Formalising Coffman Conditions in First Order Modal μ Calculus (Extended Version)

Yoshiki Kinoshita, Koki Nishizawa,
Keishi Okamoto

Research Center for Verification and Semantics (CVS),
National Institute of Advanced Industrial Science and
Technology (AIST)

Formalising Coffman Conditions in First Order Modal μ Calculus (Extended Version)

Yoshiki Kinoshita, Koki Nishizawa, Keishi Okamoto

Research Center for Verification and Semantics (CVS),
National Institute of Advanced Industrial Science and Technology (AIST)

Abstract. We formalise Coffman conditions for deadlock detection in first order modal μ calculus. Our main theorem states that any state of a first order modal μ structure subject to the theory of resource allocation systems and "mutual exclusion", "wait for" and "no preemption" conditions is deadlock if and only if it satisfies "circular wait" condition. To that end we formalise the notion of resource allocation systems, as well as all of Coffman conditions in first order modal μ calculus, which is a coherent extension of first order logic and propositional modal μ calculus recently proposed by one of the authors. Then we formalise our main theorem and prove it is true at any state of any finite resource allocation structure.

1 Introduction

Coffman [2] studied the conditions for the existence of deadlock in a data processing system. This classical work was analysed in many successors [4, 6] and is nowadays one of the materials in standard textbooks, but most of these treatments take informal approach, so considerable amount of additional task is necessary to adopt it in the modern, formal verification techniques such as model checking or proving using a proof assistant.

Coffman's conditions are about data processing systems, so it is natural to formulate it using the notion of transition system and modal μ calculus[8].

Propositional modal μ calculus, however, has no individual variables, which one would need to describe properties required for data processing systems. The states of these transition systems are graphs whose nodes are processes and resources and whose edges represent requesting or allocating relation, so one would naturally require individual variables varying over processes and resources and quantifiers upon them. This naturally leads to the use of a first order extension of modal μ calculus reported by one of the authors in [11].

This paper is organised as follows. In section 2 an overview of the basic concepts of first order modal μ calculus is given, which is a coherent extension of first order logic and propositional modal μ calculus, developed by one of the authors in [11]. We also provide a sound proof system for first order modal μ calculus. It cannot be complete, as shown in [11] that first order modal μ calculus is not recursively axiomatisable, which means that no proof system is complete for

first order modal μ calculus. In section 3, a formal theory for resource allocation systems is presented in first order modal μ calculus. Moreover, we formalise the four conditions, "mutual exclusion," "wait for," "no preemption," and "circular wait," given by Coffman as the deadlock condition. We also formulate the notion of "deadlock state" and formalise it in our formal theory. In section 5, we prove our main theorem: for any finite resource allocation system M satisfying "mutual exclusion," "wait for" and "no preemption" condition, there is a number k such that M has a deadlock state if and only if it has a cycle of size k. Note that in a finite resource allocation system, all cycles are finite, so "circular wait" condition is equivalent to the existence of pair of a natural number k and a finite cycle of size k.

2 First Order Modal μ Calculus

First order modal μ calculus [11] is a mild extension of propositional modal μ calculus [8] which allows first order variables and quantification over them.

A *signature* for first order modal μ calculus consists of sets $IVar$ of individual variables, $PVar$ of propositional variables and $Pred_n$ of n-ary predicate symbols for each natural number $n \geq 0$. Elements of $IVar$ are called *individual variables*. Elements of $PVar$ are called *propositional variables* and those of $Pred_n$ are called n-ary *predicate symbols*. Formulae, free occurrences of an individual or a propositional variable in a formula, and positive occurrences of a propositional variable in a formula are defined simultaneously by induction as follows. A negative occurrence of a propositional variable is understood to be its occurrence which is not positive.

1. If $P \in Pred_n$, x_0, x_1, ..., $x_{n-1} \in IVar$, $P(x_0, x_1, \ldots, x_{n-1})$ is a formula. Each of individual variables x_i $(0 \leq i < n)$ has an obvious unique free occurrence in this formula. There are no occurrences of any propositional variable in it.
2. If $X \in PVar$, X is a formula. No individual variable has any occurrence in this formula. The propositional variable X has an obvious unique free and positive occurrence in it. Other variables have no occurrences in X.
3. If φ is a formula, $\neg\varphi$ is a formula. Free occurrence of any variable in $\neg\varphi$ are defined to be its free occurrences in φ. Positive occurrences of any propositional variable in $\neg\varphi$ are defined to be its negative occurrences in φ.
4. If φ and ψ are formulae, $\varphi \vee \psi$ is a formula. Free occurrences of any variable in $\varphi \vee \psi$ are defined to be its free occurrences in φ and those in ψ. Positive occurrences of any propositional variable in $\varphi \vee \psi$ are defined to be its positive occurrences in φ and those in ψ.
5. If φ is a formula, $\Box\varphi$ is a formula. Free occurrences of any variable in $\Box\varphi$ are defined to be its free occurrences in φ. Positive occurrences of any propositional variable in $\Box\varphi$ are defined to be positive occurrences in φ.
6. If $x \in IVar$ and φ is a formula, then $(\forall x)\varphi$ is a formula. Free occurrences of $y \in IVar$ in $(\forall x)\varphi$ are defined to be free occurrences of y in φ if $y \neq x$; x has no free occurrences in $(\forall x)\varphi$. Free occurrences of any propositional variable

in $(\forall x)A$ are defined to be its free occurrences in φ. Positive occurrences of any propositional variable in $(\forall x)\varphi$ are defined to be positive occurrences in φ.

7. If $X \in PVar$, φ is a formula and no free occurrence of X in φ is negative, then $(\mu X)\varphi$ is a formula. Free occurrences of any individual variable in $(\mu X)\varphi$ are defined to be its free occurrences in φ. Free occurrences of $Y \in PVar$ in $(\mu X)\varphi$ are defined to be free occurrences of Y in $(\mu X)\varphi$ if $Y \neq X$; X has no free occurrences in $(\mu X)\varphi$. Positive occurrences of any propositional variable in $(\mu X)\varphi$ are defined to be its positive occurrences in φ.

For individual variables x, y and a formula φ, we write $\varphi[y/x]$ for the result of substituting y for all free occurrences of x in φ. Similarly, for a propositional variable X and formulae φ and ψ, we write $\varphi[\psi/X]$ for the result of substituting ψ for all free occurrences of X in φ. Substitutions are of course subject to usual renaming of bound variables which would otherwise be captured by quantifiers or fixpoint operators in φ.

We often write $\forall x.\varphi$ for $(\forall x)\varphi$, $\forall x, y.\varphi$ for $(\forall x)(\forall y)\varphi$, etc. Also, we write $(\nu X)\varphi$, $\Box^*\{\varphi\}$, $\Diamond^*\{\psi\}$, respectively, for $\neg(\mu X)\neg\varphi$, $(\nu Z)\varphi \wedge \Box Z$, $(\mu Z)\psi \vee \Diamond Z$, respectively.

Let τ be a signature. A τ *structure* consists of two sets S and D, a binary relation R on S and an interpretation function $I\colon (\prod n \in \mathrm{Nat})Pred_n \to S \to \mathcal{P}(D^n)$, which returns, given $n \in \mathrm{Nat}$, $P \in Pred_n$ and s, a subset of D^n. So a τ structure is a quadruple (S, D, R, I).

A *valuation* (v, V) is a pair of a function $v\colon IVar \to D$ and $V\colon PVar \to \mathcal{P}(S)$, a function mapping a predicate variable to a subset of S.

In the sequel, we fix a τ structure $\mathcal{A} = (S, D, R, I)$ and a valuation (v, V) unless otherwise stated.

We now define the denotation of formulae. By induction on the construction φ, we define

$$[\![\varphi]\!]_{\mathcal{A},(v,V)} \in \mathcal{P}(S),$$

the denotation of φ with respect to $\mathcal{A}$ and (v, V).

- $[\![P(x_1, \ldots, x_n)]\!]_{\mathcal{A},(v,V)} \stackrel{\mathrm{def}}{=} \{\, s \in S \mid (v(x_1), \ldots, v(x_n)) \in I(n, P, s) \,\}$
- $[\![X]\!]_{\mathcal{A},(v,V)} \stackrel{\mathrm{def}}{=} V(X)$
- $[\![\neg\varphi]\!]_{\mathcal{A},(v,V)} \stackrel{\mathrm{def}}{=} S \setminus [\![\varphi]\!]_{\mathcal{A},(v,V)}$
- $[\![\varphi \vee \psi]\!]_{\mathcal{A},(v,V)} \stackrel{\mathrm{def}}{=} [\![\varphi]\!]_{\mathcal{A},(v,V)} \cup [\![\psi]\!]_{\mathcal{A},(v,V)}$
- $[\![(\forall x)\varphi]\!]_{\mathcal{A},(v,V)} \stackrel{\mathrm{def}}{=} \bigcap\{[\![\varphi]\!]_{\mathcal{A},(v[x\mapsto d],V)} \mid d \in D\,\}$, where $v[x \mapsto d](y) \stackrel{\mathrm{def}}{=} v(y)$ if $y \neq x$ and $v[x \mapsto d](x) \stackrel{\mathrm{def}}{=} d$.
- $[\![\Box\varphi]\!]_{\mathcal{A},(v,V)} \stackrel{\mathrm{def}}{=} \{\, s \in S \mid \text{For all } s',\ s\ R\ s' \text{ implies } s' \in [\![\varphi]\!]_{\mathcal{A},(v,V)} \,\}$
- $[\![(\mu X)\varphi]\!]_{\mathcal{A},(v,V)} \stackrel{\mathrm{def}}{=} \bigcap\{\, T \subseteq S \mid [\![\varphi]\!]_{\mathcal{A},(v,V[X\mapsto T])} \subseteq T \,\}$ where $V[X \mapsto T](Y)$ is defined by $V[X \mapsto T](X) = T$ and $V[X \mapsto T](Y) = V(Y)$ if $Y \neq X$.

Let φ be a formula. We say φ is true at a state $s \in S$, for $\mathcal{A}$ and (v, V) if and only if $s \in [\![\varphi]\!]_{\mathcal{A},(v,V)}$ and write

$$\mathcal{A}, s, (v, V) \Vdash \varphi.$$

We also define $\mathcal{A}, (v, V) \Vdash \varphi$, $\mathcal{A}, s \Vdash \varphi$ and $\mathcal{A} \Vdash \varphi$ as follows.

$$\begin{aligned}
\mathcal{A}, (v, V) \Vdash \varphi &\overset{\text{def}}{\iff} \text{For all } s \in S,\ A, s, (v, V) \Vdash \varphi \\
\mathcal{A}, s \Vdash \varphi &\overset{\text{def}}{\iff} \text{For all valuation } (v, V),\ A, s, (v, V) \Vdash \varphi \\
\mathcal{A} \Vdash \varphi &\overset{\text{def}}{\iff} \text{For all valuation } (v, V),\ A, (v, V) \Vdash \varphi
\end{aligned}$$

We say φ is *valid* in $\mathcal{A}$ if $\mathcal{A} \Vdash \varphi$. A *model* of a formula φ is a structure which makes it valid. A model of a set of formulae is a model of each of its elements.

