A Dynamic Logic for Privacy Compliance

Guillaume Aucher
based on joint work with
Guido Boella and Leon van der Torre

University of Rennes 1 - INRIA, France

CAPPRIS seminar, 20-03-13

Plan

Website Example

A server should not disclose a mapping $\mathtt{m}$ from a given set of users to the websites they visited (which is stored in a log file). So, the names of users is replaced by numbers using a hash function *h*. We obtain:

1. A mapping from users to numbers: $\mathtt{m}_1$.
2. A mapping from numbers to websites: $\mathtt{m}_2$.

such that:

$$\models \mathtt{m}_1 \wedge \mathtt{m}_2 \rightarrow \mathtt{m}$$

Goal: specify a policy to avoid that a user infers $\mathtt{m}$.

Naive method: specify all the permitted and forbidden combinations of actions.

In our case, 4 combinations of actions

Website Example

A server should not disclose a mapping $\mathtt{m}$ from a given set of users to the websites they visited (which is stored in a log file). So, the names of users is replaced by numbers using a hash function *h*. We obtain:

1. A mapping from users to numbers: $\mathtt{m}_1$.
2. A mapping from numbers to websites: $\mathtt{m}_2$.

such that:

$$\models \mathtt{m}_1 \wedge \mathtt{m}_2 \rightarrow \mathtt{m}$$

Goal: specify a policy to avoid that a user infers $\mathtt{m}$.

Naive method: specify all the permitted and forbidden combinations of actions.

In our case, 4 combinations of actions

Website Example

- What happens if the mapping $\mathtt{m}$ is split into n mappings $\mathtt{m}_1, \ldots, \mathtt{m}_n$?
  In that case, more than $n!$ combinations of actions.

- How do we update the policy if a user obtains the hash function h?

  Problem: how do we express in a flexible way a policy on all combinations of actions?

Key principle: It is permitted for *sender* to send a message if the resulting situation **after** sending the message is permitted.

Website Example

- What happens if the mapping $\mathtt{m}$ is split into n mappings $\mathtt{m}_1, \ldots, \mathtt{m}_n$?
  In that case, more than $n!$ combinations of actions.

- How do we update the policy if a user obtains the hash function h?

  Problem: how do we express in a flexible way a policy on all combinations of actions?

  Key principle: It is permitted for *sender* to send a message if the resulting situation **after** sending the message is permitted.

Our scenarios

sender sends messages about a database to *recipient*. *sender* should comply to a privacy policy prescribing messages he is permitted or forbidden to send.

- *recipient* always believes *sender*;
- *sender* is the unique source of information about the database for *recipient*;
- *sender* knows exactly the content of the database.

Dual perspective

Our presentation will oscillate between two perspectives:

1. A '*theoretical*' perspective: analysis and formal representation of elementary concepts and their interaction: knowledge, obligation, action.

2. An '*applied*' perspective: use of these elementary notions to formalize more complex and 'applied' concepts, such as confidentiality, privacy, permission to disclose, compliance...

Plan

Plan

Plan

Language $\mathcal{L}_{EDL}$

$$\mathcal{L}^{\phi}_{EDL} : \phi ::= \mathrm{p} \mid \neg\phi \mid \phi \wedge \phi \mid K\phi \mid O\alpha$$
$$\mathcal{L}^{\alpha}_{EDL} : \alpha ::= K\phi \mid \neg\alpha \mid \alpha \wedge \alpha$$

where p ranges over a set of atomic propositions $\mathtt{ATM}$.
Formulas $\mathcal{L}^{\alpha}_{EDL}$ are always in the scope of an obligation operator O.

- $O\alpha$ reads "It is obligatory for the *sender* that α".
- $P\alpha$ abbreviates $\neg O\neg\alpha$. It reads "It is permitted for the *sender* that α".
- $K\phi$ reads "The *recipient* knows that ϕ".

Examples:

- $PK\phi$: "It is permitted for the *sender* that the *recipient* knows that ϕ".
- $\neg PK\phi$: "It is forbidden for the *sender* that the *recipient* knows that ϕ".
- $OK\phi \rightarrow \phi$, $\neg PK\phi \rightarrow \phi$,... Note that $OK\phi \rightarrow O\phi$ is not a formula of $\mathcal{L}_{EDL}$.

Semantics and truth conditions of $\mathcal{L}_{EDL}$

Definition

An *EDL-model* M is a tuple $M = (W, D, R, V)$, where W is a non-empty set of possible worlds, R is a reflexive accessibility relations and D is a serial accessibility relations on W, and V is a valuation.

The truth conditions are given by:

$$
\begin{array}{lll}
M, w \models \mathrm{p} & \text{iff} & w \in V(\mathrm{p}) \\
M, w \models \neg\phi & \text{iff} & M, w \not\models \phi \\
M, w \models \phi \wedge \psi & \text{iff} & M, w \models \phi \text{ and } M, w \models \psi \\
M, w \models O\alpha & \text{iff} & \text{for all } v \in D(w),\ M, v \models \alpha \\
M, w \models K\phi & \text{iff} & \text{for all } v \in R(w),\ M, v \models \phi
\end{array}
$$

$M \models \phi$ iff for all $w \in W$, $M, w \models \phi$.

