February 13, 2003 Technical Report WV-2003-05

The Undecidability of System NEL

Lutz Straßburger
Technische Universität Dresden
Fakultät Informatik - 01062 Dresden - Germany
lutz.strassburger@inf.tu-dresden.de

Abstract *System* NEL *is a conservative extension of multiplicative exponential linear logic* (MELL) *by a self-dual non-commutative connective called* seq *which lives between the* par *and the* times*. In this paper, I will show that system* NEL *is undecidable by encoding two counter machines into* NEL*. Although the encoding is quite simple, the proof of the faithfulness is a little intricate because there is no sequent calculus and no phase semantics available for* NEL*.*

1 Introduction

Since the beginning of linear logic [5], the complexity of the provability problem of its fragments has been studied. The multiplicative fragment is NP-complete [12], the multiplicative additive fragment is PSPACE-complete and full propositional linear logic is undecidable [19]. The decidablility of the multiplicative exponential fragment (MELL) is still an open problem. However, in in a purely non-commutative setting, i.e. in the presence of two mutually dual non-commutative connectives, the multiplicatives and the exponentials are sufficient to get undecidability [19].

In this paper, I will address the decidability question for a mixed commutative and non-commutative system in which there is only a single self-dual non-commutative connective. I will show that also in this case, the multiplicatives and the exponentials alone are sufficient to get undecidability, as it has been conjectured in [8]. For showing this, Guglielmi proposes in [6] an encoding of Post's correspondence problem, which makes the non-commutativity correspond to sequential composition of words. However, I will here use an encoding of two counter machines because it is much simpler. If it turns out that MELL is decidable (as many believe), then the border to undecidability is crossed by this new self-dual non-commutative connective. Such a connective did first occur in Retoré's pomset logic [22] and has then been rediscovered in Guglielmi's system BV [7]. It is conjectured that the two logics are the same, but the proof of this is not yet complete. The new non-commutative connective is important for applications in linguistics as well as in concurrency. Because of the self-duality it corresponds quite well to the notion of sequentiality in many process algebras. For example in [3] Bruscoli shows the correspondence to prefixing in CCS [20].

In the following, I will first (in Section 2) introduce system NEL [9], which is a conservative extension of MELL plus *mix* [4] plus *nullary mix* [1] by a self-dual non-commutative connective called *seq* [7]. It has been shown by Tiu in [24] that a logic containing that connective cannot be presented in the sequent calculus because deep rewriting is crucial for reasoning with *seq*. For that reason, I will use here the *calculus of structures* [8, 2], which is a generalisation of the one-sided sequent calculus. Rules do not work on sequents but on structures, which are intermediate expressions between formulae and sequents.

Then, in Section 3, I will introduce two counter machines [21, 18] and show in Section 4 how they are encoded in system NEL. The encoding is pretty much inspired by [14], and the proof of its completeness is an easy exercise (done in Section 5).

However, the proof of the faithfulness of the encoding is quite different from what has been done so far. There are two reasons for this: First, the simple way of extracting the computation sequence of the machine from the proof of the encoding, as done in [19, 13] for full linear logic, is not possible because the calculus of structures allows much more freedom in applying and permuting rules than the sequent calculus. And second, the use of phase spaces [5], as it has been done in [16, 17, 14] is not possible because (so far) there is no phase semantics available for NEL.

The method I will use instead is the following. The given proof in system NEL of an encoding of a two-counter machine is first transformed into a certain normal form, which allows to remove the exponentials. The resulting proof in the multiplicative fragment has as conlusion a structure which has the shape of what I call a *weak encoding*. From this proof I will extract the first computation step of the machine and another proof (in the multiplicative fragment) which has as conlusion again a weak encoding. By an inductive argument it is then possible to obtain the whole computation sequence. For this, I will first discuss the multiplicative fragment (namely Guglielmi's system BV [7, 8]) in Section 6, and then show the full proof in Section 7.

2 System NEL

In order to present a system in the calculus of structures, we first need to define a language of structures, in the same way as we need to define a language of formulae when presenting a system in the sequent calculus or natural deduction.

2.1 Definition There are countably many *positive* and *negative atoms*. They, positive or negative, are denoted by a, b, c, d, o, p and q. *Structures* are denoted by S, P, Q, R, T, U, V, W, X and Z. The structures of the *language* NEL are generated by

$$S ::= a \mid \circ \mid [\underbrace{S,\ldots,S}_{>0}] \mid (\underbrace{S,\ldots,S}_{>0}) \mid \langle\underbrace{S;\ldots;S}_{>0}\rangle \mid ?S \mid !S \mid \bar{S} \quad ,$$

where $\circ$, the *unit*, is not an atom; $[S_1,\ldots,S_h]$ is a *par structure*, $(S_1,\ldots,S_h)$ is a *times structure*, $\langle S_1;\ldots;S_h\rangle$ is a *seq structure*, $?S$ is a *why-not structure* and $!S$ is an *of-course structure*; $\bar{S}$ is the *negation* of the structure S. Structures with a hole that does not appear in the scope of a negation are denoted by $S\{\ \}$. The structure R is a *substructure* of $S\{R\}$, and $S\{\ \}$ is its *context*. I will simplify the indication of context in cases where structural parentheses fill the hole exactly: for example, $S[R,T]$ stands for $S\{[R,T]\}$.

Associativity

$$[\vec{R},[\vec{T}],\vec{U}] = [\vec{R},\vec{T},\vec{U}]$$
$$(\vec{R},(\vec{T}),\vec{U}) = (\vec{R},\vec{T},\vec{U})$$
$$\langle\vec{R};\langle\vec{T}\rangle;\vec{U}\rangle = \langle\vec{R};\vec{T};\vec{U}\rangle$$

Commutativity

$$[\vec{R},\vec{T}] = [\vec{T},\vec{R}]$$
$$(\vec{R},\vec{T}) = (\vec{T},\vec{R})$$

Unit

$$[\circ,\vec{R}] = [\vec{R}]$$
$$(\circ,\vec{R}) = (\vec{R})$$
$$\langle\circ;\vec{R}\rangle = \langle\vec{R}\rangle$$
$$\langle\vec{R};\circ\rangle = \langle\vec{R}\rangle$$

Singleton

$$[R] = (R) = \langle R\rangle = R$$

Exponentials

$$?\circ = \circ$$
$$!\circ = \circ$$
$$??R = ?R$$
$$!!R = !R$$

Negation

$$\overline{\circ} = \circ$$
$$\overline{[R_1,\dots,R_h]} = (\bar{R}_1,\dots,\bar{R}_h)$$
$$\overline{(R_1,\dots,R_h)} = [\bar{R}_1,\dots,\bar{R}_h]$$
$$\overline{\langle R_1;\dots;R_h\rangle} = \langle\bar{R}_1;\dots;\bar{R}_h\rangle$$
$$\overline{?R} = !\bar{R}$$
$$\overline{!R} = ?\bar{R}$$
$$\bar{\bar{R}} = R$$

Contextual Closure

if $R = T$ then $S\{R\} = S\{T\}$

Figure 1: Basic equations for the syntactic equivalence =

Structures come with equational theories establishing some basic, decidable algebraic laws by which structures are indistinguishable. These are analogous to the laws of associativity, commutativity, idempotency, and so on, usually imposed on sequents. The difference is the notions of formula and sequent are merged and the equations are extended to formulae. The structures of the language NEL are equivalent modulo the relation =, defined in Figure 1. There, $\vec{R}$, $\vec{T}$ and $\vec{U}$ stand for finite, non-empty sequences of structures (sequences may contain ',' or ';' separators as appropriate in the context).

There is a straightforward two-way correspondence between structures not involving seq and formulae of MELL. For example $![(?a,b),\bar{c},!\bar{d}]$ corresponds to $!((?a \otimes b) \parr c^{\perp} \parr !d^{\perp})$, and vice versa. Units are mapped into $\circ$, since $1 \equiv \perp$, when mix and mix0 are added to MELL.

The next step in defining a system is to show the inference rules. In the calculus of structures, an (*inference*) *rule* is a scheme $\rho\,\frac{T}{R}$, where ρ is the *name* of the rule, T is its *premise* and R is its *conclusion*. If a rule ρ has no premise, then it is called an *axiom*. Observe that contrary to the sequent calculus, all

$$\circ\!\downarrow \frac{}{\circ} \qquad \mathsf{ai}\!\downarrow \frac{S\{\circ\}}{S[a,\bar{a}]} \qquad \mathsf{s}\, \frac{S([R,U],T)}{S[(R,T),U]} \qquad \mathsf{q}\!\downarrow \frac{S\langle [R,U];[T,V]\rangle}{S[\langle R;T\rangle,\langle U;V\rangle]}$$

$$\mathsf{p}\!\downarrow \frac{S\{![R,T]\}}{S[!R,?T]} \qquad \mathsf{w}\!\downarrow \frac{S\{\circ\}}{S\{?R\}} \qquad \mathsf{b}\!\downarrow \frac{S[?R,R]}{S\{?R\}}$$

Figure 2: System NEL

rules have at most one premise.

A (*formal*) *system*, denoted by $\mathscr{S}$, is a set of rules. A *derivation* in a system $\mathscr{S}$ is a finite sequence of instances of rules of $\mathscr{S}$, and is denoted by Δ; a derivation can consist of just one structure. The topmost structure in a derivation is called its *premise*; the bottommost structure is called *conclusion*. A derivation Δ whose premise is T, conclusion is R, and whose rules are in $\mathscr{S}$ is denoted by $\begin{array}{c} T \\ \mathscr{S}\|\Delta \\ R \end{array}$. A derivation with no premise is called a *proof*, denoted by Π. A system $\mathscr{S}$ *proves* R if there is in the system $\mathscr{S}$ a proof Π whose conclusion is R, written $\begin{array}{c} \mathscr{S}|\!|\!|\Pi \\ R \end{array}$. The rules of *system* NEL are shown in Figure 2.

The inference rules of NEL (except for the axiom) are all of the kind $\rho\,\dfrac{S\{T\}}{S\{R\}}$. This rule scheme specifies that if a structure matches R, in a context $S\{\ \}$, it can be rewritten as specified by T, in the same context $S\{\ \}$ (or vice versa if one reasons top-down).

