{C}_G$, and $X \in \mathbf{C}$.

- X is a \simeq_R -*composite* if $X \simeq_R \alpha X'$ for some X' and α such that $X' \notin \text{Id}_R$ and $\alpha \notin \text{Rd}_R(X')$.
- X is a \simeq_R -*prime* if X is neither a \simeq_R -identity nor a \simeq_R -composite.

According to Definition 10, a constant $X \in \mathbf{C}$ must act as one of the three different roles: \simeq_R -identity, \simeq_R -composite, or \simeq_R -prime. We will use Pr_R and Cm_R to indicate the set of \simeq_R -primes and \simeq_R -composites, respectively. According to Proposition 16, $\text{Pr}_R = \text{Pr}_{\text{Id}_R}$ and $\text{Cm}_R = \text{Cm}_{\text{Id}_R}$.

Definition 11. We call $P_r.P_{r-1} \dots P_1$ a \simeq_R -*prime decomposition* of α , if $\alpha \simeq_R P_r.P_{r-1} \dots P_1$, and P_i is a \simeq_{R_i} -prime for $1 \leq i \leq r$, if $R_1 = \text{Id}_R$ and $R_{i+1} = \text{Rd}_{R_i}(P_i)$ for $1 \leq i \leq r-1$.

Note that according to Lemma 27 every R_i for $1 \leq i \leq r$ is admissible.

The following ‘relativized prime process property’ is crucial to the unique decomposition property (Theorem 3).

Lemma 28. Suppose that X, Y are \simeq_R -primes and $\alpha X \simeq_R \beta Y$. Then $X \simeq_R Y$.

Theorem 3 (Unique Decomposition Property for R -bisimilarities). Let $P_r.P_{r-1} \dots P_1$ and $Q_s.Q_{s-1} \dots Q_1$ be \simeq_R -prime decompositions. Let $R_1, S_1 = \text{Id}_R$ and let $R_{i+1} = \text{Rd}_{R_i}(P_i)$ for $1 \leq i < r$ and $S_{j+1} = \text{Rd}_{S_j}(Q_j)$ for $1 \leq j < s$. Then, $r = s$, $R_i = S_i$ and $P_i \simeq_{R_i} Q_i$ for $1 \leq i \leq r$.

IV. NORMS AND DECREASING BISIMULATIONS

A. Syntactic Norms vs. Semantic Norms

When Γ is realtime, a natural number called *norm* is assigned to every process. The *norm* of α is the least number k such that $\alpha \xrightarrow{a_1} \dots \xrightarrow{a_k} \epsilon$ for some a_1, a_2, \dots, a_k .

The norm for realtime systems is both syntactic (static) and semantic (dynamic). It is syntactic because its definition does not rely on bisimilarity, and it can be efficiently calculated via greedy strategy merely with the knowledge of rules in Δ . It is semantic, because the norm of a realtime process α is the least number k such that $\alpha \simeq \dots \xrightarrow{a_1} \dots \xrightarrow{a_2} \dots \simeq \dots \xrightarrow{a_k} \dots \simeq \epsilon$ for some a_1, a_2, \dots, a_k .

Therefore, we get the coincidence of the *syntactic norm* and *semantic norm* for realtime systems. For non-realtime systems, however, the syntactic norms and the semantic ones do not coincide any more. They must be studied separately.

B. Strong Norms and Weak Norms

We define two syntactic norms for non-realtime systems. The strong norm takes silent actions into account while the weak norm neglects the contribution of silent actions.

Definition 12. The *strong norm* of α , denoted by $|\alpha|_{\text{st}}$, is the least number k such that $\alpha \xrightarrow{\ell_1} \dots \xrightarrow{\ell_k} \epsilon$ for some $\ell_1, \ell_2, \dots, \ell_k$.

The *weak norm* of α , denoted by $|\alpha|_{\text{wk}}$, is the least number k such that $\alpha \xrightarrow{a_1} \dots \xrightarrow{a_k} \epsilon$ for some a_1, a_2, \dots, a_k .

Lemma 29. 1) $|\epsilon|_{\text{st}} = |\epsilon|_{\text{wk}} = 0$;

$$2) |\alpha\beta|_{\text{st}} = |\alpha|_{\text{st}} + |\beta|_{\text{st}}; |\alpha\beta|_{\text{wk}} = |\alpha|_{\text{wk}} + |\beta|_{\text{wk}}.$$

Lemma 30. 1) $|\alpha|_{\text{st}} = 0$ if and only if $\alpha = \epsilon$.

2) $|\alpha|_{\text{wk}} = 0$ if and only if $\alpha \in \mathbf{C}_G^*$ (i.e. $\alpha \Rightarrow \epsilon$).

Lemma 31. If $\alpha \simeq_R \beta$, then $|\alpha|_{\text{wk}} = |\beta|_{\text{wk}}$.

Lemma 32. $|X|_{\text{st}}$ is exponentially bounded for every X .

C. The Semantic Norms

The semantic norms play an important role in our algorithm. They depend on the involved semantic equivalence. Let \asymp be a process equivalence. A transition $\alpha \xrightarrow{\ell} \alpha'$ is called \asymp -preserving if $\alpha' \asymp \alpha$.

Definition 13. Let \asymp be a process equivalence. The \asymp -norm of α , denoted by $\|\alpha\|_{\asymp}$, is the least number k , such that

$$\alpha \asymp \cdot \xrightarrow{\ell_1} \cdot \asymp \cdot \xrightarrow{\ell_2} \cdot \asymp \dots \asymp \cdot \xrightarrow{\ell_k} \cdot \asymp \epsilon.$$

for some $\ell_1, \ell_2, \dots, \ell_k$. If $\|\alpha\|_{\asymp} = k$, then any transition sequence of the form

$$\alpha \xRightarrow{\asymp} \cdot \xrightarrow{\ell_1} \cdot \xRightarrow{\asymp} \cdot \xrightarrow{\ell_2} \cdot \xRightarrow{\asymp} \dots \xRightarrow{\asymp} \cdot \xrightarrow{\ell_k} \cdot \xRightarrow{\asymp} \epsilon \quad (1)$$

is called a *witness path* of \asymp -norm for α . The *length* of the witness path is k .

Clearly, the \asymp -norms have the following basic fact:

Lemma 33. If $\alpha \asymp \beta$, then $\|\alpha\|_{\asymp} = \|\beta\|_{\asymp}$.

If \asymp is an arbitrary equivalence relation, the witness path does not always exist, because it is not always the case $\alpha \xRightarrow{\asymp} \beta$ whenever $\alpha \asymp \beta$. This is one of the motivations of the forthcoming notion of *decreasing bisimulation* (Definition 15). For the moment, we introduce the \asymp -decreasing transitions.

Definition 14. A transition $\alpha \xrightarrow{\ell} \alpha'$ is \asymp -decreasing if $\|\alpha'\|_{\asymp} < \|\alpha\|_{\asymp}$.

According to Definition 13, $\|\alpha'\|_{\asymp} = \|\alpha\|_{\asymp} - 1$ if $\alpha \xrightarrow{\ell} \alpha'$ is a \asymp -decreasing transition. In witness path (1), every transition $\xrightarrow{\ell_i}$ must be \asymp -decreasing for $1 \leq i \leq k$.

Definition 15. A process equivalence \asymp is a *decreasing bisimulation*, if the following conditions are satisfied:

- 1) If $\alpha \asymp \epsilon$, then $\alpha \Rightarrow \epsilon$.
- 2) If $\alpha \asymp \beta$ and $\alpha \xrightarrow{\ell} \alpha'$ is a \asymp -decreasing transition, then there exist β'' and β' such that $\beta \xRightarrow{\asymp} \beta'' \xrightarrow{\ell} \beta'$ and $\alpha' \asymp \beta'$.

Decreasing bisimulation is a weaker version of bisimulation. The difference lies in that only decreasing transitions need to be matched. Be aware that the transition $\beta'' \xrightarrow{\ell} \beta'$ in Definition 15 is forced to be \asymp -decreasing.

Let \asymp be a decreasing bisimulation. Then any \asymp -decreasing transition of α can be extended to a witness path of \asymp -norm of α . The norm $\|\alpha\|_{\asymp}$ is equal to the least number of decreasing transitions from α to ϵ .

Nearly all equivalences appearing in this paper are decreasing bisimulation. For example:

Proposition 34. \simeq_R is a decreasing bisimulation for every $R \subseteq \mathbf{C}_G$.

There is no need to define the so-called *R-decreasing bisimulation*. The following lemma confirms that, for decreasing transitions, $\xrightarrow{\ell}_R$ and $\xrightarrow{\ell}$ are essentially the same.

Lemma 35. If $\alpha \xrightarrow{\ell}_R \beta$ is \simeq_R -decreasing, then $\alpha \xrightarrow{\ell} \beta'$ for some β' such that $\beta'_R = \beta$.

The following lemma provides a bound for semantic norms.

Lemma 36. If \asymp is a decreasing bisimulation, then $\|\alpha\|_{\asymp} \leq |\alpha|_{\text{st}}$ for every α .

Remark 7. The labelled transition graph defined by a normed BPA Γ can be perceived as a *directed graph* \mathcal{G} (with infinite number of nodes) whose nodes are the processes and whose edges are the labelled transitions. \mathcal{G} can be extended to a *weighted direct graph* in different ways. Let \mathcal{G}_{st} be the weighted extension of \mathcal{G} in which every edge of \mathcal{G} has weight *one*. Let \mathcal{G}_{wk} be the one which is the same as \mathcal{G}_{st} except that the weight of every silent transition is *zero*. The strong (resp. weak) norm of a process α is the length of the shortest path from α to ϵ in \mathcal{G}_{st} (resp. \mathcal{G}_{wk}). Let \asymp be an equivalence relation on processes. We can define the graph \mathcal{G}_{\asymp} which is the same as \mathcal{G}_{st} except that the weight of $\gamma \xrightarrow{\ell} \gamma'$ is set *zero* if $\gamma \asymp \gamma'$. A witness path of \asymp -norm of α corresponds to a shortest path from α to ϵ in \mathcal{G}_{\asymp} .

If \simeq_R is known for every R , then \simeq_R -norm of a BPA process (or constant) can be calculated via the greedy strategy in an efficient way. It depends on the following property:

- 1) $\|\alpha\|_{\simeq_R} = 0$ if and only if $\alpha \simeq_R \epsilon$.
- 2) $\|\alpha\beta\|_{\simeq_R} = \|\alpha\|_{\simeq_{R'}} + \|\beta\|_{\simeq_R}$ in which $R' = \text{Rd}_{\simeq_R}(\beta)$.

It works like a generalization of Breadth-first search, or a variant of Dijkstra's algorithm. The detail of the calculation is omitted, but this idea will be used to calculate the semantic norms $\|\cdot\|_{\simeq_R}$ later (Section VI) in the refinement procedure when constructing new base from the old.

D. Decreasing Bisimulation with R-Expansion of \simeq

Based on decreasing transitions, we can define a special notion called *decreasing bisimulation with R-expansion of \simeq* , which will be taken as the refinement operation in our algorithm. This notion is crucial to the correctness of the refinement operation. The readers are suggested to review Definition 6 and Definition 15 before going on.

Definition 16. Let \asymp and \simeq be two equivalences on processes such that $=_R \subseteq \asymp \subseteq \simeq$. We say that \asymp is an *R-expansion of \simeq* if the following conditions hold whenever $\alpha \asymp \beta$:

- 1) $\alpha \Rightarrow \epsilon$ if and only if $\beta \Rightarrow \epsilon$.
- 2) If $\alpha \not\xrightarrow{\ell} \alpha'$, then either $\beta_R \xRightarrow{\asymp} \beta' \cdot \xrightarrow{\ell}_R \beta''$ for some β' such that $\alpha' \simeq \beta''$.
- 3) If $\alpha \xrightarrow{a} \alpha'$, then $\beta_R \xRightarrow{\asymp} \beta' \cdot \xrightarrow{a}_R \beta''$ for some β' such that $\alpha' \simeq \beta''$.

We say that \succsim is a *decreasing bisimulation with R -expansion* of \simeq if \succsim is both a decreasing bisimulation and an R -expansion of \simeq .

The following lemma provides another characterization of the decreasing bisimulation with R -expansion of \simeq .

Lemma 37. Assume that $=_R \subseteq \succsim \subseteq \simeq$. \succsim is an decreasing bisimulation with R -expansion of \simeq if and only if following conditions hold whenever $\alpha \succsim \beta$ and α, β are in R -nf:

- 1) if $\alpha \xRightarrow{R} \epsilon$, then $\beta \xRightarrow{R} \epsilon$;
- 2) if $\alpha \xrightarrow{*}_R \alpha'$, being \succsim -decreasing, then $\beta \xRightarrow{R} \cdot \xrightarrow{*}_R \beta'$ for some β' such that $\alpha' \simeq \beta'$;
- 3) if $\alpha \not\xrightarrow{*}_R \alpha'$, not being \succsim -decreasing, then $\beta \xRightarrow{R} \cdot \xrightarrow{*}_R \beta'$ for some β' such that $\alpha' \simeq \beta'$;
- 4) if $\alpha \xrightarrow{a}_R \alpha'$, being \succsim -decreasing, then $\beta \xRightarrow{R} \cdot \xrightarrow{a}_R \beta'$ for some β' such that $\alpha' \simeq \beta'$;
- 5) if $\alpha \xrightarrow{a}_R \alpha'$, not being \succsim -decreasing, then $\beta \xRightarrow{R} \cdot \xrightarrow{a}_R \beta'$ for some β' such that $\alpha' \simeq \beta'$.

Remark 8. The style of the definition of ‘decreasing bisimulation with expansion’ also appears in [27]. The main difference is that in this paper, the ‘decreasing transitions’ are semantic, while in [27], the ‘decreasing transitions’ are syntactic.

The notion of ‘decreasing bisimulation with expansion’ is a better understanding of the previous refinement operations on totally normed BPA and BPP [15], [26]. Moreover, this notion is crucial to the development of a polynomial time algorithm for branching bisimilarity on totally normed BPA [27].

V. DECOMPOSITION BASES

In this section, we define a way for finitely representing a family of equivalences which satisfies unique decomposition property in the sense of Theorem 3. Such family of equivalences include $\{\simeq_R\}_R$ and all the intermediate families of equivalences constructed during the iterations. This finite representation is named decomposition base.

A. R -blocks and R -orders

To make our algorithm easy to formulate, we need some technical preparations. The reason will be clear later.

Definition 17. Let $R \subseteq \mathbf{C}_G$. We call that α is R -associate to β if $\alpha \Longleftrightarrow_R \beta$. Let $X \in \mathbf{C} \setminus R$. The R -block related to X , denoted by $[X]_R$ is the set of all the constants which is R -associate to X . Namely, $[X]_R \stackrel{\text{def}}{=} \{Y \mid X \Longleftrightarrow_R Y\}$. We use the term *block* to specify any R -block for $R \subseteq \mathbf{C}_G$.

Clearly, two R -blocks coincide when they overlap. Thus R -blocks compose a partition of $\mathbf{C} \setminus R$. The partition is denoted by $\mathbf{C}_R \stackrel{\text{def}}{=} \{[X]_R \mid X \in \mathbf{C} \setminus R\}$.

We will use the convention that the members of $[X]_R$ for different R 's are taken from different copy of \mathbf{C} . In other words, if $R_1 \neq R_2$, then $[X]_{R_1}$ and $[X]_{R_2}$ are always disjoint, and they are regarded as different objects, even if they indicate the same set.

Remark 9. The intuition of R -blocks is obvious. According to the Computation Lemma (Lemma 11), The R -associate

constants are R -bisimilar to each other, thus they can be *contracted* into a single one. In the work [27] for totally normed BPA, we prevent the occurrence of $X \Longleftrightarrow Y$ via a preprocess in which mutually associate constants are contracted into a single one. For normed BPA discussed in this paper, we take the same idea but the difficulty is that the contracting operation cannot be performed uniformly, for it depends on the reference set R . The only way we can take is to introduce the R -association and to contract R -associate constants into R -blocks for individual R 's. The members in an R -block are interchangeable.

Be aware that it is possible that $X \simeq_R \epsilon$ even if $X \notin R$. In this case we must have $[X]_R \subseteq \text{Id}_R$ by the Computation Lemma (Lemma 11). Also note that it is possible that $X \Longleftrightarrow_R \epsilon$ for some R . But these kinds of R is uninteresting because by putting such X into R we can get a larger reference set R' such that $\simeq_{R'} = \simeq_R$.

We call a reference set R *qualified* if $X \Longleftrightarrow_R \epsilon$ cannot happen for every $X \notin R$. The unqualified R 's can be pre-determined. They are useless from now to the end of this paper. From now on we assume that every reference set R is qualified. For example when we write ‘for every $R \subseteq \mathbf{C}_G$ ’, we refer to every *qualified* R which is a subset of \mathbf{C}_G . In particular, every admissible set is qualified.

Lemma 38. All constants in a block $[X]_R$ are R -bisimilar.

Lemma 39. If $[X]_R \neq [Y]_R$ and $X \xRightarrow{R} Y$, then $Y \not\xRightarrow{R} X$.

The behaviours of $[X]_R$ can be more than the total behaviours of its member constants. All the processes associate to X should be taken into account. It is possible that $X \Longleftrightarrow_R \zeta X'$ for some ground process ζ . For instance we can have $X \xRightarrow{R} Z \xRightarrow{R} \zeta Y \xRightarrow{R} Y \xRightarrow{R} X$. In this example, $X, Y, Z, \zeta X, \zeta Y, \zeta Z$ are mutually R -associate. Thus the behaviour of ζ should also be taken into account.

Definition 18. Y is an R -propagating of X (or of $[X]_R$) if $X \Longleftrightarrow_R Y \zeta X'$ for some ζ and X' . (In this case we must have $X' \Longleftrightarrow_R X$, and $Y \zeta$ is ground.)

Lemma 40. $Y \in \text{Rd}_R(X)$ if Y is an R -propagating of X .

Lemma 41. Suppose $X \Longleftrightarrow_R \zeta X' \xrightarrow{\ell}_R \zeta' X'$ such that $\zeta' X' \not\xRightarrow{R} X$. Then $X' \in [X]_R$, and $\zeta = Y \gamma$ for some Y and γ such that

- Y is an R -propagating of $[X]_R$.
- $Y \xrightarrow{\ell} \alpha$ and $\zeta' = \alpha \gamma$.
- $X \simeq_R \gamma X$. (i.e. $\gamma \in (\text{Rd}_R(X))^*$)
- $Y.X \xrightarrow{\ell}_R \alpha X$ with $Y.X \simeq_R \zeta X' \simeq_R X$ and $\alpha X \simeq_R \zeta' X \simeq_R \zeta' X'$.

Lemma 41 shows that the behaviours of $[X]_R$ are completely determined by the associate constants and the propagating constants of X , which leads to the following definition.

