Hennessy-Milner Classes and Process Algebra

Marco Hollenberg

Utrecht University, Department of Philosophy

Heidelberglaan 8, 3584 CS Utrecht, the Netherlands

E-mail: hollenb@phil.ruu.nl

WWW: http://www.phil.ruu.nl/home/marco/

Abstract

This paper studies Hennessy-Milner classes, classes of Kripke models where modal-logical equivalence coincides with bisimulation. Concepts associated with these classes in the literature (Goldblatt [6], Visser [8]) are studied and compared and the structure of the collection of maximal Hennessy-Milner classes is investigated (how many are there, what is their intersection?). The insights into these classes are applied to process algebra. This results in a Hennessy-Milner process algebra for a non-trivial process language, whose standard graph-semantics is not Hennessy-Milner.

1 Introduction

Given any two Kripke models $\mathfrak{S}$ and $\mathfrak{T}$, we can define two relations of equivalence between the points of these models. The first is a semantic one: two points s and t are *bisimilar* (notation: $s \underline{\leftrightarrow} t$) if there is a bisimulation between $\mathfrak{S}$ and $\mathfrak{T}$ (not necessarily total) connecting s and t. The second is of a syntactic nature: s and t are *modally equivalent* (notation: $s \approx t$) if s and t force the same modal formulas. It is well-known that bisimulation implies modal equivalence, but what about the other direction? It would be nice if $\approx = \underline{\leftrightarrow}$, for then if s and t were not the same semantically (i.e. they were not bisimilar) this would have syntactic consequences: there would be a modal formula true at s but not true t. This formula would thus be a linguistic *witness* to the non-bisimilarity of s and t, perhaps giving us insight into *why* these points are not bisimilar. From a purer standpoint: it would simply give us a strong connection between modal logic and its Kripke model semantics.

Alas, there are examples of models where bisimulation does not coincide with modal equivalence. We have three options when we try to fix this problem. First, we can change our modal language. Allowing infinite disjunctions and conjunctions ensures that bisimulation coincides with the notion of modal equivalence relative to these new formulas. Second, we can change the notion of bisimulation so that it fits with our original modal language. And third, we may look at restricted classes of Kripke models where bisimulation *does* coincide with modal equivalence, leaving both the language and the notion of bisimulation intact. This last route is the one this paper investigates.

Hennessy and Milner [7] were the first to present such a class: the class of all image-finite (or finitely branching) models. Goldblatt [6] investigates what he calls *Hennessy-Milner models* which are models where $\approx$ is a bisimulation (which is the same as saying that $\approx$ and $\underline{\leftrightarrow}$ conincide on this model). Following this up, we may call classes of Kripke models s.t. any two models from this class are always *logically bisimilar* (i.e. $\approx$ is a bisimulation between them, notation: $\mathfrak{S} \approx \mathfrak{T}$) *Hennessy-Milner* *classes*. Then saying that a *set* is a Hennessy-Milner class is the same as saying that the disjunct union of all models in this set is a Hennessy-Milner model.

Process algebra (see Baeten and Weijland [1]) has a standard semantics involving directed graphs. These can be seen as Kripke models, making the question whether this standard semantics is a Hennessy-Milner class a reasonable one. It is a particularly potent question in this area, for when process algebra is used to verify specifications of computer programs, modal witnesses for non-bisimularity would provide us with useful information about precisely *where* the program goes awry. A more philosophical statement can also be made. Infinite branching in process algebra is nothing but a useful abstraction: it does not occur in any real-life processes. As finite branching implies the Hennessy-Milner property a good reconciliation between the finite and the infinite in process algebra would be a Hennessy-Milner graph-semantics where infinite branching is possible. Such a graph-semantics will be discussed in this paper.

The layout of the paper is as follows. The next section compares various notions discussed in Goldblatt [6] and Visser [8] in relation to the Hennessy-Milner property. After this we mention a characterization of *maximal* Hennessy-Milner classes (due to Albert Visser). A natural maximal Hennessy-Milner class will turn out to be the class of m-saturated models, already discussed in [8]. After this some structural issues concerning the collection of maximal Hennessy-Milner classes are tackled. We give a lower bound on the number of maximal Hennessy-Milner classes, we determine the intersection of all such classes and we give an example of a curious phenomenon: two Hennessy-Milner models that are not logically bisimilar while every Hennessy-Milner model must be logically bisimilar to at least one of them. Finally we examine a rich enough language in process algebra, namely the regular operations plus infinite choice, for which the standard graph-semantics is not a Hennessy-Milner class: we remedy this by giving an alternative graph-semantics, based on the class of m-saturated models.

2 A landscape of properties

This section studies some properties of models discussed in [6] and [8] in connection with the Hennessy-Milner property, and compares them. The language we consider is that of multimodal logic, that is: we have a countable set of unary existential modal operators $\langle\alpha\rangle$, one for each label α from some nonempty set $\mathcal{A}$, and a (possibly empty) countable set of propositional variables. The dual of $\langle\alpha\rangle$ is $[\alpha] := \neg\langle\alpha\rangle\neg$. If α is clear from the context or if it is irrelevant $\langle\alpha\rangle$ will simply be written as $\Diamond$ and $[\alpha]$ as $\Box$. Models for this language are Kripke models, with a binary relation R_α (called a *transition-relation*) on the universe for each α and a valuation V that assigns to each propositional variable a subset of the universe as its interpretation.

We need a definition that is not so standard:

Definition 2.1 *For any two points s and t in two (possibly identical) models $s\mathcal{H}_\alpha t$ means that $t \Vdash \phi$ implies $s \Vdash \langle\alpha\rangle\phi$, for all modal formulas ϕ.* □

The model-properties we will study in this section are the following (let $\mathfrak{S} = (S, \{R_\alpha\}_{\alpha\in\mathcal{A}}, V)$ be some fixed model for a fixed modal language $\mathcal{L}$; we will explain each notion for this fixed model):

1. **Finiteness.** S is finite.
2. **Image-finiteness.** For each $\alpha \in \mathcal{A}$ and each $s \in S$, the set $\{t \in S \mid sR_\alpha t\}$ is finite.

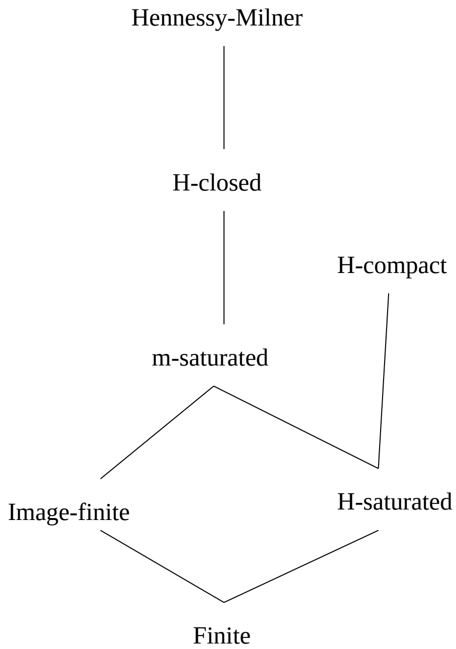

Figure 1: The landscape of properties

3. **$\mathcal{H}$-closure.** $s\mathcal{H}_\alpha t$ implies that there is a $u \in S$ s.t. $sR_\alpha u \approx t$.

4. **Compactness.** If a set of formulas $\Phi \subseteq \mathcal{L}$ is finitely satisfiable in $\mathfrak{S}$ then it is satisfiable at some point in $\mathfrak{S}$.

5. **$\mathcal{H}$-saturation.** $\mathcal{H}$-closed *and* compact.

6. **m-saturation.** If for every finite subset of Φ there is an α-successor of s that satisfies it, then there is an α-successor of s that satisfies Φ. [1]

7. **The Hennessy-Milner property.** $\approx$ is a bisimulation on $\mathfrak{S}$.

The relations between these properties can be depicted as in figure 1. An upward line indicates strict inclusion, while the absence of such a line indicates noncomparibility of the two properties (modulo transitive closure). We shall prove that this picture is correct.

The positive part of the picture, the visible lines, is the easiest to prove. We will only prove some parts of this: the remainder can easily be verified.

- **Image-finiteness implies m-saturation.**
  Suppose $\mathfrak{S}$ is image-finite. Consider a set Φ of formulas and a point $s \in S$ such that Φ is finitely satisfied in the α-successors of s. If Φ is satisfied in no α-successor of s then for every t s.t. $sR_\alpha t$ we can choose a formula $\phi_t \in \Phi$ with $t \not\Vdash \phi_t$. But $\{\phi_t \mid sR_\alpha t\}$ is finite, as $\mathfrak{S}$ is assumed to be image-finite, while it is not satisfied in any α-successor of s. Contradiction! So Φ *is* satisfied in some α-successor of s.

[1] The names compactness and $\mathcal{H}$-saturation are due to [6], while m-saturation is due to [8]. Actually, Fine [3] is first in defining these concepts. Here is the translation of Fine's terms to the terms used in this paper:

modally saturated$_1$	$\longmapsto$	compact
modally saturated$_2$	$\longmapsto$	m-saturated
modally saturated	$\longmapsto$	$\mathcal{H}$-saturated

- **$\mathcal{H}$-saturation implies m-saturation.**
  Suppose $\mathfrak{S}$ is $\mathcal{H}$-saturated and Φ is a set of formulas finitely satisfied in the α-successors of s. Define $\Psi := \{\phi \mid s \Vdash [\alpha]\phi\}$ and let $\Gamma := \Phi \cup \Psi$. We prove that Γ is finitely satisfiable in $\mathfrak{S}$. Suppose Δ is a finite subset of Γ. Δ can then be split in two parts: Δ_0 and Δ_1, subsets of respectively Φ and Ψ. As Φ is finitely satisfied in the α-successors of s there is a t s.t. $sR_\alpha t \Vdash \Delta_0$, since Δ_0 is finite. By definition $t \Vdash \Psi \supseteq \Delta_1$, so $t \Vdash \Delta$. Now, by compactness of $\mathfrak{S}$, there must be some u s.t. $u \Vdash \Gamma$. This u is such that $s\mathcal{H}_\alpha u$. For assume $u \Vdash \phi$, while $s \nVdash \langle\alpha\rangle\phi$. Then $s \Vdash [\alpha]\neg\phi$, so $\neg\phi \in \Psi \subseteq \Gamma$ and as $u \Vdash \Gamma$, $u \Vdash \neg\phi$: contradiction. By $\mathcal{H}$-closure of $\mathfrak{S}$ we conclude that there is a v s.t. $sR_\alpha v \approx u$, which implies $v \Vdash \Phi$, as $u \Vdash \Phi$.

- **m-saturation implies $\mathcal{H}$-closure.**
  Suppose $\mathfrak{S}$ is m-saturated and $s\mathcal{H}_\alpha t$. Consider the set $\Phi := \{\phi \mid t \Vdash \phi\}$. Every finite subset Δ of Φ is satisfied at some successor of s. For $t \Vdash \bigwedge\Delta$ so $s \Vdash \langle\alpha\rangle\bigwedge\Delta$ (as $s\mathcal{H}_\alpha t$), hence $u \Vdash \Delta$ for some u with $sR_\alpha u$. By m-saturation we may conclude that Φ is satisfied at some α-successor u of s. But this implies that $u \approx t$ and we have proved that $\mathfrak{S}$ is $\mathcal{H}$-closed.

- **$\mathcal{H}$-closure implies the Hennessy-Milner property.**
  This is already shown in [6]. The proof is easy: suppose $sR_\alpha t$ and $s \approx s'$. Then $s'\mathcal{H}_\alpha t$, so by $\mathcal{H}$-closure there must be a $t' \approx t$ with $s'R_\alpha t'$, which is what we needed to prove that s and t are bisimilar via $\approx$.

The negative part of the theorem involves giving counterexamples to inclusions. Again we only give the more interesting parts of the proof. Also, all our counterexamples use a single accessibility-relation (which allows us to use $\Diamond$ instead of $\langle\alpha\rangle$ without causing confusion) and no propositional variables, so if our language has more than that our examples still hold: simply assume the other relations to be empty, while having each point validate the same propositional variables (say none). As our language contains no propositional variables, we leave out the valuation in the description of our counterexamples: it is always the empty function. Finally, all our examples are *rooted*: they contain some point that can reach all other points in finitely many steps.

- **Image-finiteness does not imply compactness.**
  Consider the following model $\mathfrak{S}_1$:

S_1	$=$	$\{(m,n) \mid m,n \in \mathbb{N}, n \leq m\}$ $\cup$ $\{[m,i,j] \mid m,i,j \in \mathbb{N}, 1 \leq j \leq i \leq m\}$
R_1	$=$	$\{\langle (m,n),(m,n+1)\rangle \mid n < m\}$ $\cup$ $\{\langle (m,m),(m+1,0)\rangle \mid m \in \mathbb{N}\}$ $\cup$ $\{\langle (m,0),[m,i,1]\rangle \mid 1 \leq i \leq m\}$ $\cup$ $\{\langle [m,i,j],[m,i,j+1]\rangle \mid 1 \leq j < i \leq m\}$

  In pictorial form it is more clear which model is described here (see figure 2).

  $\mathfrak{S}_1$ is clearly image-finite. To see that it is not compact, consider the set $\Phi := \{\Diamond^n\Box\bot \mid n \geq 1\}$. This set is finitely satisfiable in $\mathfrak{S}_1$: for any nonempty finite subset Δ of Φ pick the maximum n s.t. $\Diamond^n\Box\bot \in \Delta$. Then $(n,0) \Vdash \Delta$. But Φ is not satisfiable as a whole in $\mathfrak{S}_1$. Clearly Φ is not satisfiable in any

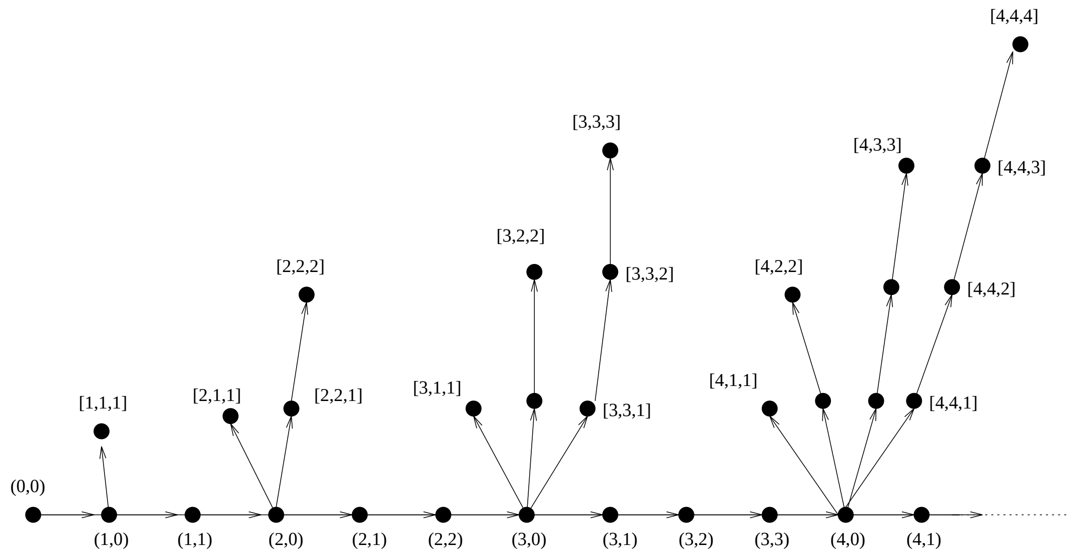

Figure 2: $\mathfrak{S}_1$: image-finite but not compact.