2.2 Example Here is an example for a proof in system NEL:

$$\mathsf{w}\!\downarrow \dfrac{\mathsf{q}\!\downarrow \dfrac{\mathsf{q}\!\downarrow \dfrac{\mathsf{ai}\!\downarrow \dfrac{\mathsf{ai}\!\downarrow \dfrac{\mathsf{ai}\!\downarrow \dfrac{\circ\!\downarrow \dfrac{}{\circ}}{[a,\bar{a}]}}{\langle [a,\bar{a}];[b,\bar{b}]\rangle}}{\langle [a,\bar{a}];[b,\bar{b}];[c,\bar{c}]\rangle}}{\langle [a,\bar{a}];[\langle b;c\rangle,\langle \bar{b};\bar{c}\rangle]\rangle}}{[\langle a;b;c\rangle,\langle \bar{a};\bar{b};\bar{c}\rangle]}}{[?(\langle c;d\rangle,\bar{c}),\langle a;b;c\rangle,\langle \bar{a};\bar{b};\bar{c}\rangle]} \quad .$$

For system NEL, the cut rule has the following shape

$$\mathsf{i}\!\uparrow \frac{S(R,\bar{R})}{S\{\circ\}} \quad .$$

2.3 Theorem (Cut elimination) *The rule* $\mathsf{i}{\uparrow}$ *is admissible for system* NEL*, in other words, for every proof* $\begin{array}{c}\Pi \| \mathsf{NEL}\cup\{\mathsf{i}{\uparrow}\} \\ R\end{array}$ *, there is a proof* $\begin{array}{c}\Pi' \| \mathsf{NEL} \\ R\end{array}$ *.*

For a proof of that result and a more detailed discussion on the proof theory of NEL, the reader is referred to [9]. For the precise relation between NEL and linear logic, the reader should consult [23] and [7].

3 Two Counter Machines

Two counter machines have been introduced by Minsky in [21] as two tape non-writing Turing machines. He showed that any (usual) Turing machine can be simulated on a two counter machine. In [18], Lambek showed that any recursive function can be computed by an n counter machine, for some number $n \in \mathbf{N}$.

3.1 Definition A *two counter machine* $\mathcal{M}$ is a tuple $(\mathcal{Q}, q_0, n_0, m_0, q_f, \mathscr{T})$, where $\mathcal{Q}$ is a finite set of *states*, $q_0 \in \mathcal{Q}$ is called the *initial state*, $q_f \in \mathcal{Q}$ is called the *final state*, the numbers $n_0, m_0 \in \mathbf{N}$ represent the initial positions of the heads on the two tapes, and $\mathscr{T} \subseteq \mathcal{Q} \times I \times \mathcal{Q}$ is a finite set of *transitions*, where

$$I = \{\mathsf{inc1}, \mathsf{dec1}, \mathsf{zero1}, \mathsf{inc2}, \mathsf{dec2}, \mathsf{zero2}\}$$

is the set of possible *instructions*. A *configuration* of $\mathcal{M}$ is given by a tuple (q, n, m), where $q \in \mathcal{Q}$ is a state and n and m are natural numbers. The configuration (q_0, n_0, m_0) is called *initial configuration*. A configuration (q', n', m') is *reachable in one step* from a configuration (q, n, m), written as $(q, n, m) \to (q', n', m')$, if one of the following six cases holds:

$$\begin{array}{rlll}
(q, \mathsf{inc1}, q') \in \mathscr{T} & \text{and} \quad n' = n + 1 & \text{and} & m' = m \quad , \\
(q, \mathsf{dec1}, q') \in \mathscr{T} & \text{and} \quad n > 0, \quad n' = n - 1 & \text{and} & m' = m \quad , \\
(q, \mathsf{zero1}, q') \in \mathscr{T} & \text{and} \quad n' = n = 0 & \text{and} & m' = m \quad , \\
(q, \mathsf{inc2}, q') \in \mathscr{T} & \text{and} \quad n' = n & \text{and} & m' = m + 1 \quad , \\
(q, \mathsf{dec2}, q') \in \mathscr{T} & \text{and} \quad n' = n & \text{and} & m > 0, \quad m' = m - 1 \quad , \\
(q, \mathsf{zero2}, q') \in \mathscr{T} & \text{and} \quad n' = n & \text{and} & m' = m = 0 \quad .
\end{array}$$

A configuration (q', n', m') is *reachable in r steps* from a configuration (q, n, m), written as $(q, n, m) \to^r (q', n', m')$, if

- $r = 0$ and $(q', n', m') = (q, n, m)$ or
- $r \geqslant 1$ and there is a configuration (q'', n'', m'') such that $(q, n, m) \to (q'', n'', m'')$ and $(q'', n'', m'') \to^{r-1} (q', n', m')$.

A configuration (q', n', m') is *reachable* from a configuration (q, n, m), written as $(q, n, m) \to^* (q', n', m')$, if there is an $r \in \mathbf{N}$ such that $(q, n, m) \to^r (q', n', m')$. In other words, the relation $\to^*$ is the reflexive and transitive closure of $\to$. A two counter machine $\mathcal{M} = (\mathcal{Q}, q_0, n_0, m_0, q_f, \mathscr{T})$ *accepts* a configuration (q, n, m), if $(q, n, m) \to^* (q_f, 0, 0)$.

3.2 Example The running example in this paper will be the following

$$\begin{array}{rcl} \mathcal{M} & = & (\{q_0, q_1, q_2\}, q_0, 1, 0, q_1, \mathscr{T}) \quad \text{, where} \\ \mathscr{T} & = & \{(q_0, \mathsf{dec2}, q_2), (q_1, \mathsf{dec1}, q_1), (q_0, \mathsf{zero2}, q_1)\} \quad . \end{array}$$

The machine accepts for example the configuration $(q_0, 8, 0)$, because $(q_0, 8, 0) \to (q_1, 8, 0) \to^8 (q_1, 0, 0)$. More precisely, it accepts any configuration $(q_0, n, 0)$ for $n \geqslant 0$. In particular it also accepts its initial configuration $(q_0, 1, 0)$.

3.3 Theorem *In general, it is undecidable whether a two counter machine accepts its initial configuration.*

3.4 Remark In Definition 3.1, I defined two counter machines to have only one final state, whereas in the standard textbook definition [21, 11, 15], they might have many final states. But this is not a problem, since any two counter machine $\mathcal{M}$ with many final states $q_{f1}, \dots, q_{fn}$ can be transformed into a two counter machine $\mathcal{M}'$ that has only one final state and that accepts the same configurations, by adding a new state q_f (which will be the new final state) and a transition $(q_{fi}, \mathsf{zero2}, q_f)$ for each $i = 1, \dots, n$.

4 Encoding Two Counter Machines in NEL

Let a be an atom and $n \in \mathbf{N}$. Then a^n denotes the structure $\langle a; a; \dots; a\rangle$ with n copies of a. More precisely, $a^0 = \circ$ and $a^n = \langle a^{n-1}; a\rangle$, for $n \geqslant 1$.

4.1 Encoding Let a two counter machine $\mathcal{M} = (\mathcal{Q}, q_0, n_0, m_0, q_f, \mathscr{T})$ be given. For each state $q \in \mathcal{Q}$, I will introduce a fresh atom, also denoted by q. Further, I will need four atoms a, b, c and d. Without loss of generality, let $\mathcal{Q} = \{q_0, q_1, \dots, q_z\}$ for some $z \geqslant 0$. Then $q_f = q_i$ for some $i \in \{0, \dots, z\}$. A configuration (q, n, m) will be encoded by the structure $\langle b; a^n; q; c^m; d\rangle$. Since $\mathscr{T}$ is finite, we have $\mathscr{T} = \{t_1, t_2, \dots, t_h\}$ for some $h \in \mathbf{N}$ (if $\mathscr{T} = \varnothing$, then $h = 0$). For each $k \in \{1, \dots, h\}$, I will define the structure T_k, that encodes the transition t_k, as follows. For all $i, j \in \{0, \dots, z\}$,

$$\begin{array}{llll} \text{if} & t_k = (q_i, \mathsf{inc1}, q_j)\ , & \text{then} & T_k = (\bar{q}_i, \langle a; q_j\rangle) \quad , \\ \text{if} & t_k = (q_i, \mathsf{dec1}, q_j)\ , & \text{then} & T_k = (\langle \bar{a}; \bar{q}_i\rangle, q_j) \quad , \\ \text{if} & t_k = (q_i, \mathsf{zero1}, q_j), & \text{then} & T_k = (\langle \bar{b}; \bar{q}_i\rangle, \langle b; q_j\rangle) \quad , \\ \text{if} & t_k = (q_i, \mathsf{inc2}, q_j)\ , & \text{then} & T_k = (\bar{q}_i, \langle q_j; c\rangle) \quad , \\ \text{if} & t_k = (q_i, \mathsf{dec2}, q_j)\ , & \text{then} & T_k = (\langle \bar{q}_i; \bar{c}\rangle, q_j) \quad , \\ \text{if} & t_k = (q_i, \mathsf{zero2}, q_j), & \text{then} & T_k = (\langle \bar{q}_i; \bar{d}\rangle, \langle q_j; d\rangle) \quad . \end{array}$$

I will say that a structure T *encodes* a transition of $\mathcal{M}$, if $T = T_k$ for some $k \in \{1, \dots, h\}$. The machine $\mathcal{M}$ is then encoded by the structure

$$\mathcal{M}_{\text{enc}} = [?T_1, \dots, ?T_h, \langle b; a^{n_0}; q_0; c^{m_0}; d\rangle, \langle \bar{b}; \bar{q}_f; \bar{d}\rangle] \quad ,$$

which is called the *encoding* of $\mathcal{M}$.

4.2 Example The machine in Example 3.2 is encoded by the structure

$$\mathcal{M}_{\text{enc}} = [?(\langle \bar{q}_0; \bar{c} \rangle, q_2), ?(\langle \bar{a}; \bar{q}_1 \rangle, q_1), ?(\langle \bar{q}_0; \bar{d} \rangle, \langle q_1; d \rangle), \langle b; a; q_0; d \rangle, \langle \bar{b}; \bar{q}_1; \bar{d} \rangle] \quad .$$

The remaining two sections are devoted to the proof of the following:

4.3 Theorem *A two counter machine $\mathcal{M}$ accepts its initial configuration if and only if its encoding $\mathcal{M}_{\text{enc}}$ is provable in* NEL*.*

The main result of this paper is an immediate consequence:

4.4 Corollary *Provability in system* NEL *is undecidable.*

5 Completeness of the Encoding

5.1 Lemma *Given a two counter machine $\mathcal{M} = (\mathcal{Q}, q_0, n_0, m_0, q_f, \mathscr{T})$.*

$$\textit{If} \quad (q_i, n, m) \to (q_j, n', m') \quad \textit{then} \quad \begin{array}{c} [?T_1, \ldots, ?T_h, \langle b; a^{n'}; q_j; c^{m'}; d \rangle, \langle \bar{b}; \bar{q}_f; \bar{d} \rangle] \\ \Vert \mathsf{NEL} \\ [?T_1, \ldots, ?T_h, \langle b; a^{n}; q_i; c^{m}; d \rangle, \langle \bar{b}; \bar{q}_f; \bar{d} \rangle] \end{array} \quad .$$

Proof: There are six possible cases how the machine $\mathcal{M}$ can go from (q_i, n, m) to (q_j, n', m'):