Axiomatization and computational complexity of $\mathcal{L}_{EDL}$

Logic *EDL*:

A_1	All propositional tautologies based on ATM
A_2	$\vdash O\alpha \rightarrow P\alpha$
A_3	$\vdash K\phi \rightarrow \phi$
A_4	$\vdash O(\alpha \rightarrow \alpha') \rightarrow (O\alpha \rightarrow O\alpha')$
A_5	$\vdash K(\phi \rightarrow \psi) \rightarrow (K\phi \rightarrow K\psi)$

R_1	If $\vdash \alpha$ then $\vdash O\alpha$
R_2	If $\vdash \phi$ then $\vdash K\phi$
R_3	If $\vdash \phi \rightarrow \psi$ and $\vdash \phi$ then $\vdash \psi$

Theorem

- *The satisfiablity problem of $\mathcal{L}_{EDL}$ is PSPACE-complete.*
- *Any instance of the model checking problem of $\mathcal{L}_{EDL}$ is solved in time $O(\mid \phi \mid \cdot ||M||)$.*

Plan

Epistemic norms and privacy policies

Definition

- An **epistemic norm** is a formula of the form $\phi \to O\alpha$ or $\phi \to P\alpha$, where $\phi \in \mathcal{L}_{EL}$ and $\alpha \in \mathcal{L}^{\alpha}_{EDL}$.
- A **privacy policy** $\mathcal{P}$ is a consistent set of epistemic norms.

Website Example: The *privacy policy* $\mathcal{P}$ is:

$$\mathcal{P} = \{PK_{\mathtt{m}_1}, PK_{\mathtt{m}_2}, \neg PK_{\mathtt{m}}\}$$

It specifies that:

- $PK_{\mathtt{m}_1}$: it is *P*ermitted to *K*now the mapping from users to numbers,
- $PK_{\mathtt{m}_2}$: it is *P*ermitted to *K*now the mapping from numbers to visited websites,
- $\neg PK_{\mathtt{m}}$: it is forbidden to *K*now the mapping from users to visited websites.

More examples of epistemic norms

- $O\neg K\mathtt{a}$: it is not permitted for the *sender* that the *recipient* knows the address ($\mathtt{a}$).
- $K\mathtt{a} \rightarrow OK\mathtt{c_a}$: if the *recipient* knows the address ($\mathtt{a}$), then the *sender* is obliged to make the *recipient* know that the address is classified ($\mathtt{c_a}$).
- $\mathtt{Admin(r)} \wedge K\mathtt{p} \rightarrow O(K\mathtt{c_p} \vee K\neg\mathtt{c_p})$: if the *recipient* has the role of administrator and *recipient* knows that $\mathtt{p}$, then it is obligatory for the *sender* that the *recipient* knows whether $\mathtt{p}$ is classified information ($\mathtt{c_p}$).

Even if policies are about the knowledge of the *recipient*, they regulate the behaviour of the *sender*.

Compliance of a situation with a privacy policy

Let (M, w) be a pointed *EDL*-model and let $\mathcal{P}$ be the following privacy policy:

$$\mathcal{P} = \{\phi_1 \rightarrow O\alpha_{\phi_1}, \ldots, \phi_n \rightarrow P\alpha_{\phi_n}\}$$

- (M, w) is **compliant** w.r.t. $\mathcal{P}$, written $M, w \models \mathtt{Cmp}$, iff $M, w \models \phi \rightarrow \alpha$ for all $\phi \rightarrow O\alpha \in \mathcal{P}$.
- (M, w) is **strongly compliant** w.r.t. $\mathcal{P}$ iff $M, w \models O\alpha \rightarrow \alpha$ for all $\alpha \in \mathcal{L}^{\alpha}_{EDL}$.

Restrictive and permissive policy

$\mathcal{E}(M, w) = \{\phi \in \mathcal{L}_{EL} \mid M, w \models \phi\}$ represents the epistemic state of the *recipient*.

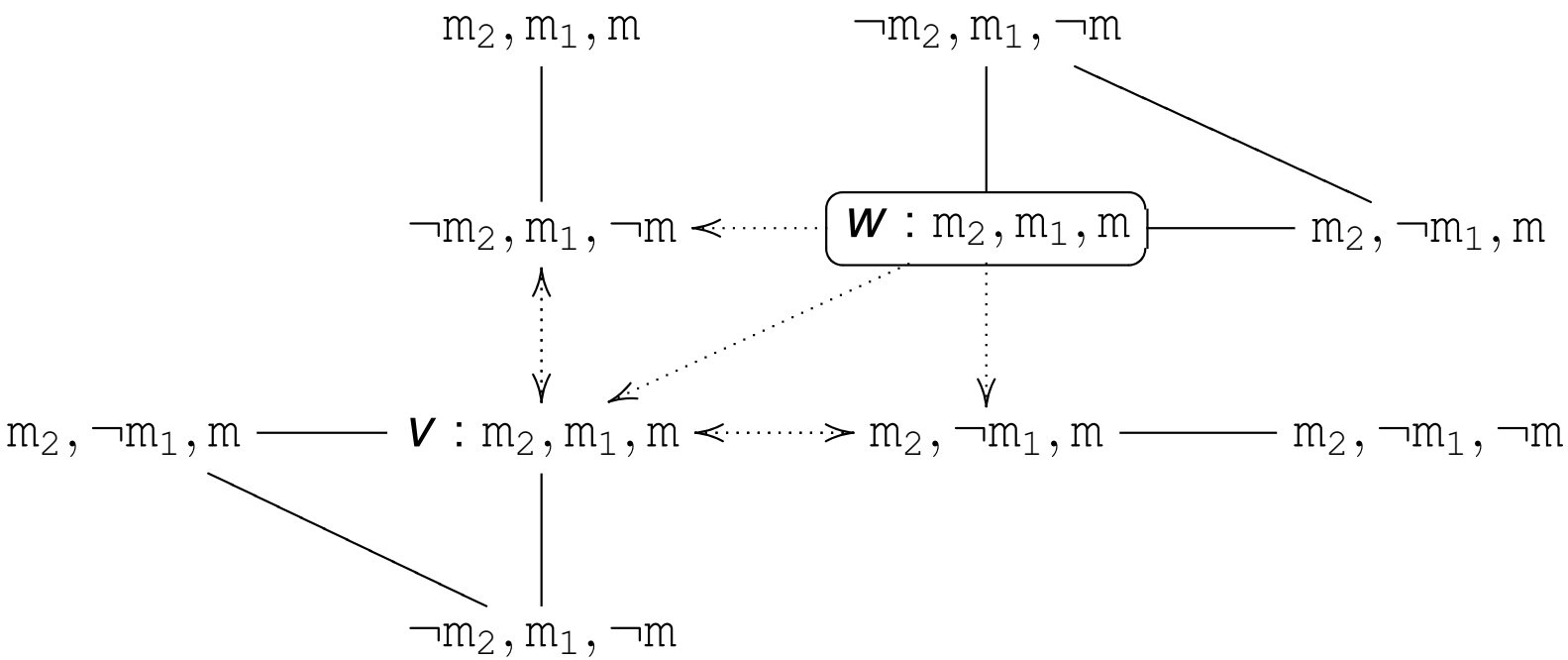
- The privacy policy $\mathcal{P}$ is **restrictive** if for all *EDL*-models (M, w), if $\mathcal{E}(M, w) \cup \mathcal{P} \nvdash P\alpha$, then $M, w \models \neg P\alpha$.
- The privacy policy $\mathcal{P}$ is **permissive** if for all *EDL*-models (M, w), if $\mathcal{E}(M, w) \cup \mathcal{P} \nvdash \neg P\alpha$, then $M, w \models P\alpha$.

