Frame Algebra with Synchronous Communication

Jan A. Bergstra[1,2] Alban Ponse[1]

[1] *University of Amsterdam, Programming Research Group*
Kruislaan 403, 1098 SJ Amsterdam, The Netherlands

[2] *Utrecht University, Department of Philosophy*
Heidelberglaan 8, 3584 CS Utrecht, The Netherlands

E-mail: `janb@fwi.uva.nl - alban@fwi.uva.nl`

Abstract. We introduce frames as basic objects for the construction of transition systems, process graphs or automata. We provide an algebraic notation for frames, and display some theoretical results.

Key words & Phrases: Frame, Process, Decidability.

1987 CR Categories: F.1.1, F.4.3, I.1.1.

1 Introduction

In this paper we propose a very simple, mathematical structure which we think to be of the type that underlies many structures modelling (concurrent) behaviour. The objects in this structure are called *frames*. We provide an axiomatic, algebraic approach to reasoning about equality between frames. Frames can be characterized as a particular kind of graphs; in fact, all frames in the present paper are labeled, directed graphs. The axioms however will allow other models. The main source of such models is the introduction of various degrees of locality (invisibility, hiding) for states. If no hiding mechanism on states is present, all states are called *sharp*. In this paper we will restrict attention to frames with sharp states only. Frames with hiding occur in [Ber89]. Typical for our approach is that frames are constructed out of *states* and *(labeled) transitions*. The states are obtained by an embedding of the natural numbers, and a pairing operation. At this point, one can imagine other choices, e.g., the set of strings over some finite alphabet.

Frames are defined by an embedding of the states, a transition function that connects two states with a labeled transition, and a small number of frame operations. First we have 'alternative composition', in the case with sharp states only defined by taking the (set-theoretic) union of the states and transitions of the two composing arguments. In fact this operation constitutes the only kind of non-trivial identifications we make on frames. We further assume that frames can be 'concurrently composed', retaining their original transitions (after projection) and obtaining new ones that reflect *(synchronous) communication*. Finally, we also consider two *system operations* on frames: 'encapsulation' for removal of transitions (but preserving states), and 'pre-abstraction' that renames some labels of transitions into a special constant t. These last two operations are included because

- both are fundamental in specifying the behaviour of concurrent systems using synchronization and abstraction (cf. [BW90]), and
- both are necessary to obtain sufficient expressivity (cf. [BBK87, Vaa93]).

We start with frames from a *finite* number of states, in Section 2. Then, in Section 3 we introduce *frame polynomials* as to specify and reason on infinite frames. The technical result in this paper, proven in Section 4, is that equality between infinite frames is decidable. Here equality is used in its most basic form: two frames are equal if they have the same states and the same transitions. This is in contrast with equality relations that make identifications on differently structured states (e.g. isomorphy) or differently structured frames (e.g. bisimularity or trace equivalence, taking connectedness into account, amongst other things). In Section 5 it is shown that allowing addition in state expressions preserves the decidability result, while the expressivity increases. In Section 6 it is shown that equality between infinite frames is undecidable for some extensions of the state domain.

Frames with sharp states, equipped with a root marker and optionally with termination markers constitute an extremely well-known category of objects, known as automata or transition systems. Automata along the lines of Rabin and Scott can be used as a basis for a theory of computation [RS59]. The structure theory of automata constitutes a large field of research; two general references, in which many others can be found, are [Buc89, Eil74]. Transition systems following Plotkin [Plo81] can be used as a basis for programming language semantics. Along the lines of de Simone [Sim85, GV92], transition systems can form a basis of a powerful model theory for process algebra. Our purpose is to develop a direct, algebraic notation for frames, to give an example of its use and some theoretical information about it.

2 Signature and Axioms

Let the symbol $\mathbb{N}$ represent the naturals given by constant 0 and successor function S (and equipped with equality predicate $=$). As usual, we represent the elements of $\mathbb{N}$ as numerals 0, 1, 2, 3,... and use meta-variables k, l, m, n for these.

Let $\mathbb{S}$ be a set of states, obtained by an embedding $i_{\mathbb{N}}$ of $\mathbb{N}$ in $\mathbb{S}$ and a pairing function $\succ\!\!\prec$. We further abbreviate $i_{\mathbb{N}}(n)$ by n.

