Consistency and Completeness of Regulations

Laurence Cholvy[1] Stéphanie Roussel[1,2]

[1]ONERA Centre de Toulouse

[2]ISAE, Toulouse

NorMAS 2008, Luxembourg, July 2008

Outline

Regulation : set of statements expressing what is obligatory, permitted, forbidden... *smoking is forbidden in any public area except specific places where smoking is permitted*

Regulation : set of statements expressing what is obligatory, permitted, forbidden... *smoking is forbidden in any public area except specific places where smoking is permitted*

Consistency :

- (Cholvy, ICAIL 1999) a regulation is consistent if there exists no possible situation which leads an agent to *contradictions* (a given behaviour is prescribed and not prescribed, or prohibited and not prohibited) or *dilemmas* (two incompatible behaviours are prescribed)

Regulation : set of statements expressing what is obligatory, permitted, forbidden... *smoking is forbidden in any public area except specific places where smoking is permitted*

Consistency :

- (Cholvy, ICAIL 1999) a regulation is consistent if there exists no possible situation which leads an agent to *contradictions* (a given behaviour is prescribed and not prescribed, or prohibited and not prohibited) or *dilemmas* (two incompatible behaviours are prescribed)

Completeness :

- (Bieber, Cuppens, DEON 1991) Confidentiality policies : *for each piece of information, the user must have either the permission to know it or the prohibition to know it*

Regulation : set of statements expressing what is obligatory, permitted, forbidden... *smoking is forbidden in any public area except specific places where smoking is permitted*

Consistency :

- (Cholvy, ICAIL 1999) a regulation is consistent if there exists no possible situation which leads an agent to *contradictions* (a given behaviour is prescribed and not prescribed, or prohibited and not prohibited) or *dilemmas* (two incompatible behaviours are prescribed)

Completeness :

- (Bieber, Cuppens, DEON 1991) Confidentiality policies : *for each piece of information, the user must have either the permission to know it or the prohibition to know it*
- (Cholvy, Roussel, ECSQARU 2007) Completeness of information exchange policies : *for each piece of information he receives, an agent must know "what to do with it"*

Regulation : set of statements expressing what is obligatory, permitted, forbidden... *smoking is forbidden in any public area except specific places where smoking is permitted*

Consistency :

- (Cholvy, ICAIL 1999) a regulation is consistent if there exists no possible situation which leads an agent to *contradictions* (a given behaviour is prescribed and not prescribed, or prohibited and not prohibited) or *dilemmas* (two incompatible behaviours are prescribed)

Completeness :

- (Bieber, Cuppens, DEON 1991) Confidentiality policies : *for each piece of information, the user must have either the permission to know it or the prohibition to know it*
- (Cholvy, Roussel, ECSQARU 2007) Completeness of information exchange policies : *for each piece of information he receives, an agent must know "what to do with it"*

Objectives : Extending this work to "general" regulations.

Outline

Requirements for a formal langage

- Reasoning with deontic notions $\Longrightarrow$ modal deontic logic ?
- Complexity of the rules $\Longrightarrow$ first order logic ?
- Temporal notions $\Longrightarrow$ temporal logic ?

Requirements for a formal langage

- Reasoning with deontic notions $\Longrightarrow$ modal deontic logic ?
- Complexity of the rules $\Longrightarrow$ first order logic ?
- Temporal notions $\Longrightarrow$ temporal logic ?

Compromise (cf Sergot 1982, Lee 1994, Halpern-Weissman 2003...)

- A typed first order language + three unary predicate symbols represent the deontic notions O, F, P.

Requirements for a formal langage

- Reasoning with deontic notions $\Longrightarrow$ modal deontic logic ?
- Complexity of the rules $\Longrightarrow$ first order logic ?
- Temporal notions $\Longrightarrow$ temporal logic ?

Compromise (cf Sergot 1982, Lee 1994, Halpern-Weissman 2003...)

- A typed first order language + three unary predicate symbols represent the deontic notions O, F, P.
- $\forall x \quad car(x) \wedge light(red) \rightarrow F(pass(x))$
  $\forall x \quad car(x) \wedge light(green) \rightarrow O(pass(x))$

Requirements for a formal langage

- Reasoning with deontic notions $\Longrightarrow$ modal deontic logic ?
- Complexity of the rules $\Longrightarrow$ first order logic ?
- Temporal notions $\Longrightarrow$ temporal logic ?