We now turn into rules of inference. As shown in [11], first order modal μ calculus is not recursively axiomatisable. So there is no hope to achieve a sound and complete set of rules of inference for first order modal μ calculus. We present a sound one here, which is powerful enough for our need. Basically it is a merge of the rules of inference of propositional modal μ calculus [1, 5, 9] and those of first order predicate logic, so valid formulae of propositional modal μ calculus are trivially provable in our inference system.

There are fourteen rules of inference for first order modal μ calculus. Let $\bot$ be an abbreviation of $\varphi \wedge \neg\varphi$ for some formula φ.

$$\frac{}{(\forall x.\, \Box\varphi) \supset \Box\forall x.\, \varphi}\ \text{BF} \qquad \frac{}{(\exists x.\, \Diamond\varphi) \supset \Diamond\exists x.\, \varphi}\ \text{CBF} \qquad \frac{\begin{array}{c}[\neg\varphi] \\ \vdots \\ \bot\end{array}}{\varphi}\ \text{RAA}$$

$$\frac{\varphi}{\varphi \vee \psi}\ \vee\text{I1} \qquad \frac{\psi}{\varphi \vee \psi}\ \vee\text{I2} \qquad \frac{\varphi \vee \psi \quad \begin{array}{c}[\varphi] \\ \vdots \\ \theta\end{array} \quad \begin{array}{c}[\psi] \\ \vdots \\ \theta\end{array}}{\theta}\ \vee\text{E}$$

$$\frac{\begin{array}{c}[\varphi] \\ \vdots \\ \bot\end{array}}{\neg\varphi}\ \neg\text{I} \qquad \frac{\varphi \quad \neg\varphi}{\bot}\ \neg\text{E} \qquad \frac{\varphi[y/x]}{\forall x.\, \varphi}\ \forall\text{I} \qquad \frac{\forall x.\, \varphi}{\varphi[z/x]}\ \forall\text{E}$$

In the rule $\forall$I, the individual variable y must not have any free occurrences in any assumption of the proof of $\varphi[y/x]$.

$$\frac{\varphi}{\Box\varphi}\ \Box\text{I} \qquad \frac{\Box(\varphi \supset \psi) \quad \Box\varphi}{\Box\psi}\ \Box\text{E} \qquad \frac{\varphi[(\mu X.\, \varphi)/X]}{\mu X.\, \varphi}\ \mu\text{I} \qquad \frac{\mu X.\, \varphi \quad \begin{array}{c}[\varphi[\psi/X]] \\ \vdots \\ \psi\end{array}}{\psi}\ \mu\text{E}$$

In the rule $\Box$I, the given proof of φ must not have any non-discharged hypotheses. In the rule μE, ψ does not depend on any other hypothesis beside $\varphi[\psi/X]$.

Example 1. Let φ and ψ be formulae. Then the followings hold for the above proof system. (We will prove the followings in lemma 3.)

1. If $\vdash \varphi \supset \psi$, then $\vdash \Diamond^*\{\varphi\} \supset \Diamond^*\{\psi\}$ and $\vdash \Box^*\{\varphi\} \supset \Box^*\{\psi\}$.
2. If $\vdash \varphi \supset \Box\varphi$, then $\vdash \varphi \supset \Box^*\{\varphi\}$.
3. $\vdash \overbrace{\Diamond \ldots \Diamond}^{n} \varphi \supset \Diamond^*\{\varphi\}$ and $\vdash \Box^*\{\psi\} \supset \overbrace{\Box \ldots \Box}^{n} \psi$ for any natural number n.
4. $\vdash \Diamond(\Diamond^*\{\varphi\}) \supset \Diamond^*\{\varphi\}$ and $\vdash \Box^*\{\psi\} \supset \Box(\Box^*\{\psi\})$.
5. $\vdash \Diamond^*\{\Diamond\varphi\} \supset \Diamond^*\{\varphi\}$ and $\vdash \Box^*\{\psi\} \supset \Box^*\{\Box\psi\}$.

3 Resource Allocation Theories

Notions of resource allocation graphs and resource allocation systems have been used for studying deadlock [2, 4, 6]. After giving proper mathematical but informal definitions for these notions, we axiomatise them and introduce resource allocation theories. Models of resource allocation theories are called resource allocation structures.

Definition 1. *A* resource allocation graph *is a triple* $(D_p, D_r, \rightarrow)$ *such that*

1. D_p *and* D_r *are mutually disjoint non-empty sets and*
2. $\rightarrow$ *is a subset of the set* $(D_p \times D_r) \cup (D_r \times D_p)$.

So, $\rightarrow$ is a binary relation on $D_p \uplus D_r$, under which elements of D_p are only related to those of D_r and elements of D_r are only related to those of D_p.

Hereafter, we fix the pair of mutually disjoint sets D_p and D_r and all resource allocation graphs considered hereafter are over these sets.

Elements of D_p are called *processes* and those of D_r *resources*. Since D_p and D_r are fixed, a resource allocation graph will be determined by the binary relation, so we shall refer to a resource allocation graph $(D_p, D_r, \rightarrow)$ only by its relation $\rightarrow$.

So, let $\rightarrow$ be a resource allocation graph, p be a process and x be a resource. We say p *is requesting* x if $p \rightarrow x$, and we say x *is allocated* to p if $x \rightarrow p$. Moreover we say p *is irrelevant* to x if p is not requesting x nor x is allocated to p.

Now we consider transitions over resource allocation graphs. The basic idea is that a resource allocation graph represents a state of the system, as for which process requests which resource and which resource is allocated to which process. So, the dynamism of the system under consideration should be captured by looking at transitions of resource allocation graphs, hence the system can be considered as a transition system.

Definition 2. *We write* RAG *for the set of all resource allocation graphs.*

There is no size problem here, since all resource allocation graphs are over the fixed D_p and D_r.

Definition 3. *A* resource allocation signature *is defined to be a signature which contains two unary predicates* `Proc` *and* `Rsrc` *and two binary predicates* `E` *and* $=$.

Definition 4. *A* resource allocation theory *is defined to be a theory over a resource allocation signature which contains the following formulae. We shall call these formulae* axioms *of resource allocation theory.*

Eq $\forall a, b.(a = b \supset \Box(a = b)) \wedge (a \neq b \supset \Box(a \neq b))$

NoMult $\neg\exists p, x.((p \leftrightarrow x))$,
which means, for any state $\rightarrow$*, there are no pairs of a process* p *and a resource* x *such that* p *is requesting* x *and* x *is allocated to* p *at* $\rightarrow$*.*

PA(N) $\forall p, x.((p \not\rightleftarrows x) \supset \Box(p \nleftarrow x))$,
which means, for any state $\rightarrow$*, if a process* p *is not requesting a resource* x *at* $\rightarrow$*, then* x *is not allocated to* p *at any state which are directly reachable from* $\rightarrow$*.*

PA(A) $\forall p, x.((p \leftarrow x) \supset \Box(p \nrightarrow x))$,
which means, for any state $\rightarrow$*, if a resource* x *is allocated to a process* p *at* $\rightarrow$*, then* p *can not be requesting* x *at any states which are directly reachable from* $\rightarrow$*.*

OA *The following four axioms mean no process can simultaneously request, cancel, get and release multiple resources.*

OA(RR) $\forall p, x, y.((p \rightarrow x) \wedge (p \rightarrow y) \supset \Box((p \leftarrow x) \supset (p \rightleftarrows y)))$

OA(RA) $\forall p, x, y.((p \rightarrow x) \wedge (p \leftarrow y) \supset \Box((p \nrightarrow x) \supset (p \leftarrow y)))$

OA(RN) $\forall p, x, y.((p \rightarrow x) \wedge (p \not\rightleftarrows y) \supset \Box((p \nrightarrow x) \supset (p \not\rightleftarrows y)))$

OA(AN) $\forall p, x, y.((p \leftarrow x) \wedge (p \not\rightleftarrows y) \supset \Box((p \nleftarrow x) \supset (p \not\rightleftarrows y)))$

OP *The following six axioms mean no two process can simulataneously request, cancel, get and release the same resource.*

OP(RR) $\forall p, q, x, y.((p \not\rightleftarrows x) \wedge (q \rightarrow y) \wedge p \neq q \supset \Box((p \rightarrow x) \supset (q \rightarrow y)))$

OP(RA) $\forall p, q, x, y.((p \not\rightleftarrows x) \wedge (q \leftarrow y) \wedge p \neq q \supset \Box((p \rightarrow x) \supset (q \leftarrow y)))$

OP(RN) $\forall p, q, x, y.((p \not\rightleftarrows x) \wedge (q \not\rightleftarrows y) \wedge p \neq q \supset \Box((p \rightarrow x) \supset (q \not\rightleftarrows y)))$

OP(AR) $\forall p, q, x, y.((p \rightarrow x) \wedge (q \rightarrow y) \wedge p \neq q \supset \Box((p \leftarrow x) \supset (q \rightarrow y)))$

OP(NR) $\forall p, q, x, y.((p \rightleftarrows x) \wedge (q \rightarrow y) \wedge p \neq q \supset \Box((p \not\rightleftarrows x) \supset (q \rightarrow y)))$

OP(NA) $\forall p, q, x, y.((p \rightleftarrows x) \wedge (q \leftarrow y) \wedge p \neq q \supset \Box((p \not\rightleftarrows x) \supset (q \leftarrow y)))$

Act(NR) $\forall p, x.((p \not\rightleftarrows x) \supset \Diamond(p \rightarrow x))$,
which means, for any states $\rightarrow$*, a process* p *can request a resource* x *in a transition* $(\rightarrow, \Rightarrow)$ *for some state* $\Rightarrow$ *if* p *is irrelevant to* x *at* $\rightarrow$*.*

We write **RAAx** for the collection of the above axoims.

Proposition 1. RAAx *is independent, i.e. for every member* φ *of* **RAAx**, *there is a model* $\mathcal{A}$ *of* $(\mathbf{RAAx} \setminus \{\varphi\})$ *but not a model of* φ*.*

Proposition 2. *The following formulae are provable from* **RAAx**. *(We will prove the followings in lemma 4)*

1. $\forall p, x, y((p \rightarrow x) \wedge (p \rightarrow y) \supset \Box((p \not\rightleftarrows x) \supset (p \nleftarrow y)))$
2. $\forall p, x, y.((p \leftarrow x) \wedge (p \rightarrow y) \supset \Box((p \nleftarrow x) \supset (p \rightarrow y)))$
3. $\forall p, x, y.((p \leftarrow x) \wedge (p \leftarrow y) \supset \Box((p \nleftarrow x) \supset (p \nrightarrow y)))$
4. $\forall p, x, y.((p \not\rightleftarrows x) \wedge (p \rightarrow y) \supset \Box((p \rightleftarrows x) \supset (p \rightarrow y)))$
5. $\forall p, x, y.((p \not\rightleftarrows x) \wedge (p \leftarrow y) \supset \Box((p \rightleftarrows x) \supset (p \leftarrow y)))$
6. $\forall p, x, y.((p \not\rightleftarrows x) \wedge (p \not\rightleftarrows y) \supset \Box((p \rightleftarrows x) \supset (p \nleftarrow y)))$

7. $\forall p, q, x, y.((p \rightarrow x) \wedge (q \leftarrow y) \wedge p \neq q \supset \Box((p \leftarrow x) \supset (q \leftarrow y)))$
8. $\forall p, q, x, y.((p \rightarrow x) \wedge (q \not\rightleftarrows y) \wedge p \neq q \supset \Box((p \leftarrow x) \supset (q \not\rightleftarrows y)))$
9. $\forall p, q, x, y.((p \rightleftarrows x) \wedge (q \not\rightleftarrows y) \wedge p \neq q \supset \Box((p \not\rightleftarrows x) \supset (q \not\rightleftarrows y)))$

We accordingly consider first order modal μ structures over resource allocation graphs, in order to interpret resource allocation theories.