Proposition

- If $\mathcal{P}$ is permissive, then compliance coincides with strong compliance.
- The situation (M, w) is strongly compliant w.r.t. $\mathcal{P}$ iff there exists $v \in D(w)$ such that $(M, R(w))$ and $(M, R(v))$ are bisimilar.

Website Example

EDL-model M: R is represented by plain arrows, D by dashed arrows.



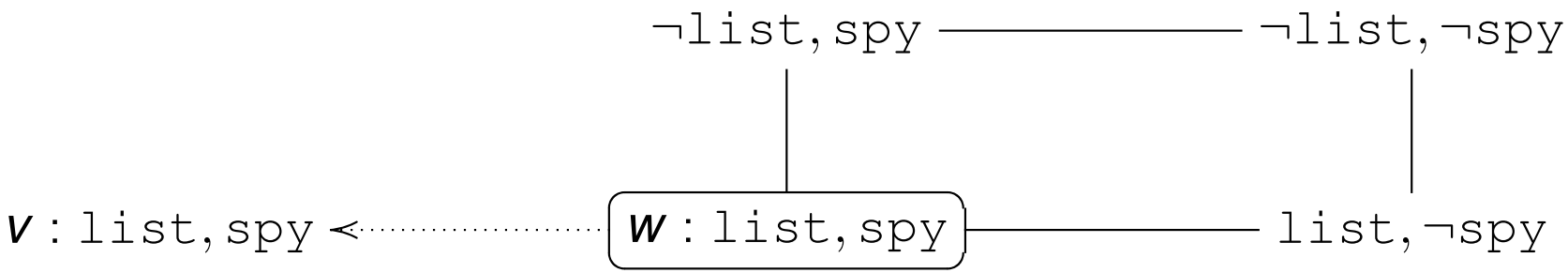
- (M, w) is strongly compliant w.r.t. $\mathcal{P} = \{PK\mathrm{m}_1, PK\mathrm{m}_2, \neg PK\mathrm{m}\}$.
- $M \models \mathrm{m}_1 \wedge \mathrm{m}_2 \rightarrow \mathrm{m}$.

Spyware Example

- `list` is a list of websites where it is possible to download softwares.
- `spy` represents the fact that such softwares might contain spywares.

If the softwares downloadable on the websites might contain some spywares (`spy`) and the *recipient* knows this list of websites (K`list`), then the *recipient* should know it (OK`spy`):

$$\mathcal{P}' = \{\texttt{spy} \wedge K\texttt{list} \rightarrow OK\texttt{spy}\}$$



Plan

Plan

Language $\mathcal{L}_{DEDL}$

Two dynamic operators for two kinds of change:

- [*s sends* ψ] affects knowledge (relation *R*):
  - [*s sends* ψ]ϕ reads 'after sending ψ, ϕ holds'
- [*s prom* α] affects obligation (relation *D*):
  - [*s prom* α]ϕ reads 'after the promulgation of α, ϕ holds'.

Definition

$$\mathcal{L}^{\phi}_{DEDL} : \phi ::= \mathrm{p} \mid \neg\phi \mid \phi \wedge \phi \mid K\phi \mid O\alpha \mid [s \text{ sends } \phi]\phi \mid [s \text{ prom } \alpha]\phi$$
$$\mathcal{L}^{\alpha}_{DEDL} : \alpha ::= K\phi \mid \neg\alpha \mid \alpha \wedge \alpha \mid [s \text{ sends } \phi]\alpha \mid [s \text{ prom } \alpha]\alpha$$

where p ranges over $\mathtt{ATM}$.