Compromise (cf Sergot 1982, Lee 1994, Halpern-Weissman 2003...)

- A typed first order language + three unary predicate symbols represent the deontic notions O, F, P.
- $\forall x \quad car(x) \wedge light(red) \rightarrow F(pass(x))$
  $\forall x \quad car(x) \wedge light(green) \rightarrow O(pass(x))$
- Relations between these predicates :
  $\forall x \quad O(not(x)) \rightarrow \neg O(x)$
  $\forall x \quad F(x) \leftrightarrow O(not(x))$
  $\forall x \quad P(x) \leftrightarrow \neg O(not(x)) \wedge \neg O(x)$
  $\forall x \quad O(not^2(x)) \leftrightarrow O(x)$

Requirements for a formal langage

- Reasoning with deontic notions $\Longrightarrow$ modal deontic logic ?
- Complexity of the rules $\Longrightarrow$ first order logic ?
- Temporal notions $\Longrightarrow$ temporal logic ?

Compromise (cf Sergot 1982, Lee 1994, Halpern-Weissman 2003...)

- A typed first order language + three unary predicate symbols represent the deontic notions O, F, P.
- $\forall x \quad car(x) \wedge light(red) \rightarrow F(pass(x))$
  $\forall x \quad car(x) \wedge light(green) \rightarrow O(pass(x))$
- Relations between these predicates :

$$\left.\begin{array}{ll}\forall x & O(not(x)) \rightarrow \neg O(x) \\ \forall x & F(x) \leftrightarrow O(not(x)) \\ \forall x & P(x) \leftrightarrow \neg O(not(x)) \wedge \neg O(x) \\ \forall x & O(not^2(x)) \leftrightarrow O(x)\end{array}\right\} \mathcal{A}$$

Definition (World)

A world W is a complete set of p-literals.

Definition (World)

A world W is a complete set of p-literals.

Definition (Consistency in a world)

Let $\mathcal{R}$ be a regulation and W a world consistent with some domain constraints Dom.
$\mathcal{R}$ *is consistent in* W *(given* Dom*)* iff $W \wedge \mathcal{R} \wedge \mathcal{A}$ is consistent

Definition (World)

A world W is a complete set of p-literals.

Definition (Consistency in a world)

Let $\mathcal{R}$ be a regulation and W a world consistent with some domain constraints Dom.

$\mathcal{R}$ is consistent in W (given Dom) iff $W \wedge \mathcal{R} \wedge \mathcal{A}$ is consistent

Example

$Dom = \emptyset$

$$\left.\begin{array}{l} \forall x \quad car(x) \wedge light(red) \rightarrow F(pass(x)) \\ \forall x \quad car(x) \wedge light(green) \rightarrow O(pass(x)) \end{array}\right\} \mathcal{R}_0$$

$$\left. car(jag), light(red), light(green) \right\} W_0$$

$W_0 \wedge \mathcal{R}_0 \wedge \mathcal{A}$ is not consistent $\Longrightarrow$ $\mathcal{R}_0$ is not consistent in W_0.

Definition (World)

A world W is a complete set of p-literals.

Definition (Consistency in a world)

Let $\mathcal{R}$ be a regulation and W a world consistent with some domain constraints Dom.
$\mathcal{R}$ *is consistent in* W *(given* Dom*)* iff $W \wedge \mathcal{R} \wedge \mathcal{A}$ is consistent

Example

$$Dom = \emptyset$$
$$\left.\begin{array}{l} \forall x \quad car(x) \wedge light(red) \rightarrow F(pass(x)) \\ \forall x \quad car(x) \wedge light(green) \rightarrow O(pass(x)) \end{array}\right\} \mathcal{R}_0$$
$$\left. car(jag), light(red), light(green) \right\} W_0$$
$$W_0 \wedge \mathcal{R}_0 \wedge \mathcal{A} \text{ is not consistent} \implies \mathcal{R}_0 \text{ is not consistent in } W_0.$$

Definition (Consistency)

$\mathcal{R}$ *is consistent* iff it is consistent in any world.