Let A be a finite set of *action symbols* or *labels*, not containing the symbol t, and let $A_t = A \cup \{t\}$. Let furthermore γ be a partial function on A^2 that is commutative and associative. We call γ the *communication function*, and write $\gamma(a,b)\uparrow$ if $\gamma(a,b)$ is not defined, and $\gamma(a,b)\downarrow$ otherwise.

We define the signature of the set $\mathbb{F}$ of *frames* by

1. An embedding $i_{\mathbb{S}}$ of $\mathbb{S}$ in $\mathbb{F}$;

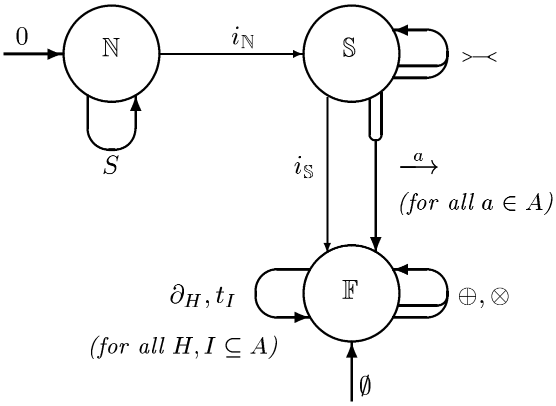
2. Operations $\xrightarrow{a}\ : \mathbb{S}^2 \to \mathbb{F}$ for all $a \in A$, so called *transitions* having a *label* in A;

3. The empty frame $\emptyset \in \mathbb{F}$;

4. The unary frame operations ∂_H, *encapsulation over* H, and t_I, *pre-abstraction over* I, for all $H, I \subseteq A$ (cf. [BW90]);

5. The binary frame operations $\oplus$, *alternative frame composition*, and $\otimes$, *concurrent frame composition*, taken from [Ber89].

We usually write n instead of $i_{\mathbb{S}}(n)$ (or $i_{\mathbb{N}}(i_{\mathbb{S}}(n))$), for instance $0 \succ\!\!\prec 1$ is a frame. This signature can be depicted as follows:



Let $s, s' \in \mathbb{S}$. Frames of the form s or $s \xrightarrow{a} s'$ are called *atomic*. The set of states of a frame X is denoted by $|X|$. Let X and Y be frames. Then the frame

$\partial_H(X)$ is defined by removing the transitions having labels from H in X, but keeping the states;

$t_I(X)$ is defined by replacing the labels in I of the transitions in X by t-labels;

$X \oplus Y$ is defined by taking the union of the states and the transitions of X and Y.

$X \otimes Y$ has as states the $\succ\!\!\prec$ image of the states of X and Y respectively, i.e.

$$|X \otimes Y| = \{s \succ\!\!\prec s' \mid s \in |X|, s' \in |Y|\}$$

and as transitions

$$s_1 \succ\!\!\prec s_2 \xrightarrow{a} t_1 \succ\!\!\prec t_2$$

whenever

$$s_1 \xrightarrow{a} t_1 \in X,\ s_2 = t_2 \in |Y|, \text{ or}$$

$$s_2 \xrightarrow{a} t_2 \in Y,\ s_1 = t_1 \in |X|, \text{ or}$$

$$\begin{cases} \gamma(b,c) = a \text{ and} \\ s_1 \xrightarrow{b} t_1 \in X,\ s_2 \xrightarrow{c} t_2 \in Y. \end{cases}$$

Clearly, $\oplus$ is an idempotent, commutative and associative operation. The operations ∂_H and t_I are also idempotent. Let $X, Y, Z, \ldots$ range over frames. Frames satisfy all axioms in Table 1.

By analogy with [BW90], we distinguish the following axiom systems:

BFA$(A, \mathbb{S})$, Basic Frame Algebra over A and $\mathbb{S}$, consisting of the axioms (FA1) – (FA6) where $a \in A$;

FA$(A, \mathbb{S})$, Frame Algebra, consisting of the axioms of BFA$(A, \mathbb{S})$ and (FC1) – (FC8) but without any reference to communication (the "if" clause in FC8) is removed) where $a \in A$;

ACF$(A, \gamma, \mathbb{S})$, the Algebra of Communicating Frames, consisting of the axioms of BFA$(A, \mathbb{S})$, a communication function γ as a parameter, the axioms (FC1) – (FC9) and (FDH1 – FDH5) where $a \in A$;

ACF$_t(A, \gamma, \mathbb{S})$, the Algebra of Communicating Frames with pre-abstraction, consisting of all axioms in Table 1. Note that in this system the label a ranges over A_t.