- The first counter has been incremented: $(q_i, \mathtt{inc1}, q_j) \in \mathscr{T}$ and $n' = n + 1$ and $m' = m$. Then we have $T_k = (\bar{q}_i, \langle a; q_j \rangle)$ for some $k \in \{1, \ldots, h\}$. Now use

$$\begin{array}{rc}
 & [?T_1, \ldots, ?T_h, \langle b; a^{n+1}; q_j; c^m; d \rangle, \langle \bar{b}; \bar{q}_f; \bar{d} \rangle] \\ \hline
\mathsf{ai}\downarrow & [?T_1, \ldots, ?T_h, \langle b; a^{n}; ([\bar{q}_i, q_i], \langle a; q_j \rangle); c^m; d \rangle, \langle \bar{b}; \bar{q}_f; \bar{d} \rangle] \\ \hline
\mathsf{s} & [?T_1, \ldots, ?T_h, \langle b; a^{n}; [(\bar{q}_i, \langle a; q_j \rangle), q_i]; c^m; d \rangle, \langle \bar{b}; \bar{q}_f; \bar{d} \rangle] \\ \hline
\mathsf{q}\downarrow & [?T_1, \ldots, ?T_h, \langle [(\bar{q}_i, \langle a; q_j \rangle), \langle b; a^{n}; q_i \rangle]; c^m; d \rangle, \langle \bar{b}; \bar{q}_f; \bar{d} \rangle] \\ \hline
\mathsf{q}\downarrow & [?T_1, \ldots, ?T_h, (\bar{q}_i, \langle a; q_j \rangle), \langle b; a^{n}; q_i; c^m; d \rangle, \langle \bar{b}; \bar{q}_f; \bar{d} \rangle] \\ \hline
\mathsf{b}\downarrow & [?T_1, \ldots, ?T_h, \langle b; a^{n}; q_i; c^m; d \rangle, \langle \bar{b}; \bar{q}_f; \bar{d} \rangle]
\end{array} \quad .$$

- The first counter has been decremented: $(q_i, \mathtt{dec1}, q_j) \in \mathscr{T}$ and $n > 0$ and $n' = n - 1$ and $m' = m$. Then we have $T_k = (\langle \bar{a}; \bar{q}_i \rangle, q_j)$ for some $k \in \{1, \ldots, h\}$. Now use

$$\begin{array}{rc}
 & [?T_1, \ldots, ?T_h, \langle b; a^{n-1}; q_j; c^m; d \rangle, \langle \bar{b}; \bar{q}_f; \bar{d} \rangle] \\ \hline
\mathsf{ai}\downarrow & [?T_1, \ldots, ?T_h, \langle b; a^{n-1}; ([\bar{q}_i, q_i], q_j); c^m; d \rangle, \langle \bar{b}; \bar{q}_f; \bar{d} \rangle] \\ \hline
\mathsf{ai}\downarrow & [?T_1, \ldots, ?T_h, \langle b; a^{n-1}; (\langle [\bar{a}, a]; [\bar{q}_i, q_i] \rangle, q_j); c^m; d \rangle, \langle \bar{b}; \bar{q}_f; \bar{d} \rangle] \\ \hline
\mathsf{q}\downarrow & [?T_1, \ldots, ?T_h, \langle b; a^{n-1}; ([\langle \bar{a}; \bar{q}_i \rangle, \langle a; q_i \rangle], q_j); c^m; d \rangle, \langle \bar{b}; \bar{q}_f; \bar{d} \rangle] \\ \hline
\mathsf{s} & [?T_1, \ldots, ?T_h, \langle b; a^{n-1}; [(\langle \bar{a}; \bar{q}_i \rangle, q_j), \langle a; q_i \rangle]; c^m; d \rangle, \langle \bar{b}; \bar{q}_f; \bar{d} \rangle] \\ \hline
\mathsf{q}\downarrow & [?T_1, \ldots, ?T_h, \langle [(\langle \bar{a}; \bar{q}_i \rangle, q_j), \langle b; a^{n}; q_i \rangle]; c^m; d \rangle, \langle \bar{b}; \bar{q}_f; \bar{d} \rangle] \\ \hline
\mathsf{q}\downarrow & [?T_1, \ldots, ?T_h, (\langle \bar{a}; \bar{q}_i \rangle, q_j), \langle b; a^{n}; q_i; c^m; d \rangle, \langle \bar{b}; \bar{q}_f; \bar{d} \rangle] \\ \hline
\mathsf{b}\downarrow & [?T_1, \ldots, ?T_h, \langle b; a^{n}; q_i; c^m; d \rangle, \langle \bar{b}; \bar{q}_f; \bar{d} \rangle]
\end{array} \quad .$$

- The first counter has been tested for zero: $(q_i, \mathsf{zero1}, q_j) \in \mathscr{T}$ and $n = n' = 0$ and $m' = m$. Then we have $T_k = (\langle \bar{b}; \bar{q}_i\rangle, \langle b; q_j\rangle)$ for some $k \in \{1, \ldots, h\}$. Now use

$$
\begin{array}{rc}
 & [?T_1,\ldots,?T_h,\langle b;q_j;c^m;d\rangle,\langle\bar b;\bar q_f;\bar d\rangle] \\ \hline
\mathsf{ai}\!\downarrow & [?T_1,\ldots,?T_h,\langle([\bar q_i,q_i],\langle b;q_j\rangle);c^m;d\rangle,\langle\bar b;\bar q_f;\bar d\rangle] \\ \hline
\mathsf{ai}\!\downarrow & [?T_1,\ldots,?T_h,\langle(\langle[\bar b,b];[\bar q_i,q_i]\rangle,\langle b;q_j\rangle);c^m;d\rangle,\langle\bar b;\bar q_f;\bar d\rangle] \\ \hline
\mathsf{q}\!\downarrow & [?T_1,\ldots,?T_h,\langle([\langle\bar b;\bar q_i\rangle,\langle b;q_i\rangle],\langle b;q_j\rangle);c^m;d\rangle,\langle\bar b;\bar q_f;\bar d\rangle] \\ \hline
\mathsf{s} & [?T_1,\ldots,?T_h,\langle[(\langle\bar b;\bar q_i\rangle,\langle b;q_j\rangle),\langle b;q_i\rangle];c^m;d\rangle,\langle\bar b;\bar q_f;\bar d\rangle] \\ \hline
\mathsf{q}\!\downarrow & [?T_1,\ldots,?T_h,(\langle\bar b;\bar q_i\rangle,\langle b;q_j\rangle),\langle b;q_i;c^m;d\rangle,\langle\bar b;\bar q_f;\bar d\rangle] \\ \hline
\mathsf{b}\!\downarrow & [?T_1,\ldots,?T_h,\langle b;q_i;c^m;d\rangle,\langle\bar b;\bar q_f;\bar d\rangle]
\end{array}
\quad .
$$

The other three cases (where the second counter is concerned) are similar. □

Now we can prove the first direction of Theorem 4.3.

5.2 Proposition *Given a two counter machine $\mathcal{M} = (\mathcal{Q}, q_0, n_0, m_0, q_f, \mathscr{T})$.*

$$\textit{If} \quad (q_0, n_0, m_0) \to^* (q_f, 0, 0) \quad \textit{then} \quad \begin{array}{c} -\!\!\!\Vert\, \mathsf{NEL} \\ \mathcal{M}_{\mathrm{enc}} \end{array} \quad .$$

Proof: Use

$$
\begin{array}{c}
\Pi \,\Vert\, \mathsf{NEL} \\
[?T_1,\ldots,?T_h,\langle b;q_f;d\rangle,\langle\bar b;\bar q_f;\bar d\rangle] \\
\Delta \,\Vert\, \mathsf{NEL} \\
[?T_1,\ldots,?T_h,\langle b;a^{n_0};q_0;c^{m_0};d\rangle,\langle\bar b;\bar q_f;\bar d\rangle]
\end{array}
\quad ,
$$

where Δ is obtained from Lemma 5.1 by an easy inductive argument and Π exists trivially (cf. Example 2.2). □

5.3 Example The proof of the encoding in Example 4.2 has the following shape:

$$
\begin{array}{c}
-\!\!\!\Vert\, \mathsf{NEL} \\
[?(\langle\bar q_0;\bar c\rangle,q_2),?(\langle\bar a;\bar q_1\rangle,q_1),?(\langle\bar q_0;\bar d\rangle,\langle q_1;d\rangle),\langle b;q_1;d\rangle,\langle\bar b;\bar q_1;\bar d\rangle] \\
\Vert\, \mathsf{NEL} \\
[?(\langle\bar q_0;\bar c\rangle,q_2),?(\langle\bar a;\bar q_1\rangle,q_1),?(\langle\bar q_0;\bar d\rangle,\langle q_1;d\rangle),\langle b;a;q_1;d\rangle,\langle\bar b;\bar q_1;\bar d\rangle] \\
\Vert\, \mathsf{NEL} \\
[?(\langle\bar q_0;\bar c\rangle,q_2),?(\langle\bar a;\bar q_1\rangle,q_1),?(\langle\bar q_0;\bar d\rangle,\langle q_1;d\rangle),\langle b;a;q_0;d\rangle,\langle\bar b;\bar q_1;\bar d\rangle]
\end{array}
$$

6 Some Facts about System BV

In order to show the other direction, I need first to establish some properties of the multiplicative fragment of system NEL. That fragment is called system BV [8, 7] and is shown in Figure 3.

One important result about this logic is Guglielmi's *Splitting Lemma*:

$$\circ\!\downarrow \frac{}{\circ} \qquad \mathsf{ai}\!\downarrow \frac{S\{\circ\}}{S[a,\bar{a}]} \qquad \mathsf{s}\,\frac{S([R,U],T)}{S[(R,T),U]} \qquad \mathsf{q}\!\downarrow \frac{S\langle[R,U];[T,V]\rangle}{S[\langle R;T\rangle,\langle U;V\rangle]}$$

Figure 3: System BV

6.1 Lemma (Splitting) *Let R, T, P be any* BV *structures and let a be an atom.*

(1) *If $[(R,T),P]$ is provable in* BV*, then there are structures P_R and P_T, such that*

$$\begin{array}{c}[P_R,P_T]\\ \| \mathsf{BV}\\ P\end{array} \quad \textit{and} \quad \begin{array}{c}-\\ \| \mathsf{BV}\\ [R,P_R]\end{array} \quad \textit{and} \quad \begin{array}{c}-\\ \| \mathsf{BV}\\ [T,P_T]\end{array} \quad .$$

(2) *If $[\langle R;T\rangle,P]$ is provable in* BV*, then there are structures P_R and P_T, such that*

$$\begin{array}{c}\langle P_R;P_T\rangle\\ \| \mathsf{BV}\\ P\end{array} \quad \textit{and} \quad \begin{array}{c}-\\ \| \mathsf{BV}\\ [R,P_R]\end{array} \quad \textit{and} \quad \begin{array}{c}-\\ \| \mathsf{BV}\\ [T,P_T]\end{array} \quad .$$

(3) *If $[a,P]$ is provable in* BV*, then there is a derivation* $\begin{array}{c}\bar{a}\\ \| \mathsf{BV}\\ P\end{array}$.