Definition 19. The R -derived transition $\xrightarrow{\ell}_R$ is defined as follows:

- 1) Let $\hat{X} \in [X]_R$ and $\hat{X} \xrightarrow{\ell}_R \alpha$. If either $\ell \neq \tau$, or $\ell = \tau$ and $\alpha \not\Rightarrow_R X$, then $[X]_R \xrightarrow{\ell}_R \alpha$.
- 2) Let Y be an R -propagating of $[X]_R$ and $Y \xrightarrow{\ell}_R \alpha$. If either $\ell \neq \tau$, or $\ell = \tau$ and $\alpha \not\Rightarrow_R \epsilon$, then $[X]_R \xrightarrow{\ell}_R \alpha.X$.

Lemma 42. Suppose $X \Longleftrightarrow_R \cdot \xrightarrow{\ell}_R \alpha$. If either $\ell \neq \tau$, or $\ell = \tau$ and $\alpha \not\Rightarrow_R X$, then $[X]_R \xrightarrow{\ell}_R \cdot \simeq_R \alpha$.

It is technically convenient to treat the R -blocks as the basic objects in the algorithm, because of the following lemma.

Lemma 43. If $[X]_R \xrightarrow{\tau}_R \cdot \Rightarrow_R Y$, then $[Y]_R \neq [X]_R$.

Finally we can define an order on R -blocks based on Lemma 39. For every R , we fix a linear order $<_R$ such that whenever $[X]_R <_R [Y]_R$, we have $X \not\Rightarrow_R Y$.

Lemma 44. If $[X]_R \xrightarrow{\tau}_R \cdot \Rightarrow_R Y$, then $[Y]_R <_R [X]_R$.

Example 2. The example illustrates why we have to introduce possibly different orders $<_R$ for different R 's.

In a normed BPA system $\Gamma = (\mathbf{C}, \mathbf{A}, \Delta)$, we can have the following fragment of definition: Let A_1, A_2, B_1, B_2 be constants in \mathbf{C}_G . We have transition rules:

$$A_1 \xrightarrow{\tau} A_2 B_1, \quad A_2 \xrightarrow{\tau} A_1 B_2.$$

There can be other transitions related to these constants which is of no importance. Now, take notice of the following facts:

- In the case of $R_1 = \{B_1\}$, we have $A_1 \xrightarrow{\tau}_{R_1} A_2$. Thus we have $[A_2]_{R_1} <_{R_1} [A_1]_{R_1}$. Or, in short, $A_2 <_{R_1} A_1$.
- In the case of $R_2 = \{B_2\}$, we have $A_2 \xrightarrow{\tau}_{R_2} A_1$. Thus we have $[A_1]_{R_2} <_{R_2} [A_2]_{R_2}$. Or, in short, $A_1 <_{R_2} A_2$.

These two orders $<_{R_1}$ and $<_{R_2}$ are clearly not consistent. This feature reflects a big difference between normed BPA and totally normed BPA.

Remark 10. There is also a big difference between normed BPA and normed BPP. In the case of normed BPP [30], [31], let us say that X generates Y if $X \Longleftrightarrow Y \parallel X$, in while ‘ \parallel ’ is the operator of *parallel composition*. Thus, if X generates Y , then $X \Longleftrightarrow Y^n \parallel X$ hence $X \simeq Y^n \parallel X$ for every $n \in \mathbb{N}$. Suppose that $X \xrightarrow{a} \epsilon$, we have

$$X \Longleftrightarrow \underbrace{Y \parallel \dots \parallel Y}_{n \text{ times}} \parallel X \xrightarrow{a} \underbrace{Y \parallel \dots \parallel Y}_{n \text{ times}}$$

for every $n \in \mathbb{N}$. Now, if all the

$$\underbrace{Y \parallel \dots \parallel Y}_{n \text{ times}} \parallel X$$

for every $n \in \mathbb{N}$ are contracted into a block $[X]$, then we have

$$[X] \xrightarrow{\ell} \underbrace{Y \parallel \dots \parallel Y}_{n \text{ times}}$$

for every $n \in \mathbb{N}$, as is done in the same way as Definition 19. This example shows that the behaviour of $[X]$ is infinite branching. Note that in the case of normed BPA, this situation is not possible. If $X \Longleftrightarrow Y \zeta X$, then actions in X can only be

activated after $Y \zeta$ is consumed completely. This nice property of normed BPA simplifies the situation greatly.

B. Decomposition Bases

A *decomposition base* \mathcal{B} is a family of $\{\mathcal{B}_R\}_{R \subseteq \mathbf{C}_G}$ in which every \mathcal{B}_R is a quintuple $(\mathbf{Id}_R^{\mathcal{B}}, \mathbf{Pr}_R^{\mathcal{B}}, \mathbf{Cm}_R^{\mathcal{B}}, \mathbf{Dc}_R^{\mathcal{B}}, \mathbf{Rd}_R^{\mathcal{B}})$.

- $\mathbf{Id}_R^{\mathcal{B}}$ is a subset of ground constants called \mathcal{B}_R -identities.
- $\mathbf{Cm}_R^{\mathcal{B}}$ specifies the set of \mathcal{B}_R -composites. A \mathcal{B}_R -composite is an $\mathbf{Id}_R^{\mathcal{B}}$ -block.
- $\mathbf{Pr}_R^{\mathcal{B}}$ specifies the set of \mathcal{B}_R -primes. A \mathcal{B}_R -prime is an $\mathbf{Id}_R^{\mathcal{B}}$ -block.
- $\mathbf{Rd}_R^{\mathcal{B}}$ is a function whose domain is $\mathbf{Pr}_R^{\mathcal{B}}$. Let $[X]_{\mathbf{Id}_R^{\mathcal{B}}}$ be a \mathcal{B}_R -prime. The value $\mathbf{Rd}_R^{\mathcal{B}}([X]_{\mathbf{Id}_R^{\mathcal{B}}})$ is a set of ground constants which are called \mathcal{B}_R -redundant over $[X]_{\mathbf{Id}_R^{\mathcal{B}}}$.
- $\mathbf{Dc}_R^{\mathcal{B}}$ is a function whose domain is $\mathbf{Cm}_R^{\mathcal{B}}$. Let $[X]_{\mathbf{Id}_R^{\mathcal{B}}}$ be a \mathcal{B}_R -composite. The value $\mathbf{Dc}_R^{\mathcal{B}}([X]_{\mathbf{Id}_R^{\mathcal{B}}})$ is called the \mathcal{B}_R -decomposition of $[X]_{\mathbf{Id}_R^{\mathcal{B}}}$, which is a string of blocks $[X_r]_{R_r} [X_{r-1}]_{R_{r-1}} \dots [X_2]_{R_2} [X_1]_{R_1}$ with $r \geq 1$, $R_1 = \mathbf{Id}_{R_1}^{\mathcal{B}}$, $[X_i]_{R_i} \in \mathbf{Pr}_{R_i}^{\mathcal{B}}$ and $R_{i+1} = \mathbf{Rd}_{R_i}^{\mathcal{B}}([X_i]_{R_i})$ for every $1 \leq i < r$.

To make a decomposition base \mathcal{B} work properly, we need the following constraints:

- 1) $R \subseteq \mathbf{Id}_R^{\mathcal{B}} \subseteq \mathbf{C}_G$.
- 2) If $R \subseteq S$, then $\mathbf{Id}_R^{\mathcal{B}} \subseteq \mathbf{Id}_S^{\mathcal{B}}$. If $R \subseteq S \subseteq \mathbf{Id}_R^{\mathcal{B}}$, then $\mathbf{Id}_R^{\mathcal{B}} = \mathbf{Id}_S^{\mathcal{B}}$. In particular, $\mathbf{Id}_{\mathbf{Id}_R^{\mathcal{B}}}^{\mathcal{B}} = \mathbf{Id}_R^{\mathcal{B}}$.
- 3) $\mathcal{B}_R = \mathbf{Id}_R^{\mathcal{B}}$ for every R . When $R = \mathbf{Id}_R^{\mathcal{B}}$, R is called \mathcal{B} -admissible. \mathcal{B} is completely determined by those \mathcal{B}_R in which R is \mathcal{B} -admissible.
- 4) If R is \mathcal{B} -admissible, then $\mathbf{Cm}_R^{\mathcal{B}}$ and $\mathbf{Pr}_R^{\mathcal{B}}$ are a partition of R -blocks: $\mathbf{Cm}_R^{\mathcal{B}} \cup \mathbf{Pr}_R^{\mathcal{B}} = R$ and $\mathbf{Cm}_R^{\mathcal{B}} \cap \mathbf{Pr}_R^{\mathcal{B}} = \emptyset$.
- 5) $\mathbf{Rd}_R^{\mathcal{B}}([X]_{\mathbf{Id}_R^{\mathcal{B}}})$ is \mathcal{B} -admissible provided that $[X]_{\mathbf{Id}_R^{\mathcal{B}}}$ is a \mathcal{B}_R -prime. Thus $\mathbf{Dc}_R^{\mathcal{B}}$ is well-defined.

A decomposition base \mathcal{B} defines a family of string rewriting system $\{\xrightarrow{\mathcal{B}}_R\}_{R \subseteq \mathbf{C}_G}$. The family of \mathcal{B}_R -reduction relations are defined according to the following structural rules.

$$\frac{\frac{X \in \mathbf{Id}_R^{\mathcal{B}}}{X \xrightarrow{\mathcal{B}}_R \epsilon} \quad \frac{X \notin \mathbf{Id}_R^{\mathcal{B}}}{X \xrightarrow{\mathcal{B}}_R [X]_{\mathbf{Id}_R^{\mathcal{B}}}} \quad \frac{\mathbf{Dc}_R^{\mathcal{B}}([X]_{\mathbf{Id}_R^{\mathcal{B}}}) = \alpha}{[X]_{\mathbf{Id}_R^{\mathcal{B}}} \xrightarrow{\mathcal{B}}_R \alpha}}{\frac{[X]_{\mathbf{Id}_R^{\mathcal{B}}} \in \mathbf{Pr}_R^{\mathcal{B}} \quad \alpha \xrightarrow{\mathcal{B}}_{\mathbf{Rd}_R^{\mathcal{B}}([X]_{\mathbf{Id}_R^{\mathcal{B}}})} \alpha'}{\alpha.[X]_{\mathbf{Id}_R^{\mathcal{B}}} \xrightarrow{\mathcal{B}}_R \alpha'} \quad \frac{\beta \xrightarrow{\mathcal{B}}_R \beta'}{\alpha.\beta \xrightarrow{\mathcal{B}}_R \alpha.\beta'}}$$

\mathcal{B}_R -reduction relations are deterministic. Thus for any process α , the \mathcal{B}_R -normal-form (in the sense of string rewriting systems) is unique, and it is called the \mathcal{B}_R -decomposition of α . We use the notation $\text{dcmp}_R^{\mathcal{B}}(\alpha)$ to indicate the \mathcal{B}_R -decomposition of α . Processes α and β are \mathcal{B}_R -equivalent, notation $\alpha \stackrel{\mathcal{B}}{=} \beta$, if they have the same \mathcal{B}_R -decomposition.

Lemma 45. $\alpha \stackrel{\mathcal{B}}{=} \beta$ if and only if $\text{dcmp}_R^{\mathcal{B}}(\alpha) = \text{dcmp}_R^{\mathcal{B}}(\beta)$.

According to \mathcal{B}_R -reduction rules, we have the following characterization of $\text{dcmp}_R^{\mathcal{B}}(\alpha)$.

Lemma 46. If R is \mathcal{B} -admissible, then

- $\text{dcmp}_R^{\mathcal{B}}(\epsilon) = \epsilon$.

- If $X \in R$, then $\text{dcmp}_R^{\mathcal{B}}(\gamma X) = \text{dcmp}_R^{\mathcal{B}}(\gamma)$.
- If $X \notin R$, then $\text{dcmp}_R^{\mathcal{B}}(\gamma X) = \text{dcmp}_R^{\mathcal{B}}(\gamma.[X]_R)$.
- If $[X]_R \in \mathbf{Cm}_R$, then
$$\text{dcmp}_R^{\mathcal{B}}(\gamma.[X]_R) = \text{dcmp}_R^{\mathcal{B}}(\gamma.\mathbf{Dc}_R([X]_R)).$$
- If $[X]_R \in \mathbf{Pr}_R$, then
$$\text{dcmp}_R^{\mathcal{B}}(\gamma.[X]_R) = (\text{dcmp}_{\mathbf{Rd}_R^{\mathcal{B}}([X]_R)}^{\mathcal{B}}(\gamma)).[X]_R.$$

If R is not \mathcal{B} -admissible, then $\text{dcmp}_R^{\mathcal{B}}(\alpha) = \text{dcmp}_{\mathbf{Id}_R^{\mathcal{B}}}^{\mathcal{B}}(\alpha)$.

We list some basic facts.

Lemma 47. $\alpha \stackrel{\mathcal{B}}{=} \beta$ if and only if $\alpha \in \mathbf{Id}_R^{\mathcal{B}}$. When R is \mathcal{B} -admissible, $\alpha \stackrel{\mathcal{B}}{=} \beta$ if and only if $\alpha \in R$.

Lemma 48. If $X_1, X_2 \in [X]_R$, then $X_1 \stackrel{\mathcal{B}}{=} X_2$ and $\|X_1\|_{\mathcal{B}} = \|X_2\|_{\mathcal{B}}$.

We can write $\|[X]_R\|_{\mathcal{B}} = \|\hat{X}\|_{\mathcal{B}}$ for any $\hat{X} \in [X]_R$.

Lemma 49. $\|X\|_{\mathcal{B}} \geq 1$ if R is \mathcal{B} -admissible and $X \notin R$.

Lemma 50. If $\stackrel{\mathcal{B}}{=}$ is a decreasing bisimulation, then the size of $\mathbf{Dc}_R^{\mathcal{B}}([X]_R)$ is exponentially bounded.

In the following the superscript \mathcal{B} will often be omitted if \mathcal{B} is clear from the context. For example sometimes we write \mathbf{Pr}_R for $\mathbf{Pr}_R^{\mathcal{B}}$.

C. Representing \simeq_R via Decomposition Base

We define a decomposition base $\hat{\mathcal{B}}$ which can represent \simeq_R for every R . That is, $\alpha \stackrel{\hat{\mathcal{B}}}{=} \beta$ if and only if $\alpha \simeq_R \beta$. Theorem 3 is crucial. Moreover, there are other subtleties which deserve to be mentioned.

Lemma 51. All constants in a block $[X]_{\mathbf{Id}_R}$ are R -bisimilar.

The description of $\hat{\mathcal{B}} = \{(\mathbf{Id}_R, \mathbf{Pr}_R, \mathbf{Cm}_R, \mathbf{Dc}_R, \mathbf{Rd}_R)\}_R$ relies on the family of orders $\{<_R\}_R$ defined in Section V-A. It contains three steps:

- In the first step, we determine \mathbf{Id}_R for every R : $\mathbf{Id}_R = \mathbf{Id}_R$. According to Proposition 14, Proposition 16 and their corollaries, \mathbf{Id}_R satisfies constraints 1–3 in Section V-B. In particular, R is admissible if and only if R is $\hat{\mathcal{B}}$ -admissible.
- In the second step, we determine other constituents of $\hat{\mathcal{B}}_R$ for every $\hat{\mathcal{B}}$ -admissible R :
 - $\mathbf{Pr}_R = \{[X]_R \mid X \in \mathbf{Pr}_R \text{ and } X \not\approx_R Y \text{ for every } Y <_R X\}$.
 - $\mathbf{Cm}_R = \{[X]_R \mid X \in \mathbf{Cm}_R, \text{ or } X \in \mathbf{Pr}_R \text{ and } X \simeq_R Y <_R X \text{ for some } Y\}$.
 - If $[X]_R \in \mathbf{Pr}_R$, then $\mathbf{Rd}_R([X]_R) = \{Y \mid YX \simeq_R X\}$. Be aware that $\mathbf{Rd}_R([X]_R)$ is admissible (also $\hat{\mathcal{B}}$ -admissible) according to Lemma 27.
 - If $[X]_R \in \mathbf{Cm}_R$, then $\mathbf{Dc}_R([X]_R) = [X_r]_{R_r} [X_{r-1}]_{R_{r-1}} \dots [X_2]_{R_2} [X_1]_{R_1}$, in which $X \simeq_R X_r.X_{r-1} \dots X_1$, $R_1 = R$, $[X_i]_{R_i} \in \mathbf{Pr}_{R_i}$ and $R_{i+1} = \mathbf{Rd}_{R_i}([X_i]_{R_i})$ for every $1 \leq i < r$. Thanks to the $\hat{\mathcal{B}}$ -admissibility of $\mathbf{Rd}_{R_i}([X_i]_{R_i})$ for $1 \leq i \leq r$, $\mathbf{Dc}_R([X]_R)$ is well-defined.

- In the third step, for every non- $\hat{\mathcal{B}}$ -admissible R , $\hat{\mathcal{B}}_{\mathbf{Id}_R}$ is assigned to $\hat{\mathcal{B}}_R$. That is, $\mathbf{Pr}_R := \mathbf{Pr}_{\mathbf{Id}_R}$, $\mathbf{Cm}_R := \mathbf{Cm}_{\mathbf{Id}_R}$, and so on.

Pay special attention to the descriptions of \mathbf{Pr}_R and \mathbf{Cm}_R . They have slightly different from \mathbf{Pr}_R and \mathbf{Cm}_R . Semantically, if $X \in \mathbf{Pr}_R$ and $X \simeq_R Y$, then $Y \in \mathbf{Pr}_R$. In the syntactic description of \mathbf{Pr}_R and \mathbf{Cm}_R , we need the $\hat{\mathcal{B}}_R$ -primes to be absolutely unique, which is accomplished via $<_R$. The orders $<_R$ take effects in double means: Let R be admissible, then

- 1) Among the R -blocks of \simeq_R -primes, there is exactly one distinguished R -block that is qualified as a $\hat{\mathcal{B}}_R$ -prime, which is the $<_R$ -minimum one in the related \simeq_R -class.
- 2) Let $[X]_R$ be a $\hat{\mathcal{B}}_R$ -prime. If $[X]_R \xrightarrow{\tau}_R \alpha$, then $X \stackrel{\hat{\mathcal{B}}}{\neq}_R \alpha$. If $X \Rightarrow_R Y \not\Rightarrow_R X$, then $X \stackrel{\hat{\mathcal{B}}}{\neq}_R Y$.

Every decomposition base constructed during the refinement procedure in our algorithm will satisfy these two properties.

Remark 11. For realtime normed BPA (or BPP), there is an even strong property. There exists a uniform order ' $<$ ' on all the constants such that, whenever $X \xrightarrow{\ell} \alpha$ is syntactically (also semantically) decreasing or \asymp -preserving (for some appropriate \asymp), all the constants in α will be strictly less than X in order ' $<$ '. In history, this property plays a significant role in the previous fast bisimilarity decision algorithms [26], [15].

For totally normed BPA, we have an adaptation of this strong property, in which the condition becomes $X \xrightarrow{\ell} \alpha$ is syntactically (no longer semantically) decreasing, or weak-norm-preserving (no longer \asymp -preserving) [27].