Definition 5. *A* resource allocation structure *is a first order modal μ structure (S, R, D, I) subject to the following conditions*

1. $D = D_p \uplus D_r$ *(for our fixed D_p and D_r)*
2. $S = \mathrm{RAG}$
3. $I(1, \mathtt{Proc}, \rightarrow) = D_p$,
4. $I(1, \mathtt{Rsrc}, \rightarrow) = D_r$,
5. $I(2, \mathtt{E}, req) = \{(d_1, d_2) \mid d_1, d_2 \in D \text{ and } d_1 \rightarrow d_2\}$ *and*
6. $I(2, =, \rightarrow) = \{(d, d) \mid d \in D\}$.

Note that there is no constraint on the transition relation (R) of a resource allocation structure.

By a *finite* resource allocation structure (S, R, D, I), we mean that the domain D is a finite set.

A transition system (RAG, R) is a *resource allocation system* if there are D and I which make (RAG, R, D, I) a resource allocation structure.

We shall use the following abbreviations.

Abbreviation 1.
- $p \rightarrow x \stackrel{\text{def}}{\Longleftrightarrow} \mathtt{Proc}(p) \wedge \mathtt{Rsrc}(x) \wedge \mathtt{E}(p, x)$
- $p \not\rightarrow x \stackrel{\text{def}}{\Longleftrightarrow} \mathtt{Proc}(p) \wedge \mathtt{Rsrc}(x) \wedge \neg\mathtt{E}(p, x)$
- $p \leftarrow x \stackrel{\text{def}}{\Longleftrightarrow} \mathtt{Proc}(p) \wedge \mathtt{Rsrc}(x) \wedge \mathtt{E}(x, p)$
- $p \not\leftarrow x \stackrel{\text{def}}{\Longleftrightarrow} \mathtt{Proc}(p) \wedge \mathtt{Rsrc}(x) \wedge \neg\mathtt{E}(x, p)$
- $p \leftrightarrow x \stackrel{\text{def}}{\Longleftrightarrow} (p \rightarrow x) \wedge (p \leftarrow x)$
- $p \rightleftarrows x \stackrel{\text{def}}{\Longleftrightarrow} (p \rightarrow x) \vee (p \leftarrow x)$
- $p \not\rightleftarrows x \stackrel{\text{def}}{\Longleftrightarrow} (p \not\rightarrow x) \wedge (p \not\leftarrow x)$

4 An Axiomatisation of Coffman Conditions and Deadlock

In this section, a set of axioms corresponding to Coffman conditions is presented in the setting of first order modal μ calculus. Coffman conditions consist of four propositions. "Mutual exclusion" requires that 'tasks claim exclusive control of the resources they require [2].' (In the sequel, phrases enclosed by single quotes are cited from [2].) "Wait for" is the condition that 'tasks hold resources already allocated to them while waiting for additional resources.' "No preemption" is the condition that 'resources cannot be forcibly removed from the tasks holding them until the resources are used to completion.' Finally, "circular wait" is the condition that 'a circular chain of tasks exists, such that each task holds one or more resources that are being requested by the next task in the chain.' In this section, we shall formulate these conditions in terms of first order modal μ calculus.

4.1 Mutual Exclusion

Our mutual exclusion condition is

$$\mathbf{ME} \wedge \mathbf{ME0}$$

where **ME** and **ME0** are defined as follows.

ME $\Box^*\{\neg\exists p, q, x.(p \neq q \wedge (p \leftarrow x) \wedge (q \leftarrow x))\}$
ME0 $\Box^*\{\forall p, x.((p \rightarrow x) \wedge \neg(\exists q.(q \leftarrow x)) \supset \Diamond(p \leftarrow x))\}$

ME claims exclusive control of resources, i.e., that any resource is allocated to at most one process at any reachable state. **ME** turns out, however, to be too weak to show later that the existence of deadlock states implies "no preemption," so we need further condition **ME0** to show it.

We really need **ME0** in the sense that **ME** does not logically imply **ME0** because there is a τ structure M and a state s of M which satisfies **ME** but falsify **ME0**.

We shall occasionally replace **ME** by a weaker form **ME1**, which requires that a resource x would never be allocated to a process p at any of next states if p is requesting x and x is allocated to some process.

ME1 $\Box^*\{\forall p, x.((p \rightarrow x) \wedge (\exists q.(q \leftarrow x)) \supset \Box(p \not\leftarrow x))\}$

ME1 is weaker than **ME** in the sense that $\vdash \mathbf{ME} \supset \mathbf{ME1}$.

4.2 No Preemption

"No preemption" condition would mean that, whenever a resource x is allocated to a process p, x is possibly deallocated from p if and only if p is not requesting any resource. States where x is deallocated from p would be expressed by $p \not\rightleftarrows x$, so "x is possibly deallocated from p" would be $\Diamond p \not\rightleftarrows x$. So, "no preemption" condition could be expressed as

$$\mathbf{NP} \quad \Box^*\{\forall p, x.\ ((p \leftarrow x) \supset (\neg(\exists y.(p \rightarrow y)) \supset\subset \Diamond(p \not\rightleftarrows x)))\}.$$

For convenience reasons, we split this into the following two formulae.

NP0 $\Box^*\{\forall p, x.((p \leftarrow x) \supset \neg(\exists y.(p \rightarrow y)) \supset \Diamond(p \not\rightleftarrows x))\}$
NP1 $\Box^*\{\forall p, x.((p \leftarrow x) \supset (\exists y.(p \rightarrow y)) \supset \Box(p \rightleftarrows x))\}$

Observe that **NP** and **NP0** $\wedge$ **NP1** are logically equivalent.

4.3 Wait for

"Wait for" condition would mean that whenever a process p is requesting a resource x, x is possibly cancelled from p if and only if there are no resources allocated to p. So, "wait for" condition could be expressed as

$$\mathbf{WF} \quad \Box^*\{\forall p, x.\ (p \rightarrow x) \supset (\neg(\exists y.\ p \leftarrow y) \supset\subset \Diamond(p \not\rightleftarrows x))\}.$$

Again, we split this into the following two formulae for convenience reasons.

WF0 $\Box^*\{\forall p, x.((p \rightarrow x) \supset (\neg\exists y.(p \leftarrow y)) \supset \Diamond(p \not\rightleftarrows x))\}$
WF1 $\Box^*\{\forall p, x.((p \rightarrow x) \supset (\exists y.(p \leftarrow y)) \supset \Box(p \rightleftarrows x))\}$

WF is logically equivalent to **WF0** $\wedge$ **WF1**.

4.4 Circular Wait

"Circular wait" condition assures existence of a cycle of arbitrarily finite size. We represent this property by providing the proposition $\mathbf{CW}_n$ for each natural number n, which claims that there is a allocate-request cycle consisting of exactly n processes and n resources. "Circular wait" condition amounts to requiring $\mathbf{CW}_n$ for some n.

So, for a natural number $n \geq 1$, let

$$C_n(p_0, \ldots, p_{n-1}, x_0, \ldots, x_{n-1}) \stackrel{\text{def}}{\Longleftrightarrow} \bigwedge_{0 \leq i \neq j \leq n-1} (p_i \neq p_j \wedge (p_i \rightarrow x_i) \wedge (p_{i+1} \leftarrow x_i))$$

where $p_n = p_0$ and we define

$$\mathbf{CW}_n \stackrel{\text{def}}{\Longleftrightarrow} \exists p_0, \ldots, p_{n-1}, x_0, \ldots, x_{n-1}. C_n(p_0, \ldots, p_{n-1}, x_0, \ldots, x_{n-1}).$$

$\mathbf{CW}_n$ says that there is a cycle of processes and resources whose length is $2n$, so we call $\mathbf{CW}_n$ *n-circular wait condition*. Let $\mathcal{A} = (S, R, D, I)$ be a resource allocation structure. A state $s \in S$ satisfies "circular wait" condition if if $\mathcal{A}, s \Vdash_v \mathbf{CW}_n$ for some natural number n and some (i.e. for any) valuation v in (S, R, D).

For a natural number $n \geq 1$, let

$$\mathbf{Chain}_n \stackrel{\text{def}}{\Longleftrightarrow} \exists u_0, \ldots, u_n. \bigwedge_{0 \leq i < n-1} (u_i \rightarrow u_{i+1}).$$

$\mathbf{Chain}_n$ says that there is a chain of processes and resources whose length is at least n, so we call $\mathbf{Chain}_n$ *n-chain condition*.

4.5 Deadlock

Let $\mathcal{A} = (S, R, D, I)$ be a resource allocation structure and $s \in S$. We say a state s is *request deadlock* if

$$\mathcal{A}, s \Vdash \exists p, x. \Box^* \{p \rightarrow x\}.$$

We say s is *allocate deadlock* if

$$\mathcal{A}, s \Vdash \exists p, x. \Box^* \{p \leftarrow x\}$$

and that s is *deadlock* if it is either request deadlock or allocation deadlock.

Deadlock of a state of transition system often means that there is no transition out of it, that is, the image of that state under the transition relation is empty. It can be shown that our definition of deadlock the emptiness of image under transition relation if the domain of the structure is finite.

We write $\mathbf{DL}$ for $(\exists p, x. \Box^* \{p \rightarrow x\}) \vee (\exists p, x. \Box^* \{p \leftarrow x\})$.

5 Main Theorem

In this section, we show Coffman conditions are necessary and sufficient for a finite resource allocation structure to be deadlock. Our main theorem is

Theorem 1. *For any finite resource allocation structure $M = (S, R, D, I)$ and any state $s \in S$, there is a natural number n which satisfies*

$$M, s \Vdash \mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{WF} \wedge \mathbf{NP} \supset (\mathbf{DL} \supset\subset \mathbf{CW}_n)$$

where $\mathbf{DL} \supset\subset \mathbf{CW}_n$ *is an abbreviation of* $(\mathbf{DL} \supset \mathbf{CW}_n) \wedge (\mathbf{DL} \subset \mathbf{CW}_n)$.

Proof. To show

$$M, s \Vdash \mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{WF} \wedge \mathbf{NP} \supset (\mathbf{CW}_n \supset \mathbf{DL}),$$

it suffices to give a formal proof of

$$\mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{WF} \wedge \mathbf{NP} \supset (\mathbf{CW}_n \supset \mathbf{DL})$$

by the soundness of the first order modal μ calculus. But this is deduced from

$$\mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{WF} \wedge \mathbf{NP} \supset \forall \bar{p}, \bar{x}.C_n(\bar{p}, \bar{x}) \supset \Box C_n(\bar{p}, \bar{x}),$$

which again is deduced from the following formal theorems of **RAAx**, that will be proved in lemma 6.