For the proof, the reader has to be referred to [7] or [10]. Here, I need it only for the proof of Lemma 6.11. Although this seems like breaking a fly on the wheel, I could not find a simpler way for proving Lemma 6.11, which is rather crucial.

If a structure R is provable in BV, then every atom a occurs as often in R as $\bar{a}$. This is easy to see: the only possibility, where an atom a can disappear is an instance of $\mathsf{ai}\!\downarrow$. But then at the same time an atom $\bar{a}$ does disappear.

6.2 Definition A set $\mathcal{P}$ of atoms is called *clean* if for all atoms $a \in \mathcal{P}$, we have $\bar{a} \notin \mathcal{P}$. Let $e : \mathcal{P} \to \mathcal{Q}$ be a mapping, where $\mathcal{P}$ and $\mathcal{Q}$ are two clean sets of atoms. The mapping $(\cdot)^e$ is defined inductively on BV structures in a natural way as follows:

$$\begin{array}{rcl}
\circ^e & = & \circ \\
a^e & = & \begin{cases} e(a) & \text{if } a \in \mathcal{P} \\ \overline{e(a)} & \text{if } \bar{a} \in \mathcal{P} \\ a & \text{otherwise} \end{cases} \\
[R_1,\dots,R_h]^e & = & [R_1^e,\dots,R_h^e] \\
(R_1,\dots,R_h)^e & = & (R_1^e,\dots,R_h^e) \\
\langle R_1;\dots;R_h\rangle^e & = & \langle R_1^e;\dots;R_h^e\rangle \\
\bar{R}^e & = & \overline{R^e}
\end{array}$$

6.3 Example Let $\mathcal{P} = \{a, b\}$ and $\mathcal{Q} = \{c\}$, and let $e(a) = e(b) = c$. Then

$$[\langle a; b; c; d\rangle, \langle \bar{a}; \bar{d}; \bar{b}; \bar{a}\rangle]^e = [\langle c; c; c; d\rangle, \langle \bar{c}; \bar{d}; \bar{c}; \bar{c}\rangle] \quad .$$

6.4 Lemma *Given two clean sets $\mathcal{P}$ and $\mathcal{Q}$ of atoms, a mapping $e : \mathcal{P} \to \mathcal{Q}$ and a structure R. If R is provable in* BV*, then R^e is also provable in* BV*.*

Proof: Let $\underset{R}{\mathsf{BV}\,\Vert\,\Pi}$ be given. Now let Π^e be the proof obtained from Π by replacing each structure S occurring inside Π by S^e. Each rule application remains valid. Hence $\underset{R^e}{\mathsf{BV}\,\Vert\,\Pi^e}$ is a valid proof. □

6.5 Example Let $\mathcal{P} = \{a, b\}$ and $\mathcal{Q} = \{c\}$, and let $e(a) = e(b) = c$ as above. Let $R = [\langle a; b; d\rangle, \langle \bar{a}; \bar{b}; \bar{d}\rangle]$, which is provable in BV. By Lemma 6.4, we have

$$\mathsf{q}\!\downarrow \frac{\mathsf{q}\!\downarrow \frac{\mathsf{ai}\!\downarrow \frac{\mathsf{ai}\!\downarrow \frac{\mathsf{ai}\!\downarrow \frac{\circ\!\downarrow \frac{}{\circ}}{[d, \bar{d}]}}{\langle [b, \bar{b}]; [d, \bar{d}]\rangle}}{\langle [a, \bar{a}]; [b, \bar{b}]; [d, \bar{d}]\rangle}}{\langle [a, \bar{a}]; [\langle b; d\rangle, \langle \bar{b}; \bar{d}\rangle]\rangle}}{[\langle a; b; d\rangle, \langle \bar{a}; \bar{b}; \bar{d}\rangle]} \quad \rightsquigarrow \quad \mathsf{q}\!\downarrow \frac{\mathsf{q}\!\downarrow \frac{\mathsf{ai}\!\downarrow \frac{\mathsf{ai}\!\downarrow \frac{\mathsf{ai}\!\downarrow \frac{\circ\!\downarrow \frac{}{\circ}}{[d, \bar{d}]}}{\langle [c, \bar{c}]; [d, \bar{d}]\rangle}}{\langle [c, \bar{c}]; [c, \bar{c}]; [d, \bar{d}]\rangle}}{\langle [c, \bar{c}]; [\langle c; d\rangle, \langle \bar{c}; \bar{d}\rangle]\rangle}}{[\langle c; c; d\rangle, \langle \bar{c}; \bar{c}; \bar{d}\rangle]} \quad .$$

The converse of Lemma 6.4 does in general not hold. For example $R = [a, \bar{b}]$ is not provable, but $R^e = [c, \bar{c}]$ is.

For a given proof Π of a structure R, I will call the *killer* (in Π) of a given occurrence atom a, that occurrence of $\bar{a}$, that vanishes together with it in an instance of $\mathsf{ai}\!\downarrow$. The situation is trivial, if in R every atom occurs exactly once. For example in the left-hand side proof in Example 6.5, the killer of $\bar{b}$ is b. In the right-hand side proof, more care is necessary: The killer of the first occurrence of $\bar{c}$ is the first c. The killer of the second c is the second $\bar{c}$.

6.6 Definition A BV structure R is called a *non-par structure* if it it does not contain a par structure as substructure, i.e. it is generated by the grammar

$$R ::= \circ \mid a \mid (\underbrace{R, \dots, R}_{>0}) \mid \langle \underbrace{R; \dots; R}_{>0} \rangle \mid \bar{R} \quad .$$

6.7 Lemma *Let V and P be* BV *structures, such that $\bar{V}$ is a non-par structure.*

$$\textit{If} \quad \underset{[\bar{V}, P]}{\Vert\,\mathsf{BV}} \quad , \quad \textit{then} \quad \begin{array}{c} V \\ \Vert\,\mathsf{BV} \\ P \end{array} \quad .$$

Proof: This lemma is an immediate consequence of Lemma 6.1. □

6.8 Definition Let R be a BV structure and let a be an atom occurring in R. I will say that the atom a is *unique* in R if it occurs exactly once.

6.9 Example In $[\langle c,c,d\rangle,\langle\bar{c},\bar{c},\bar{d}\rangle]$, the atoms d and $\bar{d}$ are unique, but not c and $\bar{c}$.

6.10 Lemma *Let $V \neq \circ$ be a BV structure and $S\{\ \}$ and $S'\{\ \}$ be two contexts, such that all atoms occuring in V are unique in $S\{V\}$.*

$$\text{If}\quad \begin{array}{c} S'\{V\} \\ \| \mathsf{BV} \\ S\{V\} \end{array} \quad,\quad \text{then}\quad \begin{array}{c} S'\{X\} \\ \| \mathsf{BV} \\ S\{X\} \end{array} \quad \text{for every structure } X \quad .$$

Proof: Pick any atom a inside V, and replace every other atom occurring in V everywhere inside $\begin{array}{c} S'\{V\} \\ \Delta \| \mathsf{BV} \\ S\{V\} \end{array}$ by $\circ$. This yields a derivation $\begin{array}{c} S'\{a\} \\ \Delta' \| \mathsf{BV} \\ S\{a\} \end{array}$, in which the atom a can everywhere be replaced by the structure X. □

The following lemma will play a crucial role in the proof of the faithfulness of the encoding of two counter machines.

6.11 Lemma *Let $R = [Z,(\bar{V},T),\langle U,V,W\rangle]$ be a BV structure, such that $\bar{V}$ is a non-par structure and all atoms occurring in V are unique in R. If R is provable in BV, then $R' = [Z,\langle U,T,W\rangle]$ is also provable in BV.*

Proof: Let $\begin{array}{c} \Pi \| \mathsf{BV} \\ [Z,(\bar{V},T),\langle U,V,W\rangle] \end{array}$ be given. By Lemma 6.1, there are structures P and Q such that

$$\begin{array}{c} [P,Q] \\ \Delta \| \mathsf{BV} \\ [Z,\langle U;V;W\rangle] \end{array} \quad\text{and}\quad \begin{array}{c} \Pi_1 \| \mathsf{BV} \\ [\bar{V},P] \end{array} \quad\text{and}\quad \begin{array}{c} \Pi_2 \| \mathsf{BV} \\ [T,Q] \end{array} \quad .$$

By applying Lemma 6.7 to Π_1, we get $\begin{array}{c} V \\ \Delta_1 \| \mathsf{BV} \\ P \end{array}$, from which we can get the following derivation:

$$\begin{array}{c} [V,Q] \\ \Delta_1 \| \mathsf{BV} \\ [P,Q] \\ \Delta \| \mathsf{BV} \\ [Z,\langle U;V;W\rangle] \end{array} \quad .$$

Now, we can apply Lemma 6.10, which gives us $\begin{array}{c} [T,Q] \\ \Delta_3 \| \mathsf{BV} \\ [Z,\langle U;T;W\rangle] \end{array}$. Composing Π_2 and Δ_3 yields the desired proof of R'. □

6.12 Definition A BV structure Q is called a *negation circle* if there is a clean set of atoms $\mathcal{P} = \{a_1,a_2,\ldots,a_n\}$, such that $Q = [Z_1,\ldots,Z_n]$, where

- $Z_j = (a_j,\bar{a}_{j+1})$ or $Z_j = \langle a_j;\bar{a}_{j+1}\rangle$ for every $j = 1,\ldots,n-1$, and

- $Z_n = (a_n, \bar{a}_1)$ or $Z_n = \langle a_n; \bar{a}_1 \rangle$.

I will say that a structure P *contains a negation circle* if there is a structure Q such that

- Q is a negation circle,
- Q can be obtained from P by replacing some atoms in P by $\circ$, and
- all atoms that occur in Q are unique in P.

6.13 Example The structure $P = [(a, c, [\bar{d}, b]), \bar{c}, \langle \bar{b}; [\bar{a}, d] \rangle]$ contains the negation circle $Q = [(a, b), \langle \bar{b}; \bar{a} \rangle]$.

6.14 Proposition *Let P be a* BV *structure. If P contains a negation circle, then P is not provable in* BV.

Proof: Let Q be the negation circle that is contained in P. By way of contradiction, assume that there is a proof of P. This proof remains valid, if all atoms that do not occur in Q are replaced by $\circ$ everywhere (some rule instances become trivial and can be removed). This yields a proof

$$\begin{array}{c} \Pi \Big\Vert \mathsf{BV} \\ [Z_1, Z_2, \dots, Z_n] \end{array} ,$$

for some $n \geqslant 1$, where $Z_1, \dots, Z_n$ are as in Definition 6.12. Now, I will proceed by induction on n to produce a contradiction.