For non-realtime normed BPA systems, the above requirement is definitely too strong to be satisfied, so that the decision algorithm must be developed in some other ways. This is the origination of putting semantic norms into the algorithm.

Ultimately we have the following coincidence result.

Proposition 52. $\alpha \simeq_R \beta$ if and only if $\alpha \stackrel{\hat{\mathcal{B}}}{=} \beta$.

VI. DESCRIPTION OF THE ALGORITHM

Our algorithm takes the partition refinement approach. The purpose is to figure out the $\hat{\mathcal{B}}$ defined in Section V-C. The strategy is to start with a special initial base \mathcal{B}_0 satisfying $\hat{\mathcal{B}} \subseteq \mathcal{B}_0$ and iteratively refine it. We will use notation $\mathcal{B} \subseteq \mathcal{D}$ to mean that $\stackrel{\mathcal{B}}{=} \subseteq \stackrel{\mathcal{D}}{=}$ for every R . The refinement operation will be denoted by Ref . By taking $\mathcal{B}_{i+1} = \text{Ref}(\mathcal{B}_i)$, we have a sequence of decomposition bases

$$\mathcal{B}_0, \mathcal{B}_1, \mathcal{B}_2, \dots$$

such that

$$\mathcal{B}_0 \supseteq \mathcal{B}_1 \supseteq \mathcal{B}_2 \supseteq \dots$$

The correctness of the refinement operation adopted in this paper depends on the following requirements, which will be proved gradually:

- 1) $\hat{\mathcal{B}} \subseteq \mathcal{B}_0$.
- 2) $\text{Ref}(\hat{\mathcal{B}}) = \hat{\mathcal{B}}$.

3) If $\widehat{\mathcal{B}} \subsetneq \mathcal{B}$, then $\widehat{\mathcal{B}} \subseteq \text{Ref}(\mathcal{B}) \subsetneq \mathcal{B}$.

According to the above three requirements, once the sequence $\{\mathcal{B}_i\}_{i \in \omega}$ becomes stable, say $\mathcal{B}_i = \mathcal{B}_{i+1}$ for some i , we can affirm that $\widehat{\mathcal{B}} = \mathcal{B}_i$.

On the whole, our algorithm is an iteration:

- 1) Compute the initial base \mathcal{B}_0 and let $\mathcal{D} := \mathcal{B}_0$.
- 2) Compute the new base \mathcal{B} from the old base \mathcal{D} .
- 3) If \mathcal{B} equals \mathcal{D} then halt and return \mathcal{B} .
- 4) $\mathcal{D} := \mathcal{B}$ and go to step 2.

Apparently, the algorithm relies on the initial base and the refinement step which computes $\mathcal{B} = \text{Ref}(\mathcal{D})$ from \mathcal{D} .

A. Relationships between Old and New Bases

Before describing the algorithm in details, we investigate the relationship between two bases \mathcal{B} and \mathcal{D} assume that $\mathcal{B} \subseteq \mathcal{D}$.

Lemma 53. If $\mathcal{B} \subseteq \mathcal{D}$, then $\text{Id}_R^{\mathcal{B}} \subseteq \text{Id}_R^{\mathcal{D}}$ for every R .

Remark 12. An interesting consequence according to Lemma 53 is that, if $R = \text{Id}_R^{\mathcal{D}}$, then $R = \text{Id}_R^{\mathcal{B}}$ must hold because $R \subseteq \text{Id}_R^{\mathcal{B}} \subseteq \text{Id}_R^{\mathcal{D}}$. This confirms the fact that, during the iteration of refinement, once a reference set R becomes \mathcal{B} -admissible, it preserves the admissibility in the future.

Lemma 54. If $\mathcal{B} \subseteq \mathcal{D}$ and $\text{Id}_R^{\mathcal{B}} = \text{Id}_R^{\mathcal{D}}$, then $\text{Pr}_R^{\mathcal{D}} \subseteq \text{Pr}_R^{\mathcal{B}}$.

Lemma 55. If $\mathcal{B} \subseteq \mathcal{D}$, $\text{Id}_R^{\mathcal{B}} = \text{Id}_R^{\mathcal{D}}$, and $\text{Pr}_R^{\mathcal{B}} = \text{Pr}_R^{\mathcal{D}}$, then $\text{Rd}_R^{\mathcal{B}} \subseteq \text{Rd}_R^{\mathcal{D}}$.

Lemma 56. If $\mathcal{B} \subseteq \mathcal{D}$, and moreover $\text{Id}_R^{\mathcal{B}} = \text{Id}_R^{\mathcal{D}}$, $\text{Pr}_R^{\mathcal{B}} = \text{Pr}_R^{\mathcal{D}}$, and $\text{Rd}_R^{\mathcal{B}} = \text{Rd}_R^{\mathcal{D}}$ for every R , then $\mathcal{B} = \mathcal{D}$.

The purpose of Lemma 53 to Lemma 56 is to get the following fact.

Proposition 57. The total number of iterations (i.e. refinement operations) in our algorithm is exponentially bounded.

B. The Initial Base

The initial base $\mathcal{B}_0 = \{\mathcal{B}_{0,R}\}_R$ is defined as follows:

- $\text{Id}_R := \mathbf{C}_G = \{X \in \mathbf{C} \mid |X|_{\text{wk}} = 0\}$ for every R .

Thus \mathbf{C}_G is the only \mathcal{B}_0 -admissible set.

- $\text{Pr}_R := \{[P]_{\mathbf{C}_G}\}$ where $[P]_{\mathbf{C}_G}$ is the $<_{\mathbf{C}_G}$ -minimum \mathbf{C}_G -block satisfying $|P|_{\text{wk}} = 1$. $\text{Pr}_R := \emptyset$ in case $\mathbf{C}_G = \mathbf{C}$.
- $\text{Cm}_R := \mathbf{C}_{\mathbf{C}_G} \setminus \text{Pr}_R$.
- $\text{Dc}_R([X]_{\mathbf{C}_G}) := \underbrace{[P]_{\mathbf{C}_G} \cdots [P]_{\mathbf{C}_G}}_{|X|_{\text{wk}} \text{ times}}$ if $[X]_{\mathbf{C}_G} \in \text{Cm}_R$.
- $\text{Rd}_R([P]_{\text{Id}_R}) := \mathbf{C}_G$, if $\text{Pr}_R = \{[P]_{\text{Id}_R}\}$.

Now $\mathcal{B}_{0,R}$ is defined as $(\text{Id}_R, \text{Pr}_R, \text{Cm}_R, \text{Dc}_R, \text{Rd}_R)$. Notice that $\mathcal{B}_{0,R}$ is the same for every $R \subseteq \mathbf{C}_G$.

Lemma 58. $\alpha \stackrel{\mathcal{B}_0}{\sim} \beta$ if and only if $|\alpha|_{\text{wk}} = |\beta|_{\text{wk}}$.

Lemma 59. $\widehat{\mathcal{B}} \subseteq \mathcal{B}_0$. Namely, $\simeq_R \subseteq \stackrel{\mathcal{B}}{=}_R$ for every R .

One can check that all the five constraints described in Section V-B are satisfied by \mathcal{B}_0 .

C. Expansion Conditions

We start to define new base \mathcal{B} from the old base \mathcal{D} . This is the core of our algorithm. The newly constructed $\stackrel{\mathcal{B}}{=}_R$ is made to be a decreasing bisimulation with R -expansion of $\stackrel{\mathcal{D}}{=}_R$. Referring to Lemma 37, we have $\stackrel{\mathcal{B}}{=}_R \subseteq \stackrel{\mathcal{D}}{=}_R$, and for every α, β in R -nf, the following conditions hold whenever $\alpha \stackrel{\mathcal{B}}{=}_R \beta$:

- 1) if $\alpha \Longrightarrow_R \epsilon$, then $\beta \Longrightarrow_R \epsilon$;
- 2) Whenever $\alpha \xrightarrow{\tau}_R \alpha'$,
 - a) if $\alpha \xrightarrow{\tau}_R \alpha'$ is $\stackrel{\mathcal{B}}{=}_R$ -decreasing, then $\beta \stackrel{\mathcal{B}}{=}_R \cdot \xrightarrow{\tau}_R \beta'$ for some β' such that $\alpha' \stackrel{\mathcal{B}}{=}_R \beta'$;
 - b) if $\alpha \xrightarrow{\tau}_R \alpha'$ is not $\stackrel{\mathcal{B}}{=}_R$ -decreasing and $\alpha \not\stackrel{\mathcal{D}}{=}_R \alpha'$, then $\beta \stackrel{\mathcal{B}}{=}_R \cdot \xrightarrow{\tau}_R \beta'$ for some β' such that $\alpha' \stackrel{\mathcal{D}}{=}_R \beta'$;
- 3) Whenever $\alpha \xrightarrow{a}_R \alpha'$,
 - a) if $\alpha \xrightarrow{a}_R \alpha'$ is $\stackrel{\mathcal{B}}{=}_R$ -decreasing, then $\beta \stackrel{\mathcal{B}}{=}_R \cdot \xrightarrow{a}_R \beta'$ for some β' such that $\alpha' \stackrel{\mathcal{B}}{=}_R \beta'$.
 - b) if $\alpha \xrightarrow{a}_R \alpha'$ is not $\stackrel{\mathcal{B}}{=}_R$ -decreasing, then $\beta \stackrel{\mathcal{B}}{=}_R \cdot \xrightarrow{a}_R \beta'$ for some β' such that $\alpha' \stackrel{\mathcal{D}}{=}_R \beta'$.

The above conditions will be called *expansion conditions* in the following. Our task is to construct \mathcal{B} from \mathcal{D} and validate these expansion conditions. From expansion conditions we can see that, in case $\stackrel{\mathcal{B}}{=}_R = \stackrel{\mathcal{D}}{=}_R$, $\stackrel{\mathcal{B}}{=}_R$ must be an R -bisimulation. Thus when $\simeq_R \subsetneq \stackrel{\mathcal{B}}{=}_R$, we must have $\stackrel{\mathcal{B}}{=}_R \subsetneq \stackrel{\mathcal{D}}{=}_R$.

Basically, the construction contains three steps:

- 1) Determine $\text{Id}_R^{\mathcal{B}}$ for every qualified R . After that, we know whether a given R is \mathcal{B} -admissible. Note that some R 's which are not \mathcal{D} -admissible can be \mathcal{B} -admissible.
- 2) Determine other constituents of \mathcal{B}_R for every \mathcal{B} -admissible R .
- 3) For non- \mathcal{B} -admissible R 's, $\mathcal{B}_{\text{Id}_R}$ is copied to \mathcal{B}_R .

The third step is relatively trivial. Its correctness depends on the following lemma.

Lemma 60. If $\simeq_{\text{Id}_R^{\mathcal{B}}} \subseteq \stackrel{\mathcal{B}}{=}_{\text{Id}_R^{\mathcal{B}}}$, then $\simeq_R \subseteq \stackrel{\mathcal{B}}{=}_R$.

The first and second steps of the construction are described in Section VI-D and Section VI-E.

D. Determining $\text{Id}_R^{\mathcal{B}}$

First of all, we must determine what $\text{Id}_R^{\mathcal{B}}$ is. This problem asks under what circumstance we can believe that $X \stackrel{\mathcal{B}}{=}_R \epsilon$ for $X \in \mathbf{C}_G$. Be aware that Lemma 53 confirms that $\text{Id}_R^{\mathcal{B}} \subseteq \text{Id}_R^{\mathcal{D}}$. The basic idea is to make use of the expansion conditions.

Definition 20. Let S be a set that makes $R \subseteq S \subseteq \text{Id}_R^{\mathcal{D}}$. We call S an $\text{Id}_R^{\mathcal{B}}$ -candidate if the following conditions are satisfied whenever $X \in S \setminus R$:

- 1) If $X \xrightarrow{\tau}_R \alpha$ and $\alpha \notin (\text{Id}_R^{\mathcal{D}})^*$, then $\epsilon \xrightarrow{\tau}_R \beta$ for some β such that $\text{dcmp}_R^{\mathcal{D}}(\alpha) = \text{dcmp}_R^{\mathcal{D}}(\beta)$.
- 2) If $X \xrightarrow{a}_R \alpha$, then $\epsilon \xrightarrow{a}_R \beta$ for some β such that $\text{dcmp}_R^{\mathcal{D}}(\alpha) = \text{dcmp}_R^{\mathcal{D}}(\beta)$.

According to Definition 20,

Figure 1. Constructing New Base: Part I

CONSTRUCTINGNEWBASE:

- 1) **for** every R
 COMPUTINGID(R).
 end for
- 2) INITIALIZING.
- 3) $m := 1$.
- 4) **repeat**
- 5) **while** their exists $[X]_R \in \mathbf{U}$ such that
 $[X]_R \xrightarrow{\ell} \gamma$ and $d_R[\gamma] = m - 1$,
 do
 select one of such $[X]_R$ which is $<_R$ -minimum.
 $d_R[[X]_R] := m$.
 if there exists δ such that
 EXPAND $_R(X, \text{dcmp}_R^{\mathcal{B}}(\delta))$, **then**
 put $[X]_R$ into $\mathbf{Cm}_R^{\mathcal{B}}$.
 $\mathbf{Dc}_R^{\mathcal{B}}([X]_R) := \text{dcmp}_R^{\mathcal{B}}(\delta)$.
 else
 put $[X]_R$ into $\mathbf{Pr}_R^{\mathcal{B}}$.
 COMPUTINGRD $_R([X]_R)$.
 end if
 move $[X]_R$ from \mathbf{U} to \mathbf{V} .
 end while
- 6) **while** their exists $[X]_R \in \mathbf{U}$ such that
 $[X]_R \xrightarrow{\tau} \gamma$ and $d_R(\gamma) = m$,
 do
 if EXPAND $_R(X, \text{dcmp}_R^{\mathcal{B}}(\gamma))$, **then**
 put $[X]_R$ into $\mathbf{Cm}_R^{\mathcal{B}}$.
 $d_R[[X]_R] := m$.
 $\mathbf{Dc}_R^{\mathcal{B}}([X]_R) := \text{dcmp}_R^{\mathcal{B}}(\alpha)$.
 move $[X]_R$ from \mathbf{U} to \mathbf{V} .
 else
 move $[X]_R$ from \mathbf{U} to \mathbf{T} .
 end if
 end while
- 7) put every block in \mathbf{T} into \mathbf{U} .
- 8) $m := m + 1$.
 until $\mathbf{U} = \emptyset$
- 9) **for** every non- \mathcal{B} -admissible R
 $\mathcal{B}'_R := \mathcal{B}'_{\text{Id}_R^{\mathcal{B}}}$.
 end for

Figure 2. Constructing New Base: Part II

cases which correspond to two different possibilities that the \mathcal{B}_R -norm of $[X]_R$ can be declared as m .

Remark 14. If R is not \mathcal{B} -admissible, the second part of the above fact cannot always be satisfied. This is one of the reasons why we must construct \mathcal{B}_R only for \mathcal{B} -admissible R 's at first and then copy back to all other R 's.

1) *Treating $[X]_R$: The First Possibility.* : There exists a witness path of $[X]_R$ starting with a \mathcal{B}_R -decreasing transition. That is, $[X]_R \xrightarrow{\ell} \gamma$ for some γ such that $\|\gamma\|_{\mathcal{B}_R} = m - 1$. This possibility is treated via the **while**-block at line 5.

At the time we have known $\text{dcmp}_R^{\mathcal{B}}(\gamma)$. The first problem is to decide whether $[X]_R$ is a prime or a composite. To this end, we try to guess a candidate for decomposition of $[X]_R$, say $[Y_k]_{R_k} [Y_{k-1}]_{R_{k-1}} \dots [Y_1]_{R_1}$ with $R_1 = R$ and $R_{i+1} = \mathbf{Rd}_{R_i}^{\mathcal{B}}(Y_i)$ for $1 \leq i < k$. If this decomposition is 'right', we will have $X \stackrel{\mathcal{B}}{=} Y_k \dots Y_1$. Since $\stackrel{\mathcal{B}}{=}_R$ will be ensured to be a decreasing bisimulation. We must have a matching of $[X]_R \xrightarrow{\ell} \gamma$ from $[Y_k]_{R_k} \dots [Y_1]_{R_1}$, which must be induced by $[Y_k]_{R_k}$. From the above investigation, we can require that $[Y_{k-1}]_{R_{k-1}} \dots [Y_1]_{R_1}$ is a suffix of $\text{dcmp}_R^{\mathcal{B}}(\gamma)$. In summary, in order to guess a candidate for decomposition of $[X]_R$, we need to:

- Guess k . Thus $[Y_{k-1}]_{R_{k-1}} \dots [Y_1]_{R_1}$ is obtained from $\text{dcmp}_R^{\mathcal{B}}(\gamma)$.
- Guess $[Y_k]_{R_k}$, which ensures that $\|Y_k \dots Y_1\|_{\mathcal{B}_R} = m$.

If $k > 1$, then every $\|Y_i\|_{\mathcal{B}_{R_i}} < m$ thus $[Y_i]_{R_i} \in \mathbf{V}$ for every $1 \leq i \leq k$. If $k = 1$, then we guess $\mathbf{Dc}_R^{\mathcal{B}}([X]_R) = [Y_1]_R$ for $Y_1 <_R X$. If every time we pick out the $<_R$ -minimum such $[X]_R$, then we can ensure that $[Y_1]_R \in \mathbf{V}$.

Remark 15. It is probable that $[X_1]_R <_R [X_2]_R$ and $[X_2]_R$ is treated before $[X_1]_R$. For example, it is probable that $\|X_2\|_{\mathcal{B}_R} <_R \|X_1\|_{\mathcal{B}_R}$. But taking our way, we can ensure that $[X_1]_R$ is treated before $[X_2]_R$ whenever $[X_1]_R <_R [X_2]_R$ and $[X_1]_R \stackrel{\mathcal{B}}{=} [X_2]_R$.

After one candidate $[Y_k]_{R_k} \dots [Y_1]_{R_1}$ is found, we will make use of the expansion conditions (Section VI-C) to decide whether $\mathbf{Dc}_R^{\mathcal{B}}([X]_R)$ can be defined as $[Y_k]_{R_k} \dots [Y_1]_{R_1}$. This is done by EXPAND $_R(X, [Y_k]_{R_k} \dots [Y_1]_{R_1})$ defined in Fig. 1.

2) *Treating $[X]_R$: The Second Possibility.* : Every witness path of $[X]_R$ starts with a \mathcal{B}'_R -preserving silent transition. That is, $\|\gamma\|_{\mathcal{B}'_R} \geq m$ for every γ such that $[X]_R \xrightarrow{\ell} \gamma$, but $[X]_R \xrightarrow{\tau} \gamma$ for some γ such that $X \stackrel{\mathcal{B}}{=} \gamma$ (which needs to be confirmed) and $\|\gamma\|_{\mathcal{B}_R} = m$. This possibility is treated via the **while**-blocks at line 6.