Definition (Completeness in a world)

$\mathcal{R}$ is complete in W for $\vdash$, $\phi(X)$ and $\psi(X)$ iff

$$W \vdash \phi(X) \implies \begin{cases} W \wedge \mathcal{R} \wedge \mathcal{A} \vdash O(\psi(X)) \text{ or} \\ W \wedge \mathcal{R} \wedge \mathcal{A} \vdash P(\psi(X)) \text{ or} \\ W \wedge \mathcal{R} \wedge \mathcal{A} \vdash F(\psi(X)) \end{cases}$$

Definition (Completeness in a world)

$\mathcal{R}$ *is complete in* W *for* $\vdash$, $\phi(X)$ *and* $\psi(X)$ iff

$$W \vdash \phi(X) \implies \begin{cases} W \wedge \mathcal{R} \wedge \mathcal{A} \vdash O(\psi(X)) \text{ or} \\ W \wedge \mathcal{R} \wedge \mathcal{A} \vdash P(\psi(X)) \text{ or} \\ W \wedge \mathcal{R} \wedge \mathcal{A} \vdash F(\psi(X)) \end{cases}$$

Example

$$\left.\begin{array}{ll} \forall x & car(x) \wedge light(red) \rightarrow F(pass(x)) \\ \forall x & car(x) \wedge light(green) \rightarrow O(pass(x)) \end{array}\right\} \mathcal{R}_0$$

Definition (Completeness in a world)

$\mathcal{R}$ *is complete in* W *for* $\vdash$, $\phi(X)$ *and* $\psi(X)$ iff

$$W \vdash \phi(X) \implies \begin{cases} W \wedge \mathcal{R} \wedge \mathcal{A} \vdash O(\psi(X)) \text{ or} \\ W \wedge \mathcal{R} \wedge \mathcal{A} \vdash P(\psi(X)) \text{ or} \\ W \wedge \mathcal{R} \wedge \mathcal{A} \vdash F(\psi(X)) \end{cases}$$

Example

$$\left.\begin{array}{l} \forall x \quad car(x) \wedge light(red) \rightarrow F(pass(x)) \\ \forall x \quad car(x) \wedge light(green) \rightarrow O(pass(x)) \end{array}\right\} \mathcal{R}_0$$

$$\left.\begin{array}{l} car(jag), light(orange) \end{array}\right\} W_0$$

Definition (Completeness in a world)

$\mathcal{R}$ is complete in W for $\vdash$, $\phi(X)$ and $\psi(X)$ iff

$$W \vdash \phi(X) \implies \begin{cases} W \wedge \mathcal{R} \wedge \mathcal{A} \vdash O(\psi(X)) \text{ or} \\ W \wedge \mathcal{R} \wedge \mathcal{A} \vdash P(\psi(X)) \text{ or} \\ W \wedge \mathcal{R} \wedge \mathcal{A} \vdash F(\psi(X)) \end{cases}$$

Example

$$\left.\begin{array}{l} \forall x \quad car(x) \wedge light(red) \rightarrow F(pass(x)) \\ \forall x \quad car(x) \wedge light(green) \rightarrow O(pass(x)) \end{array}\right\} \mathcal{R}_0$$

$$\left. car(jag), light(orange) \right\} W_0$$

$\phi(x) = car(x) \wedge light(orange)$ and $\psi(x) = pass(x)$

Definition (Completeness in a world)

$\mathcal{R}$ *is complete in* W *for* $\vdash$, $\phi(X)$ *and* $\psi(X)$ iff

$$W \vdash \phi(X) \implies \begin{cases} W \wedge \mathcal{R} \wedge \mathcal{A} \vdash O(\psi(X)) \text{ or} \\ W \wedge \mathcal{R} \wedge \mathcal{A} \vdash P(\psi(X)) \text{ or} \\ W \wedge \mathcal{R} \wedge \mathcal{A} \vdash F(\psi(X)) \end{cases}$$