Base Case: If $n = 1$, then obviously, there is no proof

$$\begin{array}{c} \Pi \Big\Vert \mathsf{BV} \\ (a_1, \bar{a}_1) \end{array} \quad \text{or} \quad \begin{array}{c} \Pi \Big\Vert \mathsf{BV} \\ \langle a_1; \bar{a}_1 \rangle \end{array} .$$

Inductive Case: Suppose there is no proof Π for all $n' < n$. Now consider the bottommost rule instance ρ in

$$\begin{array}{c} \Pi \Big\Vert \mathsf{BV} \\ [Z_1, Z_2, \dots, Z_n] \end{array} ,$$

where $Z_j = (a_j, \bar{a}_{j+1})$ or $Z_j = \langle a_j; \bar{a}_{j+1} \rangle$ for every $j = 1, \dots, n$. (For the sake of simplicity I will use the convention that $a_{n+1} = a_1$.) Without loss of generality, we can assume that ρ is not trivial.

(1) $\rho = \circ\!\downarrow$ or $\rho = \mathsf{ai}\!\downarrow$. Not possible.

(2) $\rho = \mathsf{q}\!\downarrow$. There are the following possibilities to apply $\mathsf{q}\!\downarrow \dfrac{S\langle [R, U]; [T, V] \rangle}{S[\langle R; T \rangle, \langle U; V \rangle]}$.

(i) $R = a_j, T = \bar{a}_{j+1}$ for some $j = 1, \dots, n$. Then, without loss of generality, we can assume that $j = 1$. We have the following subcases:

(a) $U = a_i$ and $V = \bar{a}_{i+1}$ for some $i = 2, \ldots, n$. Then we have a proof Π' such that

$$\mathsf{q}{\downarrow}\frac{\overset{\Pi' \| \mathsf{BV}}{[\langle [a_1, a_i]; [\bar{a}_2, \bar{a}_{i+1}] \rangle, Z_2, \ldots, Z_{i-1}, Z_{i+1}, \ldots, Z_n]}}{[\langle a_1; \bar{a}_2 \rangle, Z_2, \ldots, Z_{i-1}, \langle a_i; \bar{a}_{i+1} \rangle, Z_{i+1}, \ldots, Z_n]} \quad .$$

The proof Π' remains valid if we replace a_m and $\bar{a}_m$ by $\circ$ for every m with $2 \leqslant m \leqslant i$. Then we get

$$\overset{\Pi'' \| \mathsf{BV}}{[\langle a_1; \bar{a}_{i+1} \rangle, Z_{i+1}, \ldots, Z_n]} \quad ,$$

which is a contradiction to the induction hypothesis.

(b) $U = \circ$ and $V = [Z_{k_1}, \ldots, Z_{k_v}]$ for some $v > 0$ and $k_1, \ldots, k_v \in \{2, \ldots, n\}$. Without loss of generality, assume that $k_1 < k_2 < \ldots < k_v$. Let $\{2, \ldots, n\} \setminus \{k_1, \ldots, k_v\} = \{h_1, \ldots, h_s\}$, where $s = n - v - 1$. Then there is a proof Π' such that

$$\mathsf{q}{\downarrow}\frac{\overset{\Pi' \| \mathsf{BV}}{[\langle a_1; [\bar{a}_2, Z_{k_1}, \ldots, Z_{k_v}] \rangle, Z_{h_1}, \ldots, Z_{h_s}]}}{[\langle a_1; \bar{a}_2 \rangle, Z_2, \ldots, Z_n]} \quad .$$

The proof Π' remains valid if we replace a_m and $\bar{a}_m$ by $\circ$ for every m with $2 \leqslant m \leqslant k_v$. Then we get

$$\overset{\Pi'' \| \mathsf{BV}}{[\langle a_1; \bar{a}_{k_v+1} \rangle, Z_{k_v+1}, \ldots, Z_n]} \quad ,$$

which is a contradiction to the induction hypothesis.

(c) $U = [Z_{k_1}, \ldots, Z_{k_u}]$ and $V = \circ$ for some $u > 0$ and $k_1, \ldots, k_u \in \{2, \ldots, n\}$. Without loss of generality, assume that $k_1 < k_2 < \ldots < k_u$. Let $\{2, \ldots, n\} \setminus \{k_1, \ldots, k_u\} = \{h_1, \ldots, h_s\}$, where $s = n - u - 1$. Then there is a proof Π' such that

$$\mathsf{q}{\downarrow}\frac{\overset{\Pi' \| \mathsf{BV}}{[\langle [a_1, Z_{k_1}, \ldots, Z_{k_u}]; \bar{a}_2 \rangle, Z_{h_1}, \ldots, Z_{h_s}]}}{[\langle a_1; \bar{a}_2 \rangle, Z_2, \ldots, Z_n]} \quad .$$

The proof Π' remains valid if we replace a_m and $\bar{a}_m$ by $\circ$ for every m with $m > k_1$ and for $m = 1$. Then we get

$$\overset{\Pi'' \| \mathsf{BV}}{[\langle a_{k_1}, \bar{a}_2 \rangle, Z_2, \ldots, Z_{k_1-1}]} \quad ,$$

which is a contradiction to the induction hypothesis.

(ii) $U = a_j$ and $V = \bar{a}_{j+1}$ for some $j = 1, \ldots, n$. Similar to (i).

(iii) $R = [Z_{k_1}, \ldots, Z_{k_r}]$, $T = \circ$, $U = \circ$ and $V = [Z_{l_1}, \ldots, Z_{l_v}]$ for some $r, v > 0$ and $k_1, \ldots, k_r, l_1, \ldots, l_v \in \{1, \ldots, n\}$. Then there is a proof Π' such that

$$\mathsf{q}{\downarrow}\,\frac{\overset{\Pi' \| \mathsf{BV}}{[\langle [Z_{k_1}, \ldots, Z_{k_r}]; [Z_{l_1}, \ldots, Z_{l_v}]\rangle, Z_{h_1}, \ldots, Z_{h_s}]}}{[Z_1, Z_2, \ldots, Z_n]} \quad ,$$

where $s = n - r - v$ and $\{h_1, \ldots, h_s\} = \{1, \ldots, n\} \setminus \{k_1, \ldots, k_r, l_1, \ldots, l_v\}$. Without loss of generality, we can assume that $r = v = 1$. Otherwise we could replace

$$\mathsf{q}{\downarrow}\,\frac{[\langle [Z_{k_1}, \ldots, Z_{k_r}]; [Z_{l_1}, \ldots, Z_{l_v}]\rangle, Z_{h_1}, \ldots, Z_{h_s}]}{[Z_1, Z_2, \ldots, Z_n]} \qquad \text{by}$$

$$\mathsf{q}{\downarrow}\,\frac{\mathsf{q}{\downarrow}\,\frac{\mathsf{q}{\downarrow}\,\frac{[\langle [Z_{k_1}, \ldots, Z_{k_r}]; [Z_{l_1}, \ldots, Z_{l_v}]\rangle, Z_{h_1}, \ldots, Z_{h_s}]}{[\langle [Z_{k_1}, \ldots, Z_{k_r}]; Z_{l_1}\rangle, Z_{l_2}, \ldots, Z_{l_v}, Z_{h_1}, \ldots, Z_{h_s}]}}{[\langle Z_{k_1}; Z_{l_1}\rangle, Z_{k_2}, \ldots, Z_{k_r}, Z_{l_2}, \ldots, Z_{l_v}, Z_{h_1}, \ldots, Z_{h_s}]}}{[Z_1, Z_2, \ldots, Z_n]} \quad .$$

Now let $k = k_1$ and $l = l_1$. Then we have

$$\mathsf{q}{\downarrow}\,\frac{\overset{\Pi' \| \mathsf{BV}}{[\langle Z_k; Z_l\rangle, Z_{h_1}, \ldots, Z_{h_s}]}}{[Z_1, Z_2, \ldots, Z_n]} \quad ,$$

where $s = n - 2$. There are two subcases.

(a) $l < k$. Then replace inside Π' all atoms a_m and $\bar{a}_m$ by $\circ$ for every m with $m \leqslant l$ or $k < m$. The proof Π' then becomes

$$\overset{\Pi'' \| \mathsf{BV}}{[\langle a_k; \bar{a}_{l+1}\rangle, Z_{l+1}, \ldots, Z_{k-1}]}$$

which is a contradiction to the induction hypothesis.

(b) $k < l$. Then replace inside Π' all atoms a_m and $\bar{a}_m$ by $\circ$ for every m with $k < m \leqslant l$. The proof Π' then becomes

$$\overset{\Pi'' \| \mathsf{BV}}{[Z_1, \ldots, Z_{k-1}, \langle a_k; \bar{a}_{l+1}\rangle, Z_{l+1}, \ldots, Z_n]} \quad ,$$

which is a contradiction to the induction hypothesis.

(iv) $R = \circ$, $T = [Z_{k_1}, \ldots, Z_{k_t}]$, $U = [Z_{l_1}, \ldots, Z_{l_u}]$ and $V = \circ$ for some $t, u > 0$ and $k_1, \ldots, k_t, l_1, \ldots, l_u \in \{1, \ldots, n\}$. Similar to (iii).

(3) $\rho = \mathsf{s}$. There are three possibilities to apply $\mathsf{s}\,\dfrac{S([R,U],T)}{S[(R,T),U]}$.

(i) $R = a_j, T = \bar{a}_{j+1}$ for some $j = 1, \dots, n$. Then, without loss of generality, we can assume that $j = 1$. Further, $U = [Z_{k_1}, \dots, Z_{k_u}]$ for some $u > 0$ and $k_1, \dots, k_u \in \{2, \dots, n\}$. Without loss of generality, assume that $k_1 < k_2 < \dots < k_u$. Let $\{2, \dots, n\} \setminus \{k_1, \dots, k_u\} = \{h_1, \dots, h_s\}$, where $s = n - u - 1$. Then there is a proof Π' such that

$$\mathsf{s}\,\frac{\overset{\Pi' \| \mathsf{BV}}{[([a_1, Z_{k_1}, \dots, Z_{k_u}], \bar{a}_2), Z_{h_1}, \dots, Z_{h_s}]}}{[(a_1, \bar{a}_2), Z_2, \dots, Z_n]} \quad .$$

The proof Π' remains valid if we replace the atoms a_1, $\bar{a}_1$ and a_m, $\bar{a}_m$ for every $m \geqslant k_1$ by $\circ$. Then we get

$$\overset{\Pi'' \| \mathsf{BV}}{[(a_{k_1}, \bar{a}_2), Z_2, \dots, Z_{k-1}]} \quad ,$$

which is a contradiction to the induction hypothesis.

(ii) $R = \bar{a}_{j+1}, T = a_j$ for some $j = 1, \dots, n$. Similar to (i).