This possibility is relatively easy because there is no need to guess the candidates for decomposition of $[X]_R$. If $X \stackrel{\mathcal{B}}{=} \gamma$, we must have $\mathbf{Dc}_R^{\mathcal{B}}([X]_R) = \text{dcmp}_R^{\mathcal{B}}(\gamma)$. Let $[Y_k]_{R_k} \dots [Y_1]_{R_1}$ be $\text{dcmp}_R^{\mathcal{B}}(\gamma)$. Then we will check EXPAND $_R(X, [Y_k]_{R_k} \dots [Y_1]_{R_1})$. Note that it is unnecessary to check the second half of expansion conditions, because $[X]_R \xrightarrow{\tau} \gamma \cdot \stackrel{\mathcal{B}}{=} \gamma$ always holds.

3) *Determining $\mathbf{Rd}_R^{\mathcal{B}}([X]_R)$:* When $[X]_R$ is declared as a \mathcal{B}_R -prime. There is an extra work: define $\mathbf{Rd}_R^{\mathcal{B}}([X]_R)$. Intuitively $\mathbf{Rd}_R^{\mathcal{B}}([X]_R)$ contains all the constants Y which make $Y.X \stackrel{\mathcal{B}}{=} X$. It is necessary that $Y \in \mathbf{C}_G$. We can use the same way of determining $\mathbf{Id}_R^{\mathcal{B}}$ to determine $\mathbf{Rd}_R^{\mathcal{B}}([X]_R)$.

Definition 21. Let $[X]_R$ be a \mathcal{B}_R -prime, let T be the set $\{W \mid W.X \stackrel{\mathcal{D}}{=} X\}$, and let $S \subseteq T$. We call S an $\mathbf{Rd}_R^{\mathcal{B}}([X]_R)$ -candidate if the following conditions are satisfied whenever $Y \in S$:

- 1) If $Y \xrightarrow{\tau} \zeta$ and $\zeta \notin T^*$, then $[X]_R \xrightarrow{\tau} \beta$ for some β such that $\zeta.X \stackrel{\mathcal{D}}{=} \beta$.

- 2) If $Y \xrightarrow{a} \zeta$, then $[X]_R \xrightarrow{\tau}_R \beta$ for some β such that $\zeta.X \stackrel{D}{=}_R \beta$.

According to Definition 21,

- 1) \emptyset is an $\mathbf{Rd}_R^{\mathcal{B}}([X]_R)$ -candidate.
- 2) $\mathbf{Rd}_R^{\mathcal{B}}([X]_R)$ -candidates are closed under union.

$\mathbf{Rd}_R^{\mathcal{B}}([X]_R)$ is defined as the largest $\mathbf{Rd}_R^{\mathcal{B}}([X]_R)$ -candidate. One fast way of computing $\mathbf{Rd}_R^{\mathcal{B}}([X]_R)$ is described as procedure `COMPUTINGRDR` in Fig. 1.

4) *Basic Properties of the Construction:* We point out the following important properties.

Lemma 63. $\mathbf{Rd}_R^{\mathcal{B}}([X]_R)$ constructed above is \mathcal{B} -admissible.

Lemma 64. $d_R([X]_R)$ computed in our algorithm is equal to $\|X\|_{\mathcal{B}_R}$. As an inference, $d_R(\alpha) = \|\alpha\|_{\mathcal{B}_R}$.

Lemma 65. $\mathcal{B} \subseteq \mathcal{D}$. Moreover, if $\hat{\mathcal{B}} \subsetneq \mathcal{D}$, then $\mathcal{B} \subsetneq \mathcal{D}$.

F. The Correctness of the Refinement Operation

Remember Lemma 59 and Lemma 65. The remain thing is to confirm the following fact.

Theorem 4. Suppose that $\hat{\mathcal{B}} \subseteq \mathcal{D}$, then $\hat{\mathcal{B}} \subseteq \mathcal{B}$. Namely, $\alpha \simeq_R \beta$ implies $\alpha \stackrel{\mathcal{B}}{=}_R \beta$ for every R .

It is enough to prove Theorem 4 under the assumption that R 's are \mathcal{B} -admissible. If $\simeq_R \subseteq \stackrel{\mathcal{B}}{=}_R$ for every \mathcal{B} -admissible R 's, then for non- \mathcal{B} -admissible R we have $\simeq_R \subseteq \simeq_{\mathbf{Id}_R^{\mathcal{B}}} \subseteq \stackrel{\mathcal{B}}{=}_{\mathbf{Id}_R^{\mathcal{B}}} = \stackrel{\mathcal{B}}{=}_R$.

The correctness of Theorem 4 relies on some important observations. The following one is crucial.

Lemma 66. Let R be \mathcal{B} -admissible. Let $\gamma = Y_k \dots Y_1$ and $\delta = Z_l \dots Z_1$ such that $[Y_k]_{R_k} [Y_{k-1}]_{R_{k-1}} \dots [Y_1]_{R_1}$ and $[Z_l]_{S_l} [Z_{l-1}]_{S_{l-1}} \dots [Z_1]_{S_1}$ are two \mathcal{B}_R -decompositions, in which $R_1, S_1 = R$ and $R_{i+1} = \mathbf{Rd}_{R_i}(Y_i)$ for $1 \leq i < k$ and $S_{j+1} = \mathbf{Rd}_{S_j}(Z_j)$ for $1 \leq j < l$. If γ and δ satisfy the expansion conditions for \mathcal{B}_R , then we have $k = l$, $R_i = S_i$ and $[Y_i]_{R_i} = [Z_i]_{S_i}$ for $1 \leq i \leq k$.

Lemma 66 confirms that, when $[X]_R$ is being treated, at most one decomposition candidate $[Y_k]_{R_k} \dots [Y_1]_{R_1}$ can make `EXPANDR`($X, [Y_k]_{R_k} \dots [Y_1]_{R_1}$) return **true**. If such a candidate exists, it is declared as $\mathbf{Dc}_R^{\mathcal{B}}([X]_R)$ and $[X]_R$ is declared as a \mathcal{B}_R -composite; otherwise $[X]_R$ is declared as a \mathcal{B}_R -prime. Decreasing bisimulation property is crucial to validate Lemma 66. This is why $\stackrel{\mathcal{B}}{=}_R$ must be constructed as a decreasing bisimulation with R -expansion of $\stackrel{D}{=}_R$ (Section VI-C), rather than simply defined as R -expansion of $\stackrel{D}{=}_R$.

Apparently, the proof of Theorem 4 should be done by induction. Remember that our algorithm maintains a set \mathbf{V} , containing all the blocks which have been treated. We will suppose that R is \mathcal{B} -admissible and let $[X]_R$ be a block which is about to be put into \mathbf{V} . We try to prove Proposition 69. A process α is called $\mathcal{B}_{S, \mathbf{V}}$ -applicable if the derivation of $\alpha \xrightarrow{\mathcal{B}}_R \mathbf{dcmp}_R^{\mathcal{B}}(\alpha)$ (refer to Section V-B) only depends on the

blocks in \mathbf{V} . The following statement is used as induction hypothesis:

IH. Let S be an arbitrary \mathcal{B} -admissible set. Suppose that γ is $\mathcal{B}_{S, \mathbf{V}}$ -applicable, and $\mathbf{dcmp}_S^{\hat{\mathcal{B}}}(\gamma) = [W_u]_{S_u} \dots [W_1]_{S_1}$. Then $W_u \dots W_1$ is $\mathcal{B}_{S, \mathbf{V}}$ -applicable, and $\mathbf{dcmp}_{S, \mathbf{V}}^{\mathcal{B}}(\gamma) = \mathbf{dcmp}_{S, \mathbf{V}}^{\mathcal{B}}(W_u \dots W_1)$. That is, $\gamma \stackrel{\mathcal{B}}{=}_S W_u \dots W_1$.

When \mathbf{V} contains all blocks, we can get Theorem 4.

Making use of **IH** we can establish the following.

Lemma 67. Suppose S is \mathcal{B} -admissible and $\mathbf{dcmp}_S^{\hat{\mathcal{B}}}(W) = [W_u]_{S_u} \dots [W_1]_{S_1}$, and $W_u \dots W_1$ is $\mathcal{B}_{S, \mathbf{V}}$ -applicable.

- 1) If $\|W_u \dots W_1\|_{\mathcal{B}_S} < m$, then $[W]_S \in \mathbf{V}$ and $W \stackrel{\mathcal{B}}{=}_S W_u \dots W_1$.
- 2) If $\|W_u \dots W_1\|_{\mathcal{B}_S} = m$ and $W <_S X$, then $[W]_S \in \mathbf{V}$ and $W \stackrel{\mathcal{B}}{=}_S W_u \dots W_1$.

With Lemma 67 and **IH**, we can show the following auxiliary lemma.

Lemma 68. Suppose $[X]_R$ be a $\hat{\mathcal{B}}_R$ -composite, and assume that $\mathbf{Dc}_R^{\hat{\mathcal{B}}}([X]_R) = [Z_t]_{R_t} \dots [Z_1]_{R_1}$. Then $Z_t \dots Z_1$ is $\mathcal{B}_{R, \mathbf{V}}$ -applicable.

Now, the following Proposition 69 is obtained by Lemma 68 and Lemma 66, and finally Theorem 4 is proved.

Proposition 69. Suppose $[X]_R$ be a $\hat{\mathcal{B}}_R$ -composite, and assume that $\mathbf{Dc}_R^{\hat{\mathcal{B}}}([X]_R) = [Z_t]_{R_t} \dots [Z_1]_{R_1}$. Then $X \stackrel{\mathcal{B}}{=}_R Z_t \dots Z_1$.

G. Remark

Remark 16. The refinement steps defined in previous works [13], [15], [27] have the following interesting property, which says that $\stackrel{\mathcal{B}}{=}^{\mathcal{B}}$ is the *largest* decreasing bisimulation with expansion of $\stackrel{D}{=}^{\mathcal{B}}$, in which

- \mathcal{B} and \mathcal{D} are the new and the old base corresponding to the related works, and $\stackrel{\mathcal{B}}{=}^{\mathcal{B}}$ is the equivalence relation generated by \mathcal{B} ;
- ‘decreasing’ is syntactic;
- ‘decreasing bisimulation with expansion’ is a simplified version of the one in Definition 16.

This fact is also pointed out in [27]. Before this, a step of refinement is divided into two stages, and in [27], it is pointed out that this two-stage understanding does not fit well for branching bisimilarity, thus the notion of *decreasing bisimulation with expansion* is invented accordingly.

In this paper, however, we do not claim that $\stackrel{\mathcal{B}}{=}^{\mathcal{B}}$ is the *largest* decreasing bisimulation with expansion of $\stackrel{D}{=}^{\mathcal{B}}$. We surmise that the ‘largest’ does not always make sense, because semantic norms take the place of syntactic ones. Fortunately, the correctness of the algorithm does not rely on the ‘largest’. It only relies on the three requirements stated at the beginning of Section VI.

H. The Time Complexity

The running time of our algorithm is exponentially bounded, according to its description, together with Lemma 32, Lemma 36, Lemma 50, and Proposition 57. Finally, we can conclude.

Theorem 5. Branching bisimilarity on normed BPA is EXPTIME-complete.

VII. EXAMPLES

A. Example One

Let us illustrate the algorithm for the following normed BPA system $\Gamma = (\mathbf{C}, \mathcal{A}, \Delta)$ in which

- $\mathbf{C} = \{A_0, A_1, B, C\}$;
- $\mathcal{A} = \{a, b, \tau\}$;
- Δ contains the following rules:

$$\begin{aligned} A_0 &\xrightarrow{a} A_1, & A_1 &\xrightarrow{a} A_0, & A_0 &\xrightarrow{b} \epsilon, & A_1 &\xrightarrow{b} B, \\ B &\xrightarrow{a} \epsilon, & B &\xrightarrow{\tau} \epsilon, & C &\xrightarrow{a} C, & C &\xrightarrow{\tau} \epsilon. \end{aligned}$$

By direct observation, we have $A_0.C \simeq A_1.C$ but $A_0 \not\simeq A_1$, this observation tells us that $A_0 \simeq_{\{C\}} A_1$.

Another observation is that, $A_0.A_0.C \simeq A_1.A_0.C$ but $A_0.A_0 \not\simeq A_1.A_0$, which tells us that even if $A_0 \notin \text{Rd}(C)$, we still cannot cancel the rightmost C .

Below we will demonstrate the behaviour of the algorithm on this system Γ to get more valuable facts.

1) *Preprocessing:* The ground constants $\mathbf{C}_G = \{B, C\}$. Thus the reference set can be \emptyset , $\{B\}$, $\{C\}$, and $\{B, C\}$. All these sets are qualified. We have $[X]_R = \{X\}$ for every $R \subseteq \mathbf{C}_G$ and $X \in \mathbf{C} \setminus R$. We can also find that the R -propagating of X are always the empty set for every $R \subseteq \mathbf{C}_G$ and $X \in \mathbf{C} \setminus R$. Thus $[X]_R \mapsto_R \alpha$ if and only if $X \rightarrow_R \alpha$. Therefore, we will simply write X for $[X]_R$.

We know that \emptyset -transitions \rightarrow_{\emptyset} is exactly \rightarrow . For future use, we list the $\{B, C\}$ -transitions $\rightarrow_{\{B, C\}}$:

$$\begin{aligned} A_0 &\xrightarrow{a}_{\{B, C\}} A_1, & A_1 &\xrightarrow{a}_{\{B, C\}} A_0, & A_0 &\xrightarrow{b}_{\{B, C\}} \epsilon, \\ A_1 &\xrightarrow{b}_{\{B, C\}} \epsilon, & \epsilon &\xrightarrow{a}_{\{B, C\}} \epsilon, & \epsilon &\xrightarrow{\tau}_{\{B, C\}} \epsilon. \end{aligned}$$

The order of R -blocks does not matter in this example. We choose the following orders:

- $A_0 <_{\emptyset} A_1 <_{\emptyset} B <_{\emptyset} C$.
- $A_0 <_{\{B\}} A_1 <_{\{B\}} C$.
- $A_0 <_{\{C\}} A_1 <_{\{C\}} B$.
- $A_0 <_{\{B, C\}} A_1$.

Finally, $|B|_{\text{wk}} = |C|_{\text{wk}} = 0$; $|A_0|_{\text{wk}} = |A_1|_{\text{wk}} = 1$.

2) *The Initial Base:* Now we define the initial base \mathcal{B}_0 according to Section VI-B. We know that $\text{Id}_R = \{B, C\}$ for every $R \subseteq \{B, C\}$. The only \mathcal{B}_0 -admissible set is $\{B, C\}$. Therefore $\mathcal{B}_{0,R} = \mathcal{B}_{0,\{B, C\}}$ for every $R \subseteq \{B, C\}$, and $\mathcal{B}_{0,\{B, C\}}$ is defined as follows:

- $\text{Pr}_{\{B, C\}} = \{A_0\}$.
- $\text{Cm}_{\{B, C\}} = \{A_1\}$.
- $\text{Dc}_{\{B, C\}}(A_1) = \{A_0\}$.
- $\text{Rd}_{\{B, C\}}(A_0) = \{B, C\}$.

blocks	ord	norm	Pr	Cm	Rd	Dc
$[A_0]_{\{B, C\}}$	1	1	✓		$\{B, C\}$	
$[A_1]_{\{B, C\}}$	2	1		✓		$[A_0]_{\{B, C\}}$

Finally, \mathcal{B}_0 is assigned to \mathcal{D} .

3) *The 1st Iteration:* First, we calculate $\text{Id}_R^{\mathcal{B}}$ for every $R \subseteq \mathbf{C}_G$ via $\text{COMPUTINGID}(R)$. We obtain:

- $\text{Id}_{\emptyset}^{\mathcal{B}} = \emptyset$, and
- $\text{Id}_{\{B\}}^{\mathcal{B}} = \text{Id}_{\{C\}}^{\mathcal{B}} = \text{Id}_{\{B, C\}}^{\mathcal{B}} = \{B, C\}$.

Thus only \emptyset and $\{B, C\}$ are \mathcal{B} -admissible.

Now we go into the main part. At first,

- $\mathbf{U} = \{[A_0]_{\emptyset}, [A_1]_{\emptyset}, [B]_{\emptyset}, [C]_{\emptyset}, [A_0]_{\{B, C\}}, [A_1]_{\{B, C\}}\}$.
- $\mathbf{V} = \emptyset$.

Now let $m = 1$ and explore the **repeat**-block. Since $A_0 \xrightarrow{b} \epsilon$ and $d_{\emptyset}(\epsilon) = 0$, and moreover $[A_0]_{\emptyset}$ is $<_{\emptyset}$ minimum, $[A_0]_{\emptyset}$ is selected from \mathbf{U} . $[A_0]_{\emptyset}$ is deemed to be a \mathcal{B}_{\emptyset} -prime because there is no candidate of decomposition of $[A_0]_{\emptyset}$. Thus $[A_0]_{\emptyset}$ is put into $\text{Pr}_{\emptyset}^{\mathcal{B}}$. Then we compute $\text{Rd}_{\emptyset}^{\mathcal{B}}([A_0]_{\emptyset})$ via $\text{COMPUTINGRD}_R([A_0]_{\emptyset})$, and the result is $\text{Rd}_{\emptyset}^{\mathcal{B}}([A_0]_{\emptyset}) = \{B, C\}$. After that $[A_0]_{\emptyset}$ is put into \mathbf{V} . Next, we can select $[B]_{\emptyset}$ from \mathbf{U} . The only candidate for decomposition of $[B]_{\emptyset}$ is $[A_0]_{\emptyset}$. One can check that $\text{EXPAND}_{\emptyset}(B, [A_0]_{\emptyset})$ returns **false**, thus we can affirm that $[B]_{\emptyset}$ is a \mathcal{B}_{\emptyset} -prime, and $\text{Rd}_{\emptyset}^{\mathcal{B}}([B]_{\emptyset}) = \{B, C\}$ can be computed in the same way. Next, $[C]_{\emptyset}$, $[A_0]_{\{B, C\}}$, and $[A_1]_{\{B, C\}}$ are treated successively. $[C]_{\emptyset}$ and $[A_0]_{\{B, C\}}$ are \mathcal{B} -primes. $[A_1]_{\{B, C\}}$ is, however, a \mathcal{B} -composite because one can check $\text{EXPAND}_{\{B, C\}}(A_1, [A_0]_{\{B, C\}})$ return **true**. Now $\text{Dc}_{\{B, C\}}^{\mathcal{B}}([A_1]_{\{B, C\}}) = [A_0]_{\{B, C\}}$.

Now $m = 2$. Because $A_1 \xrightarrow{a}_{\emptyset} A_0$ and $d_{\emptyset}(A_0) = 1$, we can select $[A_1]_{\emptyset}$ from \mathbf{U} and define $d_{\emptyset}[A_1] = 2$. We can check that $[A_1]_{\emptyset}$ is prime too, and $\text{Rd}_{\{B, C\}}^{\mathcal{B}}([A_1]_{\emptyset}) = \{B, C\}$.