Observe that in FA$(A, \mathbb{S})$ (ACF$(A, \gamma, \mathbb{S})$ and ACF$_t(A, \gamma, \mathbb{S})$), one can always eliminate the $\otimes$ operations (∂_H and t_I, respectively). In the rest of this paper we shall restrict our attention to ACF$_t(A, \gamma, \mathbb{S})$.

3 Frame Polynomials

Let *iterated* alternative composition be defined by

$$\bigoplus_{i=n}^{k} F_i = \begin{cases} \emptyset & \text{if } k < n, \\ F_n \oplus \bigoplus_{i=n+1}^{k} F_i & \text{otherwise.} \end{cases}$$

Then each frame has a representation of the form $\bigoplus_{i=1}^{m} F_i$, where the F_i are atomic. In this section we shall extend this result to a more general syntax for frame representation.

Let V be a countable infinity of variables $x, y, \ldots$ (possibly primed or subscripted) over $\mathbb{N}$.

Let $\mathbb{S}[V]$ be defined as the set obtained by closure under the function $\succ\!\!\prec$ on $(\mathbb{S} \cup V)^2$, and let $i_{\mathbb{S}}$ be appropriately extended. In this section we define *frame polynomials* over V and A, the most simple example of one being x for some $x \in V$. Our operations and equalities extend to frame polynomials, for instance

$$x \otimes (0 \xrightarrow{a} S(0)) = x \succ\!\!\prec 0 \xrightarrow{a} x \succ\!\!\prec S(0).$$

Let furthermore the *generalized frame sum* $\bigoplus_x$ be defined by

$$\bigoplus_x F(x) = F[0/x] \oplus F[1/x] \oplus F[2/x] \oplus \ldots$$

where $F[n/x]$ denotes the substitution of n for x in F.

The syntax ACF$_t(A, \gamma, V, \mathbb{S})$ of *frame polynomials* over A, V and $\mathbb{S}$ is formally defined by the following BNF grammar with $s, s' \in \mathbb{S}[V]$, $a \in A_t$, $x \in V$ and $H, I \subseteq A$:

$$\begin{array}{rcl} F & ::= & \emptyset \mid s \mid (s \xrightarrow{a} s') \\ & \mid & \bigoplus_x(F) \mid \partial_H(F) \mid t_I(F) \\ & \mid & F \oplus F \mid F \otimes F \end{array}$$

Let FV(F) be the set of free variables in F. A frame polynomial is *closed* if FV$(F) = \emptyset$. A closed frame polynomial will be further referred to as a *frame*. So from now on we consider frames that may have an infinite number of states and/or transitions. An example of an infinite frame is a 'half-counter':

Table 1: The axiom system $\mathrm{ACF}_t(A, \gamma, \mathbb{S})$, where $a \in A_t$, $s, s', s'', s''' \in \mathbb{S}$ and $H, I \subseteq A$.

(FA1)	$X \oplus Y = Y \oplus X$	(FC1)	$\emptyset \otimes X = \emptyset$
(FA2)	$X \oplus (Y \oplus Z) = (X \oplus Y) \oplus Z$	(FC2)	$X \otimes \emptyset = \emptyset$
(FA3)	$X \oplus X = X$	(FC3)	$(X \oplus Y) \otimes Z = (X \otimes Z) \oplus (Y \otimes Z)$
(FA4)	$X \oplus \emptyset = X$	(FC4)	$X \otimes (Y \oplus Z) = (X \otimes Y) \oplus (X \otimes Z)$
(FA5)	$s \oplus (s \xrightarrow{a} s') = s \xrightarrow{a} s'$	(FC5)	$s \otimes s' = s \succ\!\!\prec s'$
(FA6)	$s' \oplus (s \xrightarrow{a} s') = s \xrightarrow{a} s'$	(FC6)	$s \otimes (s' \xrightarrow{a} s'') = s \succ\!\!\prec s' \xrightarrow{a} s \succ\!\!\prec s''$
		(FC7)	$(s \xrightarrow{a} s') \otimes s'' = s \succ\!\!\prec s'' \xrightarrow{a} s' \succ\!\!\prec s''$