$[m,i,j]$-node. Also $(m,n+1) \not\Vdash \Diamond\Box\bot$, while for any m: $(m,0) \not\Vdash \Diamond^{m+1}\Box\bot$. The latter is because any path of length $m+1$ from $(m,0)$ cannot go through any $[m,i,j]$-nodes, but *must* be the path $(m,0),(m,1),\ldots,(m,m),(m+1,0)$, and $(m+1,0) \not\Vdash \Box\bot$. So $\mathfrak{S}_1$ is not compact.

Notice that a much simpler counterexample exists, namely $(\mathbb{N},>)$, as the reader may verify. However, the example we give is stronger, as it also holds as a counterexample for the class of rooted models.

- **Compactness does not imply the Hennessy-Milner property.** Consider $\mathfrak{S}_2 = (\omega+2,>)$, where $\omega+2$ denotes $\mathbb{N}\cup\{\omega,\omega+1\}$ and $>$ is defined as usual. This counterexample is due to Goldblatt (personal communication).

  To prove that it is compact, suppose Φ is finitely satisfiable in $\mathfrak{S}_2$, while it is wholely satisfied nowhere. Then $\omega+1 \not\Vdash \phi_1$ and $\omega \not\Vdash \phi_0$ for some $\phi_0,\phi_1 \in \Phi$. Lemma 7 of [6] shows that for $(\omega+1,>)$ the *truth sets*, those subsets of the universe of the form $V(\phi) := \{s \in \omega+1 \mid s \Vdash \phi\}$ for any formula ϕ, are precisely

  $$\{A \subseteq \mathbb{N} \mid \ A \text{ is finite}\} \cup \{A \cup \{\omega\} \mid \ A \subseteq \mathbb{N} \text{ is cofinite }\}$$

  $(\omega+1,>)$ is the submodel of $\mathfrak{S}_2$ generated by ω, so truth at $\omega+1$-points is the same in the two models. As neither ω nor $\omega+1$ satisfies $\phi_0 \wedge \phi_1$ we must conclude that $V(\phi_0 \wedge \phi_1)$ (where the V-function is taken relative to $\mathfrak{S}_2$) is a finite subset of $\mathbb{N}$, say $\{s_1,\ldots,s_n\}$. We have assumed that for every s_i there is a $\psi_i \in \Phi$ s.t. $s_i \not\Vdash \psi_i$. So $\{\phi_0,\phi_1,\psi_1,\ldots,\psi_n\}$ is a finite subset of Φ that is not satisfied anywhere in $\mathfrak{S}_2$ and we have reached our contradiction. Hence $\mathfrak{S}_2$ is compact.

  It is not Hennessy-Milner, however. To show this we first prove that $\omega \approx \omega+1$. If $\omega+1 \Vdash \Diamond\phi$ then either $n \Vdash \phi$ for some $n \in \mathbb{N}$, in which case also $\omega \Vdash \Diamond\phi$, or $\omega \Vdash \phi$. Using lemma 7 of [6] again, the latter implies the existence of an $n \in \mathbb{N}$ satisfying ϕ, which gives us our first case again. For the other direction, if $\omega \Vdash \Diamond\phi$ then clearly $\omega+1 \Vdash \Diamond\phi$, as our model is transitive. This demonstrates that $\omega \approx \omega+1$ (the other cases of the induction are trivial). But $\omega+1$ can reach a point (ω) satisfying $\{\Diamond^n\top \mid n \in \mathbb{N}\}$, while ω can reach no such point. Therefore $\approx$ is not a bisimulation on $\mathfrak{S}_2$.

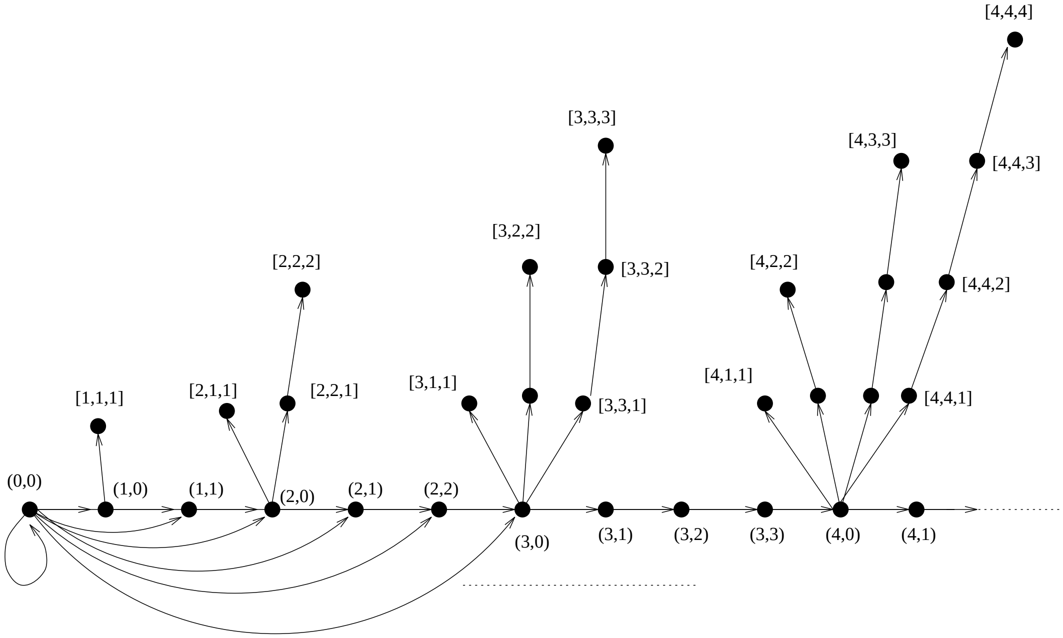

Figure 3: $\mathfrak{S}_3$: $\mathcal{H}$-closed but not m-saturated.

- **$\mathcal{H}$-closure does not imply m-saturation.**
  For this we take a model very similar to $\mathfrak{S}_1$:

S_3	$=$	S_1
R_3	$=$	$R_1 \cup \{\langle (0,0),(m,n)\rangle \mid n \leq m\}$

  For a picture, consult figure 3.

  Let us check that $\mathfrak{S}_3$ is $\mathcal{H}$-closed. So suppose $s, t \in S_3$ and $s\mathcal{H}t$. If s and t are both not the root $(0,0)$, then we need only consider the submodel generated by $(1,0)$, which is image-finite and thus $\mathcal{H}$-closed by earlier results. What remains are two cases:

  1. $(0,0)\mathcal{H}t$. If t is of the form (m,n) we have nothing to check, as then $(0,0)Rt$. If t is of the form $[m,i,j]$ then $t \Vdash \Box^n\bot$ for some n. But $(0,0) \nVdash \Diamond\Box^n\bot$, as every successor of $(0,0)$ starts an infinite branch. So $(0,0)\mathcal{H}t$ cannot be the case here.
  2. $s\mathcal{H}(0,0)$. Then $s \Vdash \Diamond^n\Box\bot$ for every $n \geq 3$. Thus s can only be $(0,0)$. As $(0,0)R(0,0)$ we are finished.

  It is furthermore easy to see that $\mathfrak{S}_3$ is not m-saturated, as $\{\Diamond^n\Box\bot \mid n \geq 1\}$ is finitely satisfiable in the successors of $(0,0)$, but not completely satisfiable there (see the argument that $\mathfrak{S}_1$ is not compact).

3 Hennessy-Milner classes

A *Hennessy-Milner class* is a class of models s.t. any two models $\mathfrak{S}$ and $\mathfrak{T}$ from this class are logically bisimilar, i.e. the relation $\approx$ between the two is a (partial) bisimulation. By *partial* we mean that not every point in the first model need be related via $\approx$ to a point in the second model, and vice-versa. So logical bisimilarity of models does *not* imply bisimilarity. An example of a Hennessy-Milner class is the class of all m-saturated models: any two m-saturated models are logically bisimilar (see [8]) [2], so the condition is met. Another example is given in [6], namely the class of $\mathcal{H}$-saturated models, but this is contained in the class of m-saturated models. It is clear that Hennessy-Milner classes can only contain Hennessy-Milner models. A class of models that only contains Hennessy-Milner models, but is not Hennessy-Milner is the class of $\mathcal{H}$-closed models: there exist two $\mathcal{H}$-closed models that are not logically bisimilar (see [6]).

This section looks at some of the structure of the collection of Hennessy-Milner classes. In particular we are interested in *maximal* Hennessy-Milner classes, Hennessy-Milner classes s.t. no extension is again Hennessy-Milner. So to say that a class K is a maximal Hennessy-Milner class is the same as saying that every model $\mathfrak{S}$ that is logically bisimilar to itself and to every model in K is already an element of K. First we'll give a characterization, due to Visser[3]of maximal Hennessy-Milner classes, using the Henkin model. In the process, it will be shown that every maximal Hennessy-Milner class can be extended to a maximal one. But first, we need some definitions.

Definition 3.1 *The* **Henkin-model** $\mathfrak{H}$ *is the model described as follows:*

universe: $\{\Theta \mid \ \Theta$ *is a maximal consistent set of modal formulas*$\}$

transitions: *For any* $\alpha \in \mathcal{A}$*:* $\Gamma R_\alpha \Delta$ *iff* $\forall \phi \in \Delta . \langle\alpha\rangle\phi \in \Gamma$

valuation: $V(p) := \{\Theta \mid p \in \Theta\}$ □

The fundamental property of the Henkin model is the following:

$$\mathfrak{H}, \Theta \Vdash \phi \text{ iff } \phi \in \Theta$$

It is easily seen to be true, using the fact that any consistent set of formulas can be extended to a maximal consistent one. For a more extensive account of the Henkin model one may consult Goldblatt [5], page 22.

Definition 3.2 *A* **Henkin-like model** *is a model* $\mathfrak{H}'$ *where the universe and the valuation are the same as in the Henkin model, and where the transitions are subsets of those of the Henkin model s.t. the fundamental property still holds, i.e.*

$$\mathfrak{H}', \Theta \Vdash \phi \textit{ iff } \phi \in \Theta$$

□

Definition 3.3 *Let* K *be a class of models. Define*

$$\mathbf{Sub}(\mathsf{K}) := \{\mathfrak{S} \mid \exists \mathfrak{T} \in \mathsf{K}.\ \mathfrak{S} \subseteq \mathfrak{T}\}$$

where $\mathfrak{S} \subseteq \mathfrak{T}$ *means that* $\mathfrak{S}$ *is a generated submodel of* $\mathfrak{T}$*. We will write* $\mathbf{Sub}(\mathfrak{S})$ *instead of* $\mathbf{Sub}(\{\mathfrak{S}\})$*.* □

Definition 3.4 *If* K *is a class of models then*

$$\mathsf{K}/_{\approxeq} := \{\mathfrak{S} \mid \exists \mathfrak{T} \in \mathsf{K}.\ \mathfrak{S} \approxeq \mathfrak{T}\}$$

where $\mathfrak{S} \approxeq \mathfrak{T}$ *iff there is a total bisimulation between the two.* □

---

[2]An easy proof is the following: assume $\mathfrak{S}$ and $\mathfrak{T}$ are m-saturated. Then their disjoint union $\mathfrak{S} \uplus \mathfrak{T}$ is also m-saturated. By results of the previous section, $\mathfrak{S} \uplus \mathfrak{T}$ is Hennessy-Milner, so $\approx$ is a bisimulation on this model. Then $\approx$ must also be a bisimulation between $\mathfrak{S}$ and $\mathfrak{T}$.

[3]Personal communication.

It is easy to prove that both **Sub** and $(\_)/_{\approx}$ preserve the Hennessy-Milner property.

Definition 3.5 *For any model $\mathfrak{S}$ and for any element s in its universe, let*

$$Th(\mathfrak{S}, s) := \{\phi \in \mathcal{L} \mid \mathfrak{S}, s \Vdash \phi\}$$

This set is clearly maximally consistent. □

Theorem 3.6 (Visser) *If $\mathfrak{H}'$ is a Henkin-like model then* $\mathbf{Sub}(\mathfrak{H}')/_{\approx}$ *is a maximal Hennessy-Milner class.*

Proof.

- **$\mathbf{Sub}(\mathfrak{H}')/_{\approx}$ is Hennessy-Milner.**
  On $\mathfrak{H}'$, $\Gamma \approx \Delta$ iff $\Gamma = \Delta$ because of the above mentioned fundamental property. So $\approx$ is the identity and therefore a bisimulation. By the fact that **Sub** and $(\_)/_{\approx}$ preserve the Hennessy-Milner property, $\mathbf{Sub}(\mathfrak{H}')/_{\approx}$ is Hennessy-Milner.