The date computed in this iteration is summarized as follows:

blocks	ord	norm	Pr	Cm	Rd	Dc
$[A_0]_{\emptyset}$	1	1	✓		$\{B, C\}$	
$[A_1]_{\emptyset}$	6	2	✓		$\{B, C\}$	
$[B]_{\emptyset}$	2	1	✓		$\{B, C\}$	
$[C]_{\emptyset}$	3	1	✓		$\{B, C\}$	
$[A_0]_{\{B, C\}}$	4	1	✓		$\{B, C\}$	
$[A_1]_{\{B, C\}}$	5	1		✓		$[A_0]_{\{B, C\}}$

Finally, \mathcal{B} is assigned to \mathcal{D} .

4) *The 2nd Iteration:* We calculate $\text{Id}_R^{\mathcal{B}}$ for every $R \subseteq \mathbf{C}_G$ via $\text{COMPUTINGID}(R)$ at first. Once again, \emptyset and $\{B, C\}$ are \mathcal{B} -admissible.

When $m = 1$, we find $[A_0]_{\emptyset}, [B]_{\emptyset}, [C]_{\emptyset} \in \text{Pr}_{\emptyset}^{\mathcal{B}}$, in which $\text{Rd}_{\emptyset}^{\mathcal{B}}([A_0]_{\emptyset}) = \text{Rd}_{\emptyset}^{\mathcal{B}}([B]_{\emptyset}) = \emptyset$ and $\text{Rd}_{\emptyset}^{\mathcal{B}}([C]_{\emptyset}) = \{B, C\}$. Then we find $[A_0]_{\{B, C\}} \in \text{Pr}_{\{B, C\}}^{\mathcal{B}}$ and $[A_1]_{\{B, C\}} \in \text{Cm}_{\{B, C\}}^{\mathcal{B}}$. When $m = 2$, we find that $[A_1]_{\emptyset} \in \text{Pr}_{\emptyset}^{\mathcal{B}}$ and $\text{Rd}_{\emptyset}^{\mathcal{B}}([A_1]_{\emptyset}) = \emptyset$.

The date computed in this iteration is summarized as follows:

blocks	ord	norm	Pr	Cm	Rd	Dc
$[A_0]_\emptyset$	1	1	✓		\emptyset	
$[A_1]_\emptyset$	6	2	✓		\emptyset	
$[B]_\emptyset$	2	1	✓		\emptyset	
$[C]_\emptyset$	3	1	✓		$\{B, C\}$	
$[A_0]_{\{B, C\}}$	4	1	✓		$\{B, C\}$	
$[A_1]_{\{B, C\}}$	5	1		✓		$[A_0]_{\{B, C\}}$

We find an interesting fact that the only difference between \mathcal{B} and \mathcal{D} is $\mathbf{Rd}_\emptyset^{\mathcal{B}} \subsetneq \mathbf{Rd}_\emptyset^{\mathcal{D}}$. Compare this fact with Lemma 55.

Finally, \mathcal{B} is assigned to \mathcal{D} .

5) *The 3rd Iteration:* In this iteration, we can obtain that $\mathcal{B} = \mathcal{D}$. Therefore the algorithm stops here. We can draw the conclusion that $\hat{\mathcal{B}} = \mathcal{D}$. In other words, $\simeq_R = \stackrel{\mathcal{D}}{=} \simeq_R$ for every $R \subseteq \mathbf{C}_G$.

6) *Conclusion:* We confirm that $A_0 \not\approx A_1$ by showing $\text{dcmp}_\emptyset^{\hat{\mathcal{B}}}(A_0) \neq \text{dcmp}_\emptyset^{\hat{\mathcal{B}}}(A_1)$. In fact, $\text{dcmp}_\emptyset^{\hat{\mathcal{B}}}(A_0) = [A_0]_\emptyset$ and $\text{dcmp}_\emptyset^{\hat{\mathcal{B}}}(A_1) = [A_1]_\emptyset$.

We can show $A_0.C \simeq A_1.C$. Using the $\hat{\mathcal{B}}$ -reduction rules defined in Section V-B, we have

- $C \xrightarrow{\hat{\mathcal{B}}} [C]_\emptyset$;
- $\mathbf{Rd}_\emptyset^{\hat{\mathcal{B}}}([C]_\emptyset) = \{B, C\}$;
- $A_0 \xrightarrow{\hat{\mathcal{B}}} [A_0]_{\{B, C\}}$;
- $A_1 \xrightarrow{\hat{\mathcal{B}}} [A_1]_{\{B, C\}} \xrightarrow{\hat{\mathcal{B}}} [A_0]_{\{B, C\}}$.

Therefore, we have

$$\text{dcmp}_\emptyset(A_0.C) = \text{dcmp}_\emptyset(A_1.C) = [A_0]_{\{B, C\}}[C]_\emptyset,$$

hence $A_0.C \simeq A_1.C$.

Actually, we can show

- 1) For every $i_1, j_1, \dots, i_t, j_t \in \{0, 1\}$, we have

$$A_{i_t} \dots A_{i_1}.C \simeq A_{j_t} \dots A_{j_1}.C.$$

- 2) For every $i_1, j_1, \dots, i_t, j_t \in \{0, 1\}$,

$$A_{i_t} \dots A_{i_1} \simeq A_{j_t} \dots A_{j_1}$$

if and only if $i_1 = j_1, \dots, i_t = j_t$.

VIII. REMARK

The algorithm described in Section VI can be further improved. For example, in the **repeat**-block at line 4, although m can be exponentially large, there is no need to enumerate every m . We can compute the next candidate of m based on the right-hand-sides of Δ . Thus only polynomial number of candidates of m is available. In addition, we notice that, although the length of the decomposition of $[X]_R$ can be exponentially large, the technique of string compression can be used such that the representation and manipulation of strings can be implemented in polynomial time. This is done in all the previous works on polynomial-time algorithms for checking bisimilarity on realtime BPA. Ultimately, the number of ground constants is essentially the only factor of the exponential time. Therefore, we claim that branching bisimilarity on normed BPA is in fact fixed parameter tractable.

ACKNOWLEDGMENT

This research is supported by the National Nature Science Foundation of China (61472240, 91318301, 61261130589).

REFERENCES

- [1] Y. Fu, "Checking equality and regularity for normed BPA with silent moves," in *Automata, Languages, and Programming - 40th International Colloquium, ICALP 2013, Riga, Latvia, July 8-12, 2013, Proceedings, Part II*, 2013, pp. 238–249.
- [2] R. Mayr, "Weak bisimilarity and regularity of context-free processes is EXPTIME-hard," *Theoretical Computer Science*, vol. 330, no. 3, pp. 553–575, Feb. 2005.
- [3] J. C. M. Baeten and W. P. Weijland, *Process Algebra*. New York, NY, USA: Cambridge University Press, 1990.
- [4] J. C. M. Baeten, J. A. Bergstra, and J. W. Klop, "Decidability of bisimulation equivalence for processes generating context-free languages," in *PARLE* (2), 1987, pp. 94–111.
- [5] J. E. Hopcroft and J. D. Ullman, *Introduction To Automata Theory, Languages, And Computation*, 1st ed. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1990.
- [6] P. Jančar and F. Moller, "Techniques for decidability and undecidability of bisimilarity," in *CONCUR*, 1999, pp. 30–45.
- [7] O. Burkart, D. Caucal, F. Moller, and B. Steffen, "Verification on infinite structures," 2000.
- [8] F. Moller, S. A. Smolka, and J. Srba, "On the computational complexity of bisimulation, redux," *Inf. Comput.*, vol. 194, no. 2, pp. 129–143, 2004.
- [9] J. Srba, "Roadmap of infinite results," *Current Trends In Theoretical Computer Science*, vol. 2, no. 201, 2004.
- [10] A. Kučera and P. Jančar, "Equivalence-checking on infinite-state systems: Techniques and results," *Theory and Practice of Logic Programming*, vol. 6, no. 201, 2006.
- [11] H. Hüttel and C. Stirling, "Actions speak louder than words: Proving bisimilarity for context-free processes," in *LICS*, 1991, pp. 376–386.
- [12] D. T. Huynh and L. Tian, "Deciding bisimilarity of normed context-free processes is in σ_2^P ," *Theor. Comput. Sci.*, vol. 123, no. 2, pp. 183–197, 1994.
- [13] Y. Hirshfeld, M. Jerrum, and F. Moller, "A polynomial algorithm for deciding bisimilarity of normed context-free processes," *Theor. Comput. Sci.*, vol. 158, no. 1&2, pp. 143–159, 1996.
- [14] S. Lasota and W. Rytter, "Faster algorithm for bisimulation equivalence of normed context-free processes," in *MFCS*, 2006, pp. 646–657.
- [15] W. Czerwinski and S. Lasota, "Fast equivalence-checking for normed context-free processes," in *FSTTCS*, 2010, pp. 260–271.
- [16] W. Czerwinski, *Partially-commutative context-free graphs*. PhD thesis, University of Warsaw, 2012.
- [17] S. Christensen, H. Hüttel, and C. Stirling, "Bisimulation equivalence is decidable for all context-free processes," in *CONCUR*, 1992, pp. 138–147.
- [18] O. Burkart, D. Caucal, and B. Steffen, "An elementary bisimulation decision procedure for arbitrary context-free processes," in *Mathematical Foundations of Computer Science 1995, 20th International Symposium, MFCS'95, Prague, Czech Republic, August 28 - September 1, 1995, Proceedings*, 1995, pp. 423–433.
- [19] P. Jančar, "Bisimilarity on basic process algebra is in 2-exptime (an explicit proof)," *Logical Methods in Computer Science*, vol. 9, no. 1, 2012.
- [20] S. Kiefer, "BPA bisimilarity is exptime-hard," *Inf. Process. Lett.*, vol. 113, no. 4, pp. 101–106, 2013.
- [21] J. Srba, "Strong bisimilarity and regularity of basic process algebra is pspace-hard," in *Automata, Languages and Programming, 29th International Colloquium, ICALP 2002, Malaga, Spain, July 8-13, 2002, Proceedings*, 2002, pp. 716–727.
- [22] R. Milner, *Communication and concurrency*, ser. PHI Series in computer science. Prentice Hall, 1989.
- [23] R. J. van Glabbeek and W. P. Weijland, "Branching time and abstraction in bisimulation semantics (extended abstract)," in *IFIP Congress*, 1989, pp. 613–618.
- [24] —, "Branching time and abstraction in bisimulation semantics," *J. ACM*, vol. 43, no. 3, pp. 555–600, 1996.
- [25] W. Czerwinski and P. Jančar, "Branching bisimilarity of normed BPA processes is in NEXPTIME," *CoRR*, vol. abs/1407.0645, 2014. [Online]. Available: <http://arxiv.org/abs/1407.0645>
- [26] Y. Hirshfeld, M. Jerrum, and F. Moller, "A polynomial-time algorithm for deciding bisimulation equivalence of normed basic parallel processes," *Mathematical Structures in Computer Science*, vol. 6, no. 3, pp. 251–259, 1996.

- [27] C. He, “A polynomial time algorithm for deciding branching bisimilarity on totally normed BPA,” *CoRR*, vol. abs/1411.4157, 2014.
- [28] H. Hüttel, “Silence is golden: Branching bisimilarity is decidable for context-free processes,” in *CAV*, 1991, pp. 2–12.
- [29] D. Caucal, D. T. Huynh, and L. Tian, “Deciding branching bimilarity of normed context-free processes is in Σ^p_2 ,” *Inf. Comput.*, vol. 118, no. 2, pp. 306–315, 1995. [Online]. Available: <http://dx.doi.org/10.1006/inco.1995.1069>
- [30] C. Stirling, “Decidability of weak bisimilarity for a subset of basic parallel processes,” *Foundations of Software Science and Computation*, 2001.
- [31] W. Czerwinski, P. Hofman, and S. Lasota, “Decidability of branching bisimulation on normed commutative context-free processes,” in *CONCUR*, 2011, pp. 528–542.

APPENDIX A PROOFS IN SECTION III

A. Proof of the Computation Lemma

1) *Proof of Lemma 1:* We present a complete proof of Lemma 1 here which depends only on Definition 1. Though Lemma 1 is well-known, the proof here has some subtleties. Importantly, the proof framework will be used to show Lemma 11.

Let

$$\alpha = \alpha_0 \xrightarrow{\tau} \alpha_1 \xrightarrow{\tau} \alpha_2 \xrightarrow{\tau} \dots \xrightarrow{\tau} \alpha_k \simeq \alpha.$$

We show that $\alpha_i \simeq \alpha_j$ for every $0 \leq i, j \leq k$. To this end, let $\mathcal{S} \stackrel{\text{def}}{=} \{(\alpha_i, \alpha_j) \mid 0 \leq i, j \leq k\}$, and construct the equivalence relation $\asymp \stackrel{\text{def}}{=} (\mathcal{S} \cup \simeq)^*$. We emphasize that \mathcal{S} can be viewed as a single ‘equivalence class’, because \mathcal{S} is both symmetric and transitive, and connective. We confirm that \asymp is a bisimulation. The crux is to show the following *key property*: For every $i, j \in \{0, 1, \dots, k\}$,

- 1) If $\alpha_i \xrightarrow{a} \gamma$, then $\alpha_j \xRightarrow{\asymp} \cdot \xrightarrow{a} \delta$ for some δ such that $\gamma \simeq \delta$.
- 2) If $\alpha_i \not\xrightarrow{a} \gamma$, then $\alpha_j \xRightarrow{\asymp} \cdot \not\xrightarrow{a} \delta$ for some δ such that $\gamma \simeq \delta$.

To show this property, we study the following two cases:

- $i \geq j$. In this case, we have $\alpha_j \xRightarrow{\asymp} \alpha_i$. By letting $\delta = \gamma$, we get the key property.
- $i < j$. In this case, we will make use of the fact $\alpha \simeq \alpha_k$. Consider the transition $\alpha \xrightarrow{\tau} \alpha_1$. Now either $\alpha_1 \simeq \alpha_k$, or $\alpha_k \xRightarrow{\asymp} \cdot \xrightarrow{\tau} \alpha'_1$ such that $\alpha_1 \simeq \alpha'_1$. In view of $(\alpha, \alpha_1) \in \mathcal{S}$, we conclude that in either case, $\alpha_k \xRightarrow{\asymp} \alpha'_1$ for some α'_1 such that $\alpha_1 \simeq \alpha'_1$. By repeatedly applying the above argument. We can show that $\alpha_k \xRightarrow{\asymp} \alpha'_i$ for some α'_i such that $\alpha_i \simeq \alpha'_i$. Since $\alpha_j \xRightarrow{\asymp} \alpha_k$, we now have $\alpha_j \xRightarrow{\asymp} \alpha'_i$ such that $\alpha_i \simeq \alpha'_i$. Now it is a routine work to justify the key property. For example, suppose that $\alpha_i \xrightarrow{a} \gamma$, then we have $\alpha_j \xRightarrow{\asymp} \alpha'_i \xRightarrow{\asymp} \cdot \xrightarrow{a} \delta$ for some δ such that $\gamma \simeq \delta$.

Remark 17. We can show the bisimulation property of \asymp by repeatedly using the *key property* and the bisimulation property of \simeq . Be very careful that it would be a mistake if the ‘key property’ was modified slightly as follows: For every $i, j \in \{0, 1, \dots, k\}$,

- 1) If $\alpha_i \xrightarrow{a} \gamma$, then $\alpha_j \xRightarrow{\asymp} \cdot \xrightarrow{a} \delta$ for some δ such that $\gamma \asymp \delta$.
- 2) If $\alpha_i \not\xrightarrow{a} \gamma$, then $\alpha_j \xRightarrow{\asymp} \cdot \not\xrightarrow{a} \delta$ for some δ such that $\gamma \asymp \delta$.

This mistake is essentially the same as the well-known mistake of ‘weak bisimulation up-to weak bisimilarity’. To get a better understanding of the mistake, readers are referred to Chapter 5 of [22], especially Section 5.7.

2) *Proof of Lemma 11:* This proof is an adaptation of the proof of Lemma 1.

Let $R \subseteq \mathbf{C}_G$ and let α be in R -nf. Suppose that

$$\alpha = \alpha_0 \xrightarrow{\tau}_R \alpha_1 \xrightarrow{\tau}_R \alpha_2 \xrightarrow{\tau}_R \dots \xrightarrow{\tau}_R \alpha_k \simeq_R \alpha.$$

We show that $\alpha_i \simeq_R \alpha_j$ for every $0 \leq i, j \leq k$. To this end, let $S \stackrel{\text{def}}{=} \{(\alpha_i, \alpha_j) \mid 0 \leq i, j \leq k\}$, and construct $\asymp \stackrel{\text{def}}{=} (S \cup \simeq_R)^*$. We confirm that \asymp is an R -bisimulation (via Proposition 9). First of all, we point out the following basic facts:

- \asymp is an equivalence relation.
- S is symmetric, transitive, and connective.
- $=_R \subseteq \asymp$. (Because $=_R \subseteq \simeq_R$ and $\simeq_R \subseteq \asymp$.)
- If $\alpha_i \Rightarrow \epsilon$ for some $0 \leq i \leq k$, then $\alpha_j \Rightarrow \epsilon$ for every $0 \leq j \leq k$.
- All α_i 's are in R -nf for $0 \leq i \leq k$.

The crux of the proof is to show the following *key property*: For every $i, j \in \{0, 1, \dots, k\}$,

- 1) If $\alpha_i \xrightarrow{a}_R \gamma$, then $\alpha_j \xRightarrow{\simeq_R}_R \cdot \xrightarrow{a}_R \delta$ for some δ such that $\gamma \simeq_R \delta$.
- 2) If $\alpha_i \xrightarrow{\neq_R}_R \gamma$, then $\alpha_j \xRightarrow{\simeq_R}_R \cdot \xrightarrow{\neq_R}_R \delta$ for some δ such that $\gamma \simeq_R \delta$.

To show this property, we study the following two cases:

- $i \geq j$. In this case, we have $\alpha_j \xRightarrow{\simeq_R}_R \alpha_i$. By letting $\delta = \gamma$, we get the key property.
- $i < j$. In this case, we will make use of the fact $\alpha \simeq_R \alpha_k$. Consider the transition $\alpha \xrightarrow{\tau}_R \alpha_1$. Now either $\alpha_1 \simeq_R \alpha_k$, or $\alpha_k \xRightarrow{\simeq_R}_R \cdot \xrightarrow{\tau}_R \alpha'_1$ such that $\alpha_1 \simeq_R \alpha'_1$. In view of $(\alpha, \alpha_1) \in S$, we conclude that in either case, $\alpha_k \xRightarrow{\simeq_R}_R \alpha'_1$ for some α'_1 such that $\alpha_1 \simeq_R \alpha'_1$. By repeatedly applying the above argument. We can show that $\alpha_k \xRightarrow{\simeq_R}_R \alpha'_i$ for some α'_i such that $\alpha_i \simeq_R \alpha'_i$. Since $\alpha_j \xRightarrow{\simeq_R}_R \alpha_k$, we now have $\alpha_j \xRightarrow{\simeq_R}_R \alpha'_i$ such that $\alpha_i \simeq_R \alpha'_i$. Now it is a routine work to justify the key property. For example, suppose that $\alpha_i \xrightarrow{a}_R \gamma$, then we have $\alpha_j \xRightarrow{\simeq_R}_R \alpha'_i \xRightarrow{\simeq_R}_R \cdot \xrightarrow{a}_R \delta$ for some δ such that $\gamma \simeq_R \delta$.