$$\text{(FC8)} \quad (s \xrightarrow{a} s') \otimes (s'' \xrightarrow{b} s''') = \begin{pmatrix} ((s \xrightarrow{a} s') \otimes (s'' \oplus s''')) \oplus \\ ((s \oplus s') \otimes (s'' \xrightarrow{b} s''')) \end{pmatrix} \quad \text{if } \gamma(a,b) \uparrow$$

$$\text{(FC9)} \quad (s \xrightarrow{a} s') \otimes (s'' \xrightarrow{b} s''') = \begin{pmatrix} ((s \xrightarrow{a} s') \otimes (s'' \oplus s''')) \oplus \\ ((s \oplus s') \otimes (s'' \xrightarrow{b} s''')) \oplus \\ ((s \succ\!\!\prec s'' \xrightarrow{\gamma(a,b)} s' \succ\!\!\prec s''')) \end{pmatrix} \quad \text{if } \gamma(a,b) \downarrow$$

(FDH1)	$\partial_H(\emptyset) = \emptyset$	(FTI1)	$t_I(\emptyset) = \emptyset$
(FDH2)	$\partial_H(s) = s$	(FTI2)	$t_I(s) = s$
(FDH3)	$\partial_H(s \xrightarrow{a} s') = s \xrightarrow{a} s'$ if $a \notin H$	(FTI3)	$t_I(s \xrightarrow{a} s') = s \xrightarrow{a} s'$ if $a \notin I$
(FDH4)	$\partial_H(s \xrightarrow{a} s') = s \oplus s'$ if $a \in H$	(FTI4)	$t_I(s \xrightarrow{a} s') = s \xrightarrow{t} s'$ if $a \in I$
(FDH5)	$\partial_H(X \oplus Y) = \partial_H(X) \oplus \partial_H(Y)$	(FTI5)	$t_I(X \oplus Y) = t_I(X) \oplus t_I(Y)$

$$\begin{tikzcd}
0 & 0 \succ\!\!\prec 0 \arrow[l, "exit"'] \arrow[r, "b"', shift right] \arrow[d, "a"'] & 1 \succ\!\!\prec 0 \arrow[l, "restart"', shift right] \\
& 0 \succ\!\!\prec 1 \arrow[r, "b"] \arrow[d, "a"'] & 1 \succ\!\!\prec 1 \arrow[u, "a"'] \\
& 0 \succ\!\!\prec 2 \arrow[r, "b"] \arrow[d, "a"'] & 1 \succ\!\!\prec 2 \arrow[u, "a"'] \\
& 0 \succ\!\!\prec 3 \arrow[r, "b"] & 1 \succ\!\!\prec 3 \arrow[u, "a"'] \\
& \vdots &
\end{tikzcd}$$

The state $0 \succ\!\!\prec 0$ represents the start-state from which the counter can either terminate with an *exit*-transition, or enter the 'add mode' by an a-transition. Change to the 'substract mode' is modelled by a b-transition, after which the half-counter can empty itself by consecutive a-transitions, and evolve into the start-state by a *restart*-transition. We can easily express this half-counter by a frame polynomial:

$$\begin{aligned}
& (0 \otimes \textstyle\bigoplus_x (x \xrightarrow{a} S(x))) \\
\oplus\ & (1 \otimes \textstyle\bigoplus_x (S(x) \xrightarrow{a} x)) \\
\oplus\ & ((0 \xrightarrow{b} 1) \otimes \textstyle\bigoplus_x (x)) \\
\oplus\ & (0 \succ\!\!\prec 0 \xrightarrow{exit} 0) \\
\oplus\ & (1 \succ\!\!\prec 0 \xrightarrow{restart} 0 \succ\!\!\prec 0).
\end{aligned}$$

[1] Frame polynomials can also be compared; an example of an obvious identity is

$$\begin{aligned}\textstyle\bigoplus_x(x \xrightarrow{a} S(x)) &= (0 \xrightarrow{a} 1)\\ &\quad \oplus \textstyle\bigoplus_x(S(x) \xrightarrow{a} S^2(x)).\end{aligned}$$

In order to formalize reasoning about equality between (closed) frame polynomials, we propose the axioms in Table 1 with the $s, ..., s'''$ now ranging over $\mathbb{S}[V]$. Moreover, we have employ for the additional axioms displayed in Table 2. In these axioms we use the proviso

"x does not occur in F".