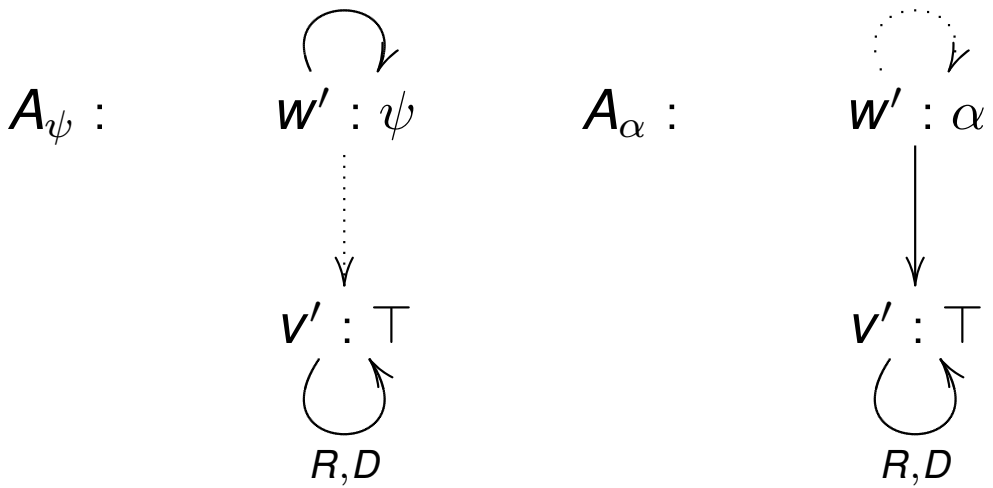
Semantics and truth conditions of $\mathcal{L}_{DEDL}$

- $M, w \models [s \text{ sends } \psi]\phi$ iff $M \oplus \psi, w \models \phi$,

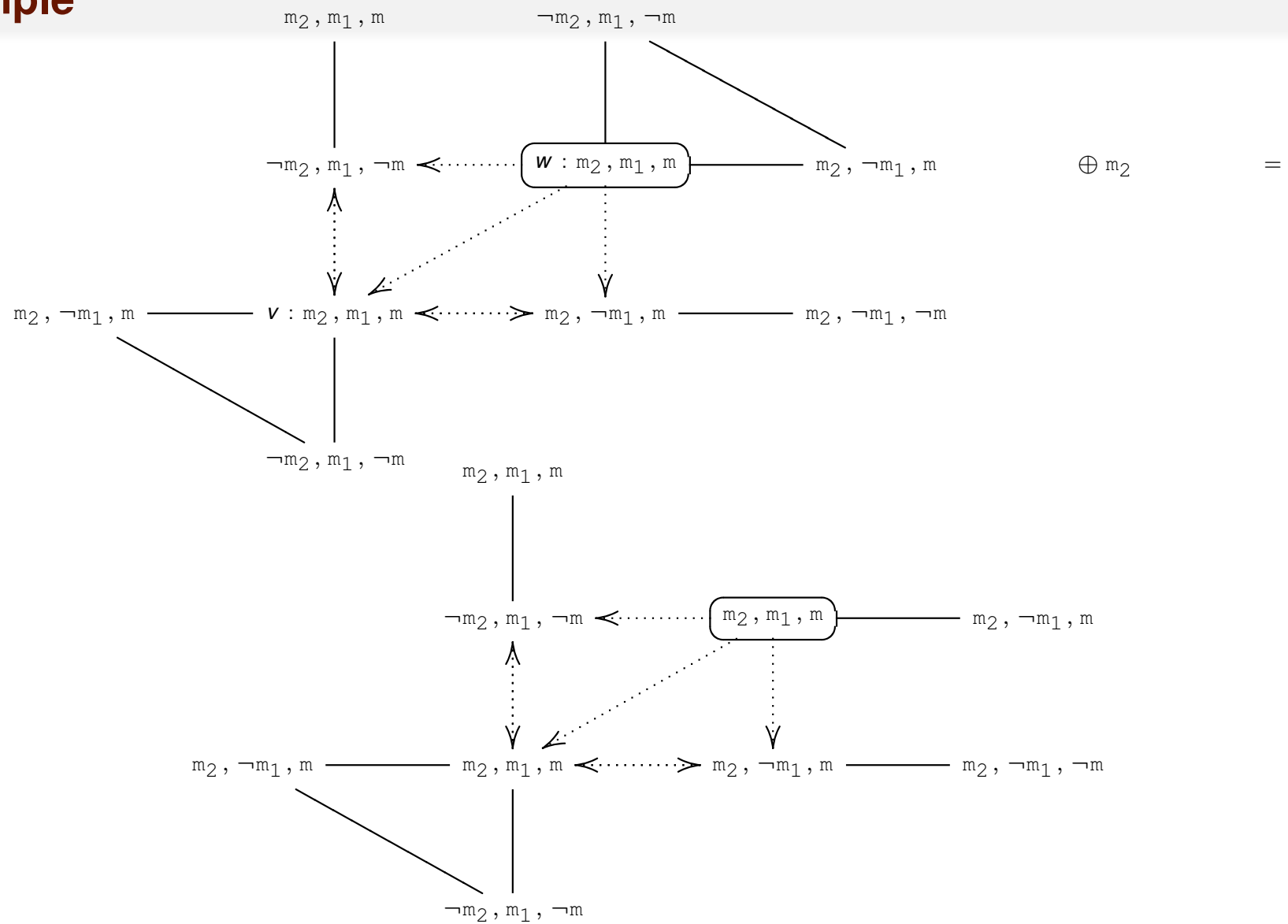
  where $(M, w) \oplus \psi = \begin{cases} (M, w) \otimes (A_\psi, w') & \text{if } M, w \models \psi \\ (M, w) & \text{otherwise;} \end{cases}$

- $M, w \models [s \text{ prom } \alpha]\phi$ iff $M \odot \alpha, w \models \phi$,