(iii) $R = \circ$, $T = [Z_{k_1}, \dots, Z_{k_t}]$ and $U = [Z_{l_1}, \dots, Z_{l_u}]$ for some $t, u > 0$ and $k_1, \dots, k_t, l_1, \dots, l_u \in \{1, \dots, n\}$. Similar to (2.iii).

□

6.15 Remark I strongly believe that the converse of Proposition 6.14 does also hold. This would then immediately imply the equivalence between Guglielmi's BV and Retoré's pomset logic [22].

7 Faithfulness of the Encoding

The main ingredient of the proof of the second direction of Theorem 4.3 is the notion of weak encoding together with a crucial use of Proposition 6.14.

7.1 Definition Let $\mathcal{M} = (\mathcal{Q}, q_0, n_0, m_0, q_f, \mathcal{T})$ be a two counter machine. Then a BV structure W is called a *weak encoding* of $\mathcal{M}$, if

$$W = [U_1, \dots, U_r, \langle b; a^n; q; c^m; d\rangle, \langle \bar{b}; \bar{q}_f; \bar{d}\rangle] \quad ,$$

for some $r, n, m \geqslant 0$ and $q \in \mathcal{Q}$, where the structures $U_1, \dots, U_r$ encode transitions of $\mathcal{M}$, i.e. for every $l \in \{1, \dots, r\}$, we have that $U_l = T_k$ for some $k \in \{1, \dots, h\}$.

Observe that in a weak encoding W of a machine $\mathcal{M}$, some transitions T_k might occur many times and some might not occur at all.

7.2 Lemma *Given a two counter machine* $\mathcal{M} = (\mathcal{Q}, q_0, n_0, m_0, q_f, \mathscr{T})$.

If $\begin{array}{c} \| \text{NEL} \\ \mathcal{M}_{\text{enc}} \end{array}$ *then there is a weak encoding* W *of* $\mathcal{M}$*, such that* $\begin{array}{c} \| \text{BV} \\ W \\ \| \{\mathsf{w}\downarrow, \mathsf{b}\downarrow\} \\ \mathcal{M}_{\text{enc}} \end{array}$.

Proof: It is easy to see that the rules $\mathsf{w}\downarrow$ and $\mathsf{b}\downarrow$ can be permuted under any other rule in system NEL (see [10] for a detailed explanation of this fact). Hence the proof $\begin{array}{c} \| \text{NEL} \\ \mathcal{M}_{\text{enc}} \end{array}$ can be decomposed into

$$\begin{array}{c} \Pi \| \{\mathsf{o}\downarrow, \mathsf{ai}\downarrow, \mathsf{s}, \mathsf{q}\downarrow, \mathsf{p}\downarrow\} \\ \mathcal{M}'_{\text{enc}} \\ \Delta \| \{\mathsf{w}\downarrow, \mathsf{b}\downarrow\} \\ \mathcal{M}_{\text{enc}} \end{array} .$$

Let W be the structure, which is obtained from $\mathcal{M}'_{\text{enc}}$ by removing all exponentials, and let Π' be the proof obtained from Π by removing the exponentials from each structure occurring inside Π. By this manipulation, all rule instances remain valid, except for the promotion rule, which becomes trivial:

$$\mathsf{p}\downarrow \frac{S\{![R,T]\}}{S[!R,?T]} \quad \rightsquigarrow \quad \mathsf{p}\downarrow' \frac{S[R,T]}{S[R,T]} ,$$

and can therefore be omitted. This means that Π' is valid proof of W in system BV. Further, $\mathcal{M}'_{\text{enc}}$ does not contain any ! because $\mathcal{M}_{\text{enc}}$ is !-free. Therefore, there is a derivation

$$\begin{array}{c} W \\ \| \{\mathsf{w}\downarrow, \mathsf{b}\downarrow\} \\ \mathcal{M}'_{\text{enc}} \end{array} \qquad \text{because of} \qquad \mathsf{w}\downarrow \frac{S\{R\}}{\mathsf{b}\downarrow \dfrac{[?R,R]}{S\{?R\}}} .$$

Hence, we have $\begin{array}{c} W \\ \| \{\mathsf{w}\downarrow, \mathsf{b}\downarrow\} \\ \mathcal{M}_{\text{enc}} \end{array}$. That W is a indeed weak encoding is obvious. □

7.3 Example In our example, we get

$$W = [(\langle \bar{a}; \bar{q}_1 \rangle, q_1), (\langle \bar{q}_0; \bar{d} \rangle, \langle q_1; d \rangle), \langle b; a; q_0; d \rangle, \langle \bar{b}; \bar{q}_1; \bar{d} \rangle] .$$

The following lemma is nothing but an act of bureaucracy. The idea is to rename the atoms $q_0, \ldots, q_z$ that encode the states of the machine in such a way that each such atom occurs only once. This will then simplify the extraction of the computation from the proof.

7.4 Lemma *Let $\mathcal{M} = (\mathcal{Q}, q_0, n_0, m_0, q_f, \mathscr{T})$ be a two counter machine and let $W = [U_1, \dots, U_r, \langle b; a^n; q; c^m; d\rangle, \langle \bar{b}; \bar{q}_f; \bar{d}\rangle]$ be a weak encoding of $\mathcal{M}$. Further, let $\mathcal{P} = \{p_0, \dots, p_r\}$ be a clean set of $r+1$ fresh atoms. If W is provable in* BV*, then there is a mapping $e : \mathcal{P} \to \mathcal{Q}$ and a structure*

$$\tilde{W} = [\tilde{U}_1, \dots, \tilde{U}_r, \langle b; a^n; p_0; c^m; d\rangle, \langle \bar{b}; \bar{p}_r; \bar{d}\rangle] \quad ,$$

such that

(1) *$\tilde{W}$ is provable in* BV*,*

(2) *all atoms $p_0, \bar{p}_0, \dots, p_r, \bar{p}_r$ occur exactly once in $\tilde{W}$,*

(3) *for every $l \in \{1, \dots, r\}$, the atoms $\bar{p}_{l-1}$ and p_l occur inside $\tilde{U}_l$,*

(4) *$\tilde{W}^e = W$, and*

(5) *for every $l \in \{1, \dots, r\}$, we have $\tilde{U}_l^e = U_{l'}$ for some $l' \in \{1, \dots, r\}$,*

Proof: Let $\mathcal{O} = \{o_0, \dots, o_r\}$ be another clean set of $r+1$ fresh atoms. The structure W contains $r+1$ occurrences of atoms $q \in \mathcal{Q}$ and $r+1$ occurrences of atoms q' with $\bar{q}' \in \mathcal{Q}$ (because each U_l for $l = 1, \dots, r$ contains exactly one $q \in \mathcal{Q}$ and one q' with $\bar{q}' \in \mathcal{Q}$). Since W is provable, each such q and q' must have its killer inside W. Now let W' be obtained from W by replacing each such q and its killer by o_l and $\bar{o}_l$, respectively, for some $l = 0, \dots, r$, such that each $o \in \mathcal{O}$ is used exactly once. Then W' is also provable because the replacement can be continued to the proof Π of W. This also yields a mapping $f : \mathcal{O} \to \mathcal{Q}$ with $f(o) = q$ if an occurrence of q has been replaced by o. We now have

$$W' = [U'_1, \dots, U'_r, \langle b; a^n; o_l; c^m; d\rangle, \langle \bar{b}; \bar{o}_{l'}; \bar{d}\rangle]$$

for some $l, l' \in \{0, \dots, r\}$. Further, all atoms $o_0, \bar{o}_0, \dots, o_r, \bar{o}_r$ occur exactly once in W'. The atom $\bar{o}_l$ must occur inside a U'_{s_1} for some $s_1 \in \{1, \dots, r\}$ (i.e. $l \neq l'$). Otherwise the atoms $o_0, \bar{o}_0, \dots, o_{l-1}, \bar{o}_{l-1}, o_{l+1}, \bar{o}_{l+1}, \dots, o_r, \bar{o}_r$ would form a negation circle inside $[U'_1, \dots, U'_r]$, which is by Proposition 6.14 a contradiction to the provability of W'. Now let W'_0 be obtained from W' by replacing o_l and $\bar{o}_l$ by p_0 and $\bar{p}_0$, respectively. Let o_{l_1} be the atom from $\mathcal{O}$ that occurs inside U'_{s_1}. Again, we have that $\bar{o}_{l_1}$ must occur inside U'_{s_2} for some $s_2 \in \{1, \dots, r\}$ (i.e. $l_1 \neq l'$), because otherwise there would be a negation circle inside $[U'_1, \dots, U'_r]$. Let W'_1 be obtained from W'_0 by replacing o_{l_1} and $\bar{o}_{l_1}$ by p_1 and $\bar{p}_1$, respectively. Repeat this to get the structures $W'_2, \dots, W'_r$. This also defines a bijective mapping $g : \mathcal{O} \to \mathcal{P}$ with $g(o) = p$ if o has been replaced by p. Now let $\tilde{W} = W'_r$ and $e(p) = f(g^{-1}(p))$. Further let $\tilde{U}_1 = {U'_{s_1}}^g$, $\tilde{U}_2 = {U'_{s_2}}^g$, and so on. Then $\tilde{W}$ is provable in BV, because W' is provable in BV. Further, all atoms $p_0, \bar{p}_0, \dots, p_r, \bar{p}_r$ occur exactly once in $\tilde{W}$ because all atoms $o_0, \bar{o}_0, \dots, o_r, \bar{o}_r$ occur exactly once in W'. The replacement of atoms is done in such a way that for every $l \in \{1, \dots, r\}$, the atoms $\bar{p}_{l-1}$ and p_l occur inside $\tilde{U}_l$ and $\tilde{W}^e = W$. □

7.5 Example For the weak encoding in Example 7.3, we get

$$\tilde{W} = [\,\underbrace{(\langle \bar{p}_0; \bar{d}\rangle, \langle p_1; d\rangle)}_{\tilde{U}_1},\ \underbrace{(\langle \bar{a}; \bar{p}_1\rangle, p_2)}_{\tilde{U}_2},\ \langle b; a; p_0; d\rangle\ ,\ \langle \bar{b}; \bar{p}_2; \bar{d}\rangle\,] \quad ,$$

with $e(p_0) = q_0$ and $e(p_1) = e(p_2) = q_1$.

7.6 Lemma *Let $\mathcal{M} = (\mathcal{Q}, q_0, n_0, m_0, q_f, \mathscr{T})$ a two counter machine and let $W = [U_1, \ldots, U_r, \langle b; a^n; q; c^m; d\rangle, \langle \bar{b}; \bar{q}_f; \bar{d}\rangle]$ be a weak encoding of $\mathcal{M}$.*

$$\textit{If} \qquad \begin{array}{c} \| \mathsf{BV} \\ W \end{array} \qquad \textit{then} \quad (q, n, m) \to^r (q_f, 0, 0) \quad .$$

Proof: By induction on r:

Base case: If $r = 0$ then $W = [\langle b; a^n; q; c^m; d\rangle, \langle \bar{b}; \bar{q}_f; \bar{d}\rangle]$. This is only provable if $n = m = 0$ and $q = q_f$, i.e. if $W = [\langle b; q_f; d\rangle, \langle \bar{b}; \bar{q}_f; \bar{d}\rangle]$. We certainly have that $(q_f, 0, 0) \to^0 (q_f, 0, 0)$.