By this proviso it is meant that x occurs neither as a free, nor as bound variable (by an $\bigoplus_x$ application) in F. Note that bound variables may always be renamed.

For convenience, we shall often write $\bigoplus_{x_1...x_n}$ instead of $\bigoplus_{x_1} \circ ... \circ \bigoplus_{x_n}$.

A frame polynomial is in *normal form* if it is of the form

$$\textstyle\bigoplus_{i=1}^k \bigoplus_{x_1...x_l} F_i$$

with all F_i atomic, i.e. each F_i is either of the form s, or $s \xrightarrow{a} s'$ for some $s, s' \in \mathbb{S}[V]$ and $a \in A_t$.

Theorem 3.1. *Each frame over* $\mathrm{ACF}_t(A, \gamma, V, \mathbb{S})$ *can be represented by a polynomial in normal form.*

Proof. We first prove that each (open) frame polynomial *without* occurrences of ∂_H and t_I can be represented in normal form. For such polynomials, it suffices to show that $\bigoplus_x F$, $F \oplus F'$ and $F \otimes F'$ have normal forms whenever F and F' do. The first two cases are trivial. For the latter case, if one of F and F' is $\emptyset$ we are done, so assume both have normal forms

$$\textstyle\bigoplus_{i=1}^k \bigoplus_{x_1...x_l} F_i \text{ and } \bigoplus_{i=1}^m \bigoplus_{y_1...y_n} G_i,$$

respectively, for $k, m \geq 1$ and F_i, G_i atomic. Then with the axiom (FC3) we obtain

$$\begin{aligned} F \otimes F' &= (\textstyle\bigoplus_{x_1...x_l}(F_1) \otimes F') \oplus \\ &\quad (\textstyle\bigoplus_{i=2}^k \bigoplus_{x_1...x_l}(F_i) \otimes F') \\ &= \\ &\ \ \vdots \\ &= (\textstyle\bigoplus_{x_1...x_l}(F_1) \otimes F') \oplus \\ &\quad\ \vdots \\ &\quad (\textstyle\bigoplus_{x_1...x_l}(F_k) \otimes F'). \end{aligned}$$

Now using (FC4), each of these summands can be further expanded, eventually yielding $k \cdot m$ summands $\bigoplus_{x_1...x_l}(F_i) \otimes \bigoplus_{y_1...y_n}(G_j)$ with $i \in \{1, ..., k\}$ and $j \in \{1, ..., m\}$. With the axioms (FPC1) and (FPC2) this leads to summands of the form $\bigoplus_{x_1...x_l, y_1...y_n}(F_i \otimes G_j)$. Finally, $F_i \otimes G_j$ can be expressed with $\rightarrowtail\!\!\!\!\prec$ applications.

Next, let F be some (closed) frame polynomial. Using an innermost-outermost strategy, it follows that F satisfies the lemma: an argument of a ∂_H or t_I operation not containing these operations can by the above be replaced by one that satisfies the representation format. As $\otimes$ is then eliminated, the ∂_H or t_I operation can be 'pushed inside' by the axioms (FDH5), (FTI5), (FPDH) and (FPTI), and on atomic frames be eliminated by (FDH1–4) or (FTI1–4). ∎

4 Decidability

Theorem 4.1. *Equality between closed frame polynomials over* $\mathrm{ACF}_t(A, \gamma, V, \mathbb{S})$ *is decidable.*

For a proof, let the relation $\leq$ between frames, called *summand inclusion*, be defined by

$$X \leq Y \text{ iff } X \oplus Y = Y.$$

and let F, G be two frames. According to Theorem 3.1, F and G have normal forms, say

$$\textstyle\bigoplus_{i=1}^k \bigoplus_{x_1...x_l} F_i$$
$$\textstyle\bigoplus_{i=1}^m \bigoplus_{y_1...y_n} G_i$$

with F_i, G_i atomic, i.e. either of the form s or $s \xrightarrow{a} s'$ for $s, s' \in \mathbb{S}[V]$ and $a \in A_t$. Let

$\vec{x}$ abbreviate $x_1...x_l$, and $\vec{y}$ abbreviate $y_1...y_n$.