- **$\mathbf{Sub}(\mathfrak{H}')/_{\approx}$ is a maximal Hennessy-Milner class.**
  Let $\mathfrak{S}$ be a model with universe S. Suppose $\mathfrak{S}$ is logically bisimilar to itself and to every model in $\mathbf{Sub}(\mathfrak{H}')/_{\approx}$. Then $\{Th(\mathfrak{S}, s) \mid s \in S\}$ is a generated subuniverse of $\mathfrak{H}'$. For suppose $Th(\mathfrak{S}, s)R_\alpha\Theta$ in $\mathfrak{H}'$. As $s \approx Th(\mathfrak{S}, s)$ (use the fundamental property in the definition of Henkin-like models) and $\approx$ is assumed to be a bisimulation between $\mathfrak{S}$ and $\mathfrak{H}'$ there must be some α-successor $s' \in S$ of s with $s' \approx \Theta$. But then $\Theta = Th(\mathfrak{S}, s')$ (again using the fundamental property). $\approx$ is clearly total between $\mathfrak{S}$ and the submodel associated with $\{\mathrm{Th}(\mathfrak{S}, s) \mid s \in S\}$. As we have assumed $\approx$ to be a bisimulation here, the two models are bisimilar and we have proved that $\mathfrak{S} \in \mathbf{Sub}(\mathfrak{H}')/_{\approx}$. □

Definition 3.7 *Let K be any class of models. Then $\mathfrak{H}(\mathsf{K})$ is the Henkin-like model with transitions defined as follows:*

$$\Gamma R_\alpha \Delta \ \text{ iff } \begin{cases} \Gamma \neq Th(\mathfrak{S}, s) \text{ for any } \mathfrak{S} \in \mathsf{K}, \text{ and } \Gamma R_\alpha \Delta \text{ in } \mathfrak{H} \\ \text{or} \\ \Gamma = Th(\mathfrak{S}, s) \text{ for some } \mathfrak{S} \in \mathsf{K} \text{ with universe } S \text{ and} \\ \text{there is a } t \in S \text{ s.t. } \Delta = Th(\mathfrak{S}, t) \text{ and } sR^{\mathfrak{S}}_\alpha t. \end{cases}$$

□

Theorem 3.8 (Visser) *For any Hennessy-Milner class K:*

$$\mathsf{K} \subseteq \mathbf{Sub}(\mathfrak{H}(\mathsf{K}))/_{\approx}$$

I.e. any Hennessy-Milner class can be extended to a maximal one.

Proof.
If $\mathfrak{S} \in \mathsf{K}$, then $\{Th(\mathfrak{S}, s) \mid s \in S\}$ (where S is again the universe of $\mathfrak{S}$) is a generated subuniverse of $\mathfrak{H}(\mathsf{K})$. $\mathfrak{S}$ turns out to be bisimilar to the submodel associated with this subuniverse, via the map $s \longmapsto Th(\mathfrak{S}, s)$.

For if $sR^{\mathfrak{S}}_\alpha t$ then $Th(\mathfrak{S}, s)R_\alpha\, Th(\mathfrak{S}, t)$ by definition. And if $Th(\mathfrak{S}, s)R_\alpha\, Th(\mathfrak{S}, t)$ then, since $\mathfrak{S} \in \mathsf{K}$, there is a model $\mathfrak{T} \in \mathsf{K}$ and $s', t' \in T$ (its universe) with $Th(\mathfrak{T}, s') = Th(\mathfrak{S}, s)$, $Th(\mathfrak{T}, t') = Th(\mathfrak{S}, t)$ and $s'R^{\mathfrak{T}}_\alpha t'$. Then $s \approx s'$. Hence, as K is Hennessy-Milner, there is a $u \in S$ s.t. $sR^{\mathfrak{S}}_\alpha u$ and $u \approx t'$. This is the desired successor of s, as $u \approx t'$ implies that $Th(\mathfrak{S}, u) = Th(\mathfrak{T}, t') = Th(\mathfrak{S}, t)$. Since our map is clearly surjective, we have proved that it is a total bisimulation between $\mathfrak{S}$ and the model associated with $\{Th(\mathfrak{S}, s) \mid s \in S\}$. Thus $\mathfrak{S} \in \mathbf{Sub}(\mathfrak{H}(\mathsf{K}))/_{\approx}$. □

The above theorems show that maximal Hennessy-Milner classes are precisely those of the form $\mathbf{Sub}(\mathfrak{H}')/_{\approxeq}$ for some Henkin-like model $\mathfrak{H}'$. The class of m-saturated models, M-SAT, turns out to be a very special maximal Hennessy-Milner class.

Proposition 3.9 M-SAT $= \mathbf{Sub}(\mathfrak{H})/_{\approxeq}$, *hence* M-SAT *is maximal.*

Proof.
First let us show that $\mathfrak{H}$ is m-saturated. Suppose Φ is a set of formulas finitely satisfiable in the α-successors of some element Θ of $\mathfrak{H}$. Then $\Phi \cup \{\phi \mid [\alpha]\phi \in \Theta\}$ is a consistent set, hence can be extended to a maximal consistent set Δ, which will be the desired α-successor of Θ in $\mathfrak{H}$ satisfying Φ.

Furthermore, as M-SAT is closed under generated submodels and under bisimulation, we may conclude that $\mathbf{Sub}(\mathfrak{H})/_{\approxeq} \subseteq$ M-SAT. But $\mathbf{Sub}(\mathfrak{H})/_{\approxeq}$ is a maximal Hennessy-Milner class and M-SAT is Hennessy-Milner. So M-SAT $= \mathbf{Sub}(\mathfrak{H})/_{\approxeq}$. □

This provides us with a first concrete example of a maximal Hennessy-Milner class. The task of the next subsection will be to give uncountably many such examples.

3.1 Uncountably many maximal Hennessy-Milner classes

This subsection will show that there are more than enough maximal Hennessy-Milner classes. In more mathematical terms: uncountably many. To show this we will construct a set (of cardinality $2^{\aleph_0}$) of concrete Hennessy-Milner models which are pairwise logically nonbisimilar. Each subset of $\mathbb{N}$ will be represented by a model in our construction, ensuring the large cardinality.

We first define models that will appear as parts of the ultimate models: see figures 4 and 5. The reader should notice that $[n]$ has branches of all lengths except $n+2$ from the root $[n]$ to some terminal point (the labels at the terminal points indicate these lengths). $[n,i]$ is similar, except it has no such branch larger than $n+i+3$, hence it is a finite model. The representing model for some set $S \subseteq \mathbb{N}$ is $\mathfrak{K}_S$ (see figure 6).

Proposition 3.10 $\mathfrak{K}_S$ *is Hennessy-Milner.*

Proof.
We have to prove that $\approx$ is a bisimulation on $\mathfrak{K}_S$. So consider two different points s and t in the model such that $s \approx t$ (equal points are trivial). There are three cases to consider:

1. **Either s or t generates an image-finite model.** Use proposition 3.13, which states that image-finite models are logically bisimilar to any other model.

2. **$s = [n]$ and $t = [m]$, with $n, m \in S$.** As we assume that $s \neq t$ and hence $n \neq m$ we know that there will be a branch of length $m+2$ starting in $[n]$ and ending in some terminal node. We cannot find such a branch emerging from $[m]$, by definition of the model. We can express this in the modal language: $[n] \Vdash \Diamond(\Box^{m+2}\bot \wedge \Diamond^{m+1}\top)$ while $[m]$ does not validate this formula. Thus $[n] \not\approx [m]$, contradicting our assumption. So this case cannot occur.

3. **$s = [n]$ and $t = \omega_S$.** This can also not be the case, as $[n] \Vdash \Diamond\Box\bot$ (via its leftmost branch) even though this is not true for ω_S. □

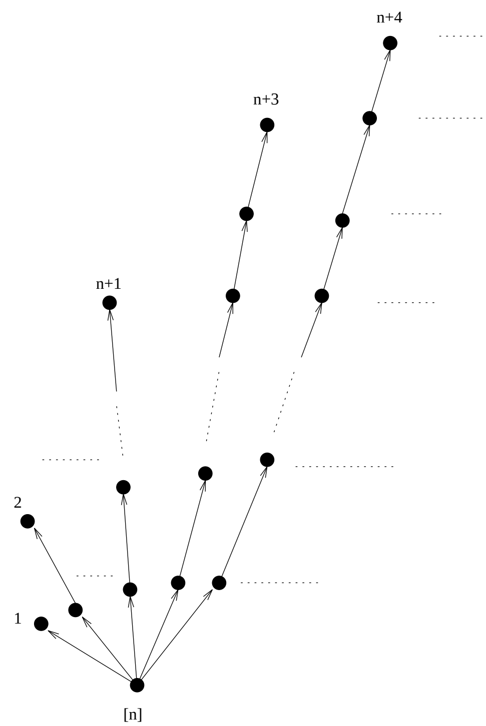

Figure 4: $[n]$, $n \in \mathbb{N}$

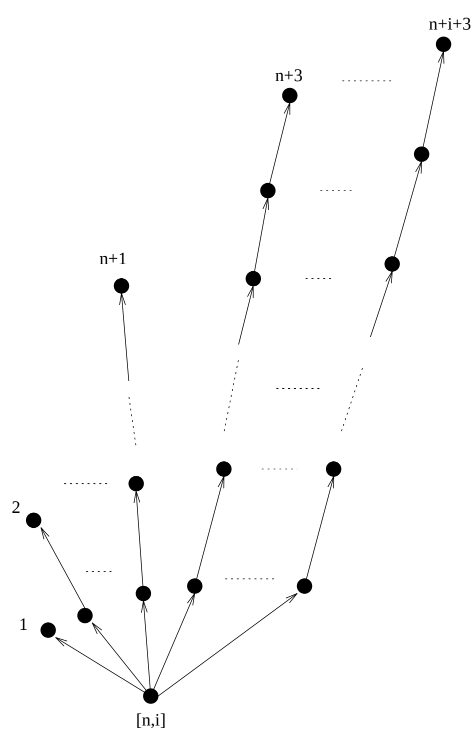

Figure 5: $[n, i]$, $n, i \in \mathbb{N}$

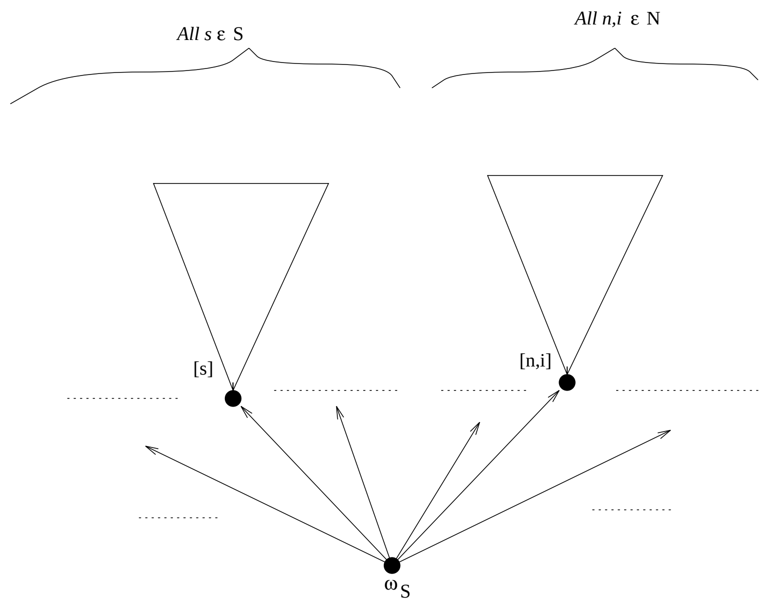

Figure 6: $\mathfrak{K}_S$: the model representing $S \subseteq \mathbb{N}$.

Proposition 3.11 *For all $S, T \subseteq \mathbb{N}$, $\omega_S \approx \omega_T$.*

Proof.
Essentially this is because up to any finite depth (as seen from the roots) ω_S and ω_T are bisimilar. □

Theorem 3.12 *If $S \neq T$ then $\mathfrak{K}_S$ is not logically bisimilar to $\mathfrak{K}_T$.*

Proof.
Without loss of generality, we may assume that there is some $s \in S$ that is not an element of T. So we have the following situation: $\omega_T \approx \omega_S R[s]$ (by the previous proposition). If $\mathfrak{K}_S$ and $\mathfrak{K}_T$ were logically bisimilar then there should be some point t in the latter model s.t. $\omega_T Rt \approx [s]$. By the proof of proposition 3.10, we know that the only point in $\mathfrak{K}_T$ that would satisfy this condition is $[s]$. But $[s]$ is not a part of $\mathfrak{K}_T$, as $s \notin T$. So $\approx$ is not a bisimulation between these two models. □

To get our set of maximal Hennessy-Milner classes, simply extend each model $\mathfrak{K}_S$ to such a class, call this K_S. This is possible, by theorem 3.8. If $S \neq T$, then $\mathsf{K}_S \neq \mathsf{K}_T$, for otherwise both $\mathfrak{K}_S$ and $\mathfrak{K}_T$ would be in K_S, implying the modal bisimilarity of the two.

3.2 The intersection:image-finite models

Now that we have discovered that there are many different maximal Hennessy-Milner classes, let us try to pinpoint the intersection of all maximal Hennessy-Milner classes. Let us call this intersection Int. For this enterprise we must find the maximal class of Hennessy-Milner models s.t. every model in this class is logically bisimilar to any other Hennessy-Milner model. For suppose a Hennessy-Milner model $\mathfrak{S}$ is logically bisimilar to all Hennessy-Milner models and suppose K is any maximal Hennessy-Milner class. $\mathsf{K} \cup \{\mathfrak{S}\}$ will then also be Hennessy-Milner and since K is maximal, $\mathfrak{S} \in \mathsf{K}$. So $\mathfrak{S}$ would be an element of Int. For the other direction, suppose

$\mathfrak{S} \in \mathsf{Int}$ and let $\mathfrak{T}$ be any Hennessy-Milner model. By theorem 3.8 we can find a maximal Hennessy-Milner class K containing $\mathfrak{T}$. But K must then also contain $\mathfrak{S}$, so $\mathfrak{S}$ must be logically bisimilar to $\mathfrak{T}$.

Thus if a class K is Hennessy-Milner then $\mathsf{K} \cup \mathsf{Int}$ will remain so. Int will turn out to be exactly the image-finite models, modulo bisimulation.

Proposition 3.13 *Every image-finite model is logically bisimilar to any other model. Therefore* Int *contains all models totally bisimilar to image-finite models.*

Proof.
Consider an image-finite model $\mathfrak{S}$ and another model $\mathfrak{T}$ (with respective universes S and T), about which we may not assume anything. We want to prove that $\approx$ is a partial bisimulation between these two models. So consider two points $s \in S$ and $t \in T$ s.t. $s \approx t$. We check the bisimulation clauses for the transition-relation R_α. By image-finiteness of $\mathfrak{S}$ we can list the α-successors of s as $s_1, s_2, \ldots, s_n$. There are two cases to consider:

1. Suppose $sR_\alpha s_i$. We need to find some $t' \approx s_i$ in $\mathfrak{T}$ s.t. $tR_\alpha t'$.

   For every $j, k \in I = \{1, \ldots, n\}$ s.t. $s_j \not\approx s_k$, choose a modal formula $\phi_{(j,k)}$ s.t. $s_j \Vdash \phi_{(j,k)}$ while $s_k \nVdash \phi_{(j,k)}$. Define $\phi_j = \bigwedge\{\phi_{(j,k)} \mid k \in I, s_j \not\approx s_k\}$. Now $s_j \Vdash \phi_j$, but if $s_j \not\approx s_k$ then $s_k \nVdash \phi_{(j,k)}$, hence $s_k \nVdash \phi_j$.