Example

$$\left.\begin{array}{l} \forall x \quad car(x) \wedge light(red) \rightarrow F(pass(x)) \\ \forall x \quad car(x) \wedge light(green) \rightarrow O(pass(x)) \end{array}\right\} \mathcal{R}_0$$

$$\left.\begin{array}{l} car(jag), light(orange) \end{array}\right\} W_0$$

$\phi(x) = car(x) \wedge light(orange)$ and $\psi(x) = pass(x)$

$$W_0 \vdash \phi(jag) \quad \text{but} \quad \begin{cases} W_0 \wedge \mathcal{R}_0 \wedge \mathcal{A} \nvdash O(\psi(jag)) \\ W_0 \wedge \mathcal{R}_0 \wedge \mathcal{A} \nvdash P(\psi(jag)) \\ W_0 \wedge \mathcal{R}_0 \wedge \mathcal{A} \nvdash F(\psi(jag)) \end{cases}$$

Definition (Completeness in a world)

$\mathcal{R}$ *is complete in* W *for* $\vdash$, $\phi(X)$ *and* $\psi(X)$ iff

$$W \vdash \phi(X) \implies \begin{cases} W \wedge \mathcal{R} \wedge \mathcal{A} \vdash O(\psi(X)) \text{ or} \\ W \wedge \mathcal{R} \wedge \mathcal{A} \vdash P(\psi(X)) \text{ or} \\ W \wedge \mathcal{R} \wedge \mathcal{A} \vdash F(\psi(X)) \end{cases}$$

Example

$$\left.\begin{array}{l} \forall x \quad car(x) \wedge light(red) \rightarrow F(pass(x)) \\ \forall x \quad car(x) \wedge light(green) \rightarrow O(pass(x)) \end{array}\right\} \mathcal{R}_0$$

$$car(jag), light(orange) \quad \} \; W_0$$

$$\phi(x) = car(x) \wedge light(orange) \quad \text{and} \quad \psi(x) = pass(x)$$

$$W_0 \vdash \phi(jag) \quad \text{but} \quad \begin{cases} W_0 \wedge \mathcal{R}_0 \wedge \mathcal{A} \nvdash O(\psi(jag)) \\ W_0 \wedge \mathcal{R}_0 \wedge \mathcal{A} \nvdash P(\psi(jag)) \\ W_0 \wedge \mathcal{R}_0 \wedge \mathcal{A} \nvdash F(\psi(jag)) \end{cases}$$

$\implies$ $\mathcal{R}_0$ is not complete in W_0 for $\vdash$, $\phi(jag)$ and $\psi(jag)$

Definition (Completeness in a world)

$\mathcal{R}$ is complete in W for $\vdash$, $\phi(X)$ and $\psi(X)$ iff

$$W \vdash \phi(X) \implies \begin{cases} W \wedge \mathcal{R} \wedge \mathcal{A} \vdash O(\psi(X)) \text{ or} \\ W \wedge \mathcal{R} \wedge \mathcal{A} \vdash P(\psi(X)) \text{ or} \\ W \wedge \mathcal{R} \wedge \mathcal{A} \vdash F(\psi(X)) \end{cases}$$

Example

$$\left.\begin{array}{l} \forall x \quad car(x) \wedge light(red) \rightarrow F(pass(x)) \\ \forall x \quad car(x) \wedge light(green) \rightarrow O(pass(x)) \end{array}\right\} \mathcal{R}_0$$

$$car(jag), light(orange) \quad \} W_0$$

$\phi(x) = car(x) \wedge light(orange)$ and $\psi(x) = pass(x)$

$$W_0 \vdash \phi(jag) \quad \text{but} \quad \begin{cases} W_0 \wedge \mathcal{R}_0 \wedge \mathcal{A} \nvdash O(\psi(jag)) \\ W_0 \wedge \mathcal{R}_0 \wedge \mathcal{A} \nvdash P(\psi(jag)) \\ W_0 \wedge \mathcal{R}_0 \wedge \mathcal{A} \nvdash F(\psi(jag)) \end{cases}$$

$\implies$ $\mathcal{R}_0$ is not complete in W_0 for $\vdash$, $\phi(jag)$ and $\psi(jag)$

Definition (Completeness)

$\mathcal{R}$ is complete for $\vdash$, $\phi(X)$ and $\psi(X)$ iff for all world W consistent with *Dom*, $\mathcal{R}$ is complete for $\vdash$, $\phi(X)$ and $\psi(X)$ in W.