[1]Note that if we replace the state consisting of a single 0 by for instance $2 \rightarrowtail\!\!\!\!\prec 0$, the half-counter can be represented by a polynomial not containing $\rightarrowtail\!\!\!\!\prec$:

$$\begin{aligned} &(0 \otimes \textstyle\bigoplus_x(x \xrightarrow{a} S(x))) \\ \oplus\ &(1 \otimes \textstyle\bigoplus_x(S(x) \xrightarrow{a} x)) \\ \oplus\ &(0 \xrightarrow{b} 1 \otimes \textstyle\bigoplus_x(x)) \\ \oplus\ &((0 \xrightarrow{exit} 2) \otimes 0) \\ \oplus\ &((1 \xrightarrow{restart} 0) \otimes 0). \end{aligned}$$

Table 2: Additional axioms for frame polynomials, $H, I \subseteq A$ and $x, y \in V$.

(FP1)	$\bigoplus_x F$	$=$	F	provided x does not occur in F
(FP2)	$\bigoplus_y F$	$=$	$\bigoplus_x F[x/y]$	provided x does not occur in F
(FP3)	$\bigoplus_x \bigoplus_y F$	$=$	$\bigoplus_y \bigoplus_x F$	
(FPA1)	$\bigoplus_x (F \oplus F')$	$=$	$\bigoplus_x (F) \oplus \bigoplus_x (F')$	
(FPA2)	$\bigoplus_x F(x)$	$=$	$F[0/x] \oplus \bigoplus_x F[S(x)/x]$	
(FPC1)	$F \otimes \bigoplus_x (F')$	$=$	$\bigoplus_x (F \otimes F')$	provided x does not occur in F
(FPC2)	$\bigoplus_x (F') \otimes F$	$=$	$\bigoplus_x (F' \otimes F)$	provided x does not occur in F
(FPDH)	$\partial_H (\bigoplus_x (F))$	$=$	$\bigoplus_x (\partial_H (F))$	
(FPTI)	$t_I (\bigoplus_x (F))$	$=$	$\bigoplus_x (t_I (F))$	

For deciding equality, it suffices to decide for all $j \in \{1, ..., k\}$

$$\bigoplus_{\vec{x}} F_j \leq \bigoplus_{i=1}^{m} \bigoplus_{\vec{y}} G_i$$

and for all $j \in \{1, ..., m\}$

$$\bigoplus_{\vec{y}} G_j \leq \bigoplus_{i=1}^{k} \bigoplus_{\vec{x}} F_i.$$

By symmetry, we only need to show that the first summand inclusion is decidable. This is the case iff

$$\bigwedge_{j=1}^{k} \forall \vec{x} \exists \vec{y} \bigvee_{i=1}^{m} F_j(\vec{x}) \leq G_i(\vec{y}).$$

Any such conjunct can be decided upon as follows:

Fix some $j \in \{1, ..., k\}$. We distinguish two cases: $F_j = s$ and $F_j = s \xrightarrow{a} s'$ for some $s, s' \in \mathbb{S}[V]$ and $a \in A_t$.

In case $F_j = s$ for some $s \in \mathbb{S}[V]$, it suffices to decide whether the binary $\succ\!\!\prec$ tree representing an arbitrary instantiation of s (by $\forall x_1 ... x_l$) can be matched by one of the (abstract) states in one of $G_1, ..., G_m$. Let the auxiliary function symbol f represent the structure of s, i.e., $f(x_1, ..., x_l) = s$. Let all states of $G_1, ..., G_m$ (at most $2m$, say m') have state structure functions $g_1, ..., g_{m'}$. Then we have to decide

$$\forall \vec{x} \exists \vec{y} \bigvee_{i=1}^{m'} f(\vec{x}) = g_i(\vec{y}). \qquad (1)$$