   So $t \approx s \Vdash \langle\alpha\rangle\phi_i$. There must then be a t' s.t. $t' \Vdash \phi_i$ and $tR_\alpha t'$. We will show that $s_i \approx t'$ as required. Suppose $t' \Vdash \psi$. Then $s \approx t \Vdash \langle\alpha\rangle(\phi_i \wedge \psi)$, which means that for some s_j, $s_j \Vdash \phi_i \wedge \psi$. By the construction of ϕ_i, s_i must be modally equivalent to s_j. Thus $s_i \Vdash \psi$ and we have proved that $s_i \approx t'$.

2. Suppose $tR_\alpha t'$. Use the definition of ϕ_i as above. Clearly $s \Vdash [\alpha](\phi_1 \vee \ldots \vee \phi_n)$. So $t' \Vdash \phi_i$ for some $i \in I$. By the same reasoning as above we conclude: $s_i \approx t'$.

□

Theorem 3.14 *If* $\mathfrak{S} \in \mathsf{Int}$ *then* $\mathfrak{S}$ *is bisimilar to an image-finite model.*

Proof.
Suppose the theorem is false. This gives us a $\mathfrak{S} \in \mathsf{Int}$ which is not bisimilar to any image-finite model. If $\mathfrak{S}$ is in Int it is Hennessy-Milner, so $\approx$ will be a bisimulation on it. Dividing out this bisimulation gives us a $\mathfrak{T} = (T, \{R_\alpha\}_{\alpha \in \mathcal{A}}, V)$ totally bisimilar to $\mathfrak{S}$ on which $\approx$ is just the identity. By assumption, $\mathfrak{T}$ is not image finite. Thus there is a $\perp \in T$ and a $\beta \in \mathcal{A}$ s.t. the set of β-successors of $\perp$ is an infinite set.

Suppose there is a β-successor t of $\perp$ s.t. for every formula ϕ true at t there is another β-successor of $\perp$ also forcing ϕ. Then we may remove the transition $\perp R_\beta t$ from $\mathfrak{T}$ without changing truth at any point.

To show this, define the model $\mathfrak{T}'$ as $(T, \{R'_\alpha\}_{\alpha \in \mathcal{A}}, V)$, where $R'_\alpha = R_\alpha$ if $\alpha \neq \beta$ and $R'_\beta = R_\beta - \{\langle \perp, t\rangle\}$. We can show $\mathfrak{T}, x \Vdash \phi$ iff $\mathfrak{T}', x \Vdash \phi$ for all $x \in T$ and all formulas ϕ, by induction on ϕ. We will demonstrate the case that $\phi = \langle\alpha\rangle\psi$. If $\mathfrak{T}, x \Vdash \langle\alpha\rangle\psi$ then there is some α-successor y of x in $\mathfrak{T}$ with $\mathfrak{T}, y \Vdash \psi$. When $\alpha \neq \beta$, $x \neq \perp$ or $y \neq t$ the transition $xR_\alpha y$ also exists in $\mathfrak{T}'$ and we can just use the induction hypothesis to show $\mathfrak{T}', x \Vdash \langle\alpha\rangle\psi$. So suppose $\alpha = \beta$, $x = \perp$ and $y = t$. We have assumed that there is another β-successor $z \neq t$ of $\perp$ satisfying ψ. So we can apply the proof of the first case again. The other direction is trivial, as all transitions in $\mathfrak{T}'$ exist in $\mathfrak{T}$.

Now if $\mathfrak{T}', x \approx \mathfrak{T}', y$ then $\mathfrak{T}, x \approx \mathfrak{T}, y$, because $\mathfrak{T}, x \approx \mathfrak{T}', x$ and $\mathfrak{T}, y \approx \mathfrak{T}', y$ by the above proof. Thus $x = y$ and $\approx$ is the identity on $\mathfrak{T}'$. So $\mathfrak{T}'$ is Hennessy-Milner. $\mathfrak{T} \in \mathsf{Int}$, so $\mathfrak{T}$ must be logically bisimilar to $\mathfrak{T}'$. Using $\perp R_\beta t$ and $\mathfrak{T}, \perp \approx \mathfrak{T}', \perp$, we may deduce that there is an $x \in T$ with $\bot R'_\beta x$ (hence $x \neq t$) s.t. $\mathfrak{T}, t \approx \mathfrak{T}', x$ (implying that $\mathfrak{T}, t \approx \mathfrak{T}, x$). But $\approx$ is the identity on $\mathfrak{T}$, so we have derived a contradiction.

Therefore every β-successor t of $\bot$ in $\mathfrak{T}$ must force a modal formula ϕ_t that is satisfied in no other β-successor of $\bot$. Define $\Phi^\neg := \{\neg\phi_t \mid \bot R_\beta t\}$. This set is finitely satisfiable in the β-successors of $\bot$. For if $\Delta \subseteq \Phi^\neg$ is a finite set $\{\neg\phi_{t_1}, \ldots, \neg\phi_{t_n}\}$, then $t_1, \ldots, t_n$ are the only β-successors of $\bot$ *not* satisfying Δ. As there are assumed to be infinitely many β-successors of $\bot$, we must be able to find one not in $\{t_1, \ldots, t_n\}$. This point will then satisfy Δ. Yet $\Phi^\neg$ is not satisfied as a whole in $\{t \in T \mid \bot R_\beta t\}$, because if $\bot R_\beta t$ then $t \Vdash \phi_t$. So $\mathfrak{T}$ is not m-saturated. But the class of m-saturated models is a maximal Hennessy-Milner class, so $\mathfrak{T} \notin \mathsf{Int}$ and hence $\mathfrak{S} \notin \mathsf{Int}$, which is in contradiction with our original assumption. □

3.3 Example: a one-step generator

There is another way of describing the results of the previous subsection. Let G be a class of Hennessy-Milner models, pairwise logically nonbisimilar. Let us call such G a *one-step generator* if for all Hennessy-Milner models $\mathfrak{S}$ there is a $\mathfrak{T} \in \mathsf{K}$ with $\mathfrak{S} \approx \mathfrak{T}$. So if G is a one-step generator, and H is the class of Hennessy-Milner models, then:

$$\mathsf{H} = \{\mathfrak{S} \in \mathsf{H} \mid \exists \mathfrak{T} \in \mathsf{G}.\, \mathfrak{S} \approx \mathfrak{T}\}$$

Clearly $\emptyset$ is not a one-step generator. The results of the previous subsection prove that the singleton one-step generators are precisely those of the form $\{\mathfrak{S}\}$ for $\mathfrak{S}$ a finitely branching model. This section will give an example of a one-step generator with *two* elements.

The two models we will examine here are discussed also in [6]. We will repeat their definition here.

$$\mathfrak{S}_4 = (\omega + 1, >)$$

$$\mathfrak{S}_5 = (\omega + 1, > \cup \{\langle\omega, \omega\rangle\})$$

For reference, let us call the root ω in $\mathfrak{S}_4$: ω_0, while that in $\mathfrak{S}_5$: ω_1.

Proposition 3.15 $\mathfrak{S}_4 \not\approx \mathfrak{S}_5$.

Proof.
First we prove that $\omega_0 \approx \omega_1$. As ω_1 has an infinite branch, while ω_0 does not, it follows that $\mathfrak{S}_4$ and $\mathfrak{S}_5$ cannot be logically bisimilar.

We prove $\omega_0 \approx \omega_1$ by induction on formulas. The only interesting case is of course the diamond-case. So suppose $\omega_0 \Vdash \Diamond\phi$. Then $n \Vdash \phi$ for some natural number n. The points labelled with natural numbers generate the same submodels in $\mathfrak{S}_4$ and $\mathfrak{S}_5$, so we may conclude $\omega_1 \Vdash \Diamond\phi$.

Now suppose $\omega_1 \Vdash \Diamond\phi$. There are two cases. If $n \Vdash \phi$ for some $n \in \mathbb{N}$, then clearly $\omega_0 \Vdash \Diamond\phi$. If $\omega_1 \Vdash \phi$ then, by the induction hypothesis, $\omega_0 \Vdash \phi$. At this point we may use lemma 7 of [6] again (see page 5) to show that ϕ is forced at some $n \in \mathbb{N}$, so we may apply the reasoning as above. □

To prove the main theorem of this section (Theorem 3.19) we first need some further definitions and propositions.

Definition 3.16 *Let us call a point s in a model $\mathfrak{S}$* **branch-saturated** *if whenever s has branches emerging from it of all finite lengths (i.e. $s \Vdash \{\Diamond^n\top \mid n \in \mathbb{N}\}$), then it also starts an infinite branch $sRs_1Rs_2R\ldots$. We call a model branch-saturated, if every point in it is branch-saturated.* □

Proposition 3.17 *If $\mathfrak{S}$ is branch-saturated then $\mathfrak{S} \approx \mathfrak{S}_5$.*

Proof.
We check the bisimulation clauses. The cases shown prove something a little more general than what is necessary for the proposition, but we will need these general statements later. We use n to denote points not equal to ω_1 in $\mathfrak{S}_5$.

1. **If s is branch-saturated and $s \approx \omega_1$ then there is some t s.t. sRt and $t \approx \omega_1$.**
   As $s \approx \omega_1 \Vdash \Diamond^n \top$ for any n, we know that s has branches of any finite depth. By branch-saturation, we may conclude that it also has an infinite branch $s = s_0 R s_1 R s_2 \ldots$. Suppose $s_1 \not\approx \omega_1$. Then there must be a ϕ s.t. $s_1 \Vdash \phi$ while $\omega_1 \not\Vdash \phi$. As $\omega_1 \approx s \Vdash \Diamond\phi$ we know that there is an n in $\mathfrak{S}_5$ with $n \Vdash \phi$. By lemma 7 of [6] mentioned above, together with the proof of proposition 3.15, the set of points where ϕ holds is finite, as $\omega_1 \notin V(\phi)$. Therefore we can even find the *maximum* n s.t. $n \Vdash \phi$. Thus $s \approx \omega_1 \Vdash \Box(\phi \rightarrow \Box^{n+1}\bot)$. So $s_1 \Vdash \Box^{n+1}\bot$, which contradicts the fact that s_1 starts an infinite branch. We conclude $s_1 \approx \omega_1$.

2. **If $s \approx x \in S_5$ and xRn then there is a t s.t. sRt and $t \approx n$.**
   n is the only point in $\mathfrak{S}_5$ where $\Diamond^n\top \wedge \Box^{n+1}\bot$ holds. Therefore $s \approx x \Vdash \Diamond(\Diamond^n\top \wedge \Box^{n+1}\bot)$ which means that there is some t with sRt and $t \Vdash \Diamond^n\top \wedge \Box^{n+1}\bot$. Suppose $t \Vdash \phi$. Then $x \approx s \Vdash \Diamond(\phi \wedge \Diamond^n\top \wedge \Box^{n+1}\bot)$. As n is the only point where $\Diamond^n\top \wedge \Box^{n+1}\bot$ holds, n must also satisfy ϕ. We may conclude that $t \approx n$.

3. **If $\omega_1 \approx sRt$ and t starts an infinite branch then $t \approx \omega_1$.**
   See the proof of case 1.

4. **If $s \approx x \in S_5$, sRt and t does not have branches of all finite lengths then there exists an n s.t. xRn and $t \approx n$.**
   Saying that t does not have branches of all finite lengths is the same as saying that $t \Vdash \Box^{n+1}\bot$ for some n. Find the *smallest* such n. Then $t \Vdash \Diamond^n\top$ so $x \Vdash \Diamond(\Diamond^n\top \wedge \Box^{n+1}\bot)$. As n is the only point in $\mathfrak{S}_5$ where $\Diamond^n\top \wedge \Box^{n+1}\bot$ holds, xRn. To prove $t \approx n$ see case 2.

To show that for any s in $\mathfrak{S}$ with $s \approx xR^{\mathfrak{S}_5}y$ there is a t s.t. $sR^{\mathfrak{S}}t$ and $t \approx y$, use the cases 1 and 2. Because in a branch-saturated model a point either starts an infinite branch or has finite depth, cases 3 and 4 prove the other bisimulation clause. $\Box$

We now prove a counterpart of the above proposition for $\mathfrak{S}_4$.

Proposition 3.18 *Let $\mathfrak{S}$ be a model with universe S s.t.*

$$\mathfrak{S}, s \Vdash \{\Diamond^n\top \mid n \in \mathbb{N}\}, sRt \Longrightarrow \mathfrak{S}, t \not\Vdash \{\Diamond^n\top \mid n \in \mathbb{N}\}$$

Then $\mathfrak{S} \approx \mathfrak{S}_4$.

Proof.
The statement follows from the following three cases. m, n are used to denote elements of $\mathfrak{S}_4$ not equal to ω_0.

1. **If $s \approx x$ with x in $\mathfrak{S}_4$ and $x > n$ then there is a t with sRt and $t \approx n$.**
   Because of proposition 3.15 this is just case 2 from the proof of the previous proposition.

2. **If $s \approx \omega_0$ with s satisfying the condition of the proposition and sRt then there is an n s.t. $t \approx n$.**
   Because the premiss implies that t does not branches of all finite lengths, we may use case 4 of the previous proposition.

3. **If $s \approx n$ and sRt then there is an $m \approx t$ with $n > m$.**
   Because the model generated by n is finite we may use proposition 3.13. □

Theorem 3.19 *If $\mathfrak{S}_4 \not\approx \mathfrak{T} \approx \mathfrak{U} \not\approx \mathfrak{S}_5$ then $\mathfrak{T}$ is not Hennessy-Milner.*

Proof.
Suppose $\mathfrak{T}$ *is* Hennessy-Milner: we derive a contradiction.

As $\mathfrak{S}_4 \not\approx \mathfrak{T}$ there are points s in $\mathfrak{S}_4$ and t in $\mathfrak{T}$ with $s \approx t$ that do not satisfy the bisimulation conditions. As n can only reach finitely many points, we must assume that $s = \omega_0$, otherwise the bisimulation conditions would be satisfied (with proposition 3.13). There are two possibilities:

1. $\omega_0 Rn$ while there is no $t' \approx n$ with tRt'. This is impossible by proposition 3.18, case 1.