1. $\forall \bar{p}, \bar{x}.(C_n(\bar{p}, \bar{x}) \supset \Box p_i \neq p_j) \quad (0 \leq i \neq j \leq n)$
2. $\mathbf{NP1} \supset \forall \bar{p}, \bar{x}.(C_n(\bar{p}, \bar{x}) \supset \Box(p_{i+1} \leftarrow x_i)) \quad (0 \leq i \leq n, p_{n+1} = p_0)$
3. $\mathbf{WF1} \supset \forall \bar{p}, \bar{x}.(C_n(\bar{p}, \bar{x}) \supset \Box(p_i \rightleftarrows x_i)) \quad (0 \leq i \leq n, x_{-1} = x_n)$
4. $\mathbf{ME1} \supset \forall \bar{p}, \bar{x}.(C_n(\bar{p}, \bar{x}) \supset \Box(p_j \nleftarrow x_{i-1})) \quad (0 \leq i \neq j \leq n, x_{-1} = x_n)$
5. $\mathbf{ME1} \wedge \mathbf{WF1} \supset \forall \bar{p}, \bar{x}.(C_n(\bar{p}, \bar{x}) \supset \Box(p_i \rightarrow x_i)) \quad (0 \leq i \leq n)$

To show the converse

$$M, s \Vdash \mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{WF} \wedge \mathbf{NP} \supset (\mathbf{DL} \supset \mathbf{CW}_n), \tag{1}$$

we shall use the finiteness of M. Note that in a finite model of size m (i.e., if the domain consists of exactly m elements), any chain of length more than m contains a cycle. In other words, for each m and each state s of M,

$M, s \Vdash \mathbf{Chain}_m$ implies that there is $n \leq m$ such that $M, s \Vdash \mathbf{CW}_n$.

So, in order to prove (1), it suffices to show

$$M, s \Vdash \mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{WF} \wedge \mathbf{NP} \supset (\mathbf{DL} \supset \mathbf{Chain}_m),$$

which is equivalent to

$$M, s \Vdash \mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{WF} \wedge \mathbf{NP} \supset (\neg\mathbf{Chain}_m \supset \neg\mathbf{DL}).$$

Note that $\neg\mathbf{DL}$ is logically equivalent to

$$(\forall p, x.\Diamond^*\{p \nleftarrow x\}) \wedge (\forall p, x.\Diamond^*\{p \nrightarrow x\}),$$

Furthermore, $\forall p, x.\Diamond^*\{p \not\rightleftarrows x\}$ is its sufficient condition. So, it suffices to show

$$M, s \Vdash \mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{WF} \wedge \mathbf{NP} \supset (\neg\mathbf{Chain}_m \supset \forall p, x.\Diamond^*\{p \not\rightleftarrows x\}). \qquad (2)$$

Now, we say p is *reducible* if and only if p only requests resources which is allocated to no process: $\forall x.((p \rightarrow x) \supset \neg\exists q.(q \leftarrow x))$. A process is said to be *active* if and only if either p requests some resource or some resource is allocated to p: $\exists x.(p \rightarrow x) \vee (p \leftarrow x)$. It is *inactive* if it is not active. Then, (2) follows from the Lemma 1 and Lemma 2.

Lemma 1. *Assume a state s in a resource allocation structure M satisfies* $\mathbf{ME}\wedge\mathbf{ME0}\wedge\mathbf{WF}\wedge\mathbf{NP}$ *and length of chains in s is finitely bounded. Then the existence of active process in s implies the existence of active and reducible process in s. More formally,*

$$M, s \Vdash \mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{WF} \wedge \mathbf{NP} \wedge \neg\mathbf{Chain}_k \wedge \exists p.\mathrm{active}(p)$$

for some k implies

$$M, s \Vdash \exists p.\mathrm{active}(p) \wedge \mathrm{reducible}(p).$$

Proof. Assume $\mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{WF} \wedge \mathbf{NP} \wedge \neg\mathbf{Chain}_k$ holds at s for some natural number k. Suppose a process p is active in s. We shall argue by reductio ad absurdum and assume

$$M, s \Vdash \neg\exists q.(\mathrm{active}(q) \wedge \mathrm{reducible}(q)).$$

Since p is active, p is not reducible at s, so there exist x and p' such that $(p \rightarrow x) \wedge (p' \leftarrow x)$. Now p' is active, hence not reducible at s. This can be iterated for arbitrary many times, so there exists a chain of arbitrary (finite) length at s; in particular, we can form a chain of length k, which contradicts to our assumption $\neg\mathbf{Chain}_k$. Therefore, $M, s \Vdash \exists q.(\mathrm{active}(q) \wedge \mathrm{reducible}(q))$, as was to be shown.

Lemma 2. *Let $M = (S, R, D, I)$ be a resource allocation structure and s be a state in M. Assume* $\mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{WF} \wedge \mathbf{NP}$ *holds at s. Assume* $\mathrm{active}(p) \wedge \mathrm{reducible}(p)$ *also holds in s. Then there is a state s' in M subject to the following conditions.*

1. *s' is reachable from s, i.e., $s\ R^*\ s'$, where R^* is the reflexive transitive closure of R.*
2. *p is inactive at s'.*
3. *Any inactive process in s is also inactive in s'.*

More formally, for all $\pi \in D$ and for all valuations v such that $v(p) = \pi$,

$$M, s, v \Vdash \mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{WF} \wedge \mathbf{NP} \wedge (\neg\mathbf{isolated}(p) \wedge \mathbf{reducible}(p))$$

implies

> *there is a state s' such that $s\ R^*\ s'$, $M, s', v \Vdash \mathrm{inactive}(p)$ and, for all q, $M, s, v \Vdash \mathrm{inactive}(q)$ implies $M, s', v \Vdash \mathrm{inactive}(q)$.*

Proof. Assume $\mathrm{active}(p) \wedge \mathrm{reducible}(p)$ holds at s. **ME0** says that each resource requested by p at s is possibly allocated to p at some s_1 directly reachable from s. Since M is a resource allocation structure, request-allocate relation remains as for s and s_1 are exactly the same except for the request of p. By iterating this finitely many times, we can reach a state s'' where p requests no resources and the request-allocate relation remain exactly the same except for request of p because D is finite. **NP0** says that each resource allocated to p at s'' is possibly deallocated at some s_1'' directly reachable from s''. Again, the request-allocate relation at s'' remains the same at s_1'' except for allocation to p. Again, M is finite, so we can find a state s' where p is inactive, by iterating the above for finitely many times. Request-allocate relation at s' is the same as that at s except for allocation to p and request of p, as was to be shown.

This completes the proof of Theorem 1.

6 Conclusion and Future Work

In the framework of first order modal μ calculus, we have formalised Coffman's condition [2] and the notion of resource allocation system [10], both floating around for years but never formalised in a formal system, so far as we are aware of. Furthermore, we have shown that, in a finite resource allocation system which satisfies "mutual exclusion," "wait for" and "no preemption" conditions, there is a natural number n such that the system has a deadlock state if and only if it has a cycle of length n. The finiteness condition was not explicit in [2].

Our proof is based on satisfaction relation ($\Vdash$) and it remains to investigate whether the same theorem can be shown within our inference system, i.e., based on $\vdash$ relation. We expect that we shall need to develop number theory for that, and we shall need manipulate function symbols in some way, which is not provided in our first order modal μ calculus nor in usual predicate modal logics.

7 Appendix A (Formal Proofs)

Lemma 3. *Let φ and ψ be formulae, then the followings hold.*

1. *If $\vdash \varphi \supset \psi$, then $\vdash \Diamond^*\{\varphi\} \supset \Diamond^*\{\psi\}$ and $\vdash \Box^*\{\varphi\} \supset \Box^*\{\psi\}$.*
2. *If $\vdash \varphi \supset \Box\varphi$, then $\vdash \varphi \supset \Box^*\{\varphi\}$.*
3. *$\vdash \overbrace{\Diamond \ldots \Diamond}^{n} \varphi \supset \Diamond^*\{\varphi\}$ and $\vdash \Box^*\{\psi\} \supset \overbrace{\Box \ldots \Box}^{n} \psi$ for any natural number n.*

4. $\vdash \Diamond(\Diamond^*\{\varphi\}) \supset \Diamond^*\{\varphi\}$ *and* $\vdash \Box^*\{\psi\} \supset \Box(\Box^*\{\psi\})$.
5. $\vdash \Diamond^*\{\Diamond\varphi\} \supset \Diamond^*\{\varphi\}$ *and* $\vdash \Box^*\{\psi\} \supset \Box^*\{\Box\psi\}$.

Proof. We show only for first claims of (1), (3), (4) and (5), then we can show second claims of them similarly.
(1)

$$\dfrac{\dfrac{[\mu X.\, \varphi \vee \Diamond X] \qquad \dfrac{\dfrac{\overline{\varphi \supset \psi} \quad [(\varphi \vee \Diamond X)[(\mu Y.\, \psi \vee \Diamond Y)/X]]^{\mu\mathrm{E}}}{\vdots}}{\psi \vee \Diamond(\mu Y.\, \psi \vee \Diamond Y)}}{\mu Y.\, \psi \vee \Diamond Y}\ \mu\mathrm{E}}{(\mu X.\, \varphi \vee \Diamond X) \supset (\mu Y.\, \psi \vee \Diamond Y)}\ \mu\mathrm{I}$$

(2)

$$\dfrac{\dfrac{[\varphi]^{\supset\mathrm{I}} \qquad \dfrac{[\mu X.\, \neg\varphi \vee \Diamond X]^{\neg\mathrm{I}} \qquad \dfrac{\dfrac{[\varphi]^{\neg\mathrm{I}} \quad [\neg\varphi \vee \Diamond\neg\varphi]^{\mu\mathrm{E}}}{\neg\Box\varphi} \qquad \dfrac{[\varphi]^{\neg\mathrm{I}} \quad \overline{\varphi \supset \Box\varphi}}{\Box\varphi}}{\dfrac{\bot}{\neg\varphi}\ \neg\mathrm{I}}\ \mu\mathrm{E}}{\neg\varphi}}{\dfrac{\bot}{\neg(\mu X.\, \neg\varphi \vee \Diamond X)}\ \neg\mathrm{I}}}{\varphi \supset \neg(\mu X.\, \neg\varphi \vee \Diamond X)}\ \supset\mathrm{I}$$

Recall that $\nu X.\, \varphi \wedge \Box X$ is an abbreviation of $\neg\mu X.\, \neg\varphi \vee \Diamond X$.
(3) We only show cases $n = 0$ and $n = 1$.

$$\dfrac{\dfrac{[\varphi]}{\varphi \vee \Diamond(\mu Z.\, \varphi \vee \Diamond Z)}\ \vee\mathrm{I}}{\dfrac{\mu Z.\, \varphi \vee \Diamond Z}{\varphi \supset (\mu Z.\, \varphi \vee \Diamond Z)}\ \supset\mathrm{I}}\ \mu\mathrm{I} \qquad \dfrac{\dfrac{\dfrac{[\Diamond\varphi]}{\vdots}\ \vee\mathrm{I}}{\varphi \vee \Diamond(\varphi \vee \Diamond(\mu Z.\, \varphi \vee \Diamond Z))}}{\vdots}\ \mu\mathrm{I}}{\dfrac{\varphi \vee \Diamond(\mu Z.\, \varphi \vee \Diamond Z)}{\Diamond\varphi \supset (\mu Z.\, \varphi \vee \Diamond Z)}\ \supset\mathrm{I}}\ \mu\mathrm{I}$$

(4)

$$\dfrac{\dfrac{\dfrac{[\Diamond(\mu X.\, \varphi \vee \Diamond X)]}{\varphi \vee \Diamond(\mu X.\, \varphi \vee \Diamond X)}\ \vee\mathrm{I}}{\mu X.\, \varphi \vee \Diamond X}\ \mu\mathrm{I}}{\Diamond(\mu X.\, \varphi \vee \Diamond X) \supset (\mu X.\, \varphi \vee \Diamond X)}$$

(5)

$$\dfrac{\dfrac{[\mu X.\,(\Diamond\varphi)\vee\Diamond X] \qquad \dfrac{\dfrac{[((\Diamond\varphi)\vee\Diamond X)[(\mu Y.\,\varphi\vee\Diamond Y)/X]]^{\mu\mathrm{E}}}{\vdots\ (3)}}{\dfrac{\Diamond(\mu Y.\,\varphi\vee\Diamond Y)\vee\Diamond(\mu Y.\,\varphi\vee\Diamond Y)}{\Diamond(\mu Y.\,\varphi\vee\Diamond Y)}}}{\vdots\ (4)}}{\dfrac{\mu Y.\,\varphi\vee\Diamond Y}{(\mu X.\,(\Diamond\varphi)\vee\Diamond X)\supset(\mu Y.\,\varphi\vee\Diamond Y)}\ \supset\mathrm{I}}\ \mu\mathrm{E}$$

Lemma 4. *The following formulae are theorems of* **RAAx**.