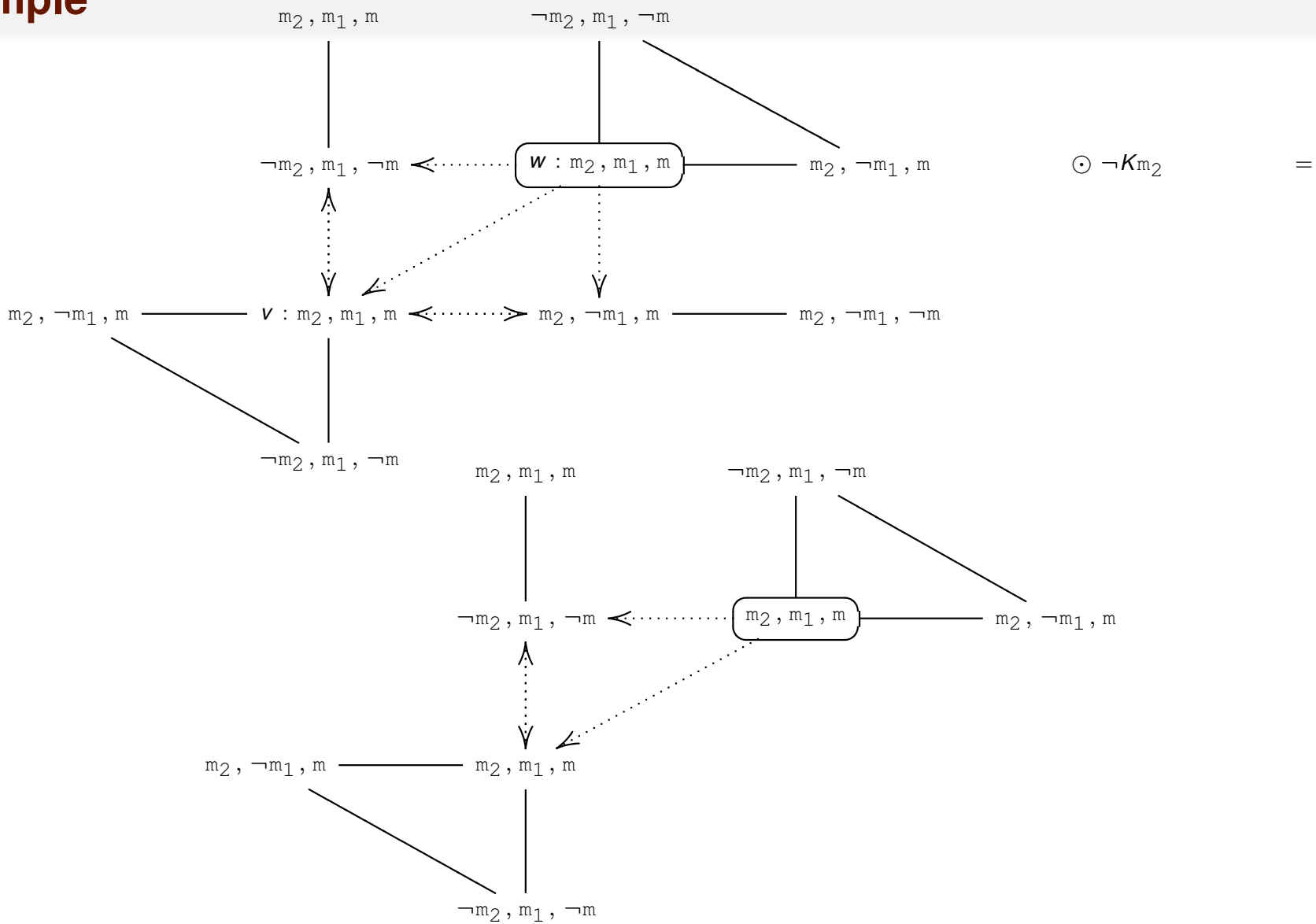
  where $(M, w) \odot \alpha = \begin{cases} (M, w) \otimes (A_\alpha, w') & \text{if } M, w \models \alpha \\ (M, w) & \text{otherwise.} \end{cases}$



Example


m2 , m1 , m
¬m2 , m1 , ¬m
w : m2 , m1 , m
¬m2 , m1 , ¬m
m2 , ¬m1 , m
⊕ m2
=
m2 , ¬m1 , m
v : m2 , m1 , m
m2 , ¬m1 , m
m2 , ¬m1 , ¬m
¬m2 , m1 , ¬m
m2 , m1 , m
¬m2 , m1 , ¬m
m2 , m1 , m
m2 , ¬m1 , m
m2 , ¬m1 , m
m2 , m1 , m
m2 , ¬m1 , m
m2 , ¬m1 , ¬m
¬m2 , m1 , ¬m

Example


m2 , m1 , m
¬m2 , m1 , ¬m
w : m2 , m1 , m
m2 , ¬m1 , m
⊙ ¬Km2
=
m2 , ¬m1 , m
v : m2 , m1 , m
m2 , ¬m1 , m
m2 , ¬m1 , ¬m
¬m2 , m1 , ¬m
m2 , m1 , m
¬m2 , m1 , ¬m
m2 , m1 , m
m2 , ¬m1 , m
m2 , ¬m1 , m
m2 , m1 , m
¬m2 , m1 , ¬m

Axiomatization of $\mathcal{L}_{DEDL}$

Logic *DEDL*:

EDL	All the axiom schemes and inference rules of *EDL*
A_6	$\vdash \psi \rightarrow ([s \text{ sends } \psi]K\phi \leftrightarrow K(\psi \rightarrow [s \text{ sends } \psi]\phi))$
A_7	$\vdash \neg\psi \rightarrow ([s \text{ sends } \psi]\phi \leftrightarrow \phi)$
A_8	$\vdash [s \text{ sends } \psi]O\alpha \leftrightarrow O\alpha$
A_9	$\vdash [s \text{ prom } \alpha]K\phi \leftrightarrow K\phi$
A_{10}	$\vdash \alpha \rightarrow ([s \text{ prom } \alpha]O\alpha' \leftrightarrow O(\alpha \rightarrow \alpha'))$
A_{11}	$\vdash \neg\alpha \rightarrow ([s \text{ prom } \alpha]\phi \leftrightarrow \phi)$
A_{12}	$\vdash \Box \mathrm{p} \leftrightarrow \mathrm{p}$
A_{13}	$\vdash \Box\neg\phi \leftrightarrow \neg\Box\phi$
A_{14}	$\vdash \Box(\phi \rightarrow \psi) \rightarrow (\Box\phi \rightarrow \Box\psi)$
R_4	If $\vdash \phi$ then $\vdash \Box\phi$

where $\Box$ stands for $[s \text{ sends } \psi]$ or $[s \text{ prom } \alpha]$.

Theorems of *DEDL*

- It holds that $\vdash [s \textit{ sends } \psi]K\phi \leftrightarrow ((\psi \rightarrow K(\psi \rightarrow \phi)) \wedge (\neg\psi \rightarrow K\phi))$. So, after sending any truthful information ψ, the recipient knows that ψ holds:

$$\vdash \psi \rightarrow [s \textit{ sends } \psi]K\psi$$

- Sending messages do not change epistemic norms if these norms do not depend on the epistemic state of the agent:

$$\vdash \chi \rightarrow [s \textit{ sends } \psi]\chi$$

where $\chi = \phi_{\mathrm{p}} \rightarrow O\alpha$ or $\chi = \phi_{\mathrm{p}} \rightarrow P\alpha$ with ϕ_{p} propositional.

Plan

Permitted message

Definition

We say that **it is permitted to send message** ϕ according to $\mathcal{P}$ in (M, w), written $M, w \models P(s \text{ sends } \phi)$, if $M, w \models \phi$ and $(M \oplus \phi, w)$ is compliant with respect to $\mathcal{P}$.

Website example:

$$\not\vdash P(s \text{ sends } \phi) \wedge P(s \text{ sends } \psi) \rightarrow P(s \text{ sends } (\phi \wedge \psi))$$

Instance of the **Inference problem**: the permission to disclose the full names of users also allows to disclose their family names:

$$\text{If } \vdash \phi \rightarrow \psi \text{ then } \vdash \mathtt{Cmp} \rightarrow (P(s \text{ sends } \phi) \rightarrow P(s \text{ sends } \psi))$$

Obligatory message

We say that ϕ **is more informative than** ψ for the *recipient* in the situation (M, w), written $M, w \models \phi \geq \psi$, if $M, w \models K(\phi \to \psi)$.

We say that ϕ **is *strictly* more informative than** ψ for the *recipient* in the situation (M, w), written $M, w \models \phi > \psi$, when $M, w \models \phi \geq \psi$ but not $M, w \models \psi \geq \phi$.

Definition

We say that **it is obligatory to send message** ϕ according to $\mathcal{P}$ in (M, w), written $M, w \models O(s \textit{ sends } \phi)$, if

1. the situation (M, w) is not compliant w.r.t. $\mathcal{P}$,
2. sending ϕ restores compliance,
3. sending a message strictly less informative than ϕ does not restore compliance.

Permitted and obligatory messages

- If ϕ is strictly more informative that ψ, then the obligation to send ϕ entails that sending ψ is not permitted:

$$\vdash \phi > \psi \rightarrow (O(s \textit{ sends } \phi) \rightarrow \neg P(s \textit{ sends } \psi)) .$$

- In the website example, it is prohibited to disclose the mapping from numbers to websites visited but it does not entail that it is obligatory to disclose a modified version of this mapping. So,

$$\nvdash O(s \textit{ sends } \phi) \leftrightarrow \neg P(s \textit{ sends } \neg\phi).$$

Website Example

It is permitted to send one of the mappings:

$$M, w \models P(s \text{ sends } \mathtt{m}_1) \wedge P(s \text{ sends } \mathtt{m}_2)$$

But after sending one ($\mathtt{m}_2$) it is *not* permitted to send the other ($\mathtt{m}_1$):

$$M, w \models [s \text{ sends } \mathtt{m}_2] \neg P(s \text{ sends } \mathtt{m}_1)$$
$$M, w \models [s \text{ sends } \mathtt{m}_1] \neg P(s \text{ sends } \mathtt{m}_2)$$

This is because in both cases we would violate the epistemic norm $\neg PK\mathtt{m}$:

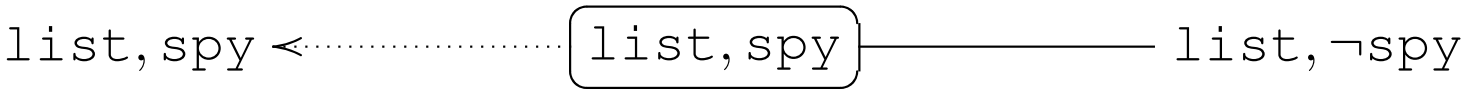
$$M, w \models [s \text{ sends } \mathtt{m}_2][s \text{ sends } \mathtt{m}_1] (K\mathtt{m} \wedge \neg PK\mathtt{m})$$
$$M, w \models [s \text{ sends } \mathtt{m}_1][s \text{ sends } \mathtt{m}_2] (K\mathtt{m} \wedge \neg PK\mathtt{m}) .$$

Spyware Example

It is forbidden to disclose $\texttt{list}$:

$$M, w \models \neg P(s \textit{ sends } \texttt{list})$$

But if it is disclose, then we obtain the following situation $M \oplus \texttt{list}$:



In that situation, it is obligatory to disclose $\texttt{spy}$:

$$M \oplus \texttt{list}, w \models O(s \textit{ sends } \texttt{spy})$$

So, we have that

$$M, w \models [s \textit{ sends } \texttt{list}] O(s \textit{ sends } \texttt{spy})$$
$$M, w \models \neg P(s \textit{ sends } \texttt{list}) \wedge P(s \textit{ sends } (\texttt{list} \wedge \texttt{spy}))$$

As it turns out, after sending the message $\texttt{spy}$ we reach a compliant situation.