In the case that $F_j = s \xrightarrow{a} s'$ for some $s, s' \in \mathbb{S}[V]$ and $a \in A_t$, let G_a be the polynomial obtained from G by deleting all G_i that do not represent an a-transition, and assume $G_a = \bigoplus_{i=1}^{m'} \bigoplus_{\vec{y}} G_i$. It is sufficient to decide whether

$$\bigoplus_{\vec{x}} F_j \leq \bigoplus_{i=1}^{m'} \bigoplus_{\vec{y}} G_i.$$

This reduces the question to whether each instantiation of s and s' can be matched by a *single* G_i. To phrase this more formally, let f, f' be the state structure functions of s and s', respectively and let g_i, g'_i be those of G_i, i.e.,

$$G_i = g_i(\vec{y}) \xrightarrow{a} g'_i(\vec{y}).$$

Then the decidability reduces to that of

$$\forall \vec{x} \exists \vec{y} \bigvee_{i=1}^{m'} f(\vec{x}) = g_i(\vec{y}) \wedge f'(\vec{x}) = g'_i(\vec{y}). \qquad (2)$$

Now both (1) and (2) relate to *Presburger Arithmetic* (without having the $+$ on $\mathbb{N}$, see [Pre29]). Because Presburger Arithmetic is decidable ([Pre29]), we find that (1) and (2) are decidable, and hence that equality between (closed) frame polynomials is as well.

5 Adding Addition

Adding $+$ to $\mathbb{N}$ preserves the decidability result (now fully exploiting the decidability of Presburger arithmetic).

However, with $+$ the expressivity increases. In order to prove this, we shall give an argument on the structure of frames. Let the *in-degree* of a state of any frame be the number of ingoing transitions.

Lemma 5.1. *A closed frame polynomial F in normal form that does not contain $+$, specifies a frame of which the in-degree of each state is either ω, or polynomial in the length of F.*

Proof. Assume

$$F = \bigoplus_{i=1}^{k} \bigoplus_{x_1 \ldots x_l} F_i$$

with all F_i atomic. The in-degree of each state of one of the k summands $\bigoplus_{x_1 \ldots x_l} F_i$ is either 0, 1 or ω. This follows by case distinction on the structure of the atomic frames F_i:

Case $s \in \mathbb{S}[V]$. Then the in-degree of each s instance is 0.

Case $s \xrightarrow{a} s'$ and $\mathrm{FV}(s) \setminus \mathrm{FV}(s') = \emptyset$. Then the in-degree of each s instance is 0, and of each s' instance is 1.

Case $s \xrightarrow{a} s'$ and $\mathrm{FV}(s) \setminus \mathrm{FV}(s') \neq \emptyset$. Then any $\mathrm{FV}(s')$ instance has in-degree ω due to all $\mathrm{FV}(s) \setminus \mathrm{FV}(s')$ variables.

So, by $\bigoplus_{i=1}^{k}$ defined as set-theoretic union, we see that the in-degree of each state in F is an element of $\{0, ..., k\}$ or ω. ∎

Theorem 5.2. *Adding $+$ to $\mathbb{N}$ increases the expressivity of* $\mathrm{ACF}_t(A, \gamma, V, \mathbb{S})$.

Proof. Let F be defined by

$$\bigoplus_{x,y} (x \succ\!\!\prec y \xrightarrow{a} x + y)$$

(recall that the states of F are numerals $S(...S(0)...)$ or $\succ\!\!\prec$ combinations of these). Clearly F has arbitrary large, finite in-degrees. Assume $F = G$ with G not containing $+$. Then by Theorem 3.1, $F = G'$ with G' in normal form and not containing $+$. By the lemma above, this contradicts the assumption. ∎

6 Undecidability Results

Equality between frames with states over the full language of number theory (i.e. with multiplication) is not decidable. This can be seen as follows: let $P(y)$ be an undecidable, arithmetical predicate:

$$P(y) \stackrel{\text{def}}{=} \exists \bar{x}\ (p_1(\bar{x}) = p_2(\bar{x}, y))$$

for certain polynomials p_1, p_2 with positive, integer coefficients.[2] Define a frame $G(y)$ by

$$G(y) = \bigoplus_{\bar{x}} p_1(\bar{x}) \xrightarrow{a} p_2(\bar{x}, y).$$

Clearly, $G(y)$ has a transition $n \xrightarrow{a} n$ if and only if $P(y)$ holds. Next define

$$F = \bigoplus_{nm} ((n \xrightarrow{a} n + S(m)) \oplus (n + S(m) \xrightarrow{a} n)).$$