1. $\forall p,x,y.\,((p\to x)\wedge(p\to y)\supset\Box((p\not\rightleftarrows x)\supset(p\nleftarrow y)))$ (**OA**(**RR′**))
2. $\forall p,x,y.\,((p\leftarrow x)\wedge(p\to y)\supset\Box((p\nleftarrow x)\supset(p\to y)))$ (**OA**(**AR**))
3. $\forall p,x,y.\,((p\leftarrow x)\wedge(p\leftarrow y)\supset\Box((p\nleftarrow x)\supset(p\nrightarrow y)))$ (**OA**(**AA**))
4. $\forall p,x,y.\,((p\not\rightleftarrows x)\wedge(p\to y)\supset\Box((p\rightleftarrows x)\supset(p\to y)))$ (**OA**(**NR**))
5. $\forall p,x,y.\,((p\not\rightleftarrows x)\wedge(p\leftarrow y)\supset\Box((p\rightleftarrows x)\supset(p\leftarrow y)))$ (**OA**(**NA**))
6. $\forall p,x,y.\,((p\not\rightleftarrows x)\wedge(p\not\rightleftarrows y)\supset\Box((p\rightleftarrows x)\supset(p\nleftarrow y)))$ (**OA**(**NN**))
7. $\forall p,q,x,y.\,((p\to x)\wedge(q\leftarrow y)\wedge p\neq q\supset\Box((p\leftarrow x)\supset(q\leftarrow y)))$ (**OP**(**AA**))
8. $\forall p,q,x,y.\,((p\to x)\wedge(q\not\rightleftarrows y)\wedge p\neq q\supset\Box((p\leftarrow x)\supset(q\not\rightleftarrows y)))$ (**OP**(**AN**))
9. $\forall p,q,x,y.\,((p\rightleftarrows x)\wedge(q\not\rightleftarrows y)\wedge p\neq q\supset\Box((p\not\rightleftarrows x)\supset(q\not\rightleftarrows y)))$ (**OP**(**NN**))

Proof. We show only (2) and (7), then we can also show others similarly.
(2)

$$\dfrac{\dfrac{[p\leftarrow x)\wedge(p\to y)] \qquad \dfrac{[\mathbf{OA}(\mathbf{RA})]}{(p\to y)\wedge(p\leftarrow x)\supset\Box((p\nrightarrow y)\supset(p\leftarrow x))}}{\Box((p\nrightarrow y)\supset(p\leftarrow x))}}{\vdots}$$
$$\dfrac{\Box((p\nleftarrow x)\supset(p\to y))}{(p\leftarrow x)\wedge(p\to y)\supset\Box((p\nleftarrow x)\supset(p\to y))}$$

(7)

$$\dfrac{\dfrac{[\mathbf{PA}(\mathbf{A})]}{\vdots}}{\dfrac{(q\leftarrow y)\supset\Box((q\nleftarrow y)\supset(q\not\rightleftarrows y)) \qquad \dfrac{\dfrac{[\mathbf{OP}(\mathbf{NR})]}{(q\rightleftarrows y)\wedge(p\to x)\wedge p\neq q\supset\Box((q\not\rightleftarrows y)\supset(p\to x))}}{\dfrac{(q\leftarrow y)\wedge(p\to x)\wedge p\neq q\supset\Box((q\not\rightleftarrows y)\supset(p\to x))}{\vdots\ \mathbf{NoMult}}}}{(q\leftarrow y)\wedge(p\to x)\wedge p\neq q\supset\Box((q\not\rightleftarrows y)\supset(p\nleftarrow x))}}{\dfrac{(q\leftarrow y)\wedge(p\to x)\wedge p\neq q\supset\Box((q\nleftarrow y)\supset(p\nleftarrow x))}{\vdots}}$$
$$(p\to x)\wedge(q\leftarrow y)\wedge p\neq q\supset\Box((p\leftarrow x)\supset(q\leftarrow y))$$

Lemma 5. *The following variant* **ME1***b of* **ME1** *is provable from* **RAAx**, **ME**, *i.e.* **ME** $\supset$ **ME1***b is a theorem of* **RAAx**.

$$\Box^*\{\,\forall p,q,x.\,((p\leftarrow x)\supset\Box(p\neq q\supset(q\nleftarrow x)))\,\}\quad(\mathbf{ME1}b)$$

Proof. Let φ and ψ be formulae. To show that $\vdash \Box^*\{\,\varphi\,\} \supset \Box^*\{\,\psi\,\}$, it suffices to show that $\vdash \varphi \supset \psi$ by lemma 3. So let $\mathbf{ME}'$ be the formula $\neg\exists p, q, x.\,(p \neq q \wedge (p \leftarrow x) \wedge (q \leftarrow x))$ and then we show that $\mathbf{ME}' \supset \forall p, q, x.\,((p \leftarrow x) \supset \Box(p \neq q \supset (q \nleftarrow x)))$ is a theorem of **RAAx**.

$$\dfrac{\dfrac{[\mathbf{Eq}]}{p \neq q \supset \Box p \neq q} \quad \dfrac{\dfrac{\dfrac{\Delta_2}{\bot}}{\Box(q \nleftarrow x)}\,\mathbf{RAA}}{(p \leftarrow x) \wedge p \neq q \supset \Box(q \nleftarrow x)}}{\begin{array}{c}(p \leftarrow x) \wedge (\Box p \neq q) \supset \Box(q \nleftarrow x) \\ \vdots \\ (p \leftarrow x) \supset \Box(p \neq q \supset (q \nleftarrow x)) \\ \hline \forall p, q, x.\,((p \leftarrow x) \supset \Box(p \neq q \supset (q \nleftarrow x)))\end{array}}$$

$$\dfrac{\dfrac{[\Diamond(q \leftarrow x)] \quad \Box(p \neq q \wedge ((q \leftarrow x) \supset (p \leftarrow x)))}{\Diamond((q \leftarrow x) \wedge (p \leftarrow x) \wedge p \neq q)} \quad \dfrac{\begin{array}{c}(p \leftarrow x) \wedge p \neq q \wedge (q \nleftarrow x) \\ \vdots\ \mathbf{OP}(\mathbf{AA}) \\ [(p \leftarrow x) \wedge p \neq q] \\ \vdots \\ (p \leftarrow x) \wedge p \neq q \supset (q \nleftarrow x)\end{array}}{\Box((p \leftarrow x) \wedge p \neq q \supset (q \nleftarrow x))}}{\Delta_2}$$

Lemma 6. *The following formulae are theorems of* **RAAx** *for any natural number* $n \geq 1$.

1. $\forall \bar{p}, \bar{x}.\,(C_n(\bar{p}, \bar{x}) \supset \Box(p_i \neq p_j)) \quad (0 \leq i \neq j \leq n)$
2. $\mathbf{NP1} \supset \forall \bar{p}, \bar{x}.\,(C_n(\bar{p}, \bar{x}) \supset \Box(p_{i+1} \leftarrow x_i)) \quad (0 \leq i \leq n, p_{n+1} = p_0)$
3. $\mathbf{WF1} \supset \forall \bar{p}, \bar{x}.\,(C_n(\bar{p}, \bar{x}) \supset \Box(p_i \rightleftarrows x_i)) \quad (0 \leq i \leq n, x_{-1} = x_n)$
4. $\mathbf{ME} \supset \forall \bar{p}, \bar{x}.\,(C_n(\bar{p}, \bar{x}) \supset \Box(p_j \nleftarrow x_{i-1})) \quad (0 \leq i \neq j \leq n, x_{-1} = x_n)$
5. $\mathbf{ME} \wedge \mathbf{WF1} \supset \forall \bar{p}, \bar{x}.\,(C_n(\bar{p}, \bar{x}) \supset \Box(p_i \rightarrow x_i)) \quad (0 \leq i \leq n)$
6. $\mathbf{ME} \wedge \mathbf{WF1} \wedge \mathbf{NP1} \supset \forall \bar{p}, \bar{x}.\,(C_n(\bar{p}, \bar{x}) \supset \Box C_n(\bar{p}, \bar{x}))$

Proof. Since (5) is clearly shown by (3) and (4), we show (1),(2),(3) and (4). Then we have (6) from (5).
(1)

$$\dfrac{\dfrac{[C_n(\bar{p}, \bar{x})]}{\vdots}}{\dfrac{p_i \neq p_j}{\dfrac{\Box p_i \neq p_j}{C_n(\bar{p}, \bar{x}) \supset \Box p_i \neq p_j}}} \quad \dfrac{\dfrac{[\mathbf{Eq}]}{\vdots\ \forall\mathrm{E}, \wedge\mathrm{E}}}{p_i \neq p_j \supset \Box(p_i \neq p_j)}$$

where $0 \leq i \neq j \leq n$.