Meta-policy

If the *recipient* knows the privacy policy, he might infer some secret information: if the *recipient* learns that it is prohibited that he knows p, then he might infer that p holds.

Formally, if we extend our language and also our logic with the following axiom schema:

$$\vdash' O(\phi \to \alpha) \leftrightarrow (\phi \to O\alpha),$$

then we have that the following holds:

$$\vdash' [s \textit{ sends } \neg PK\mathrm{p}]K\mathrm{p}.$$

We can avoid this situation by enforcing the following privacy policy:

$$\mathcal{P}'' = \{\neg PK\mathrm{p}, \neg PK\neg PK\mathrm{p}\}$$

In that case, sending the message $\neg PK\mathrm{p}$ will lead to a violation:

$$\vdash' \mathcal{P}'' \to \neg P(s \textit{ sends } \neg PK\mathrm{p}).$$

Plan

Motivations

Goal of the Security Monitor (SM):

- Decide which actions to execute and which message to send so as to enforce and maintain a privacy policy given by a law/policy maker.

Method:

- Implement an *EDL*-model representing the current state of affairs;
- Check compliance and decide which actions to execute by model checking this *EDL*-model

Problems with the current language $\mathcal{L}_{DEDL}$:

- The SM could not check whether a situation is compliant;
- The SM could not express that an epistemic norm is added or removed to/from the privacy policy by the law/policy maker;
- The SM could not express that under the current privacy policy he is permitted to disclose information ϕ;

$\Rightarrow$ We need to define a new language $\mathcal{L}_{PL}$.

Language $\mathcal{L}_{PL}$

$$\mathcal{L}_{PL} : \phi ::= \psi \mid (\chi \in \mathcal{P}) \mid \mathtt{Cmp} \mid \mathtt{Cmp}' \mid P(s \text{ sends } \psi) \mid [s \text{ sends } \psi]\phi \mid$$
$$[s \text{ prom } \alpha]\phi \mid [+\chi]\phi \mid [-\chi]\phi \mid \neg\phi \mid \phi \wedge \phi$$

where $\psi \in \mathcal{L}_{DEDL}$ and $\alpha \in \mathcal{L}^{\alpha}_{DEDL}$. The set of epistemic norms $\mathcal{EN}$ is *finite*.

- $(\chi \in \mathcal{P})$: 'χ is an epistemic norm of the current privacy policy';
- $\mathtt{Cmp}$: 'the current situation is compliant with respect to the current privacy policy';
- $\mathtt{Cmp}'$: 'the current situation is *regulatory* compliant with respect to the current privacy policy';
- $[+\chi]\phi$: 'after adding the epistemic norm χ to the current privacy policy, ϕ holds';
- $[-\chi]\phi$: 'after removing the epistemic norm χ from the current privacy policy, ϕ holds';
- $P(s \text{ sends } \psi)$: 'sending the message ψ is permitted'.

Semantics and truth conditions of $\mathcal{L}_{PL}$

A pointed privacy model is a pair $\{(M, w), \mathcal{P}\}$ where (M, w) is a pointed *EDL*-model and $\mathcal{P}$ is a privacy policy.

$\{(M, w), \mathcal{P}\} \models \psi$	iff	$M, w \models \psi$
$\{(M, w), \mathcal{P}\} \models (\chi \in \mathcal{P})$	iff	$\chi \in \mathcal{P}$
$\{(M, w), \mathcal{P}\} \models \mathtt{Cmp}$	iff	$M, w \models i \rightarrow \alpha$ for all $i \rightarrow O\alpha \in \mathcal{P}$
$\{(M, w), \mathcal{P}\} \models \mathtt{Cmp}'$	iff	$M, w \models \chi$ for all $\chi \in \mathcal{P}$
$\{(M, w), \mathcal{P}\} \models P(s \text{ sends } \psi)$	iff	$M, w \models \psi$ and $\{(M, w), \mathcal{P}\} \models [s \text{ sends } \psi]\mathtt{Cmp}$
$\{(M, w), \mathcal{P}\} \models [s \text{ sends } \psi]\phi$	iff	$\{(M \oplus \psi, w), \mathcal{P}\} \models \phi$
$\{(M, w), \mathcal{P}\} \models [s \text{ prom } \alpha]\phi$	iff	$\{(M \odot \alpha, w), \mathcal{P}\} \models \phi$
$\{(M, w), \mathcal{P}\} \models [+\chi]\phi$	iff	$\{(M, w), \mathcal{P} \cup \{\chi\}\} \models \phi$
$\{(M, w), \mathcal{P}\} \models [-\chi]\phi$	iff	$\{(M, w), \mathcal{P} - \{\chi\}\} \models \phi$