Outline

Completion Rules

- Idea : Adapt Reiter's CWA (Closed World Assumption) defined for incomplete databases in order to complete them.
  - (CWA) If a literal l is not deduced (from the database) then it is assumed that its negation is deduced.
  - Motivation underlying CWA : : In the real world, whether l is true or l is false i.e, $\models l \otimes \neg l$

Completion Rules

- Idea : Adapt Reiter's CWA (Closed World Assumption) defined for incomplete databases in order to complete them.
  - (CWA) If a literal l is not deduced (from the database) then it is assumed that its negation is deduced.
  - Motivation underlying CWA : : In the real world, whether l is true or l is false i.e, $\models l \otimes \neg l$
- Here we have : $\mathcal{A} \models O(l) \otimes F(l) \otimes P(l)$.

Completion Rules

- Idea : Adapt Reiter's CWA (Closed World Assumption) defined for incomplete databases in order to complete them.
  - (CWA) If a literal l is not deduced (from the database) then it is assumed that its negation is deduced.
  - Motivation underlying CWA : : In the real world, whether l is true or l is false i.e, $\models l \otimes \neg l$
- Here we have : $\mathcal{A} \models O(l) \otimes F(l) \otimes P(l)$.
- This leads to several completion rules

Completion Rules

- Idea : Adapt Reiter's CWA (Closed World Assumption) defined for incomplete databases in order to complete them.
  - (CWA) If a literal l is not deduced (from the database) then it is assumed that its negation is deduced.
  - Motivation underlying CWA : : In the real world, whether l is true or l is false i.e, $\models l \otimes \neg l$
- Here we have : $\mathcal{A} \models O(l) \otimes F(l) \otimes P(l)$.
- This leads to several completion rules

NOTATION :

$$\mathcal{R} \textit{ incomplete for } X \textit{ in } W \begin{cases} W \vdash \phi(X) \\ W \wedge \mathcal{R} \wedge \mathcal{A} \not\vdash O(\psi(X)) \\ W \wedge \mathcal{R} \wedge \mathcal{A} \not\vdash P(\psi(X)) \\ W \wedge \mathcal{R} \wedge \mathcal{A} \not\vdash F(\psi(X)) \end{cases}$$

Definition (Completion rules)

In order to be as general as possible, we parametrize the completion rules by some conditions E_0, E_P, E_F.

$$(R_{E_O}) \qquad \frac{\mathcal{P}\ \textit{incomplete for}\ X\ \textit{in}\ W \qquad W \vdash E_O(X)}{O(\psi(X))}$$

$$(R_{E_F}) \qquad \frac{\mathcal{P}\ \textit{incomplete for}\ X, \textit{in}\ W \qquad W \vdash E_F(X)}{F(\psi(X))}$$

$$(R_{E_P}) \qquad \frac{\mathcal{P}\ \textit{incomplete for}\ X, \textit{in}\ W \qquad W \vdash E_P(X)}{P(\psi(X))}$$

Let $\vdash_*$ denotes the inference defined by $\vdash + R_{E_F} + R_{E_P} + R_{E_0}$

Main result (necessary and sufficient condition)
$\mathcal{R}$ is complete and consistent for $\vdash_*$ in W iff for any X so that $\mathcal{R}$ is incomplete for X in W, we have :

$$W \vdash E_F(X) \otimes E_T(X) \otimes E_O(X)$$

Main result (necessary and sufficient condition)
$\mathcal{R}$ is complete and consistent for $\vdash_*$ in W iff for any X so that $\mathcal{R}$ is incomplete for X in W, we have :

$$W \vdash E_F(X) \otimes E_T(X) \otimes E_O(X)$$

Weaker result (sufficient condition)
If for any X we have : $W \vdash \phi(X) \rightarrow E_F(X) \otimes E_P(X) \otimes E_O(X)$
then $\mathcal{R}$ is complete and consistent for $\vdash_*$ in W

Main result (necessary and sufficient condition)
$\mathcal{R}$ is complete and consistent for $\vdash_*$ in W iff for any X so that $\mathcal{R}$ is incomplete for X in W, we have :

$$W \vdash E_F(X) \otimes E_T(X) \otimes E_O(X)$$

Weaker result (sufficient condition)
If for any X we have : $W \vdash \phi(X) \rightarrow E_F(X) \otimes E_P(X) \otimes E_O(X)$ then $\mathcal{R}$ is complete and consistent for $\vdash_*$ in W

Weaker result (sufficient condition)
If $\vdash Dom \rightarrow E_F(X) \otimes E_P(X) \otimes E_O(X)$ then $\mathcal{R}$ is complete and consistent for $\vdash_*$.