B. Proof of Proposition 14

Suppose $R_1 \subseteq R_2$. We show that

$$\asymp \stackrel{\text{def}}{=} (\simeq_{R_1} \cup \simeq_{R_2})^*$$

is an R_2 -bisimulation.

We emphasize the following basic facts:

- $\simeq_{R_1} \subseteq \asymp$ and $\simeq_{R_2} \subseteq \asymp$.
- $=_{R_2} \subseteq \asymp$.
- $\simeq_{R_1}, \simeq_{R_2}, \asymp$ are all equivalence relations.

In order to show that \asymp is an R_2 -bisimulation, we design the following property **I** and **II**:

- I.** Suppose there are α and β satisfying $\alpha \simeq_{R_1} \beta$, then
 - 1) if $\alpha \Rightarrow \epsilon$, then $\beta \Rightarrow \epsilon$;
 - 2) if $\alpha \xrightarrow{\neq_R}_R \alpha'$, then $\beta_{R_2} \xRightarrow{\simeq_R}_{R_2} \cdot \xrightarrow{\neq_R}_{R_2} \beta'$ for some β' such that $\alpha' \simeq_{R_1} \cdot \simeq_{R_2} \beta'$;
 - 3) if $\alpha \xrightarrow{a}_R \alpha'$, then $\beta_{R_2} \xRightarrow{\simeq_R}_{R_2} \cdot \xrightarrow{a}_{R_2} \beta'$ for some β' such that $\alpha' \simeq_{R_1} \cdot \simeq_{R_2} \beta'$.
- II.** Suppose there are α and β satisfying $\alpha \simeq_{R_2} \beta$, then
 - 1) if $\alpha \Rightarrow \epsilon$, then $\beta \Rightarrow \epsilon$;
 - 2) if $\alpha \xrightarrow{\neq_R}_R \alpha'$, then $\beta_{R_2} \xRightarrow{\simeq_R}_{R_2} \cdot \xrightarrow{\neq_R}_{R_2} \beta'$ for some β' such that $\alpha' \simeq_{R_2} \beta'$;

- 3) if $\alpha \xrightarrow{a}_R \alpha'$, then $\beta_{R_2} \xRightarrow{\simeq_R}_{R_2} \cdot \xrightarrow{a}_{R_2} \beta'$ for some β' such that $\alpha' \simeq_{R_2} \beta'$.

Note that, if $\alpha \asymp \beta$, then we must have

$$\alpha \simeq_{R_{i_1}} \cdot \simeq_{R_{i_2}} \cdot \dots \cdot \simeq_{R_{i_n}} \beta$$

for some $n \in \mathbb{N}$ and $i_k \in \{1, 2\}$ for every $1 \leq k \leq n$. Therefore, by repeatedly using the property **I** and **II**, we can obtain that \asymp is a bisimulation.

We can observe that the property **II** is an direct inference of the bisimulation property of \simeq_{R_2} . Thus it suffices to prove property **I**.

Condition 1 (i.e. ground preservation) is trivial. Other two conditions have the same structures and Condition 3 cannot be more difficult than Condition 2. Thus we choose to prove Condition 2.

Suppose there are α and β satisfying $\alpha \simeq_{R_1} \beta$. According to Definition 6, we have:

- if $\alpha \xrightarrow{\neq_{R_1}} \alpha'$, then $\beta_{R_1} \xRightarrow{\simeq_{R_1}}_{R_1} \cdot \xrightarrow{\neq_{R_1}}_{R_1} \beta'$ for some β' such that $\alpha' \simeq_{R_1} \beta'$.

Assume $\alpha \xrightarrow{\neq_R}_R \alpha'$. Because $\simeq_{R_1} \subseteq \asymp$, we must have $\alpha \xrightarrow{\neq_{R_1}} \alpha'$. We can find β' such that $\beta_{R_1} \xRightarrow{\simeq_{R_1}}_{R_1} \cdot \xrightarrow{\neq_{R_1}}_{R_1} \beta'$ and $\alpha' \simeq_{R_1} \beta'$. In view of Lemma 6 and Lemma 7, we have

$$\beta =_{R_1} \cdot \xRightarrow{\simeq_{R_1}} \cdot \xrightarrow{\neq_{R_1}} \cdot =_{R_1} \beta'$$

for some β' such that $\alpha' \simeq_{R_1} \beta'$. Since $R_1 \subseteq R_2$, we have $=_{R_1} \subseteq =_{R_2}$. Also note that $\simeq_{R_1} \subseteq \asymp$. Thus

$$\beta =_{R_2} \cdot \xRightarrow{\simeq_R} \beta'' \xrightarrow{\tau} \cdot =_{R_2} \beta'$$

for some β', β'' such that $\alpha' \simeq_{R_1} \beta'$. We can ensure that $\beta'' \neq \beta'$, because $\beta'' \asymp \beta \asymp \alpha \neq \alpha' \asymp \beta'$. Therefore,

$$\beta =_{R_2} \cdot \xRightarrow{\simeq_R} \cdot \xrightarrow{\neq_R} \cdot =_{R_2} \beta'$$

for some β' such that $\alpha' \simeq_{R_1} \beta'$. Applying Lemma 6 and Lemma 7 repeatedly, and remembering $=_{R_2} \subseteq \simeq_{R_2}$, we have

$$\beta_{R_2} \xRightarrow{\simeq_R}_{R_2} \cdot \xrightarrow{\neq_R}_{R_2} \beta'_{R_2}$$

for some β'_{R_2} such that $\alpha' \simeq_{R_1} \cdot \simeq_{R_2} \beta'_{R_2}$.

Remark 18. We make a mistake in the previous version, because we take the following slightly different variant of property **I** and **II**:

- I'**. Suppose there are α and β satisfying $\alpha \simeq_{R_1} \beta$, then
 - 1) if $\alpha \Rightarrow \epsilon$, then $\beta \Rightarrow \epsilon$;
 - 2) if $\alpha \xrightarrow{\neq_R}_R \alpha'$, then $\beta_{R_2} \xRightarrow{\simeq_R}_{R_2} \cdot \xrightarrow{\neq_R}_{R_2} \beta'$ for some β' such that $\alpha' \asymp \beta'$;
 - 3) if $\alpha \xrightarrow{a}_R \alpha'$, then $\beta_{R_2} \xRightarrow{\simeq_R}_{R_2} \cdot \xrightarrow{a}_{R_2} \beta'$ for some β' such that $\alpha' \asymp \beta'$.
- II'**. Suppose there are α and β satisfying $\alpha \simeq_{R_2} \beta$, then
 - 1) if $\alpha \Rightarrow \epsilon$, then $\beta \Rightarrow \epsilon$;
 - 2) if $\alpha \xrightarrow{\neq_R}_R \alpha'$, then $\beta_{R_2} \xRightarrow{\simeq_R}_{R_2} \cdot \xrightarrow{\neq_R}_{R_2} \beta'$ for some β' such that $\alpha' \asymp \beta'$;
 - 3) if $\alpha \xrightarrow{a}_R \alpha'$, then $\beta_{R_2} \xRightarrow{\simeq_R}_{R_2} \cdot \xrightarrow{a}_{R_2} \beta'$ for some β' such that $\alpha' \asymp \beta'$.

It will run into trouble when using property **I'** and **II'** to prove bisimulation property of \asymp . The reason is the same as in the situation of 'weak bisimulation up to weak bisimilarity' [22]. To get a better understanding of this mistake, readers are referred to Chapter 5 of [22], especially Section 5.7.

C. Proof of Proposition 16

Because $R \subseteq \text{Id}_R$, by Proposition 14, we know that $\simeq_R \subseteq \simeq_{\text{Id}_R}$. Thus it suffices to show $\simeq_{\text{Id}_R} \subseteq \simeq_R$. Let $S = \text{Id}_R$, it suffices to show that \simeq_S is an R -bisimulation.

Clearly, \simeq_S is an equivalence relation, and $=_R \subseteq \simeq_S$. Thus it suffices to prove the following property: Whenever $\alpha \simeq_S \beta$,

- 1) if $\alpha \implies \epsilon$, then $\beta \implies \epsilon$;
- 2) if $\alpha \xrightarrow{\tau}_S \alpha'$, then $\beta_R \xrightarrow{\tau}_R \beta'$ for some β' such that $\alpha' \simeq_S \beta'$;
- 3) if $\alpha \xrightarrow{a}_S \alpha'$, then $\beta_R \xrightarrow{a}_R \beta'$ for some β' such that $\alpha' \simeq_S \beta'$.

Condition 1 is trivial. Other two conditions have the same structures. As usual we choose to prove Condition 2.

Suppose that $\alpha \simeq_S \beta$ and $\alpha \xrightarrow{\tau}_S \alpha'$. By Definition 6, we have:

$$\beta_S \xrightarrow{\tau}_S \beta' \text{ for some } \beta' \text{ such that } \alpha' \simeq_S \beta'.$$

Now there are two cases:

- $\beta_S = \epsilon$. In this case, we have $\beta \in S^* = (\text{Id}_R)^*$ thus $\beta \simeq_R \epsilon$ by Lemma 13. Since $\simeq_R \subseteq \simeq_S$, we have $\beta_S \simeq_S \epsilon$. Consider any β'' such that $\beta_S \xrightarrow{\tau}_S \beta''$. We have the following properties.
 - $\beta'' \implies \epsilon$ (because $\beta'' \simeq_S \epsilon$).
 - There exists $X \in S$ such that $X \xrightarrow{\tau}_S \gamma$ and $\gamma_S = \beta''$. (By Lemma 7)

Now we have $\epsilon \simeq_R X \xrightarrow{\tau}_R \gamma \implies \epsilon$ and by Lemma 6,

$$\epsilon \simeq_R X_R \xrightarrow{\tau}_R \gamma_R \implies \epsilon.$$

According to Computation Lemma (Lemma 11), $\gamma \simeq_R \epsilon$, and thus by Lemma 13, $\gamma \in (\text{Id}_R)^* = S^*$. Therefore $\beta'' = \gamma_S = \epsilon$. This crucial fact leads to the following assertion:

Whenever $\beta_S \xrightarrow{\tau}_S \beta'' \xrightarrow{\tau}_S \beta'$, β'' must be ϵ .

Therefore, we confirm that

$$\beta_S \xrightarrow{\tau}_S \beta' \text{ for some } \beta' \text{ such that } \alpha' \simeq_S \beta'.$$

Now according to Lemma 7, there exists $X \in S$ such that $X \xrightarrow{\tau}_S \hat{\beta}'$ for some $\hat{\beta}'$ and $\hat{\beta}'_S = \beta'$. Knowing $\simeq_R \subseteq \simeq_S$, we have $X \xrightarrow{\tau}_R \hat{\beta}'$. Because $X \in S = \text{Id}_R$, we have $X \simeq_R \epsilon$. Now according to Definition 6,

$$\epsilon \xrightarrow{\tau}_R \hat{\beta}' \xrightarrow{\tau}_R \gamma' \simeq_R \hat{\beta}' \simeq_R \beta'$$

for some γ' , which implies that

$$\epsilon \xrightarrow{\tau}_R \gamma'' \xrightarrow{\tau}_R \gamma' \simeq_R \alpha'$$

for some γ', γ'' . Finally we can observe $\gamma'' \not\simeq_S \gamma'$, for $\gamma'' \simeq_S \epsilon \simeq_S \beta \simeq_S \alpha \not\simeq_S \alpha' \simeq_S \gamma'$. Above all, we find such γ that $\beta_R \xrightarrow{\tau}_R \gamma' \text{ and } \alpha' \simeq_S \gamma'$.

- $\beta_S \neq \epsilon$. In this case, there are several subcases, depending on the path $\beta_S \xrightarrow{\tau}_S \cdot \xrightarrow{\tau}_S \beta'$:

- $\beta_S \xrightarrow{\tau}_S \beta'$. We can show by applying Lemma 7 that $\beta \xrightarrow{\tau} \hat{\beta}'$ for some $\hat{\beta}'$ such that $\alpha' \simeq_S \hat{\beta}'$. By Lemma 6, we have $\beta_R \xrightarrow{\tau}_R \hat{\beta}'_R$. Knowing the fact that $\hat{\beta}'_R \simeq_R \hat{\beta}'$ and $\simeq_R \subseteq \simeq_S$, we have $\hat{\beta}'_R \simeq_S \hat{\beta}'$, and thus $\alpha' \simeq_S \hat{\beta}'_R$. Finally it is a routine work to observe $\beta_R \not\simeq_S \hat{\beta}'_R$. In summary, we have $\beta_R \xrightarrow{\tau}_R \hat{\beta}'_R$ and $\alpha' \simeq_S \hat{\beta}'_R$.
- $\beta_S \xrightarrow{\tau}_S \eta \xrightarrow{\tau}_S \cdot \xrightarrow{\tau}_S \beta'$. We can show by applying Lemma 7 that $\beta \xrightarrow{\tau} \hat{\eta}$ for some $\hat{\eta}$ such that $\hat{\eta}_S = \eta$. In view of $\simeq_R \subseteq \simeq_S$, and by Lemma 6, we have $\beta_R \xrightarrow{\tau}_R \hat{\eta}_R$ and $\alpha \simeq_S \hat{\eta}_R$ (because $\alpha \simeq_S \beta \simeq_S \eta \simeq_S \hat{\eta} \simeq_R \hat{\eta}_R$). Remember the fact $\hat{\eta}_S = \eta$, we can now use induction to confirm that

$$\hat{\eta}_R \xrightarrow{\tau}_R \cdot \xrightarrow{\tau}_R \beta'$$

for some β' such that $\alpha' \simeq_S \beta'$. Put them together, we get

$$\beta_R \xrightarrow{\tau}_R \hat{\eta}_R \xrightarrow{\tau}_R \cdot \xrightarrow{\tau}_R \beta'$$

for some β' such that $\alpha' \simeq_S \beta'$.

D. Proof of Theorem 1 and Theorem 2

Since Theorem 1 is a special case of Theorem 2. We only prove Theorem 2. The proof is divided into the following two lemmas: Lemma 70 and Lemma 71.

Lemma 70. If $S = \text{Rd}_R(\gamma)$, then $\alpha \simeq_S \beta$ implies $\alpha\gamma \simeq_R \beta\gamma$.

Proof: We can assume that $\gamma \notin R^*$. If not, we will have $S = \text{Id}_R$ and thus according to Proposition 14, $\simeq_S = \simeq_R$. The result of this lemma holds accordingly.

Let \simeq be the relation $\{(\alpha\gamma, \beta\gamma) \mid \alpha \simeq_S \beta\}$. Define the relation

$$\asymp \stackrel{\text{def}}{=} (\simeq \cup \simeq_R)^*.$$

We show that \asymp is an R -bisimulation.

We point out the following basic facts:

- $\simeq \subseteq \asymp$, $=_R \subseteq \simeq_R \subseteq \asymp$, and $\simeq \circ \simeq_R \subseteq \asymp$.
- $\mathcal{I} \subseteq \simeq_R$, in which $\mathcal{I} = \{(\zeta, \zeta) \mid \zeta \in \mathbf{C}^*\}$, which is the identical relation on \mathbf{C}^* .
- \simeq is symmetric and transitive.
- \simeq_R, \asymp are all equivalence relations.

Now consider an arbitrary pair (ζ, η) such that $\zeta \asymp \eta$. We will prove

- 1) if $\zeta \implies \epsilon$, then $\eta \implies \epsilon$; (trivial)
- 2) if $\zeta \xrightarrow{\tau} \zeta'$, then $\eta_R \xrightarrow{\tau}_R \cdot \xrightarrow{\tau}_R \eta'$ for some η' such that $\zeta' \asymp \eta'$;
- 3) if $\zeta \xrightarrow{a} \zeta'$, then $\eta_R \xrightarrow{a}_R \cdot \xrightarrow{a}_R \eta'$ for some η' such that $\zeta' \asymp \eta'$.

As usual (similar to the proof of Proposition 14), we show the following property **I** and **II**:

I. Suppose there are ζ and η satisfying $\zeta \simeq \eta$, then

- 1) if $\zeta \implies \epsilon$, then $\eta \implies \epsilon$;

- 2) if $\zeta \xrightarrow{*} \zeta'$, then $\eta_R \xrightarrow{\simeq}_R \cdot \xrightarrow{*}_R \eta'$ for some η' such that $(\zeta', \eta') \in (\simeq \cdot \simeq_R) \cup \mathcal{I}$;
- 3) if $\zeta \xrightarrow{a} \zeta'$, then $\eta_R \xrightarrow{\simeq}_R \cdot \xrightarrow{a}_R \eta'$ for some η' such that $(\zeta', \eta') \in (\simeq \cdot \simeq_R) \cup \mathcal{I}$.

II. Suppose there are ζ and η satisfying $\zeta \simeq_R \eta$, then

- 1) if $\zeta \Rightarrow \epsilon$, then $\eta \Rightarrow \epsilon$;
- 2) if $\zeta \xrightarrow{*} \zeta'$, then $\eta_R \xrightarrow{\simeq}_R \cdot \xrightarrow{*}_R \eta'$ for some η' such that $\zeta' \simeq_R \eta'$;
- 3) if $\zeta \xrightarrow{a} \zeta'$, then $\eta_R \xrightarrow{\simeq}_R \cdot \xrightarrow{a}_R \eta'$ for some η' such that $\zeta' \simeq_R \eta'$.

Now assume that $\zeta \asymp \eta$, we must have $\zeta \simeq_R \cdot \simeq \cdot \simeq_R \dots \simeq \cdot \simeq_R \beta$. (Think why.) Thus we can show that \asymp is an R -bisimulation by applying property **I** and **II** finitely many times.

Since property **II** is trivial, it suffices to prove property **I**.

If $(\zeta, \eta) \in \simeq$. Now we must have $\zeta = \alpha\gamma$ and $\eta = \beta\gamma$ such that $\alpha \simeq_S \beta$. There are two cases:

- 1) $\alpha \neq \epsilon$. In this case $\zeta \xrightarrow{\ell} \zeta'$ is induced by $\alpha\gamma \xrightarrow{\ell} \alpha'\gamma$.
 - If $\ell = \tau$ and $\alpha\gamma \neq \alpha'\gamma$. In this case, we must have $\alpha' \not\simeq_S \alpha$. According to the fact $\alpha \simeq_S \beta$ and Definition 6, we have

$$\beta_S \xrightarrow{\simeq}_S \cdot \xrightarrow{\neq_S}_S \hat{\beta}$$

for some $\hat{\beta}$ such that $\alpha' \simeq_S \hat{\beta}$. The above path from β_S to $\hat{\beta}$ can be written as follows:

$$\beta_S = \beta_0 \xrightarrow{\simeq}_S \beta_1 \xrightarrow{\simeq}_S \dots \xrightarrow{\simeq}_S \beta_k \xrightarrow{\neq_S}_S \hat{\beta}.$$

Consider this path. We have two possibilities:

- $\beta_i \neq \epsilon$ for every $0 \leq i \leq k$. If so, according to Lemma 7, we have

$$\beta \xrightarrow{\simeq}_S \cdot \xrightarrow{\neq_S}_S \beta' \simeq_S \hat{\beta}$$

for some β' . Actually we have $\beta \xrightarrow{\simeq}_S \beta'' \xrightarrow{\tau}_S \beta'$ with $\alpha' \simeq_S \beta'$. Therefore we have $\beta\gamma \xrightarrow{\simeq}_S \beta''\gamma \xrightarrow{\neq}_S \beta'\gamma$, and $\alpha'\gamma \simeq \beta'\gamma$. Furthermore, because $=_R \subseteq \simeq_R$, we have

$$\beta\gamma_R \xrightarrow{\simeq}_R \beta''\gamma_R \xrightarrow{\neq}_R \beta'\gamma_R$$

with $\alpha'\gamma \simeq \cdot \simeq_R \beta'\gamma_R$. Note that the reason for $\beta''\gamma_R \neq \beta'\gamma_R$ is that $\beta''\gamma_R \asymp \beta\gamma_R \asymp \alpha\gamma_R \neq \alpha'\gamma_R \asymp \beta'\gamma_R$.