Note that for all $n, m \in \mathbb{N}$, the frame F has transitions $n \xrightarrow{a} m$ for all $n \neq m$, and no transition $n \xrightarrow{a} n$. Hence

$$F = F \oplus G(y) \iff \neg P(y)$$

or, in other words: frame equality is reduced to solving an undecidable problem. Replacing multiplication and its axioms by the unary operation symbol K denoting the operation of squaring a number, and the axioms

$$K(0) = 0$$
$$K(S(x)) = K(x) + S(x + x)$$

one can define multiplication by

$$u = y \cdot z \longleftrightarrow (u + u) + (K(y) + K(z)) = K(y + z)$$

(cf. [Tar53]), and hence the undecidability result is preserved in this setting.

Furthermore, we state without proof that isomorphy is undecidable for frames, even in the case that $+$ and $\cdot$ are not added to the signature.

7 Conclusions

Instead of adding $+$, one might imagine the atomic states to be generated by a finite number of successor functions $S_1, ..., S_k$ and generalized frame sum having its parameter ranging over $\{1, ..., n\}^*$. This allows a more expressive notation, generalizing the one above and leading to similar representation and decidability results, now based on the decidability result of Büchi [Buc62].

[2] In [Mat70], the existence of such a predicate is proved.

References

[BBK87] J.C.M. Baeten, J.A. Bergstra, and J.W. Klop. On the consistency of Koomen's fair abstraction rule. *Theoretical Computer Science*, 51(1/2):129–176, 1987.

[BW90] J.C.M. Baeten and W.P. Weijland. *Process Algebra.* Cambridge Tracts in Theoretical Computer Science 18. Cambridge University Press, 1990.

[Ber89] J.A. Bergstra. Algebra of states and transitions. Report P8909, Programming Research Group, University of Amsterdam, 1989.

[Buc62] J.R. Büchi. On a decision method in restricted second order arithmetic. *Logic, Methodology and Philosophy of Science*, Proceedings 1960 International Congress (E. Nagel, P. Suppes and A. Tarski, editors.), Stanford University Press, 1–11, 1962.

[Buc89] J.R. Büchi. *Finite Automata, Their Algebras and Grammars.* Edited by D. Siefkes. Springer-Verlag, 1989.

[Eil74] S. Eilenberg. *Automata, Languages and Machines* (Vol. A). Academic Press, 1974.

[GV92] J.F. Groote and F.W. Vaandrager. Structured operational semantics and bisimulation as a congruence. *Information and Computation*, 100(2):202–260, October 1992.

[Mat70] J.V. Matijasevič. Enumerable sets are diophantine. *Soviet Math. Dokl.*, 11:354–358, 1970.

[Plo81] G.D. Plotkin. A structural approach to operational semantics. Report DAIMI FN-19, Computer Science Department, Aarhus University, 1981.

[Pre29] M. Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. *Congr. Math. des Pays Slaves, Warsaw*, 1: 92–101, 1929.

[RS59] M.O. Rabin and D. Scott. Finite automata and their decision problems. *IBM Journal of Research and Development*, 3(2):114–125, 1959.

[Sim85] R. de Simone. Higher-level synchronising devices in MEIJE–SCCS. *Theoretical Computer Science*, 37:245–267, 1985.

[Tar53] A. Tarski, in collaboration with A. Mostowski and R.M. Robinson. *Undecidable Theories.* Studies in Logic and the Foundations of Mathematics. North-Holland, 1953.

[Vaa93] F.W. Vaandrager. Expressiveness results for process algebras. In J.W. de Bakker, W.P. de Roever, and G. Rozenberg, editors, *Proceedings REX Workshop on Semantics: Foundations and Applications,* Beekbergen, The Netherlands, June 1992, volume 666 of *Lecture Notes in Computer Science*, pages 609–638. Springer-Verlag, 1993.