Inductive case: By Lemma 7.4, there is a set $\mathcal{P} = \{p_0, \ldots, p_r\}$ of $r+1$ fresh atoms, a mapping $e : \mathcal{P} \to \mathcal{Q}$ and a provable structure

$$\tilde{W} = [\tilde{U}_1, \ldots, \tilde{U}_r, \langle b; a^n; p_0; c^m; d\rangle, \langle \bar{b}; \bar{p}_r; \bar{d}\rangle] \quad ,$$

with $\tilde{W}^e = W$, and such that the killer $\bar{p}_0$ of p_0 is inside $\tilde{U}_1$. Now we have six cases:

(1) $\tilde{U}_1 = (\bar{p}_0, \langle a; p_1\rangle)$. Then

$$\tilde{W} \quad = \quad [\,\tilde{U}_2, \ldots, \tilde{U}_r, \underbrace{(\bar{p}_0, \langle a; p_1\rangle)}_{\tilde{U}_1}, \langle b; a^n; p_0; c^m; d\rangle, \langle \bar{b}; \bar{p}_r; \bar{d}\rangle\,] \quad .$$

Since $\tilde{W}$ is provable in BV, we have by Lemma 6.11 that

$$\tilde{W}' \quad = \quad [\,\tilde{U}_2, \ldots, \tilde{U}_r, \langle b; a^n; a; p_1; c^m; d\rangle, \langle \bar{b}; \bar{p}_r; \bar{d}\rangle\,]$$

is also provable. Let now $W' = \tilde{W}'^e$ and assume $e(p_1) = q'$. Then

$$W' \quad = \quad [\,U_1, \ldots, U_{l-1}, U_{l+1}, \ldots, U_r, \langle b; a^{n+1}; q'; c^m; d\rangle, \langle \bar{b}; \bar{q}_f; \bar{d}\rangle\,] \quad ,$$

for some $l \in \{1, \ldots, r\}$. We have that W' is a weak encoding of $\mathcal{M}$ because W is a weak encoding of $\mathcal{M}$. By Lemma 6.4, W' is provable in BV. Hence, we can apply the induction hypothesis and get

$$(q', n+1, m) \to^{r-1} (q_f, 0, 0) \quad .$$

Further, we have that

$$U_l = \tilde{U}_1^e = (\bar{q}, \langle a; q'\rangle) \quad .$$

Therefore $(q, \mathsf{inc1}, q') \in \mathscr{T}$. Hence

$$(q, n, m) \to (q', n+1, m) \quad ,$$

which gives us

$$(q, n, m) \to^r (q_f, 0, 0) \quad .$$

(2) $\tilde{U}_1 = (\langle \bar{a}; \bar{p}_0 \rangle, p_1)$. Then

$$\tilde{W} \quad = \quad [\ \underbrace{(\langle \bar{a}; \bar{p}_0 \rangle, p_1)}_{\tilde{U}_1}, \tilde{U}_2, \ldots, \tilde{U}_r, \langle b; a^n; p_0; c^m; d \rangle, \langle \bar{b}; \bar{p}_r; \bar{d} \rangle\ ] \quad .$$

Mark inside $\tilde{W}$ the atom $\bar{a}$ inside $\tilde{U}_1$ by $\bar{a}^\bullet$ and its killer by $a^\bullet$. By way of contradiction, assume now that $a^\bullet$ occurs inside $\tilde{U}_l = (\bar{p}_{l-1}, \langle a^\bullet; p_l \rangle)$ for some $l \in \{2, \ldots, r\}$. This means that

$$\begin{aligned} \tilde{W} \quad = \quad & [\ \underbrace{(\langle \bar{a}^\bullet; \bar{p}_0 \rangle, p_1)}_{\tilde{U}_1}, \tilde{U}_2, \ldots, \tilde{U}_{l-1}, \underbrace{(\bar{p}_{l-1}, \langle a^\bullet; p_l \rangle)}_{\tilde{U}_l}, \tilde{U}_{l+1}, \ldots, \tilde{U}_r, \\ & \langle b; a^n; p_0; c^m; d \rangle, \langle \bar{b}; \bar{p}_r; \bar{d} \rangle\ ] \quad . \end{aligned}$$

But then $\tilde{W}$ contains a negation circle:

$$[(\bar{a}^\bullet, p_1), (\bar{p}_1, p_2), \ldots, (\bar{p}_{l-1}, a^\bullet)] \quad ,$$

which is (by Proposition 6.14) a contradiction to the provability of $\tilde{W}$. Hence, the atom $a^\bullet$ must occur inside the encoding of the configuration, which means that $n > 0$. Further, we have that

$$\tilde{W} \quad = \quad [\ \underbrace{(\langle \bar{a}^\bullet; \bar{p}_0 \rangle, p_1)}_{\tilde{U}_1}, \tilde{U}_2, \ldots, \tilde{U}_r, \langle b; a^{n'}; a^\bullet; a^{n''}; p_0; c^m; d \rangle, \langle \bar{b}; \bar{p}_r; \bar{d} \rangle\ ] \quad ,$$

for some n', n'' with $n = n' + 1 + n''$. I will now show that $n'' = 0$. For this, assume by way of contradiction, that $n'' > 0$. Mark the first atom a in $a^{n''}$ by a° and its killer by $\bar{a}^\circ$. Then $\bar{a}^\circ$ must occur inside $\tilde{U}_k = (\langle \bar{a}^\circ; \bar{p}_{k-1} \rangle, p_k)$ for some $k \in \{2, \ldots, r\}$. Then we have that

$$\begin{aligned} \tilde{W} \quad = \quad & [\ \underbrace{(\langle \bar{a}^\bullet; \bar{p}_0 \rangle, p_1)}_{\tilde{U}_1}, \tilde{U}_2, \ldots, \tilde{U}_{k-1}, \underbrace{(\langle \bar{a}^\circ; \bar{p}_{k-1} \rangle, p_k)}_{\tilde{U}_k}, \tilde{U}_{k+1}, \ldots, \tilde{U}_r, \\ & \langle b; a^{n'}; a^\bullet; a^\circ; a^{n''-1}; p_0; c^m; d \rangle, \langle \bar{b}; \bar{p}_r; \bar{d} \rangle\ ] \quad . \end{aligned}$$

But then $\tilde{W}$ contains a negation circle:

$$[\langle a^\bullet; a^\circ \rangle, \langle \bar{a}^\circ; \bar{p}_{k-1} \rangle, (p_{k-1}, \bar{p}_{k-2}), \ldots, (p_2, \bar{p}_1), (p_1, \bar{a}^\bullet)] \quad ,$$

which is (by Proposition 6.14) a contradiction to the provability of $\tilde{W}$. Hence, the atom a° cannot exist, which means that $n'' = 0$ and $n' = n - 1$. This means that

$$\tilde{W} \quad = \quad [\ \tilde{U}_2, \ldots, \tilde{U}_r, \underbrace{(\langle \bar{a}^\bullet; \bar{p}_0 \rangle, p_1)}_{\tilde{U}_1}, \langle b; a^{n-1}; a^\bullet; p_0; c^m; d \rangle, \langle \bar{b}; \bar{p}_r; \bar{d} \rangle\ ] \quad .$$

Since this is provable in BV, we have (by Lemma 6.11) that

$$\tilde{W}' \quad = \quad [\ \tilde{U}_2, \ldots, \tilde{U}_r, \langle b; a^{n-1}; p_1; c^m; d\rangle, \langle \bar{b}; \bar{p}_r; \bar{d}\rangle\ ]$$

is also provable. Let now $W' = \tilde{W}'^e$ and $e(p_1) = q'$. Then

$$W' \quad = \quad [\ U_1, \ldots, U_{l-1}, U_{l+1}, \ldots, U_r, \langle b; a^{n-1}; q'; c^m; d\rangle, \langle \bar{b}; \bar{q}_f; \bar{d}\rangle\ ] \quad ,$$

for some $l \in \{1, \ldots, r\}$. As before, W' is a weak encoding of $\mathcal{M}$ and (by Lemma 6.4) provable in BV. Hence, we can apply the induction hypothesis and get

$$(q', n-1, m) \rightarrow^{r-1} (q_f, 0, 0) \quad .$$

Further, we have that

$$U_l = \tilde{U}_1^e = (\langle \bar{a}; \bar{q}\rangle, q') \quad .$$

Therefore $(q, \mathtt{dec1}, q') \in \mathscr{T}$. Since we also have $n > 0$, we have

$$(q, n, m) \rightarrow (q', n-1, m) \quad ,$$

which gives us

$$(q, n, m) \rightarrow^{r} (q_f, 0, 0) \quad .$$

(3) $\tilde{U}_1 = (\langle \bar{b}; \bar{p}_0\rangle, \langle b; p_1\rangle)$. Then

$$\tilde{W} \quad = \quad [\ \underbrace{(\langle \bar{b}; \bar{p}_0\rangle, \langle b; p_1\rangle)}_{\tilde{U}_1}, \tilde{U}_2, \ldots, \tilde{U}_r, \langle b; a^n; p_0; c^m; d\rangle, \langle \bar{b}; \bar{p}_r; \bar{d}\rangle\ ] \quad .$$

Mark inside $\tilde{W}$ the atom $\bar{b}$ inside $\tilde{U}_1$ by $\bar{b}^\bullet$ and its killer by $b^\bullet$. By way of contradiction, assume now that $b^\bullet$ occurs inside $\tilde{U}_l = (\langle \bar{b}; \bar{p}_{l-1}\rangle, \langle b^\bullet; p_l\rangle)$ for some $l \in \{2, \ldots, r\}$ (it can certainly not be inside $\tilde{U}_1$). Then we have that

$$\begin{aligned}\tilde{W} \quad = \quad [\ & \underbrace{(\langle \bar{b}^\bullet; \bar{p}_0\rangle, \langle b; p_1\rangle)}_{\tilde{U}_1}, \tilde{U}_2, \ldots, \tilde{U}_{l-1}, \underbrace{(\langle \bar{b}; \bar{p}_{l-1}\rangle, \langle b^\bullet; p_l\rangle)}_{\tilde{U}_l}, \tilde{U}_{l+1}, \ldots, \tilde{U}_r, \\ & \langle b; a^n; p_0; c^m; d\rangle, \langle \bar{b}; \bar{p}_r; \bar{d}\rangle\ ] \quad .\end{aligned}$$