- $\beta_i = \epsilon$ for some $0 \leq i \leq k$. Choose the largest i such that $\beta_i = \epsilon$. Then according to Lemma 7, we have

$$\beta_S \xrightarrow{\simeq}_S \epsilon =_S X \xrightarrow{\simeq}_S \beta'' \xrightarrow{\neq_S}_S \beta' \simeq_S \hat{\beta}$$

for some β' . Then we have the following facts.

- a) Because $\beta_S \xrightarrow{\simeq}_S \epsilon$, by Lemma 8 we have $\beta \xrightarrow{\simeq}_S \epsilon$. Then we have $\alpha \simeq_S \beta \simeq_S \epsilon$ and $\beta\gamma \xrightarrow{\simeq}_S \gamma$.
- b) We know $X_S = \epsilon$, or equivalently $X \in \text{Rd}_R(\gamma)$, which means that $X\gamma \simeq_R \gamma$. Then,

because $\alpha \simeq_S \beta \simeq_S \epsilon$, we have $\alpha \simeq_S X$, thus $\alpha\gamma \simeq X\gamma$.

- c) According to $\alpha\gamma \simeq X\gamma$ and $X \xrightarrow{\simeq}_S \beta'' \xrightarrow{\neq_S}_S \beta'$, we can now take the way in the first possibility to obtain the following fact: $X\gamma \xrightarrow{\simeq}_S \beta''\gamma \xrightarrow{\neq}_S \beta'\gamma$ with $\alpha'\gamma \simeq \beta'\gamma$.
- d) Now remember $X\gamma \simeq_R \gamma$, we have $\gamma_R \xrightarrow{\simeq}_R \gamma''_R \xrightarrow{\tau}_R \gamma'_R$ for some γ'' and γ' such that $\beta''\gamma \simeq_R \gamma''$ and $\beta'\gamma \simeq_R \gamma'$.

In all, we have

$$\beta\gamma_R \xrightarrow{\simeq}_R \gamma_R \xrightarrow{\simeq}_R \gamma''_R \xrightarrow{\tau}_R \gamma'_R$$

such that $\alpha\gamma \asymp \gamma''$ and $\alpha'\gamma \simeq \cdot \simeq_R \gamma'$. To see $\gamma'' \neq \gamma'$, we notice that $\gamma'' \asymp \beta\gamma \asymp \alpha\gamma \neq \alpha'\gamma \asymp \gamma'$.

- $\ell \neq \tau$. This case can be proved in the same way as the case $\ell = \tau$ and $\alpha\gamma \neq \alpha'\gamma$.

- 2) $\alpha = \epsilon$. In this case $\zeta \xrightarrow{\ell} \zeta'$ is induced by $\gamma \xrightarrow{\ell} \gamma'$. Now we have $\beta \xrightarrow{\simeq}_S \epsilon$. Thus $\beta\gamma_R \xrightarrow{\simeq}_R \gamma_R \xrightarrow{\ell}_R \gamma'_R$, with $\alpha\gamma = \gamma \asymp \gamma$ and $(\gamma', \gamma') \in \mathcal{I}$.

■

Lemma 71. Suppose $S = \text{Rd}_R(\gamma)$, then $\alpha\gamma \simeq_R \beta\gamma$ implies $\alpha \simeq_S \beta$.

Proof: Define the set

$$\asymp \stackrel{\text{def}}{=} \{(\alpha, \beta) \mid \alpha\gamma \simeq_R \beta\gamma\}$$

As before we can assume $\gamma \notin R^*$. Otherwise the conclusion of the lemma is relatively trivial.

We show that \asymp is an S -bisimulation. It is easy to see that \asymp is an equivalence relation indeed.

Now we check the properties in Definition 6.

- 1) We show $=_S \subseteq \asymp$. Let $\alpha =_S \beta$. According to Definition 3, there exist $\alpha', \beta' \in S^* = (\text{Rd}_R(\gamma))^*$ and a process ζ such that $\alpha = \zeta\alpha'$ and $\beta = \zeta\beta'$. Now $\alpha\gamma = \zeta\alpha'\gamma \simeq_R \zeta\gamma \simeq_R \zeta\beta'\gamma = \beta\gamma$. Therefore $\alpha \asymp \beta$ by the definition of \asymp .
- 2) If $\alpha \asymp \beta$ and $\alpha \Rightarrow \epsilon$, we show $\beta \Rightarrow \epsilon$. According to the definition of \asymp , $\alpha\gamma \simeq_R \beta\gamma$. Now $\alpha\gamma_R \Rightarrow_R \gamma_R$ must be matched by $\beta\gamma_R$. Let us suppose that the matching is $\beta\gamma_R \Rightarrow_R \beta'\gamma_R \simeq_R \gamma_R$, which is induced by $\beta \Rightarrow \beta'$. Otherwise we will have $\beta \Rightarrow \epsilon$ immediately. Now we have $\beta'\gamma \simeq_R \gamma$, which implies $\beta' \Rightarrow \epsilon$ and consequently $\beta \Rightarrow \epsilon$.
- 3) If $\alpha \asymp \beta$ and $\alpha \xrightarrow{*} \alpha'$, then we show that $\beta_S \xrightarrow{\simeq}_S \cdot \xrightarrow{*}_S \beta'$ for some β' such that $\alpha' \asymp \beta'$. According to definition of \asymp , we have $\alpha\gamma \simeq_R \beta\gamma$. Moreover, $\alpha \xrightarrow{*} \alpha'$ is equivalent to $\alpha\gamma \xrightarrow{\neq_R}_R \alpha'\gamma$. There are two cases:
 - $\alpha \notin (\text{Rd}_R(\gamma))^*$. In this case we also have $\beta \notin (\text{Rd}_R(\gamma))^*$. Thus the action $\alpha\gamma \xrightarrow{\neq_R}_R \alpha'\gamma$ must be matched by $\beta\gamma_R \xrightarrow{\simeq}_R \beta''\gamma_R \xrightarrow{\neq_R}_R \beta'\gamma_R$ for some β'' and β' with $\alpha'\gamma \simeq_R \beta'\gamma$. This is equal to $\beta \xrightarrow{\simeq}_S \beta'' \xrightarrow{\neq_S}_S \beta'$ with $\alpha' \asymp \beta'$, which implies

- $\alpha \in (\text{Rd}_R(\gamma))^*$. In this case we have $\alpha\gamma \simeq_R \gamma \simeq_R \beta\gamma$ hence $\beta \in (\text{Rd}_R(\gamma))^*$. In other words, $\alpha, \beta \in S^*$. Now we have $\beta\gamma \xrightarrow{\simeq}_R \gamma$, or equivalently $\beta \xrightarrow{\simeq} \epsilon$. Now remember $\epsilon =_S \alpha$ and $\alpha \xrightarrow{*} \alpha'$. Combine these transitions we have $\beta \xrightarrow{\simeq} \epsilon =_S \alpha \xrightarrow{*} \alpha'$, and thus $\beta_S \xrightarrow{\simeq}_S \epsilon = \alpha_S \xrightarrow{*}_S \alpha'_S$ and trivially $\alpha' \simeq \alpha'_S$. We are done.

5

Proofs of Lemma 62: It is a routine work to check that $\{X \mid X \simeq_R \epsilon\}$ is an \mathbf{Id}_R^B -candidate.

Proofs of Lemma 63: We need to show that, $\text{Id}_{\text{Rd}_R^{\mathcal{B}}([X]_R)} = \text{Rd}_R^{\mathcal{B}}([X]_R)$. To this end, we show $\text{Id}_{\text{Rd}_R^{\mathcal{B}}([X]_R)}$ is an $\text{Rd}_R^{\mathcal{B}}([X]_R)$ -candidate.

As before we let $T \stackrel{\text{def}}{=} \{W \mid W.X \stackrel{\mathcal{D}}{=} X\}$. First we confirm $\text{Id}_{\text{Rd}_R^{\mathcal{B}}([X]_R)} \subseteq T$. By induction T is a \mathcal{D} -admissible set thus it is also \mathcal{B} -admissible set, hence $\text{Id}_T^{\mathcal{B}} = T$. Because $\text{Rd}_R^{\mathcal{B}}([X]_R) \subseteq T$, we have $\text{Id}_{\text{Rd}_R^{\mathcal{B}}([X]_R)}^{\mathcal{B}} \subseteq \text{Id}_T^{\mathcal{B}} = T$.

Now we check the conditions of $\text{Rd}_R^{\mathcal{B}}([X]_R)$ -candidate. Let $Y \in \text{Id}_{\text{Rd}_R^{\mathcal{B}}([X]_R)}^{\mathcal{B}}$. If $Y \in \text{Rd}_R^{\mathcal{B}}([X]_R)$, then nothing need to. Now we suppose that $Y \notin \text{Rd}_R^{\mathcal{B}}([X]_R)$.

- 1) If $Y \xrightarrow{\tau} \zeta$ and $\zeta \notin T^*$. In this case, because $\text{Id}_{\text{Rd}_R^{\mathcal{B}}([X]_R)}^{\mathcal{B}} \subseteq T$, we have $\zeta \notin (\text{Id}_{\text{Rd}_R^{\mathcal{B}}([X]_R)}^{\mathcal{B}})^*$. Thus $Y \xrightarrow{\tau} \text{Rd}_R^{\mathcal{B}}([X]_R) \hat{\zeta} = \text{Rd}_R^{\mathcal{B}}([X]_R) \zeta$. Now according to the definition of $\text{Id}_{\text{Rd}_R^{\mathcal{B}}([X]_R)}^{\mathcal{B}}$, we have $\epsilon \xrightarrow{\tau} \text{Rd}_R^{\mathcal{B}}([X]_R) \hat{\eta}$ for some $\hat{\eta}$ such that $\text{dcmp}_{\text{Rd}_R^{\mathcal{B}}([X]_R)}^{\mathcal{D}}(\hat{\zeta}) = \text{dcmp}_{\text{Rd}_R^{\mathcal{B}}([X]_R)}^{\mathcal{D}}(\hat{\eta})$. In other words, there is $Z \in \text{Rd}_R^{\mathcal{B}}([X]_R)$ and $Z \xrightarrow{\tau} \eta$ for some η such that $\text{dcmp}_{\text{Rd}_R^{\mathcal{B}}([X]_R)}^{\mathcal{D}}(\hat{\zeta}) = \text{dcmp}_{\text{Rd}_R^{\mathcal{B}}([X]_R)}^{\mathcal{D}}(\eta)$. This makes $\zeta X \stackrel{\mathcal{D}}{=} \eta X$. Now, we use the fact that $\text{Rd}_R^{\mathcal{B}}([X]_R)$ itself is an $\text{Rd}_R^{\mathcal{B}}([X]_R)$ -candidate. Thus it satisfies the relevant conditions. That is, $[X]_{\text{Id}_R} \xrightarrow{\tau} \beta$ for some β such that $\eta.X \stackrel{\mathcal{D}}{=} \beta$. And finally we have $\zeta X \stackrel{\mathcal{D}}{=} \beta$.
- 2) If $Y \xrightarrow{a} \zeta$. The proof is complete the same as the first case.

Proof of Lemma 64: Apparently we can only prove the proposition for \mathcal{B} -admissible R 's.

The proof is by induction. Assume at some time in the execution of the algorithm, we have the set \mathbf{V} which contains all the treated blocks, and we have a current value of m , and current block $[X]_R$. The induction hypothesis is the following:

If $[X]_R \in \mathbf{V}$, then $d_R([X]_R) = \|X\|_{\mathcal{B}_R}$; if α satisfies $\text{dcmp}_R(\alpha) \in \mathbf{V}^*$, then $d_R(\alpha) = \|\alpha\|_{\mathcal{B}_R}$.

According to the algorithm, it is clear that $d_R([X]_R) \geq \|X\|_{\mathcal{B}_R}$. The reason is elaborated as follows.

- 1) If $d_R([X]_R) = m$ via the fact $[X]_R \xrightarrow{\ell} \gamma$ and $d_R(\gamma) = m - 1$. Then there is a path from X to γ with length 1 and there is a path from γ to ϵ with length $m - 1$. Thus totally we have a path from X to ϵ with length m .
- 2) If $d_R([X]_R) = m$ via the fact $[X]_R \xrightarrow{\ell} \gamma$, $d_R(\gamma) = m$ and $X \stackrel{\mathcal{B}}{=} \gamma$. Then there is a path from X to γ with length 0 and there is a path from γ to ϵ with length m . Thus totally we have a path from X to ϵ with length m .

Thus in both case we have $d_R([X]_R) \geq \|X\|_{\mathcal{B}_R}$.

Now assume, for contradiction, that $d_R([X]_R) > \|X\|_{\mathcal{B}_R}$. In other words, $m > \|X\|_{\mathcal{B}_R}$. Then according to induction hypothesis, for every $[Y]_S \in \mathbf{V}$, $d_R([Y]_S) = \|Y\|_{\mathcal{B}_S}$. Now consider the time when m is assigned to $d_R([X]_R)$. There are two possibilities:

- 1) $[X]_R \xrightarrow{\ell} \gamma$ and $d_R(\gamma) = m - 1$. In this case, by induction $d_R(\gamma) = \|\gamma\|_{\mathcal{B}_R} = m - 1$. There can not be

other transition of $[X]_R$ such as $[X]_R \xrightarrow{\ell} \zeta$ that

- a) either $d_R(\zeta) < m - 1$,
- b) or $d_R(\zeta) = m - 1$ and $\zeta \stackrel{\mathcal{B}}{=} X$.

If so, $m - 1$ would be assigned to $d_R([X]_R)$ and the block $[X]_R$ should have already been put into \mathbf{V} . This is a contradiction.

- 2) $[X]_R \xrightarrow{\ell} \gamma$, $d_R(\gamma) = m$ and $X \stackrel{\mathcal{B}}{=} \gamma$. In this case, by induction $d_R(\gamma) = \|\gamma\|_{\mathcal{B}_R} = m$, thus we must have $\|X\|_{\mathcal{B}_R} = \|\gamma\|_{\mathcal{B}_R} = m$. This is a contradiction.

APPENDIX C

PROOF OF THEOREM 4

A. Proof of Lemma 66

There are several cases according to the values of k and l :

- If $k, l > 1$. In this case we can assume that $\|\gamma\|_{\mathcal{B}_R} = \|\delta\|_{\mathcal{B}_R}$, which is already known, and we can tell whether a given action is $\stackrel{\mathcal{B}}{=} \text{decreasing}$. Suppose we have a decreasing transition of $\gamma \iff \cdot \xrightarrow{\ell} \eta.Y_{k-1} \dots Y_1$ which is induced by $[Y_k]_{R_k} \xrightarrow{\ell} \eta$. Now we have the matching transition $\delta \iff \cdot \xrightarrow{\ell} \zeta.Z_{l-1} \dots Z_1$ which is induced by $[Z_l]_{R_l} \xrightarrow{\ell} \zeta$. Moreover, we have

$$\eta.Y_{k-1} \dots Y_1 \stackrel{\mathcal{B}}{=} \zeta.Z_{l-1} \dots Z_1$$

Now we must have $Y_1 = Z_1$. And the process $Y_k \dots Y_2$ and $Z_l \dots Z_2$ also satisfy the expansion property for \mathcal{B}_R . The result of the lemma can be obtained by induction.

- If $k = 1$ and $l > 1$. In this case, $[Y_1]_R$ must not be a prime. According to our algorithm, one of the candidates will be defined as $\text{Dc}_R^{\mathcal{B}}([Y_1]_R)$ if there exist some candidates which can pass the expansion testing.
- If $k = l = 1$. If $[Z_1]_R <_R [Y_1]_R$, then this is the same as the above case. Otherwise we can change the role of Y_1 and Z_1 .

B. Preparations for the Proof of Theorem 4

To make things clear, we introduce some new terminologies. Note that the program in Fig. 2 maintains a set \mathbf{V} of the blocks which have already been treated. During the execution of the algorithm, \mathbf{V} start from \emptyset and get larger and larger. Intuitively these blocks in \mathbf{V} contain part of information of \mathcal{B} . Formally, we can define the *partial decomposition base* $\mathcal{B}_{\mathbf{V}} = \{\mathcal{B}_{R,\mathbf{V}}\}_{R \subseteq C_G}$ in which $\mathcal{B}_{R,\mathbf{V}} = (\text{Id}_{R,\mathbf{V}}^{\mathcal{B}}, \text{Pr}_{R,\mathbf{V}}^{\mathcal{B}}, \text{Cm}_{R,\mathbf{V}}^{\mathcal{B}}, \text{Dc}_{R,\mathbf{V}}^{\mathcal{B}}, \text{Rd}_{R,\mathbf{V}}^{\mathcal{B}})$ where

- $\text{Pr}_{R,\mathbf{V}}^{\mathcal{B}} = \text{Pr}_R^{\mathcal{B}} \cap \mathbf{V}$.
- $\text{Cm}_{R,\mathbf{V}}^{\mathcal{B}} = \text{Cm}_R^{\mathcal{B}} \cap \mathbf{V}$.
- $\text{Dc}_{R,\mathbf{V}}^{\mathcal{B}}([X]_R) = \begin{cases} \text{Dc}_R^{\mathcal{B}}([X]_R) & \text{if } [X]_R \in \text{Cm}_{R,\mathbf{V}}^{\mathcal{B}} \\ \text{undefined} & \text{otherwise} \end{cases}$
- $\text{Rd}_{R,\mathbf{V}}^{\mathcal{B}}([X]_R) = \begin{cases} \text{Rd}_R^{\mathcal{B}}([X]_R) & \text{if } [X]_R \in \text{Pr}_{R,\mathbf{V}}^{\mathcal{B}} \\ \text{undefined} & \text{otherwise} \end{cases}$

$\mathcal{B}_{\mathbf{V}}$ is called *partial* in the sense that $\text{Pr}_{R,\mathbf{V}}^{\mathcal{B}} \cup \text{Cm}_{R,\mathbf{V}}^{\mathcal{B}} = \text{C}_R \cap \mathbf{V} \subseteq \text{C}_R$. Comparatively, $\text{Pr}_R^{\mathcal{B}} \cup \text{Cm}_R^{\mathcal{B}} = \text{C}_R$.