2. There remains just one possibility: there is a t' s.t. tRt' while for no n: $n \approx t'$.

By proposition 3.18, case 2, we know that t' must have branches of all finite lengths. Furthermore, t' is modally equivalent to ω_0 and therefore to t. For assume $\omega_0 \Vdash \phi$. Then $\neg\phi$ only holds in finitely many places in $\mathfrak{S}_4$. So $t \approx \omega_0 \Vdash \Box(\neg\phi \to \Box^n \bot)$ for some $n \in \mathbb{N}$. As t' has branches of any lenghth, we must conclude that $t' \Vdash \phi$.

We assumed that $\mathfrak{T}$ is Hennessy-Milner. Thus $t \approx t'$ and tRt' gives us a t'' s.t. $t' \approx t''$ and $t'Rt''$. Repeating this argument gives us an infinite branch $tRt'Rt''R\ldots$.

From $\mathfrak{U} \not\approx \mathfrak{S}_5$ we can again conclude the existence of a point $u \approx \omega_1$ in $\mathfrak{U}$ satisfying one of the following:

1. uRu' while there is no point $s \approx u'$ with $\omega_1 Rs$. Then $\omega_1 \not\approx u'$. This means that there must be a ϕ with $\omega_1 \Vdash \phi$ while $u' \not\Vdash \phi$. So there are only finitely many points in $\mathfrak{S}_5$ which validate $\neg\phi$, say $\{n_1, \ldots, n_k\}$. Let $\psi_n := \Diamond^n \top \wedge \Box^{n+1}\bot$. Then ψ_n is only true at the point n in $\mathfrak{S}_4$. Now
   $$u \approx \omega_1 \Vdash \Box(\neg\phi \to (\psi_{n_1} \vee \ldots \vee \psi_{n_k}))$$
   So $u' \Vdash \psi_{n_1} \vee \ldots \vee \psi_{n_k}$, say $u' \Vdash \psi_{n_i}$. Now if $u' \Vdash \chi$ then $\omega_1 \approx u \Vdash \Diamond(\chi \wedge \psi_{n_i})$. Thus $n_i \Vdash \chi$, as n_i is the only point validating ψ_{n_i}. We conclude that $n_i \approx u'$, which contradicts our assumption.

2. The only viable option then seems to be that for some $s \in S_5$ there is no point u' with uRu' and $u' \approx s$. If $s \in \mathbb{N}$ then s is the unique point in $\mathfrak{S}_5$ validating ψ_s (as above). But then u will have a successor also forcing ψ_s: thus, by reasoning we have encountered before, this successor will be modally equivalent to s. Thus s must be ω_1. As ω_1 is a reflexive point this would contradict the logical bisimilarity of $\mathfrak{U}$ and $\mathfrak{S}_5$, as required. By case 1 of proposition 3.17 we may conclude that u is not branch-saturated and hence does not have an infinite branch.

We finally reach our contradiction: as $t \approx \omega_0 \approx \omega_1 \approx u$ and $\mathfrak{T} \approx \mathfrak{U}$ it cannot be the case that t starts an infinite α-branch while u does not. □.

The following corollary easily follows from theorem 3.19 and in combination with proposition 3.15 proves that $\{\mathfrak{S}_4, \mathfrak{S}_5\}$ is a one-step generator.

Corollary 3.20 *If $\mathfrak{T}$ is Hennessy-Milner then either $\mathfrak{S}_4 \approx \mathfrak{T}$ or $\mathfrak{S}_5 \approx \mathfrak{T}$.* □

4 Process algebra

Process algebra is the name given to a wide range of algebras each of which has as its objects processes, abstractions of computer programs. It has both practical and theoretical applications. It provides a tool with which to verify specifications of programs, but it can also provide a semantics for parallel computation. See Baeten and Weijland [1] for an introduction.

The standard semantics of process algebra has as its elements *process graphs*, which can easily be interpreted as Kripke models. Furthermore, the standard semantics has bisimulation as its notion of equality, making process algebra susceptible to modal-logical analysis. A question arises: is this standard semantics a Hennessy-Milner class? This question is particularly potent in the setting of process algebra, for if the graph-semantics would be Hennessy-Milner, nonequality of processes would then give us a modal formula distinguishing between the two. This modal formula would be a kind of *trace*, explaining where things go wrong, i.e. where the two processes diverge. We will examine a particular process algebra language, one rich enough to let the standard semantics of this language be a non-Hennessy-Milner class. A remedy will be suggested, making heavy use particularly of our insights into m-saturation.

4.1 The standard model

Process algebra languages are just like any other algebraic languages. They consist of terms constructed from function-symbols and variables. The only formulas are equalities between terms. Consider the process language, whose terms are constructed from the following ingredients:

variables: $x_0, x_1, x_2, \ldots$
constants: δ (deadlock), ε (success), $a_0, a_1, a_2, \ldots$ (basic programs)
operations:

$+$ (binary, nondeterministic choice)

$\cdot$ (binary, sequential composition)

$*$ (unary, iteration)

$\sum_{n\in\mathbb{N}}$ (ω-ary,infinite choice)

This language is infinitary: with $\sum_{n\in\mathbb{N}}$ we may construct infinite terms. After each constant and operation we have added its intended interpretation in terms of processes. In addition, for each operation we state its arity. The binary $+$ and $\cdot$ are written as infix-operators, we write $*$ as a postfix-operator while if $(t_n)_{n\in\mathbb{N}}$ is a sequence of terms then $\sum_{n\in\mathbb{N}} t_n$ is another term, which can be thought of as $t_0 + t_1 + t_2 + \ldots$. So our language consists of the regular operations plus infinite choice.

The standard model has as objects bisimulation-classes of labelled directed graphs, i.e. equivalence classes of such graphs under the bisimulation-equivalence relation. These graphs are to be seen as processes. Vertices are then computation states, say a description of the data at that point of the computation, while edges are nondetermistic operations on these states. As processes, they have a unique starting vertex, the state at which the computation starts, but any amount of success vertices, states where the computation halts and maybe gives some kind of output. As for the notion of bisimulation, it is the obvious one, with the added demand that the bisimulation relates the starting vertices, and that a success vertex can only be bisimilar to another success vertex. Let us give an example. Figure 7

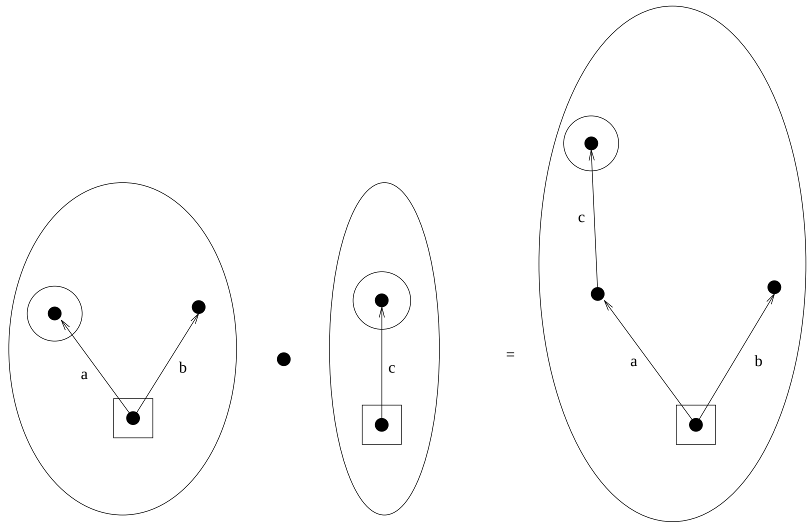

Figure 7: Example of sequential composition.

shows what the sequential composition operation does on two particular processes. The picture should be interpreted as follows: an encircled state is a success state, while the unique state in the square is the starting vertex. The leftmost process must choose between two actions, an a-action or a b-action. After the a-action a success state is reached, while the b-action results in *deadlock*: it cannot execute any more actions but it can also not terminate as it is not in a success state. Next to this process is the basic process c. The final process is the result of sequentially composing the two previous processes.

Note that these process graphs are really nothing other than rooted Kripke models with a binary relation R_{a_i} for each edge-label a_i (so $\mathcal{A} = \{a_0, a_1, a_2, \ldots\}$). The language of these Kripke models has just a single propositional variable $\surd$, which in a model is interpreted as the set of success states. So this is the connection between process algebra and modal logic: the objects of the standard semantics of process algebra are bisimulation-classes of Kripke models and its operations are operations on (bisimulation-classes of) Kripe models. Therefore process algebra can be seen as an *external* language over Kripke models: its sentences express bisimulation between Kripke models. Modal logic has an *internal* language: it talks of truth at a given point inside a Kripke model.

We need to say a little about what we mean by rooted models. Given an ordinary Kripke model $\mathfrak{S}$, and a point s in its universe S, $(\mathfrak{S}, s)$ is a rooted Kripke model, with s as its root. Note that this does not entail that every point in S is reachable from s. We could have chosen to demand precisely this of rooted models but in order to facilitate the definitions of operations on rooted models, we simply ignore all points not reachable from the root. Two rooted models $(\mathfrak{S}, s)$ and $\mathfrak{T}, t)$ are called bisimilar if there is a bisimulation between them that connects the roots. This entails that $\mathfrak{S}_s$ (the submodel of $\mathfrak{S}$ generated by s) is bisimilar to $\mathfrak{T}_t$. All operations on rooted Kripke models we will define will be invariant under this rooted version of bisimulation so that they may also be viewed as operations on bisimulation-classes of models.

Let us define the process algebra operations on rooted Kripke models. Because there is just a single proposition letter in our language, we may as well write a model $(S, \{R_a\}_{a \in \mathcal{A}}, V, s)$ as $(S, \{R_a\}_{a \in \mathcal{A}}, \surd_S, s)$, where $\surd_S = V(\surd)$. Let

$(\mathfrak{S}_0, s_0), (\mathfrak{S}_1, s_1), (\mathfrak{S}_2, s_2), \ldots$ be a sequence of models, where

$$\mathfrak{S}_i = (S_i, \{R_{(i,a)}\}_{a \in \mathcal{A}}, \surd_{S_i})$$

We assume all these models to have disjoint universes. Of course, if we have a sequence of models which are not disjoint, the operations are the same, except we first *make* the universes disjoint in the standard way.

- $(\mathfrak{S}_0, s_0) + (\mathfrak{S}_1, s_1)$ is defined as follows:

  universe: $S_0 \cup S_1 \cup \{\bot\}$, where $\bot$ does not occur in the S_i.

  transitions: Define, for each $a \in \mathcal{A}$:

  $$R_a := R_{(0,a)} \cup R_{(1,a)} \cup \{\langle \bot, x \rangle \mid s_0 R_{(0,a)} x \vee s_1 R_{(1,a)} x\}$$

  success states: $\surd_{S_0} \cup \surd_{S_1} \cup \{\bot \mid s_0 \in \surd_{S_0} \vee s_1 \in \surd_{S_1}\}$

  root: $\bot$.

- $(\mathfrak{S}_0, s_0) \cdot (\mathfrak{S}_1, s_1)$ is defined thus:

  universe: $S_0 \cup S_1$.

  transitions: Define, for each $a \in \mathcal{A}$:

  $$R_a := R_{(0,a)} \cup R_{(1,a)} \cup (\surd_{S_0} \times \{x \in S_1 \mid s_1 R_{(1,a)} x\})$$

  success states: $\surd_{S_1} \cup \{s \in \surd_{S_0} \mid s_1 \in \surd_{S_1}\}$.

  root: s_0.

- $(\mathfrak{S}_0, s_0)^*$ iterates $(\mathfrak{S}_0, s_0)$ a finite number of times before succeeding.

  universe: S_0.

  transitions: For each $a \in \mathcal{A}$:

  $$R_a := R_{(0,a)} \cup (\surd_{S_0} \times \{x \in S_0 \mid s_0 R_{(0,a)} x\})$$

  success states: $\{s_0\} \cup \surd_{S_0}$.

  root: s_0.

- $\sum_{n \in \mathbb{N}} (\mathfrak{S}_n, s_n)$ is just the infinite version of $+$.

  universe: $\bigcup_{n \in \mathbb{N}} S_n \cup \{\bot\}$, where $\bot$ is again disjoint from the S_i.

  transitions: For each $a \in \mathcal{A}$, define:

  $$R_a := \bigcup_{n \in \mathbb{N}} (R_{(n,a)} \cup \{\langle \bot, x \rangle \mid s_n R_{(n,a)} x\})$$

  success states: $\bigcup_{n \in \mathbb{N}} \surd_{S_n} \cup \{\bot \mid \exists n \in \mathbb{N}. s_n \in \surd_{S_n}\}$

  root $\bot$.

- δ is a process in deadlock:

  $$\delta := (\{\bullet\}, \{R_a\}_{a \in \mathcal{A}}, \emptyset, \bullet)$$

  where $R_a = \emptyset$ for each a.

- ε can only succeed: it is the same as δ except that the set of success states is $\{\bullet\}$.

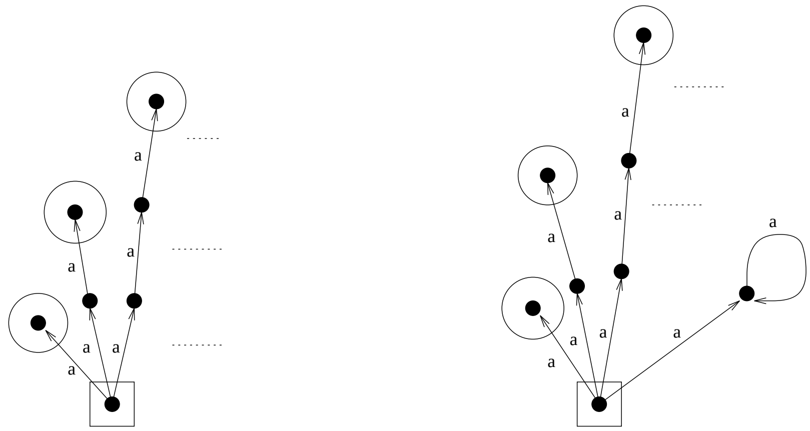

Figure 8: $\sum_{n\in\mathbb{N}} a^{n+1}$ and $(\sum_{n\in\mathbb{N}} a^{n+1}) + (a^* \cdot \delta)$.