But then we have a negation circle inside $\tilde{W}$:

$$[(\bar{b}^\bullet, p_1), (\bar{p}_1, p_2), \ldots, (\bar{p}_{l-1}, b^\bullet)] \quad ,$$

which is (by Proposition 6.14) a contradiction to the provability of $\tilde{W}$. Hence, the atom $b^\bullet$ must occur inside the encoding of the configuration. This means that

$$\tilde{W} \quad = \quad [\ \underbrace{(\langle \bar{b}^\bullet; \bar{p}_0\rangle, \langle b; p_1\rangle)}_{\tilde{U}_1}, \tilde{U}_2, \ldots, \tilde{U}_r, \langle b^\bullet; a^n; p_0; c^m; d\rangle, \langle \bar{b}; \bar{p}_r; \bar{d}\rangle\ ] \quad .$$

I will now show that $n = 0$. For this, assume by way of contradiction, that $n > 0$. Mark the first atom a in a^n by a° and its killer by $\bar{a}^\circ$. Then $\bar{a}^\circ$ must occur inside $\tilde{U}_k = (\langle \bar{a}^\circ; \bar{p}_{k-1}\rangle, p_k)$ for some $k \in \{2, \ldots, r\}$. This means that

$$\begin{array}{rcl}\tilde{W} & = & [\ \underbrace{(\langle \bar{b}^\bullet; \bar{p}_0\rangle, \langle b; p_1\rangle)}_{\tilde{U}_1}, \tilde{U}_2, \ldots, \tilde{U}_{k-1}, \underbrace{(\langle \bar{a}^\circ; \bar{p}_{k-1}\rangle, p_k)}_{\tilde{U}_k}, \tilde{U}_{k+1}, \ldots, \tilde{U}_r, \\ & & \langle b^\bullet; a^\circ; a^{n-1}; p_0; c^m; d\rangle, \langle \bar{b}; \bar{p}_r; \bar{d}\rangle\ ] \quad .\end{array}$$

But then $\tilde{W}$ contains a negation circle:

$$[\langle b^\bullet; a^\circ\rangle, \langle \bar{a}^\circ; \bar{p}_{k-1}\rangle, (p_{k-1}, \bar{p}_{k-2}), \ldots, (p_2, \bar{p}_1), (p_1, \bar{b}^\bullet)] \quad ,$$

which is (by Proposition 6.14) a contradiction to the provability of $\tilde{W}$. Hence, the atom a° cannot exist, which means that $n = 0$. This means that

$$\tilde{W} \quad = \quad [\ \tilde{U}_2, \ldots, \tilde{U}_r, \underbrace{(\langle \bar{b}^\bullet; \bar{p}_0\rangle, \langle b; p_1\rangle)}_{\tilde{U}_1}, \langle b^\bullet; p_0; c^m; d\rangle, \langle \bar{b}; \bar{p}_r; \bar{d}\rangle\ ] \quad .$$

Since this is provable in BV, we have (by Lemma 6.11) that

$$\tilde{W}' \quad = \quad [\ \tilde{U}_2, \ldots, \tilde{U}_r, \langle b; p_1; c^m; d\rangle, \langle \bar{b}; \bar{p}_r; \bar{d}\rangle\ ]$$

is also provable. Let now $W' = \tilde{W}'^e$ and $e(p_1) = q'$. Then

$$W' \quad = \quad [\ U_1, \ldots, U_{l-1}, U_{l+1}, \ldots, U_r, \langle b; q'; c^m; d\rangle, \langle \bar{b}; \bar{q}_f; \bar{d}\rangle\ ] \quad ,$$

for some $l \in \{1, \ldots, r\}$. As before, W' is a weak encoding of $\mathcal{M}$ and (by Lemma 6.4) provable in BV. Hence, we can apply the induction hypothesis and get

$$(q', 0, m) \to^{r-1} (q_f, 0, 0) \quad .$$

Further, we have that

$$U_l = \tilde{U}_1^e = (\langle \bar{b}; \bar{q}\rangle, \langle b; q'\rangle) \quad .$$

Therefore $(q, \mathsf{zero1}, q') \in \mathscr{T}$. Since we also have $n = 0$, we have

$$(q, 0, m) \to (q', 0, m) \quad ,$$

which gives us

$$(q, n, m) \to^r (q_f, 0, 0) \quad .$$

(4) $\tilde{U}_1 = (\bar{p}_0, \langle p_1; c\rangle)$. Similar to (1).

(5) $\tilde{U}_1 = (\langle \bar{p}_0; \bar{c}\rangle, p_1)$. Similar to (2).

(6) $\tilde{U}_1 = (\langle \bar{p}_0; \bar{d}\rangle, \langle p_1; d\rangle)$. Similar to (3). □

7.7 Proposition *Given a two counter machine* $\mathcal{M} = (\mathcal{Q}, q_0, n_0, m_0, q_f, \mathscr{T})$.

$$\text{If} \quad \begin{array}{c} \Pi\,\mathsf{NEL} \\ \mathcal{M}_{\text{enc}} \end{array} \quad \text{then} \quad (q_0, n_0, m_0) \to^* (q_f, 0, 0) \quad .$$

Proof: First apply Lemma 7.2 to get

$$\begin{array}{c} \Pi\,\mathsf{BV} \\ W \\ \Vert\,\{\mathsf{w}\downarrow, \mathsf{b}\downarrow\} \\ \mathcal{M}_{\text{enc}} \end{array} \quad ,$$

where W is a weak encoding of $\mathcal{M}$. Since the rules $\mathsf{w}\downarrow$ and $\mathsf{b}\downarrow$ cannot modify the substructure $\langle b; a^{n_0}; q_0; c^{m_0}; d\rangle$ of $\mathcal{M}_{\text{enc}}$, this substructure must still be present in W. Hence, we have that

$$W = [U_1, \ldots, U_r, \langle b; a^{n_0}; q_0; c^{m_0}; d\rangle, \langle \bar{b}; \bar{q}_f; \bar{d}\rangle] \quad ,$$

for some $r \geqslant 0$. By Lemma 7.6, we have that $(q_0, n_0, m_0) \to^* (q_f, 0, 0)$. □

Proof of Theorem 4.3: For the first direction use Proposition 5.2 and for the second direction use Proposition 7.7. □

References

[1] Samson Abramsky and Radha Jagadeesan. Games and full completeness for multiplicative linear logic. *Journal of Symbolic Logic*, 59(2):543–574, June 1994.

[2] Kai Brünnler and Alwen Fernanto Tiu. A local system for classical logic. In R. Nieuwenhuis and A. Voronkov, editors, *LPAR 2001*, volume 2250 of *Lecture Notes in Artificial Intelligence*, pages 347–361. Springer-Verlag, 2001.

[3] Paola Bruscoli. A purely logical account of sequentiality in proof search. In Peter J. Stuckey, editor, *Logic Programming, 18th International Conference*, volume 2401 of *Lecture Notes in Artificial Intelligence*, pages 302–316. Springer-Verlag, 2002.

[4] Arnaud Fleury and Christian Retoré. The mix rule. *Mathematical Structures in Computer Science*, 4(2):273–285, 1994.

[5] Jean-Yves Girard. Linear logic. *Theoretical Computer Science*, 50:1–102, 1987.

[6] Alessio Guglielmi. Butterflies, 2002. On the web at: http://www.ki.inf.tu-dresden.de/˜guglielm/Research/Notes/AG7.pdf.

[7] Alessio Guglielmi. A system of interaction and structure. Technical Report WV-02-10, Technische Universität Dresden, 2002. Submitted. On the web at: http://www.ki.inf.tu-dresden.de/˜guglielm/Research/Gug/Gug.pdf.

[8] Alessio Guglielmi and Lutz Straßburger. Non-commutativity and MELL in the calculus of structures. In Laurent Fribourg, editor, *Computer Science Logic, CSL 2001*, volume 2142 of *LNCS*, pages 54–68. Springer-Verlag, 2001.

[9] Alessio Guglielmi and Lutz Straßburger. A non-commutative extension of MELL. In Matthias Baaz and Andrei Voronkov, editors, *Logic for Programming, Artificial Intelligence, and Reasoning, LPAR 2002*, volume 2514 of *LNAI*, pages 231–246. Springer-Verlag, 2002.

[10] Alessio Guglielmi and Lutz Straßburger. A non-commutative extension of multiplicative exponential linear logic. Technical Report WV-2002-03, Technische Universität Dresden, 2002. On the web at: http://www.ki.inf.tu-dresden.de/~lutz/NELbig.pdf.

[11] John E. Hopcroft and Jeffrey D. Ullman. *Introduction to automata theory, languages and computation.* Addison-Wesley, 1979.

[12] Max I. Kanovich. The complexity of Horn fragments of linear logic. *Annals of Pure and Applied Logic*, 69(2–3):195–241, 1994.

[13] Max I. Kanovich. The direct simulation of Minsky machines in linear logic. In Jean-Yves Girard, Yves Lafont, and Laurent Regnier, editors, *Advances in Linear Logic*, pages 123–145. Cambridge University Press, 1995.

[14] Max I. Kanovich. Simulating computations in second order non-commutative linear logic. In Jean-Yves Girard, Mitsuhiro Okada, and Andre Scedrov, editors, *Electronic Notes in Theoretical Computer Science*, volume 3. Elsevier Science Publishers, 2000.

[15] Dexter C. Kozen. *Automata and Computability.* Springer-Verlag, 1997.

[16] Yves Lafont. The undecidability of second order linear logic without exponentials. *The Journal of Symbolic Logic*, 61(2):541–548, 1996.

[17] Yves Lafont and Andre Scedrov. The undecidability of second order multiplicative linear logic. *Information and Computation*, 125:46–51, 1996.

[18] Joachim Lambek. How to program an infinite abacus. *Canad. Math. Bull.*, 4(3):295–302, 1961.

[19] P. Lincoln, J. Mitchell, A. Scedrov, and N. Shankar. Decision problems for propositional linear logic. *Annals of Pure and Applied Logic*, 56(1–3):239–311, 1992.

[20] Robin Milner. *Communication and Concurrency.* International Series in Computer Science. Prentice Hall, 1989.

[21] Marvin L. Minsky. Recursive unsolvability of Post's problem of "tag" and other topics in theory of Turing machines. *The Annals of Mathematics*, 74(3):437–455, 1961.

[22] Christian Retoré. Pomset logic: A non-commutative extension of classical linear logic. In Ph. de Groote and J. R. Hindley, editors, *Typed Lambda Calculus and Applications, TLCA'97*, volume 1210 of *Lecture Notes in Computer Science*, pages 300–318, 1997.

[23] Lutz Straßburger. MELL in the Calculus of Structures. Technical Report WV-01-03, Technische Universität Dresden, 2001. Accepted for publication in Theoretical Computer Science.

[24] Alwen Fernanto Tiu. Properties of a logical system in the calculus of structures. Technical Report WV-01-06, Technische Universität Dresden, 2001. On the web at: http://www.cse.psu.edu/~tiu/thesisc.pdf.