(2)

$$\dfrac{\dfrac{\dfrac{\dfrac{[C_n(\bar{p},\bar{x})]}{\vdots}}{\dfrac{p_{i+1}\to x_{i+1}}{\exists x.\, p_{i+1}\to x}} \quad \dfrac{\dfrac{[C_n(\bar{p},\bar{x})]}{\vdots}}{p_{i+1}\leftarrow x_i}}{(\exists x.\, p_{i+1}\to x)\wedge(p_{i+1}\leftarrow x_i)} \quad \dfrac{[\mathbf{NP1}]}{(\exists x.\, p_{i+1}\to x)\wedge(p_{i+1}\leftarrow x_i)\supset\Box(p_{i+1}\leftarrow x_i)}}{\Box(p_{i+1}\leftarrow x_i)}}{C_n(\bar{p},\bar{x})\supset\Box(p_{i+1}\leftarrow x_i)}$$

where $0\le i\le n, p_{n+1}=p_0$.
(3)

$$\dfrac{\dfrac{\dfrac{[C_n(\bar{p},\bar{x})]}{\vdots}}{p_i\to x_i} \quad \dfrac{\dfrac{[C_n(\bar{p},\bar{x})]}{\vdots}}{\dfrac{p_i\leftarrow x_{i-1}}{\exists x.\,(p_i\leftarrow x)}}}{(p_i\to x_i)\wedge\exists x.\,(p_i\leftarrow x)} \quad \dfrac{[\mathbf{WF1}]}{(p_i\to x_i)\wedge(\exists x.\, p_i\leftarrow x)\supset\Box(p_i\rightleftarrows x_i)}}{\Box(p_i\rightleftarrows x_i)}}{C_n(\bar{p},\bar{x})\supset\Box(p_i\rightleftarrows x_i)}$$

where $0\le i\le n$ and $x_{-1}=x_n$.
(4)

$$\dfrac{\dfrac{\dfrac{\dfrac{[C_n(\bar{p},\bar{x})]}{\vdots}}{p_i\leftarrow x_{i-1}} \quad \dfrac{\dfrac{[C_n(\bar{p},\bar{x})]}{\vdots}}{\Box(p_i\neq p_j)}}{(p_i\leftarrow x_{i-1})\wedge\Box(p_i\neq p_j)} \quad \dfrac{\dfrac{[\mathbf{ME1}b]}{\vdots}}{(p_i\leftarrow x_{i-1})\wedge\Box(p_i\neq p_j)\supset\Box(p_j\nleftarrow x_{i-1})}}{\Box(p_j\nleftarrow x_{i-1})}}{C_n(\bar{p},\bar{x})\supset\Box(p_j\nleftarrow x_{i-1})}$$

where $0\le i\ne j\le n$ and $x_{-1}=x_n$. Thus

$$\mathbf{ME}\wedge\mathbf{WF1}\wedge\mathbf{NP1}\supset C_n(\bar{p},\bar{x})\supset\bigwedge_{0\le i\ne j\le n}\Box((p_i\neq p_j)\wedge(p_i\to x_i)\wedge(p_{i+1}\leftarrow x_i)),$$

is a theorems of **RAAx**, hence so is

$$\mathbf{ME}\wedge\mathbf{WF1}\wedge\mathbf{NP1}\supset\forall\bar{p},\bar{x}.\,(C_n(\bar{p},\bar{x})\supset\Box C_n(\bar{p},\bar{x})).$$

Lemma 7. *The followings are theorems of* **RAAx**.

1. $\mathbf{ME}\wedge\mathbf{WF1}\wedge\mathbf{NP1}\supset C(p,q,x,y)\wedge(p\leftarrow z)\supset\Box^*\{C(p,q,x,y)\wedge(p\leftarrow z)\}$
2. $\mathbf{ME}\wedge\mathbf{WF1}\wedge\mathbf{NP1}\supset C(p,q,x,y)\wedge(p\to z)\supset\Box^*\{C(p,q,x,y)\wedge(p\rightleftarrows z)\}$
3. $\mathbf{ME}\wedge\mathbf{WF1}\wedge\mathbf{NP1}\wedge C(p,q,x,y)\supset\mathbf{RL}\wedge\mathbf{AL}$

Proof. (3) is easily shown by (1) and (2), so we show only (1) and (2).
(1)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[C(p,q,x,y)]}{(p \to x)}}{\exists w.\,(p \to w)} \quad [p \leftarrow z]}{(\exists w.\,(p \to w)) \wedge (p \leftarrow z)} \quad \dfrac{[\mathbf{NP1}]}{(\exists w.\,(p \to w)) \wedge (p \leftarrow z) \supset \Box(p \leftarrow z)}}{\Box(p \leftarrow z)}}{\Box(C(p,q,x,y) \wedge (p \leftarrow z))}}{C(p,q,x,y) \wedge (p \leftarrow z) \supset \Box(C(p,q,x,y) \wedge (p \leftarrow z))}}{C(p,q,x,y) \wedge (p \leftarrow z) \supset \Box^*\{C(p,q,x,y) \wedge (p \leftarrow z)\}}$$

(2)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[C(p,q,x,y)]}{(p \leftarrow y)}}{\exists u.\,(p \leftarrow u)} \quad \dfrac{[\mathbf{WF1}]}{(p \to z) \wedge (\exists u.\,(p \leftarrow u)) \supset \Box(p \rightleftarrows z)}}{\Box(p \rightleftarrows z)}}{\Box(C(p,q,x,y) \wedge (p \rightleftarrows z))}}{C(p,q,x,y) \wedge (p \to z) \supset \Box(C(p,q,x,y) \wedge (p \rightleftarrows z))}$$

Let C be an abbreviation of $C(p,q,x,y)$, R that of $p \to z$ and A that of $p \leftarrow z$.

$$\dfrac{\dfrac{[C \wedge (R \vee A)] \quad \Box(C \wedge (R \vee A)) \quad \dfrac{\Box(C \wedge A)}{\Box(C \wedge (R \vee A))}}{\Box(C \wedge (R \vee A))}\ \vee\mathrm{E}}{C \wedge (R \vee A) \supset \Box(C \wedge (R \vee A))}\ \supset \mathrm{I}$$

where $[C \wedge R]^{\vee\mathrm{E}}$ is discharged by (2) and $[C \wedge A]^{\vee\mathrm{E}}$ by (1).

Then the following is a theorem of **RAAx**

$\mathbf{ME} \wedge \mathbf{WF} \wedge \mathbf{NP} \supset \forall p,q,x,y,z.\,(C(p,q,x,y) \wedge (p \rightleftarrows z) \supset \Box^*\{C(p,q,x,y) \wedge (p \rightleftarrows z)\})$,

hence so is

$\mathbf{ME} \wedge \mathbf{WF} \wedge \mathbf{NP} \supset \forall p,q,x,y,z.\,(C(p,q,x,y) \wedge (p \to z) \supset \Box^*\{C(p,q,x,y) \wedge (p \rightleftarrows z)\})$.

8 Appendix B (Soundness)

Lemma 8 (Substitution Lemma). *Let $\mathcal{A} = (S,R,D,I)$ be a structure, (v,V) a valuation and φ, ψ formulae. Then the following holds.*

$$[\![\varphi[\psi/X]]\!]_{(v,V)} = [\![\varphi]\!]_{(v,V[[\![\psi]\!]_{(v,V)}/X])}.$$

Proof. We show the lemma by induction on the construction of a formula φ. We skip proofs of cases in which φ is an atomic formula or of the form $\neg\theta, \theta \vee \theta', \Box\theta$ for some formulae θ and θ'.

Case: φ is a formula of the form $\forall x.\, \theta$ We may assume that ψ has no free occurrence of x. Then the following holds.

$$\begin{aligned}
[\![(\forall x.\, \theta)[\psi/X]]\!]_{(v,V)} &= [\![\forall x.\, (\theta[\psi/X])]\!]_{(v,V)} \\
&= \bigcap \{\, [\![\theta[\psi/X]]\!]_{(v[d/x],V)} \mid d \in D \,\} \\
&= \bigcap \{\, [\![\theta]\!]_{(v[d/x],V[[\![\psi]\!]_{(v[d/x],V)}/X])} \mid d \in D \,\} \\
&= \bigcap \{\, [\![\theta]\!]_{(v[d/x],V[[\![\psi]\!]_{(v,V)}/X])} \mid d \in D \,\} \\
&= [\![\forall x.\, \theta]\!]_{(v,V[[\![\psi]\!]_{(v,V)}/X])}
\end{aligned}$$

Case: φ is a formula of the form $\mu Y.\, \theta$ We may assume that ψ has no free occurrence of Y. Then the following holds.

$$\begin{aligned}
[\![(\mu Y.\, \theta)[\psi/X]]\!]_{(v,V)} &= [\![\mu Y.\, (\theta[\psi/X])]\!]_{(v,V)} \\
&= \bigcap \{\, T \mid [\![\theta[\psi/X]]\!]_{(v,V[T/Y])} \subseteq T \,\} \\
&= \bigcap \{\, T \mid [\![\theta]\!]_{(v,V[T/Y][[\![\psi]\!]_{(v,V[T/Y])}/X])} \subseteq T \,\} \\
&= \bigcap \{\, T \mid [\![\theta]\!]_{(v,V[T/Y][[\![\psi]\!]_{(v,V)}/X])} \subseteq T \,\} \\
&= [\![\mu Y.\, \theta]\!]_{(v,V[[\![\psi]\!]_{(v,V)}/X])}
\end{aligned}$$

Now we prove soundness of our proof system. For showing soundness, it suffices to show the following (more generalized) theorem, because provable formulae have derivations without uncancelled hypotheses. For a derivation $\mathcal{D}$ with conclusion φ, we write $\Gamma(\mathcal{D}, \varphi)$ for the collection of all uncancelled hypotheses in $\mathcal{D}$.

Theorem 2 (Soundness). *Let φ be a formula and $\mathcal{D}$ a derivation with conclusion φ. Then the following holds for any structure $\mathcal{A}$ and any valuation (v, V)*

$$\bigcap \{\, [\![\theta]\!]^{\mathcal{A}}_{(v,V)} \mid \theta \in \Gamma(\mathcal{D}, \varphi) \,\} \subseteq [\![\varphi]\!]^{\mathcal{A}}_{(v,V)}$$

provided that $\bigcap \{\, [\![\theta]\!]^{\mathcal{A}}_{(v,V)} \mid \theta \in \Gamma(\mathcal{D}, \varphi) \,\} = S$ if $\Gamma(\mathcal{D}, \varphi) = \emptyset$ (i.e. φ is provable).

Proof. We prove the theorem by induction on a derivation with conclusion φ. We fix a structure $\mathcal{A} = (S, R, D, I)$ and a valuation (v, V) unless stated otherwise.

If a derivation $\mathcal{D}$ with conclusion φ has one unique element, then the hypothese of $\mathcal{D}$ must be φ, so $\Gamma(\mathcal{D}, \varphi) = \{\, \varphi \,\}$, hence the claim clearly holds.

If a derivation $\mathcal{D}$ has more than one element, the we prove the claim for each inference rule applied to $\mathcal{D}$ in the end. We remark that the set $\bigcap \{\, [\![\theta]\!]^{\mathcal{A}}_{(v,V)} \mid \theta \in \Gamma(\mathcal{D}, \varphi) \,\}$ may be equal to S in the following cases but $\neg$E. Besides, we skip proofs for cases $\vee$I1, $\vee$I2, $\forall$E and $\Box$E.

Case: BF and CBF In these cases, there are no uncancelled hypotheses in derivations, so we need to show that

$$[\![(\forall x.\, \Box\varphi) \supset \Box\forall x.\, \varphi]\!]^{\mathcal{A}}_{(v,V)} = [\![(\Box\forall x.\, \varphi) \supset \forall x.\, \Box\varphi]\!]^{\mathcal{A}}_{(v,V)} = S.$$

This is shown by the following fact.

$$[\![\Box\forall x.\, \varphi]\!]^{\mathcal{A}}_{(v,V)} = [\![\forall x.\, \Box\varphi]\!]^{\mathcal{A}}_{(v,V)}$$

In the sequel, we write $[\![\varphi]\!]_{(v,V)}$ or $[\![\varphi]\!]$ for $[\![\varphi]\!]^{\mathcal{A}}_{(v,V)}$ if $\mathcal{A}$ and (v, V) are understood.