- Atomic processes: $a_i := (\{0,1\}, \{R_a\}_{a\in\mathcal{A}}, \{1\}, 0)$, where $R_a = \{\langle 0,1\rangle\}$ if $a = a_i$, otherwise it is empty.

The reader should notice that e.g. + as in the definition of process algebra terms and + in the definition directly above are two different entities: the latter is not a symbol of our language but an operation on rooted Kripke models. As an example of these operations, consider again figure 7, which can now be seen to state that $[a + (b \cdot \delta)] \cdot c = (a \cdot c) + (b \cdot \delta)$ (all points not reachable from the root are ignored and therefore not shown in the figure).

A question we may ask ourselves is: is this standard graph-semantics of process algebra a Hennessy-Milner class? If we take two bisimulation-classes from this algebra and one Kripke model from each, is $\approx$ then a bisimulation between them? We don't require that $\approx$ is a rooted bisimulation, just that it is an ordinary bisimulation on the points reachable from the roots.

The answer must of course be *no*, because the standard algebra as we defined it is the class of all rooted models. But even if we restrict ourselves to interpretations of closed terms, we don't get a Hennessy-Milner class. For consider the following two terms: $\sum_{n\in\mathbb{N}} a^{n+1}$ and $(\sum_{n\in\mathbb{N}} a^{n+1}) + (a^* \cdot \delta)$, where $a^{n+1} = a \cdot \ldots \cdot a$ $(n+1$ times). The interpretations of these terms are respectively the left and the right models of figure 8. The two roots satisfy the same formulas, because up to finite depth they are bisimilar, yet they are not bisimilar, as the second has an infinite branch while the first does not.

The problem we address in the next section is to find a reasonable graph-semantics of process algebra that *does* enjoy the Hennessy-Milner property. This graph-semantics will consist of all m-saturated models, which we know to be a Hennessy-Milner class.

4.2 The m-saturated models as a process algebra

When we say that a rooted model is m-saturated we mean that relativized to the root: we don't need to check the m-saturation condition for points not reachable from the root. From proposition 3.9 we can construct an operation on rooted models that always returns an m-saturated model:

Definition 4.1 *Let for any rooted model $(\mathfrak{S}, s)$, $\mathfrak{H}(\mathfrak{S}, s) := (\mathfrak{H}_s, Th(\mathfrak{S}, s))$, where $\mathfrak{H}_s$ is the submodel of $\mathfrak{H}$ (the Henkin model) generated by $Th(\mathfrak{S}, s)$.* □

Because $\mathfrak{H}$ is m-saturated, any generated submodel of it is also m-saturated. Therefore for any $(\mathfrak{S}, s)$, $\mathfrak{H}(\mathfrak{S}, s) \in \textsf{M-SAT}$. Furthermore, if $(\mathfrak{S}, s)$ is m-saturated then $\mathfrak{S}_s \approx \mathfrak{H}_s$ (as both are m-saturated). But $s \approx \mathrm{Th}(\mathfrak{S}, s)$, hence $(\mathfrak{S}, s) \approxeq (\mathfrak{S}_s, s) \approxeq (\mathfrak{H}_s, \mathrm{Th}(\mathfrak{S}, s)) = \mathfrak{H}(\mathfrak{S}, s)$. So:

Proposition 4.2 *Let* M-SAT *now be the class of* rooted *m-saturated models. Then*

$$\textsf{M-SAT} = \{\mathfrak{H}(\mathfrak{S}, s) \mid (\mathfrak{S}, s) \text{ a rooted model}\}/_{\approxeq}$$

For the current purposes, another operation than $\mathfrak{H}$ is of more use to us, even though it turns out to be the same modulo bisimulation.

Definition 4.3 *Let* $\mathfrak{S} = (S, \{R_a\}_{a\in\mathcal{A}}, V)$ *be any non-rooted model. Then its* **canonical extension** *is* $\mathfrak{Ce}\mathfrak{S} := (\mathtt{ultra}(S), \{\mathfrak{R}_a\}_{a\in\mathcal{A}}, \mathfrak{V})$*, described as follows:*

universe: $\mathtt{ultra}(S) := \{\mathcal{U} \subseteq \wp(S) \mid \mathcal{U} \text{ is an ultrafilter on } S\}$

transitions: $\mathcal{U}\mathfrak{R}_a\mathcal{V}$ *iff* $\forall A \in \mathcal{V}.\ [l_{R_a}(A) \in \mathcal{U}]$*, where*

$$l_{R_a}(A) := \{x \in S \mid \exists y \in A.xR_a y\}$$

valuation: $\mathfrak{V}(p) := \{\mathcal{U} \in \mathtt{ultra}(S) \mid V(p) \in \mathcal{U}\}$

On rooted models the definition is as follows: $\mathfrak{Ce}(\mathfrak{S}, s) := (\mathfrak{Ce}\mathfrak{S}, \pi_s)$*, where* π_s *is the principal ultrafilter* $\{A \subseteq S \mid s \in A\}$. □

Goldblatt [4] contains good material on this operation. As an example, the model on the right in figure 8 is the canonical extension of the model on the left, modulo bisimulation. Some known facts about $\mathfrak{Ce}$ are:

- $\mathfrak{R}_a$ has an alternative yet equivalent definition:

  $$\mathcal{U}\mathfrak{R}_a\mathcal{V} \text{ iff } \forall A \subseteq S.[m_{R_a}(A) \in \mathcal{U} \Rightarrow A \in \mathcal{V}]$$

  where $m_{R_a}(A) := \{x \in S \mid \forall y \in S.(xR_a y \Rightarrow y \in A)\}$.

- $\mathfrak{Ce}\mathfrak{S}, \mathcal{U} \Vdash \phi$ iff $V(\phi) \in \mathcal{U}$, where $V(\phi) := \{s \in S \mid \mathfrak{S}, s \Vdash \phi\}$. Applied to the principal ultrafilter π_s this gives us that $s \approx \pi_s$.

- $\mathfrak{Ce}$ preserves bisimulations (both rooted and non-rooted).

- $\mathfrak{Ce}\mathfrak{S}$ is $\mathcal{H}$-saturated (proved in [6]). This implies that canonical extensions are m-saturated.

The last fact also implies that $\mathfrak{Ce}\mathfrak{S} \approx \mathfrak{H}_s$. What's more, $\pi_s \approx s \approx \mathrm{Th}(\mathfrak{S}, s)$. Therefore $\mathfrak{Ce}(\mathfrak{S}, s) \approxeq \mathfrak{H}(\mathfrak{S}, s)$.

Using this machinery, we will prove that M-SAT is closed under all our operations, except for infinite choice.

Theorem 4.4 M-SAT *is closed under* $+$.

Proof.
Suppose $(\mathfrak{S}, s)$ and $(\mathfrak{T}, t)$ are m-saturated. Consider a point x in their sum, reachable from $\bot$, and a set of modal formulas Φ, finitely satisfiable in the a-successors of x. We need to find an a-successor of x satisfying Φ. The only nontrivial case is if $x = \bot$. Suppose Φ is *not* satisfied in any of the a-successors of $\bot$. Then Φ is not satisfied in any a-successor of s nor in any of t. As $(\mathfrak{S}, s)$ and $(\mathfrak{T}, t)$ are both m-saturated there must be finite subsets Δ_0 and Δ_1 of Φ unsatisfiable in the a-successors of s, respectively in those of t. As $\Delta_0 \cup \Delta_1$ is also a finite subset of Φ it will be satisfiable in some a-successor of $\bot$. Because this will also be an a-successor of either s or t, we have a contradiction. □

Theorem 4.5 *For any two disjoint rooted models* $(\mathfrak{S}, s)$ *and* $(\mathfrak{T}, t)$, $\mathfrak{Ce}((\mathfrak{S}, s)\cdot(\mathfrak{T}, t))$ *and* $\mathfrak{Ce}(\mathfrak{S}, s) \cdot \mathfrak{Ce}(\mathfrak{T}, t)$ *are isomorphic, hence bisimilar. Notation:*

$$\mathfrak{Ce}((\mathfrak{S}, s) \cdot (\mathfrak{T}, t)) \cong \mathfrak{Ce}(\mathfrak{S}, s) \cdot \mathfrak{Ce}(\mathfrak{T}, t)$$

Therefore M-SAT *is closed under sequential composition.*

Proof.
We have to deal with seven different models in this proof, so the proof may sometimes be a bit confusing. Let us therefore not confuse matters more, and leave out the labels of the transition relations. But we still need different names for the transition-relations in the different models.These are given by the following table:

model	transition relation
$(\mathfrak{S}, s)$	R_1
$(\mathfrak{T}, t)$	R_2
$(\mathfrak{S}, s) \cdot (\mathfrak{T}, t)$	R_3

Because of the lengthy notation of the models we are trying to prove are isomorphic, let us introduce some pseudonyms:

$$\mathfrak{A} \quad := \quad \mathfrak{Ce}((\mathfrak{S}, s) \cdot (\mathfrak{T}, t)) \qquad\qquad \mathfrak{B} \quad := \quad \mathfrak{Ce}(\mathfrak{S}, s) \cdot \mathfrak{Ce}(\mathfrak{T}, t)$$

The universe of the $\mathfrak{A}$ is $\texttt{ultra}(S \cup T)$ while that of $\mathfrak{B}$ is $\texttt{ultra}(S) \cup \texttt{ultra}(T)$. A bijection $f : \texttt{ultra}(S \cup T) \to \texttt{ultra}(S) \cup \texttt{ultra}(T)$ can be defined as follows:

$$f(\mathcal{U}) := \begin{cases} \{A \subseteq S \mid A \in \mathcal{U}\} & \text{if } S \in \mathcal{U} \\ \{B \subseteq T \mid B \in \mathcal{U}\} & \text{if } T \in \mathcal{U} \end{cases}$$

This is a function because for any ultrafilter $\mathcal{U}$ on $S \cup T$, $S \cup T$ must be an element of $\mathcal{U}$, hence either $S \in \mathcal{U}$ or $T \in \mathcal{T}$, but not both, as S and T are assumed to be disjoint. Its inverse is given by:

$$g(\mathcal{U}) := \{A \subseteq S \cup T \mid \exists B \in \mathcal{U}.B \subseteq A\}$$

The reader may verify that these functions are well-defined and are each others inverses. Let us prove that f and g preserve the structure of the models:

f (and therefore g) preserves roots.
The roots of both models are principal ultrafilters generated by s. Let us denote the root of $\mathfrak{A}$ by π_s^1 (an ultrafilter on $S \cup T$) and the root of $\mathfrak{B}$ by π_s^2 (an ultrafilter on S). As $s \in S$ we know $S \in \pi_s^1$. Thus:

$$f(\pi_s^1) = \{A \subseteq S \mid A \in \pi_s^1\} = \{A \subseteq S \mid s \in A\} = \pi_s^2$$

f preserves the transitions.
Suppose $\mathcal{U}R\mathcal{V}$ in $\mathfrak{A}$. We need to prove that $f(\mathcal{U})Rf(\mathcal{V})$ in $\mathfrak{B}$. There are three cases:

- **$S \in \mathcal{V}$.**
  Then $l_{R_3}(S) \in \mathcal{U}$. As $l_{R_3}(S) \subseteq S$, $S \in \mathcal{U}$. So $f(\mathcal{U})$ and $f(\mathcal{V})$ are both elements of $\mathfrak{Ce}\mathfrak{S}$. Suppose $A \in f(\mathcal{V})$. Then $A \in \mathcal{V}$, hence $l_{R_3}(A) \in \mathcal{V}$. But $A \subseteq S$, so $l_{R_3}(A) = l_{R_1}(A) \subseteq S$. Therefore $l_{R_1}(A) \in f(\mathcal{U})$ and we have shown that $f(\mathcal{U})Rf(\mathcal{V})$ in $\mathfrak{Ce}\mathfrak{S}$, hence also in $\mathfrak{B}$.

- **$S \in \mathcal{U}$ and $T \in \mathcal{V}$.**
  Now $l_{R_3}(T) \in \mathcal{U}$, as $\mathcal{U}R\mathcal{V}$ in $\mathfrak{A}$. So $S \cap l_{R_3}(T) \in \mathcal{U}$. But if $x \in S$ and there is a $y \in T$ with xR_3y then x must be in $\surd_S$. So $S \cap l_{R_3}(T) \subseteq \surd_S \in \mathcal{U}$, hence $\surd_S \in f(\mathcal{U})$, which implies that $\mathfrak{Ce}\mathfrak{S}, f(\mathcal{U}) \Vdash \surd$.

Since $\surd_S \subseteq m_{R_3}(S \cup \{x \in T \mid tR_2x\})$ this latter set must be in $\mathcal{U}$. Therefore $S \cup \{x \in T \mid tR_2x\}$ is in $\mathcal{V}$, as $\mathcal{U}R\mathcal{V}$. But $T \in \mathcal{V}$, so $\{x \in T \mid tR_2x\} \in \mathcal{V}$ and thus in $f(\mathcal{V})$. This means that $\pi_t R f(\mathcal{V})$ in $\mathfrak{Ce}\mathfrak{T}$. For if $A \in f(\mathcal{V})$ then $A \cap \{x \in T \mid tR_2x\} \in f(\mathcal{V})$. This last set cannot be empty, say $tR_2x \in A$. Thus $t \in l_{R_2}(A)$, hence $l_{R_2}(A) \in \pi_t$.

So $\mathfrak{Ce}\mathfrak{S}, f(\mathcal{U}) \Vdash \surd$ and $\pi_t R f(\mathcal{V})$ in $\mathfrak{Ce}\mathfrak{T}$: we may conclude that $f(\mathcal{U}) R f(\mathcal{V})$ in $\mathfrak{B}$.