At some time in the execution of the algorithm, we get a specific value of \mathbf{V} , then $\mathcal{B}_{\mathbf{V}}$ is already known at that time. Now

we can define $\text{dcmp}_{R,V}^{\mathcal{B}}(\alpha)$ for any process α . $\text{dcmp}_{R,V}^{\mathcal{B}}(\alpha) = \text{dcmp}_R^{\mathcal{B}}(\alpha)$ if the derivation of $\alpha \xrightarrow{\mathcal{B}}_R \text{dcmp}_R^{\mathcal{B}}(\alpha)$ (refer to Section V-B) only relies on the information provided in \mathcal{B}_V . Otherwise $\text{dcmp}_{R,V}^{\mathcal{B}}(\alpha)$ is undefined. In the following, a process α is called $\mathcal{B}_{R,V}$ -applicable if $\text{dcmp}_{R,V}^{\mathcal{B}}(\alpha)$ is defined.

Now we prepare to confirm the important result: $\alpha \simeq_R \beta$ implies $\alpha \stackrel{\mathcal{B}}{=} \beta$.

First of all, we find that it is enough to prove the result under the assumption that R is \mathcal{B} -admissible. Note that If $\simeq_R \subseteq \stackrel{\mathcal{B}}{=} \simeq_R$ for every \mathcal{B} -admissible R 's, then for every R we have $\simeq_R \subseteq \simeq_{\text{Id}_R^{\mathcal{B}}} \subseteq \stackrel{\mathcal{B}}{=} \text{Id}_R^{\mathcal{B}} = \stackrel{\mathcal{B}}{=} \simeq_R$. Thus in the rest of this section we assume R to be \mathcal{B} -admissible.

With the help of Lemma 66, we are able to establish Theorem 4.

We take the following approach to prove Theorem 4. Remember that our algorithm maintains a set V , containing all the blocks which have been treated. We will suppose that R is \mathcal{B} -admissible. Let $[X]_R$ be a block which is about to be put into V . We try to prove that if $[X]_R$ is a $\hat{\mathcal{B}}_R$ -composite, and let $\text{Dc}_R^{\hat{\mathcal{B}}}([X]_R) = [Z_t]_{R_t} \dots [Z_1]_{R_1}$, then $X \stackrel{\mathcal{B}}{=} Z_t \dots Z_1$.

Apparently, the proof must be done by induction. However, this is not an easy task. We will choose the following statements as our induction hypotheses:

- I. Let R be an arbitrary \mathcal{B} -admissible set. Suppose that γ is $\mathcal{B}_{R,V}$ -applicable, and $\text{dcmp}_R^{\hat{\mathcal{B}}}(\gamma) = [W_u]_{R_u} \dots [W_1]_{R_1}$. Then $W_u \dots W_1$ is $\mathcal{B}_{R,V}$ -applicable, and $\text{dcmp}_{R,V}^{\mathcal{B}}(\gamma) = \text{dcmp}_{R,V}^{\mathcal{B}}(W_u \dots W_1)$. That is, $\gamma \stackrel{\mathcal{B}}{=} W_u \dots W_1$.

We remark that at the time the algorithm terminates when V contains every blocks, the statement I implies Theorem 4.

The readers are suggested to imagine the following picture in mind. Although R_1, \dots, R_t are all $\hat{\mathcal{B}}$ -admissible according to the definition of decomposition base, we cannot draw the conclusion that R_1, \dots, R_t are all \mathcal{B} -admissible. It may indeed happen that $Z_i \in \text{Id}_{R_i}^{\mathcal{B}}$, which means that Z_i is \mathcal{B}_{R_i} -redundant. However, since $R_1 = R$ is \mathcal{B} -admissible, we do have $Z_1 \notin \text{Id}_{R_1}^{\mathcal{B}}$. This fact will be used in the proof.

C. Proof of Lemma 67

This fact can be proved by induction on $d = \|W_u \dots W_1\|_{\mathcal{B}_R}$, and by studying a witness path of \simeq_R -norm for W . Then using hypothesis I and by inspecting the algorithm we can show that when $W \simeq_R W_u \dots W_1$, W should have already been put into V .

D. Proof of Lemma 68

We use δ to indicate $Z_t \dots Z_1$. The lemma confirms that, when $[X]_R$ is about to be put into V , $\text{dcmp}_{R,V}^{\mathcal{B}}(Z_t \dots Z_1)$ has already been defined. This fact is proved by induction, using the induction hypotheses. The way is to choose a process γ such that $[X]_R \xrightarrow{\ell}_R \gamma$ is on a $\stackrel{\mathcal{B}}{=} \simeq_R$ -witness path of X . Now γ is $\mathcal{B}_{R,V}$ -applicable, thus we try to use induction hypotheses on γ . There are two cases:

- If there exist γ such that $[X]_R \xrightarrow{\ell}_R \gamma$ and $\|\gamma\|_{\mathcal{B}_R} = m - 1$. In this case, the algorithm is

running in the first **while**-loop in Fig. 2. Since $X \simeq_R \delta$, there is a matching of $[X]_R \xrightarrow{\ell}_R \gamma$ from δ , say $\delta \xrightarrow{\ell}_R \cdot \xrightarrow{\ell}_R \zeta$ for some ζ that $\gamma \simeq_R \zeta$. Because δ is itself a \simeq_R -prime-decomposition, we must have $\delta \iff \cdot \xrightarrow{\ell}_R \zeta$, which is induced by $[Z_t]_{R_t} \xrightarrow{\ell}_{R_t} \eta$ for some η , and $\zeta = \eta \cdot Z_{t-1} \dots Z_1$. Suppose $\text{dcmp}_{R_t}^{\hat{\mathcal{B}}}(\eta) = [Y_s] \dots [Y_1]$ ($s \geq 0$), then $\text{dcmp}_R^{\hat{\mathcal{B}}}(\zeta)$ must be in the form $[Y_s] \dots [Y_1] \cdot [Z_{t-1}]_{R_{t-1}} \dots [Z_1]_{R_1}$. Because $\gamma \simeq_R \zeta$, we have $\text{dcmp}_R^{\hat{\mathcal{B}}}(\gamma) = [Y_s] \dots [Y_1] \cdot [Z_{t-1}]_{R_{t-1}} \dots [Z_1]_{R_1}$. According to induction hypothesis I, $\gamma \stackrel{\mathcal{B}}{=} Y_s \dots Y_1 \cdot Z_{t-1} \dots Z_1$, thus $\|Y_s \dots Y_1 \cdot Z_{t-1} \dots Z_1\|_{\mathcal{B}_R} = m - 1$. Now since $\text{dcmp}_R^{\hat{\mathcal{B}}}(\zeta) = [Y_s] \dots [Y_1] \cdot [Z_{t-1}]_{R_{t-1}} \dots [Z_1]_{R_1}$, by Lemma 67, $\zeta \stackrel{\mathcal{B}}{=} Y_s \dots Y_1 \cdot Z_{t-1} \dots Z_1$ and thus $\|\zeta\|_{\mathcal{B}_R} = m - 1$. Since $\delta \iff \cdot \xrightarrow{\ell}_R \zeta$, we have $\|\delta\|_{\mathcal{B}_R} \leq m$. In summary, we have:

$$\begin{aligned} - \|\zeta\|_{\mathcal{B}_R} &= \|Y_s \dots Y_1 \cdot Z_{t-1} \dots Z_1\|_{\mathcal{B}_R} = \|\eta \cdot Z_{t-1} \dots Z_1\|_{\mathcal{B}_R} = m - 1. \\ - \|Z_{t-1} \dots Z_1\|_{\mathcal{B}_R} &\leq m - 1. \\ - \|\delta\|_{\mathcal{B}_R} &\leq m. \\ - \|Z_1\|_{\mathcal{B}_R} &> 0. \end{aligned}$$

There are two possibilities:

- EITHER $\|Z_i\|_{\mathcal{B}_{R_i}} < m$ for every $1 \leq i \leq t$. In this case we have $\delta = Z_t \dots Z_1$ is $\mathcal{B}_{R,V}$ -applicable trivially.
- OR $t = 1$ and $\|Z_1\|_{\mathcal{B}_R} = m$. In this case, we have $[Z_1]_R <_R [X]_R$ and $\|Z_1\|_{\mathcal{B}_R} = \|X\|_{\mathcal{B}_R}$. Thus $[Z_1]_R \in V$ and thus $\delta = Z_1$ is $\mathcal{B}_{R,V}$ -applicable.
- If for every γ such that $[X]_R \xrightarrow{\ell}_R \gamma$, we do not have $\|\gamma\|_{\mathcal{B}_R} < m$. In this case, the algorithm is running in the second **while**-loop in Fig. 2. We are able to find a γ which is $\mathcal{B}_{R,V}$ -applicable such that $[X]_R \xrightarrow{\tau}_R \gamma$ and $X \stackrel{\mathcal{B}}{=} \gamma$, and $\|\gamma\|_{\mathcal{B}_R} = \|X\|_{\mathcal{B}_R} = m$. If it happens that we can find such γ satisfying $X \simeq_R \gamma$, we can use the induction hypothesis I to confirm immediately that δ is $\mathcal{B}_{R,V}$ -applicable and $\gamma \stackrel{\mathcal{B}}{=} \delta$ (hence $X \stackrel{\mathcal{B}}{=} \delta$). Thus in the following we will assume that $\gamma \not\simeq_R X$. That is, $[X]_R \xrightarrow{\tau}_R \gamma \not\simeq_R X$. Since $X \simeq_R \delta$, there is a matching of $[X]_R \xrightarrow{\tau}_R \gamma$ from δ , say $\delta \xrightarrow{\tau}_R \cdot \xrightarrow{\tau}_R \zeta$ for some ζ such that $\gamma \simeq_R \zeta$. Because δ is itself a \simeq_R -prime-decomposition, we must have $\delta \iff \cdot \xrightarrow{\tau}_R \zeta \simeq_R \gamma$, which is induced by $[Z_t]_{R_t} \xrightarrow{\tau}_{R_t} \eta$ for some η , and $\zeta = \eta \cdot Z_{t-1} \dots Z_1$. Suppose $\text{dcmp}_{R_t}^{\hat{\mathcal{B}}}(\eta) = [Y_s] \dots [Y_1]$ ($s \geq 0$), then $\text{dcmp}_R^{\hat{\mathcal{B}}}(\zeta)$ must be in the form $[Y_s] \dots [Y_1] \cdot [Z_{t-1}]_{R_{t-1}} \dots [Z_1]_{R_1}$. Because $\gamma \simeq_R \zeta$, we have $\text{dcmp}_R^{\hat{\mathcal{B}}}(\gamma) = [Y_s] \dots [Y_1] \cdot [Z_{t-1}]_{R_{t-1}} \dots [Z_1]_{R_1}$. According to induction hypothesis I, $\gamma \stackrel{\mathcal{B}}{=} Y_s \dots Y_1 \cdot Z_{t-1} \dots Z_1$, thus $\text{dcmp}_R^{\hat{\mathcal{B}}}(\zeta)$ is $\mathcal{B}_{R,V}$ -applicable, and $\|\text{dcmp}_R^{\hat{\mathcal{B}}}(\zeta)\|_{\mathcal{B}_R} = \|Y_s \dots Y_1 \cdot Z_{t-1} \dots Z_1\|_{\mathcal{B}_R} = m$. In summary:

- $\|Y_s \dots Y_1 Z_{t-1} \dots Z_1\|_{\underline{B}_R} = m$.
- $\|Z_{t-1} \dots Z_1\|_{\underline{B}_R} \leq m$.
- $\|Z_1\|_{\underline{B}_R} > 0$.

Now we have two possibilities:

- If $t \geq 2$. Because $\|Z_1\|_{\underline{B}_R} > 0$, thus $\|Z_{t-1} \dots Z_1\|_{\underline{B}_R} > 0$. Let $S = \mathbf{Rd}_R^{\underline{B}}(Z_{t-1} \dots Z_1)$. By induction $R_t \subseteq S$. Then we have $\|Y_s \dots Y_1\|_{\underline{B}_S} < m$. Since $\eta \simeq_{R_t} Y_s \dots Y_1$, it is clear $\eta \simeq_S Y_s \dots Y_1$, by Lemma 67, η is $\mathcal{B}_{S, \mathbf{V}}$ -applicable, $\eta \stackrel{\underline{B}}{=}_S Y_s \dots Y_1$, and $\|\eta\|_{\underline{B}_S} = \|Y_s \dots Y_1\|_{\underline{B}_S} < m$. Now let us investigate Z_t . If $Z_t \in \underline{B}_S$, $Z_t \dots Z_1$ is trivially $\mathcal{B}_{R, \mathbf{V}}$ -applicable. If $Z_t \notin S$, we have got the fact that $[Z_t]_S \stackrel{\tau}{\mapsto} \eta$ and $\|\eta\|_{\underline{B}_S} < m$. This fact tells us that $[Z_t]_S$ should have been treated before $[X]_R$. In other words, $[Z_t]_S \in \mathbf{V}$, which means that $\delta = Z_t \dots Z_1$ is $\mathcal{B}_{R, \mathbf{V}}$ -applicable.
- If $t = 1$. In this case, we have the following facts: $[Z_1]_R \stackrel{\tau}{\mapsto}_R \eta$, $\text{dcmp}_R^{\underline{B}}(\eta) = [Y_s] \dots [Y_1]$, and $\|Y_s \dots Y_1\|_{\underline{B}_R} = m$. We can show $\|Y_1\|_{\underline{B}_R} > 0$, using the same argument for proving $\|Z_1\|_{\underline{B}_R} > 0$ before. Let us say $\eta = \eta'.W$ (η' can be ϵ), and let $S = \mathbf{Rd}_R(W)$. Thus $\text{dcmp}_R^{\underline{B}}(W) = [Y_i] \dots [Y_1]$ and $\text{dcmp}_S^{\underline{B}}(\eta') = [Y_s] \dots [Y_{i+1}]$ for some $1 \leq i \leq s$. and η' is $\mathcal{B}_{R, S}$ -applicable by induction.

- 1) If $\|Y_i \dots Y_1\|_{\underline{B}_R} < m$. we can use Lemma 67 to prove:

- * W is $\mathcal{B}_{R, \mathbf{V}}$ -applicable and $W \stackrel{\underline{B}}{=}_{\underline{B}_R} Y_i \dots Y_1$, and
- * $S \subseteq \mathbf{Rd}_R^{\underline{B}}(W)$.

Since we know $\eta' \simeq_S Y_s \dots Y_{i+1}$, then $\eta' \simeq_{\mathbf{Rd}_R^{\underline{B}}(W)} Y_s \dots Y_{i+1}$. Because $\|Y_s \dots Y_{i+1}\|_{\underline{B}_{\mathbf{Rd}_R^{\underline{B}}(W)}} < m$, we can use induction to prove η' is $\mathcal{B}_{\mathbf{Rd}_R^{\underline{B}}(W), \mathbf{V}}$ -applicable and $\eta' \stackrel{\underline{B}}{=}_{\mathbf{Rd}_R^{\underline{B}}(W)} Y_s \dots Y_{i+1}$. In summary, η is $\mathcal{B}_{R, \mathbf{V}}$ -applicable and $\eta \stackrel{\underline{B}}{=}_{\underline{B}_R} Y_s \dots Y_1$.

- 2) If $\|Y_i \dots Y_1\|_{\underline{B}_R} = m$. In this case, $Y_s \dots Y_{i+1} \in \mathbf{Rd}_R^{\underline{B}}(Y_i \dots Y_1)$, this implies that $Y_s \dots Y_{i+1} \Rightarrow \epsilon$, and therefore

$$\eta = \eta'.W \simeq_R Y_s \dots Y_1 \Rightarrow Y_i \dots Y_1 \simeq_R W$$

which implies $\eta \Rightarrow_R W$. Now we have $Z_1 \Rightarrow_R \eta \Rightarrow_R W$, thus $[W]_R <_R [Z_1]_R$. On the other hand, by $[Z_1]_R = \text{dcmp}_R^{\underline{B}}([X]_R)$, we have $[Z_1]_R < [X]_R$. Therefore $W <_R Z_1 <_R X$. By Lemma 67, W is $\mathcal{B}_{R, \mathbf{V}}$ -applicable and $W \stackrel{\underline{B}}{=}_{\underline{B}_R} Y_i \dots Y_1$. Now in the same way of case 1, we can prove η' is $\mathcal{B}_{\mathbf{Rd}_R^{\underline{B}}(W), \mathbf{V}}$ -applicable and $\eta' \stackrel{\underline{B}}{=}_{\mathbf{Rd}_R^{\underline{B}}(W)} Y_s \dots Y_{i+1} \stackrel{\underline{B}}{=}_{\mathbf{Rd}_R^{\underline{B}}(W)} \epsilon$. In summary, η is $\mathcal{B}_{R, \mathbf{V}}$ -applicable and $\eta \stackrel{\underline{B}}{=}_{\underline{B}_R} Y_s \dots Y_1$.

Up to now, we have shown that $[Z_1]_R <_R [X]_R$ and $[Z_1]_R \stackrel{\tau}{\mapsto}_R \eta$ such that $X \stackrel{\underline{B}}{=}_{\underline{B}_R} \gamma \stackrel{\underline{B}}{=}_{\underline{B}_R} \eta$ with $\|\eta\|_{\underline{B}_R} = m$. This fact means that $[Z_1]_R$ should be chosen to test the expansion condition in the **while**-loop before $[X]_R$. Now we can do without difficulty to check expansion conditions to ensure that $[Z_1]_R$ is put into \mathbf{V} before $[X]_R$.

E. Proof of Proposition 69

We use δ to indicate $Z_t \dots Z_1$. By Lemma 68, δ is $\mathcal{B}_{R, \mathbf{V}}$ -applicable. In other words, $\text{dcmp}_{R, \mathbf{V}}^{\underline{B}}(\delta)$ is known.

The proof goes by directly exploring the expansion conditions. Only to remember the following fact:

- 1) If $\alpha \simeq_R \beta$, then $\alpha \stackrel{\mathcal{D}}{=} \beta$.
- 2) If $\alpha \simeq_R \beta$, and α, β are $\mathcal{B}_{R, \mathbf{V}}$ -applicable, then $\alpha \stackrel{\underline{B}}{=} \beta$.

By studying the the expansion conditions, we can confirm that $\text{dcmp}_{R, \mathbf{V}}^{\underline{B}}(\delta)$ can successfully pass this testing. Now it is important to take notice of Lemma 66. It ensures that at most one decomposition candidate can pass the testing. Thus we can confirm that $\mathbf{Dc}_R^{\underline{B}}([X]_R) = \text{dcmp}_{R, \mathbf{V}}^{\underline{B}}(\delta)$, which implies $X \stackrel{\underline{B}}{=}_{\underline{B}_R} Z_t \dots Z_1$.