Case: $\vee E$ By induction hypothesis, we have

- $\bigcap\{\, [\![\theta]\!] \mid \theta \in \Gamma(\mathcal{D}, \chi)\,\} \subseteq [\![\varphi \vee \psi]\!]$,
- $[\![\varphi]\!] \cap \bigcap\{\, [\![\theta]\!] \mid \theta \in \Gamma(\mathcal{D}, \chi)\,\} \subseteq [\![\chi]\!]$ and
- $[\![\psi]\!] \cap \bigcap\{\, [\![\theta]\!] \mid \theta \in \Gamma(\mathcal{D}, \chi)\,\} \subseteq [\![\chi]\!]$.

Then $\bigcap\{\, [\![\theta]\!] \mid \theta \in \Gamma(\mathcal{D}, \chi)\,\} \subseteq [\![\chi]\!]$.

Case: $\neg I$ By induction hypothesis, we have

- $[\![\varphi]\!] \cap \bigcap\{\, [\![\theta]\!] \mid \theta \in \Gamma(\mathcal{D}, \neg\varphi)\,\} \subseteq [\![\bot]\!]\ (= \emptyset)$.

Then $\bigcap\{\, [\![\theta]\!] \mid \theta \in \Gamma(\mathcal{D}, \neg\varphi)\,\} \subseteq [\![\neg\varphi]\!]$.

Case: $\neg E$ By induction hypothesis, we have

- $\bigcap\{\, [\![\theta]\!] \mid \theta \in \Gamma(\mathcal{D}, \bot)\,\} \subseteq [\![\varphi]\!]$ and
- $\bigcap\{\, [\![\theta]\!] \mid \theta \in \Gamma(\mathcal{D}, \bot)\,\} \subseteq [\![\neg\varphi]\!]$.

Then the set $\bigcap\{\, [\![\theta]\!] \mid \theta \in \Gamma(\mathcal{D}, \bot)\,\}$ must be the empty set, because $[\![\varphi]\!] \cap [\![\neg\varphi]\!] = \emptyset$ (i.e. $\bot$ is not provable). Thus we have

$$\bigcap\{\, [\![\theta]\!] \mid \theta \in \Gamma(\mathcal{D}, \bot)\,\} \subseteq [\![\bot]\!].$$

Case: RAA By induction hypothesis, we have

- $[\![\neg\varphi]\!] \cap \bigcap\{\, [\![\theta]\!] \mid \theta \in \Gamma(\mathcal{D}, \varphi)\,\} \subseteq [\![\bot]\!]\ (= \emptyset)$.

Then we also have $\bigcap\{\, [\![\theta]\!] \mid \theta \in \Gamma(\mathcal{D}, \varphi)\,\} \subseteq [\![\varphi]\!]$.

Case: $\forall I$ By induction hypothesis, for any $d \in D$, we have

$$\bigcap_{\theta}\{\, [\![\theta]\!]_{(v[d/y],V)} \mid \theta \in \Gamma(\mathcal{D}, \forall x.\, \varphi)\,\} \subseteq [\![\varphi[y/x]]\!]_{(v[d/y],V)},$$

and then we also have

$$\bigcap_{d\in D}\bigcap_{\theta}\{\, [\![\theta]\!]_{(v[d/y],V)} \mid \theta \in \Gamma(\mathcal{D}, \forall x.\, \varphi)\,\} \subseteq [\![\forall x.\, \varphi]\!]_{(v,V)}.$$

On the other hand, there are no formulae θ of $\Gamma(\mathcal{D}, \forall x.\, \varphi)$ containing a free occurrence of y by a side condition of $\forall$I. Then $[\![\theta]\!]_{(v[d/y],V)} = [\![\theta]\!]_{(v,V)}$ for any $d \in D$ and any $\theta \in \Gamma(\mathcal{D}, \forall x.\, \varphi)$, so we have

$$\bigcap\{\, [\![\theta]\!]_{(v,V)} \mid \theta \in \Gamma(\mathcal{D}, \forall x.\, \varphi)\,\} = \bigcap_{d\in D}\bigcap_{\theta}\{\, [\![\theta]\!]_{(v[d/y],V)} \mid \theta \in \Gamma(\mathcal{D}, \forall x.\, \varphi)\,\}.$$

Case: $\Box I$ By a side condition of $\Box$I, the subderivation $\mathcal{D}'$ of $\mathcal{D}$ with conclusion φ, which is the premise of $\Box\varphi$ in $\mathcal{D}$, has no uncancelled hypotheses. So $[\![\varphi]\!] = S$ by induction hypothes. Thus, by definition of $[\![\Box\varphi]\!]$, we have $[\![\Box\varphi]\!] = S$.

Case: μI By induction hypothese, we have

- $\bigcap\{[\![\theta]\!]_{(v,V)} \mid \theta \in \Gamma(\mathcal{D}, \mu X.\, \varphi)\} \subseteq [\![\varphi[(\mu X.\, \varphi)/X]]\!]_{(v,V)}$.

On the other hand, $[\![\mu X.\, \varphi]\!]_{(v,V)}$ is the least fixed-point of the function $F^{\varphi}_{X} : T \mapsto [\![\varphi]\!]_{(v,V[T/X])}$ on $\mathcal{P}(S)$. Then

$$[\![\varphi[(\mu X.\, \varphi)/X]]\!]_{(v,V)} = [\![\varphi]\!]_{(v,V[[\![\mu X.\, \varphi]\!]_{(v,V)}/X])} = [\![\mu X.\, \varphi]\!]_{(v,V)}.$$

by lemma 8. Thus we have

$$\bigcap\{\, [\![\theta]\!]_{(v,V)} \mid \theta \in \Gamma(\mathcal{D}, \mu X.\, \varphi)\,\} \subseteq [\![\mu X.\, \varphi]\!]_{(v,V)}.$$

Case: μE By a side condition of the inference rule μE, the subderivation $\mathcal{D}'$ of $\mathcal{D}$ with conclusion ψ, which is a premise of the conclusion ψ of $\mathcal{D}$, has only one uncancelled hypothese $\varphi[\psi/X]$. Then, by induction hypothese, we have

- $\bigcap\{[\![\theta]\!]_{(v,V)} \mid \theta \in \Gamma(\mathcal{D}, \psi)\} \subseteq [\![\mu X.\, \varphi]\!]_{(v,V)}$ and
- $[\![\varphi[\psi/X]]\!]_{(v,V)} \subseteq [\![\psi]\!]_{(v,V)}$.

Then, by lemma 8, $[\![\psi]\!]_{(v,V)}$ is a pre-fixed point of the function $F^{\varphi}_{X} : T \mapsto [\![\varphi]\!]_{(v,V[T/X])}$ on $\mathcal{P}(S)$, hence $[\![\mu X.\, \varphi]\!]_{(v,V)} \subseteq [\![\psi]\!]_{(v,V)}$. Finally we have

$$\bigcap\{\, [\![\theta]\!]_{(v,V)} \mid \theta \in \Gamma(\mathcal{D}, \psi)\,\} \subseteq [\![\psi]\!]_{(v,V)}.$$

9 Appendix C (Necessity of Other Coffman Conditions)

We formalised Coffman conditions and deadlock as $\mathbf{ME}, \mathbf{ME0}, \mathbf{WF}, \mathbf{NP}, \mathbf{CW}$ and $\mathbf{DL}$ and show that for every natural number n, $\mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{WF} \wedge \mathbf{NP} \supset (\mathbf{CW}_n \supset\subset \mathbf{DL})$ is a theorem of a resource allocation theory. It is natural to show that "wait for" and "no preemption" conditions are also necessary for deadlock, i.e.

1. $\mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{NP} \wedge \mathbf{CW}_n \supset (\neg\mathbf{WF} \supset \neg\mathbf{DL})$ and
2. $\mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{WF} \wedge \mathbf{CW}_n \supset (\neg\mathbf{NP} \supset \neg\mathbf{DL})$

are theorems of a resource allcoation theory for any natural number n. But not postulating "wait for" ("no preemption") conditon can not been expressed $\neg\mathbf{WF}$ (respectively $\neg\mathbf{NP}$), because they are conditions for a system, i.e. conditions saying that certain property hold for any processes and resources at any reachable state, so they are of the form $\Box^*\{\forall p, x.\, \varphi\}$. In this section we introduce formule **WF2** and **NP2** to formalise "not postulating wait for" condition as $\mathbf{WF0} \wedge \mathbf{WF2}$ and "not postulating no preemption" conditions as $\mathbf{NP0} \wedge \mathbf{NP2}$,

and then show necessity of them. Now we formalise "not postulating wait for condition" and "not postulating no preemption condition".

Not postulating "wait for" conditon would mean that, whenever a process p is requesting a resour x, p can possibly cancell x, and this could be expressed as

$$\Box^*\{\forall p, x.\, ((p \to x) \supset \Diamond(p \not\rightleftarrows x))\}$$

which is logically equivalent to the conjunction of **WF0** and

WF2 $\Box^*\{\forall p, x.\, ((p \to x) \supset (\exists y.\, (p \leftarrow y)) \supset \Diamond(p \not\rightleftarrows x))\}$.

Moreover **WF2** is opposite to **WF1** in a sense, because

$$\mathbf{RAAx} \vdash\ (p \to x) \wedge (\exists y.\, (p \leftarrow y)) \supset (\neg\Box(p \not\rightleftarrows x) \supset\subset \Diamond(p \not\rightleftarrows x)).$$

We say that a resource allocation structure does not satisfy "wait for" condition if **WF0** and **WF2** are valid in it.

Not postulating "no preemption" conditon would mean that, whenever a resource x is allocated to a process p, x is possibly deallocated from p, and this could be expressed as

$$\Box^*\{\forall p, x.\, ((p \leftarrow x) \supset \Diamond(p \not\rightleftarrows x))\}.$$

So we also introduce

NP2 $\Box^*\{\forall p, x.\, ((p \leftarrow x) \supset (\exists y.\, (p \to y)) \supset \Diamond(p \not\rightleftarrows x))\}$

and say that a resource allocation structure does not satisfy "no preemption" condition if **NP0** and **NP2** are valid in it.

9.1 Finite Branching Resource Allocation Theories

In our resource allocation structure, the number of requests by a process may be infinite. But in classical deadlock problems, it is always finite. This cause problems, for example, let $\mathcal{A} = \langle S, R, D, I\rangle$ be a resource allocation structure satisfying "mutual exclusion", "wait for" and "no preemption" conditions, s a state. Suppose that

$$\mathcal{A}, s, (v, V) \Vdash p \leftarrow x \wedge \neg\exists y, q.\, ((p \to y) \wedge (q \leftarrow y)).$$

Of course $v(x)$ possibly deallocate from $v(p)$ if the number of requests of $v(p)$ is finite. On the other hand, $v(x)$ is allocated to $v(p)$ at any reachable state from s if it is infinite , because $v(p)$ must satisfy its inifitely many requests before deallocating $v(x)$, hence s is deadlock. But this contradicts to necessity of "circular wait" condition for deadlock.

To overcome the gap between finite and infinite, we adopt the axioms below

- $\forall q.\, ((\forall y.\, \varphi \wedge (q \to y) \supset \Diamond(\varphi \wedge (q \nrightarrow y))) \supset (\varphi \supset \Diamond^*\{\varphi \wedge \neg\exists y.\, (q \to y)\})$
- $\forall q.\, ((\forall y.\, \psi \wedge (q \leftarrow y) \supset \Diamond(\psi \wedge (q \not\rightleftarrows y))) \supset (\psi \supset \Diamond^*\{\psi \wedge \neg\exists y.\, (q \leftarrow y)\})$

for formulas φ and ψ, and call them *finite branching axioms* We say that a resource allocation theory is *finite branching* if it contains all the axioms above.