- **$T \in \mathcal{U}$ and $T \in \mathcal{V}$.**
  Then both $f(\mathcal{U})$ and $f(\mathcal{V})$ are in $\mathfrak{Ce}\mathfrak{T}$. Suppose $A \in f(\mathcal{V})$. Then $A \in \mathcal{V}$. As $\mathcal{U}R\mathcal{V}$ we conclude $l_{R_3}(A) \in \mathcal{U}$. But $T \in \mathcal{U}$, so $l_{R_3}(A) \cap T = l_{R_2}(A) \in \mathcal{U}$. Therefore $l_{R_2}(A) \in f(\mathcal{U})$ and we have shown that $f(\mathcal{U}) R f(\mathcal{V})$ in $\mathfrak{Ce}\mathfrak{T}$. This is also a transition in $\mathfrak{B}$ so we are done.

g preserves transitions.
Suppose $\mathcal{U}R\mathcal{V}$ in $\mathfrak{B}$. We will show that then also $g(\mathcal{U}) R g(\mathcal{V})$ in $\mathfrak{A}$. So suppose $A \in g(\mathcal{V})$: we must prove that $l_{R_3}(A) \in g(\mathcal{U})$. There are again three possibilities:

- **$\mathcal{V}$ is an ultrafilter on S.**
  Then $\mathcal{U}$ must also be an ultrafilter on S, as $\mathcal{U}R\mathcal{V}$ in $\mathfrak{B}$. So $\mathcal{U}R\mathcal{V}$ in $\mathfrak{Ce}\mathfrak{S}$. As $A \in g(\mathcal{V})$ there is a $B \in \mathcal{V}$ with $B \subseteq A$. But S is also in $\mathcal{V}$, so $B \cap S \subseteq A \cap S \in \mathcal{V}$. Thus $l_{R_1}(A \cap S) \in \mathcal{U}$. But $l_{R_1}(A \cap S) \subseteq l_{R_3}(A)$, so the latter set is in $g(\mathcal{U})$.

- **$\mathcal{U}$ is an ultrafilter on S, while $\mathcal{V}$ is one on T.**
  Then $\mathfrak{Ce}\mathfrak{S}, \mathcal{U} \Vdash \surd$ (i.e. $\surd_S \in \mathcal{U}$) and $\pi_t R \mathcal{V}$ in $\mathfrak{Ce}\mathfrak{T}$. As $m_{R_2}(\{x \in T \mid tR_2x\}) \in \pi_t$ and as $A \in g(\mathcal{V})$, $A \cap \{x \in T \mid tR_2x\} \in \mathcal{V}$. Since $\mathcal{V}$ is ultra, the latter set is nonempty, say $tR_2t' \in A$. Now, if $x \in \surd_S$ then xR_3t', by definition of sequential composition, so $x \in l_{R_3}(A)$. So $\surd_S \subseteq l_{R_3}(A)$. Because $\surd_S \in \mathcal{U}$, $l_{R_3}(A)$ must be in $g(\mathcal{U})$.

- **$\mathcal{U}$ and $\mathcal{V}$ are both ultrafilters on T.**
  Then $\mathcal{U}R\mathcal{V}$ in $\mathfrak{Ce}\mathfrak{T}$. Now $A \cap T \in \mathcal{V}$, so $l_{R_2}(A \cap T) \in \mathcal{U}$. As $l_{R_2}(A \cap T) \subseteq l_{R_3}(A)$, the latter is in $g(\mathcal{V})$.

f preserves success.
Suppose $\mathcal{U}$ is an ultrafilter on $S \cup T$, and $\mathfrak{A}, \mathcal{U} \Vdash \surd$. Then

$$\surd_T \cup \{x \in \surd_S \mid t \in \surd_T\} \in \mathcal{U}$$

because these are precisely the points in $(\mathfrak{S}, s) \cdot (\mathfrak{T}, t)$ where $\surd$ is true. Because $\mathcal{U}$ is an ultrafilter, there are two cases:

1. If $\surd_T \in \mathcal{U}$ then $\surd_T \in f(\mathcal{U})$, hence $\mathfrak{Ce}\mathfrak{T}, f(\mathcal{U}) \Vdash \surd$, so also $\mathfrak{B}, f(\mathcal{U}) \Vdash \surd$ (success-states in the second component of a sequential composition are also success-states in this composition).

2. Now suppose $\{x \in \surd_S \mid t \in \surd_T\} \in \mathcal{U}$. This set must then be nonempty, so $\surd_S \in \mathcal{U}$ and $t \in \surd_T$ (and so $\surd_T \in \pi_t$). Therefore $\mathfrak{Ce}\mathfrak{S}, f(\mathcal{U}) \Vdash \surd$ and $\mathfrak{Ce}\mathfrak{T}, \pi_t \Vdash \surd$. By definition of sequential composition: $\mathfrak{B}, f(\mathcal{U}) \Vdash \surd$.

g preserves success.
Suppose $\mathfrak{B}, \mathcal{U} \Vdash \surd$. We need to show that $\surd_T \cup \{x \in \surd_S \mid t \in \surd_T\} \in g(\mathcal{U})$. There are two cases to consider:

1. $\mathcal{U}$ is in $\mathfrak{Ce}\mathfrak{T}$ and $\surd_T \in \mathcal{U}$. As $\surd_T \subseteq \surd_T \cup \{x \in \surd_S \mid t \in \surd_T\}$ we are done.

2. $\mathcal{U}$ is in $\mathfrak{Ce}\mathfrak{S}$, $\surd_T \in \pi_t$ and $\surd_S \in \mathcal{U}$. As this entails that $t \in \surd_T$, we have that $\surd_S \subseteq \surd_T \cup \{x \in \surd_S \mid t \in \surd_T\}$ and we are again finished. □

Theorem 4.6 *Let $(\mathfrak{S}, s)$ be any rooted model. Then $(\mathfrak{Ce}(\mathfrak{S}, s))^* \cong \mathfrak{Ce}((\mathfrak{S}, s)^*)$. So* M-SAT *is closed under iteration.*

Proof.
We again prove it for a single transition-relation: the proof carries over to multiple transition-relations. The universe of $(\mathfrak{Ce}(\mathfrak{S}, s))^*$ and of $\mathfrak{Ce}((\mathfrak{S}, s)^*)$ is the set of ultrafilters on S. The roots are in each case π_s. We will prove that the identity on $\mathtt{ultra}(S)$ is our desired isomorphism.

If $\mathcal{U}R\mathcal{V}$ in $(\mathfrak{Ce}(\mathfrak{S}, s))^*$ then $\mathcal{U}R\mathcal{V}$ in $\mathfrak{Ce}((\mathfrak{S}, s)^*)$.
Suppose $A \in \mathcal{V}$. We have to prove that $l_{R_*}(A) \in \mathcal{U}$, where R_* is the transition-relation of $(\mathfrak{S}, s)^*$. There are two cases.

1. $\surd_S \in \mathcal{U}$ and $\pi_s R\mathcal{V}$ in $\mathfrak{Ce}\mathfrak{S}$. Then $\{x \in S \mid sRx\} \in \mathcal{V}$, so $A \cap \{x \in S \mid sRx\} \in \mathcal{V}$. Say $y \in A \cap \{x \in S \mid sRx\}$. Then $sRy \in A$. Now if $x \in \surd_S$ then $xR_*y \in A$, i.e. $\surd_S \subseteq l_{R_*}(A) \in \mathcal{U}$.

2. $\mathcal{U}R\mathcal{V}$ in $\mathfrak{Ce}\mathfrak{S}$. Then $l_R(A) \in \mathcal{U}$. Since $l_R(A) \subseteq l_{R_*}(A)$ we are done.

If $\mathcal{U}R\mathcal{V}$ in $\mathfrak{Ce}((\mathfrak{S}, s)^*)$ then $\mathcal{U}R\mathcal{V}$ in $(\mathfrak{Ce}(\mathfrak{S}, s))^*$.
We have to show that either $\mathcal{U}R\mathcal{V}$ in $\mathfrak{Ce}\mathfrak{S}$ or $\surd_S \in \mathcal{U}$ and $\pi_s R\mathcal{V}$ in $\mathfrak{Ce}\mathfrak{S}$. Suppose $\mathcal{V}$ is *not* a successor of $\mathcal{U}$ in $\mathfrak{Ce}\mathfrak{S}$. Then there must be an $A \in \mathcal{V}$ s.t. $l_R(A) \notin \mathcal{U}$. So $l_{R_*}(A) \in \mathcal{U}$ and $S - l_R(A) \in \mathcal{U}$, hence $l_{R_*}(A) \cap [S - l_R(A)] \in \mathcal{U}$. Suppose $x \in l_{R_*}(A) \cap [S - l_R(A)]$. Then, for some $y \in A$, xR_*y and as $x \notin l_R(A)$, xRy cannot be true, so $x \in \surd_S$ and sRy. Thus $l_{R_*}(A) \cap [S - l_R(A)] \subseteq \surd_S \in \mathcal{U}$.

Now all that remains to be proved is that $\pi_s R\mathcal{V}$ in $\mathfrak{Ce}\mathfrak{S}$. So suppose $B \in \mathcal{V}$. We need to show that $l_R(B) \in \pi_s$. Note that

$$l_{R_*}(A) \cap [S - l_R(A)] \subseteq m_{R_*}[\{x \in S \mid \exists y \in l_{R_*}(A) \cap [S - l_R(A)].yRx\} \cup \{x \in S \mid sRx\}]$$

This set must then be in $\mathcal{U}$, therefore

$$\{x \in S \mid \exists y \in l_{R_*}(A) \cap [S - l_R(A)].\ yRx\} \cup \{x \in S \mid sRx\} \in \mathcal{V}$$

So $[\{x \in S \mid \exists y \in l_{R_*}(A) \cap [S - l_R(A)].\ yRx\} \cup \{x \in S \mid sRx\}] \cap A \cap B \in \mathcal{V}$. This set must be nonempty, say y is an element of it. There are two possibilities.

1. There is a $z \in l_{R_*}(A) \cap [S - l_R(A)]$ s.t. zRy. But $y \in A$, so $z \in l_R(A)$: contradiction.

2. sRy. As $y \in B$, we may conclude that $l_R(B) \in \pi_s$, which is what we had to prove to show $\pi_t R\mathcal{V}$.

$(\mathfrak{Ce}(\mathfrak{S}, s))^*, \mathcal{U} \Vdash \surd$ iff $\mathfrak{Ce}((\mathfrak{S}, s)^*), \mathcal{U} \Vdash \surd$.
We leave out the proof of this: it is trivial. □

Atomic processes, the deadlock process and the success process are all finite, hence m-saturated. What remains is $\sum_{n\in\mathbb{N}}$. This operation clearly does not preserve m-saturation. Take for example the model on the left in figure 8. Its component parts (a^{n+1}) are all finite, yet their infinite sum is not: $\{\langle a\rangle^n \top \mid n \in \mathbb{N}\}$ is finitely satisfiable in the a-successors of the root, yet it is not satisfiable as a whole there. To forge M-SAT into a process algebra for infinite choice, we therefore need a different interpretation of $\sum_{n\in\mathbb{N}}$.

Definition 4.7 *The interpretation of* $\sum_{n\in\mathbb{N}}$ *in* M-SAT *is*

$$\sum\!\!\!\sum_{n\in\mathbb{N}}(\mathfrak{S}_n, s_n) := \mathfrak{Ce}(\sum_{n\in\mathbb{N}}(\mathfrak{S}_n, s_n))$$

□

Clearly this operation preserves m-saturation, as canonical extensions are always m-saturated. So we now have a new model of the given process language. The interesting question is: what is the connection to the standard model? The rest of this section is devoted to exactly this question.

Let us, for clarity, state which algebras we have to compare:

	Standard algebra $\mathbb{S}$	M-SAT-based algebra $\mathbb{M}$
Domain:	$\{\{(\mathfrak{S}, s)\}/_{\approxeq} \mid (\mathfrak{S}, s) \text{ a model}\}$	$\{\{(\mathfrak{S}, s)\}/_{\approxeq} \mid (\mathfrak{S}, s) \text{ m-saturated}\}$
Operations/ constants:	interpreted by the operations and models as defined on page 18.	the same as for $\mathbb{S}$, except for $\sum_{n\in\mathbb{N}}$ which is interpreted by $\sum\!\!\!\sum_{n\in\mathbb{N}}$.

Note that both domains are not sets. This is of no real importance in this setting. To avoid any problems we could pick a large enough set (say the set of reals) and restrict ourselves to models that take their points from this set.

If t is a term in the process language and $(\mathfrak{S}_n, s_n)$ is a rooted model for every $n \in \mathbb{N}$, then let $t^{\mathbb{S}}[x_n := (\mathfrak{S}_n, s_n)]$ be the term t as interpreted in $\mathbb{S}$, with each variable x_n replaced by the model $(\mathfrak{S}_n, s_n)$. Then $\mathbb{S} \models t_1 = t_2$ states nothing else than that for every sequence of models $(\mathfrak{S}_0, s_0), (\mathfrak{S}_1, s_1), (\mathfrak{S}_2, s_2), \ldots$:

$$t_1^{\mathbb{S}}[x_n := (\mathfrak{S}_n, s_n)] \approxeq t_2^{\mathbb{S}}[x_n := (\mathfrak{S}_n, s_n)]$$

The same can be defined for $\mathbb{M}$.

$\mathfrak{Ce}$ turns out to be a homomorphism from $\mathbb{S}$ onto $\mathbb{M}$. By standard arguments from universal algebra [4](carried over to the infinitary case) this implies that:

Theorem 4.8 $\mathbb{S} \models t_1 = t_2$ *implies that* $\mathbb{M} \models t_1 = t_2$ *for all terms* t_1 *and* t_2.

To see that $\mathfrak{Ce}$ is onto it is enough to note that $\mathfrak{Ce}(\mathfrak{S}, s) \approxeq (\mathfrak{S}, s)$ for every m-saturated $(\mathfrak{S}, s)$. To see that it is a homomorphism we need some lemmas:

Lemma 4.9 *Let, for each* $n \in \mathbb{N}$, $(\mathfrak{S}_n, s_n)$ *be disjoint rooted models. Then:*

$$\sum\!\!\!\sum_{n\in\mathbb{N}} \mathfrak{Ce}(\mathfrak{S}_n, s_n) \approxeq \sum\!\!\!\sum_{n\in\mathbb{N}}(\mathfrak{S}_n, s_n)$$

Proof.

Let us concentrate on a single transition-relation. For each of the models we denote these as follows:

models	transitions
$\mathfrak{S}_n$	R_n
$\mathfrak{Ce}\mathfrak{S}_n$	$\mathfrak{R}_n$
$\sum_{n\in\mathbb{N}}(\mathfrak{S}_n, s_n)$	R_+
$\sum_{n\in\mathbb{N}} \mathfrak{Ce}(\mathfrak{S}_n, s_n)$	$\mathfrak{R}_n$

Denote the root of $\sum_{n\in\mathbb{N}} \mathfrak{Ce}(\mathfrak{S}_n, s_n)$ by $\perp_0$ and that of $\sum_{n\in\mathbb{N}}(\mathfrak{S}_n, s_n)$ by $\perp_1$. We abbreviate

$$\mathfrak{T} := \sum\!\!\!\sum_{n\in\mathbb{N}} \mathfrak{Ce}(\mathfrak{S}_n, s_n) \qquad \mathfrak{U} := \sum\!\!\!\sum_{n\in\mathbb{N}}(\mathfrak{S}_n, s_n)$$

[4] An excellent text on this subject is Burris and Sankappanavar [2].