Some basic E_i

- $E_F = True$, $E_P = False$ et $E_O = False \Rightarrow$
  Everything which is not explicitely obligatory nor permitted is forbidden
  This applies to regulations which regulate highly secured systems where any action has to be explicitely permitted before being performed.
- $E_F = False$, $E_P = True$ et $E_O = False \Rightarrow$
  Everything which is not explicitely forbidden nor obligatory is permitted.
  This applies to "tolerant" regulations which regulate dimmed weakly secured system where, unless contrary, anything is permitted.
- $E_F = False$, $E_P = False$ et $E_O = True \Rightarrow$
  This means that any action which is not explicitely forbidden nor permitted is obligatory.
  This applies for instance to mail servers which must let pass every mail except spams.

Outline

Information exchange policies

$$\phi(x, i, y) = \mathit{Receives}(x, i) \wedge \mathit{Agent}(y) \wedge \neg(x = y)$$

$$\psi(x, i, y) = \mathit{tell}(x, i, y)$$

Security policies

$$\phi_1(x, y) = User(x) \wedge Permanent(x) \wedge File(y)$$

$$\phi_2(x, y) = User(x) \wedge Temporary(x) \wedge File(y)$$

$$\psi_1(x, y) = read(x, y)$$

$$\psi_2(x, y) = write(x, y)$$

A security policy may be complete (in a world W) for $\phi_1(x, y)$ and $\psi_1(x, y)$, $\phi_1(x, y)$ and $\psi_2(x, y)$ but may be incomplete for $\phi_2(x, y)$ and $\psi_1(x, y)$, $\phi_2(x, y)$ and $\psi_2(x, y)$.
This means that the policy completely prescribes the behaviour of permanent users regarding reading and writing files, but is incomplete as for temporary users and reading or writing files.

Outline

- Study of consistency and completeness :
  - definitions
  - method to consistently complete an incomplete regulation

- Study of consistency and completeness :
  - definitions
  - method to consistently complete an incomplete regulation
- Relation with Reiter's defaults

$$(d_F) \quad \frac{\phi(X) \wedge E_F(X) \ : \ F(\psi(X))}{F(\psi(X))}$$

$$(d_P) \quad \frac{\phi(X) \wedge E_P(X) \ : \ P(\psi(X))}{P(\psi(X)))}$$

$$(d_O) \quad \frac{\phi(X) \wedge E_O(X) \ : \ O(\psi(X))}{O(\psi(X))}$$

- Study of consistency and completeness :
  - definitions
  - method to consistently complete an incomplete regulation
- Relation with Reiter's defaults

$$(d_F) \quad \frac{\phi(X) \wedge E_F(X) \; : \; F(\psi(X))}{F(\psi(X))}$$

$$(d_P) \quad \frac{\phi(X) \wedge E_P(X) \; : \; P(\psi(X))}{P(\psi(X)))}$$

$$(d_O) \quad \frac{\phi(X) \wedge E_O(X) \; : \; O(\psi(X))}{O(\psi(X))}$$

- "Local completeness" (cf databases : *for any employee, the database should know its phone number*)

- Study of consistency and completeness :
  - definitions
  - method to consistently complete an incomplete regulation
- Relation with Reiter's defaults

$$(d_F) \quad \frac{\phi(X) \wedge E_F(X) \ : \ F(\psi(X))}{F(\psi(X))}$$

$$(d_P) \quad \frac{\phi(X) \wedge E_P(X) \ : \ P(\psi(X))}{P(\psi(X)))}$$

$$(d_O) \quad \frac{\phi(X) \wedge E_O(X) \ : \ O(\psi(X))}{O(\psi(X))}$$

- "Local completeness" (cf databases : *for any employee, the database should know its phone number*)
- Extensions :
  - Modal logic
  - Time