Now we show necessity of the rest of Coffman conditions. But we often show only sketches of proofs instead of complete formal proofs.

Proposition 3. *The followings are theorems of a finite branching resource allocation theory.*

1. $\mathbf{ME0} \wedge \mathbf{NP0} \wedge \mathbf{WF2} \supset \forall p, x.\, ((p \to x) \supset \Diamond^*\{(p \leftarrow x)\})$
2. $\mathbf{NP0} \wedge \mathbf{WF2} \supset \forall p, x.\, ((p \leftarrow x) \supset \Diamond^*\{(p \not\rightleftarrows x)\})$
3. $\mathbf{ME0} \wedge \mathbf{NP0} \supset (\mathbf{WF2} \supset \neg\mathbf{DL})$

Proof. We show that (1) and (2) are theorems of a finite branching resource allocation theory because (3) is provable from (1) and (2) in general.

proof of (1) To show that (1) is a theorem of the theory, it suffices to show that (1a), (1b) and (1c) are theorems of the theory.

1a $\mathbf{ME0} \supset ((p \to x) \wedge (\neg\exists q.\, (q \leftarrow x)) \supset \Diamond(p \leftarrow x))$
1b $\mathbf{ME0} \wedge \mathbf{NP0} \supset ((p \to x) \wedge (q \leftarrow x) \wedge (\neg\exists y.\, (q \to y)) \supset \Diamond\Diamond(p \leftarrow x))$
1c $\mathbf{WF2} \supset ((p \to x) \wedge (q \leftarrow x) \wedge (\exists y.\, (q \to y) \supset \Diamond^*\{(p \leftarrow x)\})$

(1a) and (1b) are theorems of **RAAx** by lemma 3, so we only show that (1c) is a theorem of a finite branching resource allocation theory. By the way, the following is a theorem of **RAAx**.

$$\mathbf{WF2} \supset ((p \to x) \wedge (q \leftarrow x) \wedge (q \to y) \supset \Diamond((p \to x) \wedge (q \leftarrow x) \wedge (q \not\rightleftarrows y)))$$

Then the formula

$$\mathbf{WF2} \supset ((p \to x) \wedge (q \leftarrow x) \supset \Diamond^*\{(p \to x) \wedge (q \leftarrow x) \wedge \neg\exists y.\, (q \to y)\})$$

is a theorem of the finite branching resource allocation theory, hence so is the following by lemma 3 and (1b).

$$\mathbf{ME0NP0} \wedge \mathbf{WF2} \supset ((p \to x) \wedge (q \leftarrow x) \supset \Diamond^*\{p \leftarrow x\}).$$

proof of (2) To show that (2) is a theorem of the theory, it suffices to show that (2a) and (2b) are theorems of the theory.

2a $\mathbf{NP0} \supset ((p \leftarrow x) \wedge (\neg\exists y.\, (p \to y)) \supset \Diamond(p \not\rightleftarrows x))$
2b $\mathbf{NP0} \wedge \mathbf{WF2} \supset ((p \leftarrow x) \wedge (\exists y.\, (p \to y)) \supset \Diamond^*\{p \not\rightleftarrows x\})$

Since (2a) is **NP0** itself, we only show that (2b) is a theorem of the theory. On the other hand, formulae

- $\mathbf{WF2} \supset ((p \leftarrow x) \wedge (p \to y) \supset \Diamond((p \leftarrow x) \wedge (p \nrightarrow y)))$ and
- $(p \to y) \wedge (p \nrightarrow z) \supset \Box((p \nrightarrow y) \supset (p \nrightarrow z))$

are theorems of **RAAx**, so the following is a theorem of the finite branching resource allocation theory by finite branching axioms.

$$\mathbf{WF2} \supset (p \leftarrow x) \supset \Diamond^*\{(p \leftarrow x) \wedge \neg\exists y.\,(p \rightarrow y)\}$$

Thus, by lemma 3 and (2a), the following is a theorem of the theory.

$$\mathbf{NP0} \wedge \mathbf{WF2} \supset (p \leftarrow x) \supset \Diamond^*\{p \not\rightleftarrows x\}.$$

Proposition 4. *The followings are theorems of a resource allocation theory.*

1. $\mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{NP0} \wedge \mathbf{NP2} \supset \forall p, x.\,((p \rightarrow x) \supset (\Diamond(p \leftarrow x)) \vee (\Diamond\Diamond(p \leftarrow x)))$
2. $\mathbf{NP0} \wedge \mathbf{NP2} \supset \forall p, x.\,((p \leftarrow x) \supset \Diamond(p \not\rightleftarrows x))$
3. $\mathbf{ME} \wedge \mathbf{ME0} \supset (\mathbf{NP0} \wedge \mathbf{NP2} \supset \neg\mathbf{DL})$

Proof. Since $\mathbf{NP0} \wedge \mathbf{NP2}$ and $\Box^*\{\forall p, x.\,((p \leftarrow x) \supset \Diamond(p \not\rightleftarrows x))\}$ are logically equivalent as we sated before, (2) is shown by lemma 3. On the other hand, (3) is easily shown by (1) and (2). So we only show that (1) is a theorem of **RAAx**. Moreover it suffices to show that the following (1b) is a theorem of **RAAx**.

1a $\mathbf{ME} \wedge \mathbf{NP0} \wedge \mathbf{NP2} \supset \forall q, y.\,((q \leftarrow y) \supset \Diamond\forall r.\,(r \nleftarrow y))$
1b $\mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{NP0} \wedge \mathbf{NP2} \supset \forall p, x.\,((p \rightarrow x) \wedge (\exists q.\,(q \leftarrow x)) \supset \Diamond\Diamond(p \leftarrow x))$

(1a)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[q \leftarrow y] \quad (q \leftarrow y) \supset \Diamond(q \nleftarrow y)}{\Diamond(q \nleftarrow y)} \quad \dfrac{\dfrac{[q \leftarrow y] \quad (q \leftarrow y) \supset \forall r.\,\Box(q \neq r \supset (r \nleftarrow y))}{\forall r.\,\Box(q \neq r \supset (r \nleftarrow y))}}{\Box\forall r.\,(q \neq r \supset (r \nleftarrow y))}}{(\Diamond(q \nleftarrow y)) \wedge \Box\forall r.\,(q \neq r \supset (r \nleftarrow y))}}{\Diamond((q \nleftarrow y) \wedge \forall r.\,(q \neq r \supset (r \nleftarrow y))}}{\Diamond\forall r.\,(r \nleftarrow y)}}{(q \leftarrow y) \supset \Diamond\forall r.\,(r \nleftarrow y)}}{\forall q, y.\,((q \leftarrow y) \supset \Diamond\forall r.\,(r \nleftarrow y))}$$

[**NP0**], [**NP2**], [**ME1***b*], **BF**, $\supset I$, $\forall$I

(1b)

$$\dfrac{\dfrac{\dfrac{\dfrac{[p \rightarrow x] \quad \dfrac{[\exists q.\,(q \leftarrow x)]}{\vdots\ \mathbf{ME1}}}{\Box(p \nleftarrow x)} \quad \dfrac{[\exists q.\,(q \leftarrow x)]}{\vdots\ 1\text{a}}}{\Diamond((p \nleftarrow x) \wedge \neg\exists r.\,(r \leftarrow x))} \quad \dfrac{[\mathbf{ME0}]}{\vdots}}{\Box((p \rightarrow x) \wedge \neg\exists r.\,(r \leftarrow x)) \supset \Diamond(p \leftarrow x)}}{\Diamond\Diamond(p \leftarrow x)}}{(p \rightarrow x) \wedge (\exists q.\,(q \leftarrow x)) \supset \Diamond\Diamond(p \leftarrow x)}}{\forall p, x.\,((p \rightarrow x) \wedge (\exists q.\,(q \leftarrow x)) \supset \Diamond\Diamond(p \leftarrow x))}$$

[**ME1**], 1a, [**ME0**]

Corollary 1. *For any natural number n, the followings are theorems of a resource allocation theory.*

1. $\mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{NP} \wedge \mathbf{CW}_n \supset (\mathbf{WF0} \wedge \mathbf{WF2} \supset \neg\mathbf{DL})$
2. $\mathbf{ME} \wedge \mathbf{ME0} \wedge \mathbf{WF} \wedge \mathbf{CW}_n \supset (\mathbf{NP0} \wedge \mathbf{NP2} \supset \neg\mathbf{DL})$

Proof. By propositions 3 and 4.

Acknowledgements

We wish to express my thanks to members of Research Center for Verification and Semantics (CVS) of AIST. Especially we thank to Izumi Takeuti for valuable discussions. We are also grateful to Yukie Sakanaka for her secretarial support.

References

1. Arnon Avron, Furio Honsell, Marino Miculan and Cristian Paravano, *Encoding Modal Logics in Logical Frameworks*, Studia Logica 60 (1998) pp.161-208
2. E. G.Coffman Jr., M. J.Elphic and A. Shoshani, *System Deadlocks*, Computing Surveys, Vol.3, No.2, June 1971, 67-78
3. M. Fitting and R. L.Mendelsohn, *First-Order Modal Logic*, Synthese Library/Volume 277, Kluwer Academic Publishers
4. J. W.Havender, *Avoiding deadlock in multitasking systems*, IBM Systems Journal 2 (1968), 74-84
5. G. E.Hughes and M. J.Cresswell, *A new introduction to Modal Logic*, Routledge 1996
6. R. C.Holt, *Some Deadlock Properties of Computer Systems*, Computing Surveys, Vol.4, No.3, September 1972, 179-196
7. Ian Hodkinson, Frank Wolter and Michael Zakharyaschev, *Decidable fragments of first-order temporal logics*, Annals of Pure and Applied Logic 106 (2000) 85-134
8. Dexter Kozen, *Results on the Propositional μ-calculus*, Theoretical Computer Science 27 (1983) 333-354
9. Marino Miculan, *A Natural Deduction Style Proof System for Propositional μ-calculus and Its Formalization in Inductive Type Theories*, In Proceedings of ICTCS'98. World Scientific (1998)
10. Gary Nutt, *Operating Systems: A Modern Perspective, Third Edition*, Addison Wesley (2004)
11. Keishi Okamoto, *A First-Order Extension of Modal μ-calculus*, Programming Science Technical Report, AIST/CVS (2006), http://unit.aist.go.jp/cvs/tr-data/PS06-003.pdf

一階様相 μ 計算による Coffman 条件の形式化（Extended Version）
（in English）
(算譜科学研究速報)
発行日：2006 年 10 月 5 日
編集・発行：独立行政法人産業技術総合研究所システム検証研究センター
同連絡先：〒661-0974 兵庫県尼崎市若王寺 3-11-46
e-mail：informatics-inquiry@m.aist.go.jp
本掲載記事の無断転載を禁じます

Formalising Coffman Conditions in First Order Modal μ Calculus
（Extended Version）
(Programming Science Technical Report)
Oct. 5, 2006
Research Center for Verification and Semantics (CVS)
National Institute of Advanced Industrial Science and Technology (AIST)
1-8-31 Midorigaoka, Ikeda, Osaka, 563-8577, Japan
e-mail: informatics- inquiry@m.aist.go.jp
・Reproduction in whole or in part without written permission is prohibited.