We will define a p-morphism (a functional bisimulation) f from $\mathfrak{T}$ to $\mathfrak{U}$. This will use the function $g : \wp(\bigcup_{n\in\mathbb{N}} S_n \cup \{\bot_1\}) \to \wp(\bigcup_{n\in\mathbb{N}} \mathtt{ultra}(S_n) \cup \{\bot_0\})$ defined thus:

$$g(A) := \bigcup_{n\in\mathbb{N}} \{\mathcal{U} \in \mathtt{ultra}(S_n) \mid A \cap S_n \in \mathcal{U}\} \cup \{\bot_0 \mid \bot_1 \in A\}$$

We are ready to define our p-morphism f:

$$f(\mathcal{U}) := \{A \subseteq \bigcup_{n\in\mathbb{N}} S_n \cup \{\bot_1\} \mid g(A) \in \mathcal{U}\}$$

$f(\mathcal{U})$ is an ultrafilter on $\bigcup_{n\in\mathbb{N}} S_n \cup \{\bot_1\}$.
It is easy to verify that $g(A \cap B) = g(A) \cap g(B)$, hence $f(\mathcal{U})$ is closed under $\cap$, and that g is monotone, implying that it is upwards closed. As $g(\emptyset) = \emptyset$, $\emptyset \notin f(\mathcal{U})$. Finally $g(A^c) = g(A)^c$, hence if $g(A) \notin \mathcal{U}$ then $g(A^c) \in \mathcal{U}$.

f preserves roots.
The root of $\mathfrak{T}$ is $\pi_{\bot_0}$, while that of $\mathfrak{U}$ is $\pi_{\bot_1}$. If $A \in \pi_{\bot_1}$ then $\bot_1 \in A$. Thus $\bot_0 \in g(A)$. Hence $A \in f(\pi_{\bot_0})$ and we have proved that $\pi_{\bot_1} \subseteq f(\pi_{\bot_0})$. As we're speaking of ultrafilters (maximal proper filters w.r.t. $\subseteq$), $\pi_{\bot_1} = f(\pi_{\bot_0})$.

Suppose $\mathcal{U}R\mathcal{V}$ in $\mathfrak{T}$. Then $f(\mathcal{U})Rf(\mathcal{V})$ in $\mathfrak{U}$.
Suppose $A \in f(\mathcal{V})$. We need to show that $l_{R_+}(A) \in f(\mathcal{U})$, i.e. that $g(l_{R_+}(A)) \in \mathcal{U}$. As $A \in f(\mathcal{V})$, $g(A) \in \mathcal{V}$, by definition of f. Therefore $l_{\mathfrak{R}_+}(g(A)) \in \mathcal{V}$.

Suppose $\mathcal{B} \in l_{\mathfrak{R}_+}(g(A)) \cap \mathtt{ultra}(S_n)$. Then there must be a $\mathcal{C}$ with $\mathcal{B}\mathfrak{R}_+\mathcal{C} \in g(A)$. This implies that $\mathcal{B}\mathfrak{R}_n\mathcal{C}$ (by definition of $\sum_{n\in\mathbb{N}}$) and that $A \cap S_n \in \mathcal{C}$. Therefore $l_{R_n}(A \cap S_n) = l_{R_+}(A) \cap S_n \in \mathcal{B}$. So $\mathcal{B} \in g(l_{R_+}(A))$.

Now suppose $\bot_0 \in l_{\mathfrak{R}_+}(g(A))$. Then there is a $\mathcal{B} \in \mathtt{ultra}(S_n)$ for some n with $\bot_0\mathfrak{R}_+\mathcal{B} \in g(A)$ (hence $A \cap S_n \in \mathcal{B}$). This entails $\pi_{s_n}\mathfrak{R}_n\mathcal{B}$ and as $m_{R_n}(\{x \in S_n \mid s_nR_nx\}) \in \pi_{s_n}$, $\{x \in S_n \mid s_nR_nx\} \in \mathcal{B}$. Thus $A \cap \{x \in S_n \mid s_nR_nx\} \in \mathcal{B}$. This set can therefore not be empty, say $x \in A$ with s_nR_nx. So $\bot_1R_+x$ and $\bot_1 \in l_{R_+}(A)$. But then $\bot_0 \in g(l_{R_+}(A))$.

We have proved above that $l_{\mathfrak{R}_+}(g(A)) \subseteq g(l_{R_+}(A))$. As the former is in $\mathcal{V}$, the second must also, which is what we set out to prove.

If $f(\mathcal{U})R\mathcal{V}$ in $\mathfrak{U}$ then there must be an $\mathcal{X}$ s.t. $\mathcal{U}R\mathcal{X}$ in $\mathfrak{T}$ and $f(\mathcal{X}) = \mathcal{V}$.
Define $\Delta := \{g(A) \mid A \in \mathcal{V}\} \cup \{X \subseteq \bigcup_{n\in\mathbb{N}} \mathtt{ultra}(S_n) \cup \{\bot_0\} \mid m_{\mathfrak{R}_+}(X) \in \mathcal{U}\}$. We will show that Δ has the fip. Both parts of Δ are closed under intersection, so it suffices to show that for any $A \in \mathcal{V}$ and $m_{\mathfrak{R}_+}(X) \in \mathcal{U}$, $g(A) \cap X \neq \emptyset$. Assume the premiss. $A \in \mathcal{V}$ implies that $l_{R_+}(A) \in f(\mathcal{U})$, as $f(\mathcal{U})R\mathcal{V}$ in $\mathfrak{U}$. So $g(l_{R_+}(A)) \in \mathcal{U}$. Therefore $g(l_{R_+}(A)) \cap m_{\mathfrak{R}_+}(X) \in \mathcal{U}$, say $x \in g(l_{R_+}(A)) \cap m_{\mathfrak{R}_+}(X)$. There are two possibilities:

- $x = \mathcal{B} \in \mathtt{ultra}(S_n)$.
  Then $l_{R_+}(A) \cap S_n = l_{R_n}(A \cap S_n) \in \mathcal{B}$. It is therefore possible to find a successor $\mathcal{C}$ of $\mathcal{B}$ in $\mathfrak{Ce}\mathfrak{S}_n$ with $A \cap S_n \in \mathcal{C}$ (hence $\mathcal{C} \in g(A)$). But $\mathcal{B}\mathfrak{R}_n\mathcal{C}$ implies $\mathcal{B}\mathfrak{R}_+\mathcal{C}$, so $\mathcal{C} \in X$, since $\mathcal{B} \in m_{\mathfrak{R}_+}(X)$. Thus we have found an element $\mathcal{C} \in g(A) \cap X$.
- $x = \bot_0$.
  Then $\bot_1 \in l_{R_+}(A)$, say $\bot_1R_+y \in A$. So s_nR_ny for some n, and $y \in A \cap S_n$. Therefore $\pi_{s_n}\mathfrak{R}_n\pi_y \in g(A)$. But then, by definition of $\sum_{n\in\mathbb{N}}$, $\bot_0\mathfrak{R}_+\pi_y$. Thus $\pi_y \in X$ and we have again found an element in $g(A) \cap X$.

So Δ can be extended to an ultrafilter $\mathcal{X}$ which is clearly a successor of $\mathcal{U}$, because for every $m_{\mathfrak{R}_+}(X) \in \mathcal{U}$, $X \in \mathcal{X}$. Also $f(\mathcal{X}) = \mathcal{V}$. For if $g(A) \in \mathcal{X}$ while $A^c \in \mathcal{V}$, then $g(A^c) \in \Delta \subseteq \mathcal{X}$. But $g(A^c) = g(A)^c$, so we have a contradiction.

$\mathfrak{T}, \mathcal{U} \Vdash \surd$ iff $\mathfrak{U}, f(\mathcal{U} \Vdash \surd$.
Easy to verify. □

Lemma 4.10 $\mathfrak{Ce}((\mathfrak{S}, s) + (\mathfrak{T}, t)) \approxeq \mathfrak{Ce}(\mathfrak{S}, s) + \mathfrak{Ce}(\mathfrak{T}, t)$.

Proof.
Let the root of $(\mathfrak{S}, s) + (\mathfrak{T}, t)$ be $\bot_0$ and let that of $\mathfrak{Ce}(\mathfrak{S}, s) + \mathfrak{Ce}(\mathfrak{T}, t)$ be $\bot_1$. We show that $\bot_0 \approx \bot_1$.

Suppose $\bot_0 \Vdash \langle a \rangle \phi$. Then there is an $x \in S \cup T$ with $\bot_1 R_a x \Vdash \phi$ in $(\mathfrak{S}, s)+(\mathfrak{T}, t)$. Say $x \in S$. Then $s R_a x \Vdash \phi$ in $(\mathfrak{S}, s)$. But then $\pi_s R_a \pi_x \Vdash \phi$ in $\mathfrak{Ce}\mathfrak{S}$, so $\bot_1 R_a \pi_x$ and $\bot_1 \Vdash \langle a \rangle \phi$. If $x \in T$, the proof is similar.

For the other direction, let $\bot_1 \Vdash \langle a \rangle \phi$. Say $\bot_1 R_a \mathcal{U} \Vdash \phi$, with $\mathcal{U}$ in $\mathfrak{Ce}\mathfrak{S}$. Then $\pi_s R_a \mathcal{U}$, hence $\pi_s \approx s \Vdash \langle a \rangle \phi$. Therefore there is an $x \in S$ with $s R_a x \Vdash \phi$, hence $\bot_0 R_a x$ and $\bot_0 \Vdash \langle a \rangle \phi$.

The other cases of the induction are again trivial. Since $+$ preserves m-saturation and $\mathfrak{Ce}\mathfrak{S}$ and $\mathfrak{Ce}\mathfrak{T}$ are m-saturated, $\mathfrak{Ce}(\mathfrak{S}, s) + \mathfrak{Ce}(\mathfrak{T}, t)$ must be m-saturated. Hence $\mathfrak{Ce}((\mathfrak{S}, s)+(\mathfrak{T}, t)) \approxeq \mathfrak{H}((\mathfrak{S}, s)+(\mathfrak{T}, t)) \approx \mathfrak{Ce}(\mathfrak{S}, s)+\mathfrak{Ce}(\mathfrak{T}, t)$, as M-SAT is a Hennessy-Milner class. But the roots of the last two models are modally equivalent ($Th((\mathfrak{S}, s) + (\mathfrak{T}, t), \bot_0) \approx \bot_0 \approx \bot_1$) so $\mathfrak{H}((\mathfrak{S}, s) + (\mathfrak{T}, t)) \approxeq \mathfrak{Ce}(\mathfrak{S}, s) + \mathfrak{Ce}(\mathfrak{T}, t)$. □

Now we are finally ready to prove that $\mathfrak{Ce}$ is a homomorphism between $\mathbb{S}$ and $\mathbb{M}$. Clearly the constants are preserved, because all interpretations of constants are finite, hence m-saturated, so they are bisimilar to their canonical extensions. That $\mathfrak{Ce}$ preserves $+$, $\cdot$ and $*$ is shown in respectively lemma 4.10 and theorems 4.5 and 4.6. That $\mathfrak{Ce}$ preserves $\sum$ is shown by lemma 4.9, because this states that $\mathfrak{Ce}(\sum_{n\in\mathbb{N}}(\mathfrak{S}_n, s_n)) \approxeq \sum_{n\in\mathbb{N}}(\mathfrak{Ce}(\mathfrak{S}_n, s_n)$.

5 Future research

There is still much work to be done in this area.

1. Concerning the characterisation of maximal Hennessy-Milner classes in terms of Henkin-like models, consider the following ordering on these models:

$$\mathfrak{H}_1 \sqsubseteq \mathfrak{H}_2 \iff \forall \alpha \in \mathcal{A}.\ R_{(1,\alpha)} \subseteq R_{(2,\alpha)}$$

   where $R_{(i,\alpha)}$ is a transition-relation of $\mathfrak{H}_i$. This induces an ordering on maximal Hennessy-Milner classes. M-SAT is clearly maximal in this ordering. Are there any minimal ones?

2. Now that we have given a model $\mathbb{M}$ for a fragment of process algebra, we should investigate precisely which equations are valid in $\mathbb{M}$. Can we axiomatize this set of equations in some way? Clearly not if we allow just any sequence of terms $(t_n)_{n\in\mathbb{N}}$ as input for the operation $\sum_{n\in\mathbb{N}}$. But if we restruct ourselves to recursive sequences, is it then possible to give an axiomatization?

3. The results on closure of M-SAT under the various process-operations might be a consequence of a more general result. If an operation on rooted Kripke models preserves bisimulation and finite branching, and is first-order definable in the input-models, does that operation then preserve m-saturation? Such a result may save some work when considering other process operations than the ones we have considered here.

Acknowledgements
Obviously Albert Visser was extremly helpful in the preparation of this paper: he suggested this topic and is responsible for the result on Henkin-like models. But I am also grateful for Rob Goldblatt and Yde Venema for reading and commenting on an earlier version. Finally I want to mention Jan-Friso Groote who helped me with the process-algebra part.

References

[1] J.C.M. Baeten and W.P. Weijland, *Process Algebra*, Cambridge Tracts in Theoretical Computer Science 18, Cambridge University Press, 1990.

[2] S. Burris and H.P. Sankappanavar, *A Course in Universal Algebra*, Springer Verlag, Berlin, 1981.

[3] K. Fine, "Some connections between elementary and modal logic", in *Proceedings of the Third Scandinavian Logic Symposium, Uppsala 1973*, North-Holland, Amsterdam, 1975, 15-31.

[4] R.I. Goldblatt, "Metamathematics of modal logic", *Reports on Mathematical Logic*, vol. **6** (1976), 41-77 and vol. **7** (1976), 21-52.

[5] R.I. Goldblatt, *Logics of Time and Computation*, CSLI Lecture Notes No. 7, Centre for the Study of Language and Information, Stanford University, 1987.

[6] R.I. Goldblatt, "Saturation and the Hennessy-Milner property", Research report 94-145, Victoria University of Wellington, 1994.

[7] M. Hennessy, R. Milner, "Algebraic Laws for Nondeterminism and Concurrency", *J. Assoc. Comput. Mach.*, **32** (1985) 137-161.

[8] A. Visser, "Modal Logic and Bisimulation", Tutorial for the workshop "Three days of bisimulation", Amsterdam, 1994.