Axiomatization and computational complexity of $\mathcal{L}_{PL}$

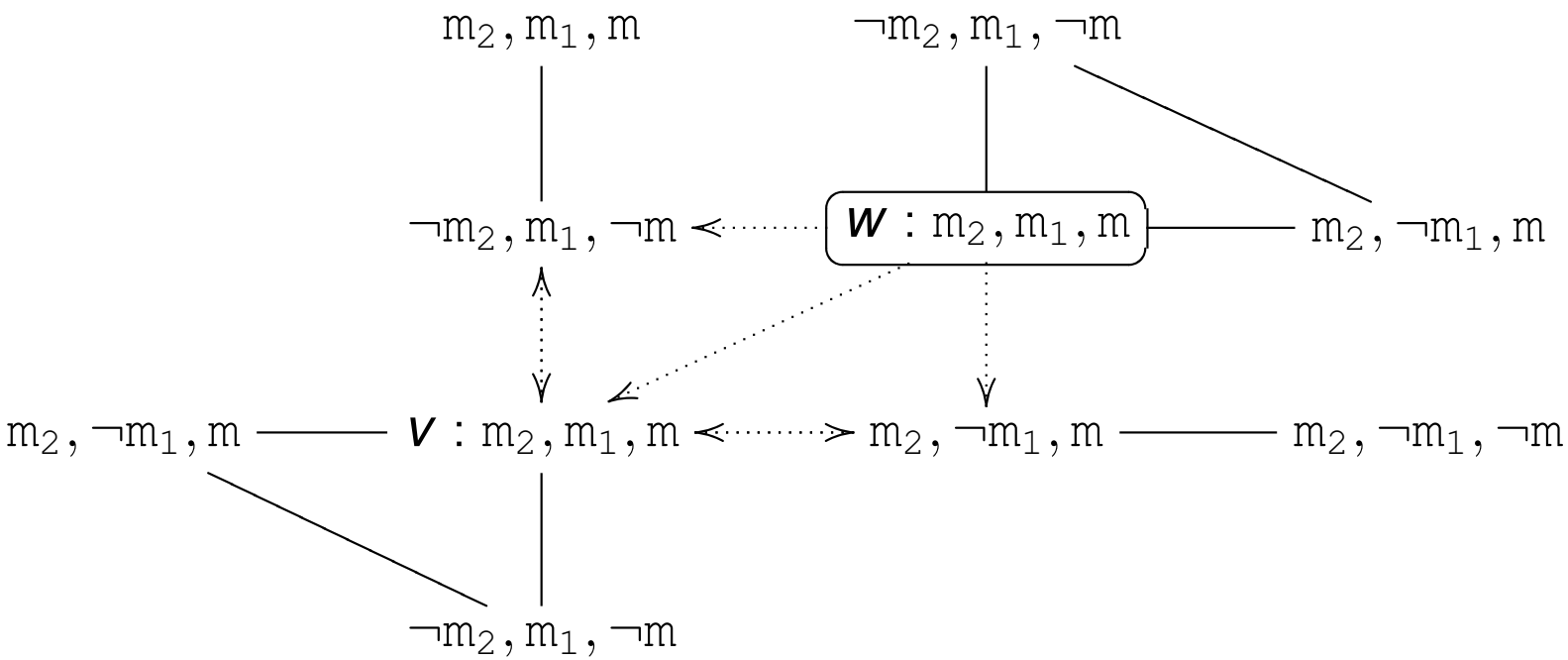
Axiom schemes and inference rules of *DEDL* together with: ($\chi_o = i \rightarrow O\alpha$, $\Box = [s \text{ sends } \psi]$ or $[s \text{ prom } \alpha]$, and $[\pm\chi] = [+\chi]$ or $[-\chi]$)

P_1	$\vdash \mathtt{Cmp} \leftrightarrow \bigwedge_{\chi_o \in \mathcal{EN}} ((\chi_o \in \mathcal{P}) \rightarrow (i_\chi \rightarrow \alpha_\chi))$	P_8	$\vdash [+\chi](\chi \in \mathcal{P})$
P_2	$\vdash \mathtt{Cmp}' \leftrightarrow \bigwedge_{\chi \in \mathcal{EN}} ((\chi \in \mathcal{P}) \rightarrow \chi)$	P_9	$\vdash [-\chi]\neg(\chi \in \mathcal{P})$
P_4	$\vdash P(s \text{ sends } \psi) \leftrightarrow \psi \wedge [s \text{ sends } \psi]\mathtt{Cmp}$	P_{10}	$\vdash [\pm\chi](\chi' \in \mathcal{P}) \leftrightarrow (\chi' \in \mathcal{P})$
P_5	$\vdash \Box(\chi \in \mathcal{P}) \leftrightarrow (\chi \in \mathcal{P})$	P_{11}	$\vdash [\pm\chi]\psi \leftrightarrow \psi$
P_6	$\vdash \Box\neg\phi \leftrightarrow \neg\Box\phi$	P_{12}	$\vdash [\pm\chi]\neg\phi \leftrightarrow \neg[\pm\chi]\phi$
P_7	$\vdash \Box(\phi \rightarrow \phi') \rightarrow (\Box\phi \rightarrow \Box\phi')$	P_{13}	$\vdash [\pm\chi](\phi \rightarrow \phi') \rightarrow ([\pm\chi]\phi \rightarrow [\pm\chi]\phi')$
R_P	If $\vdash \phi$ then $\vdash [\pm\chi]\phi$		

Theorem

- *The satisfiability problem of $\mathcal{L}_{PL}$ is decidable.*
- *Any instance of the model checking problem of $\mathcal{L}_{PL}$ is solved in time $O((||M|| + |\mathcal{P}|) \times (|\phi| + |\mathcal{P}|))$.*

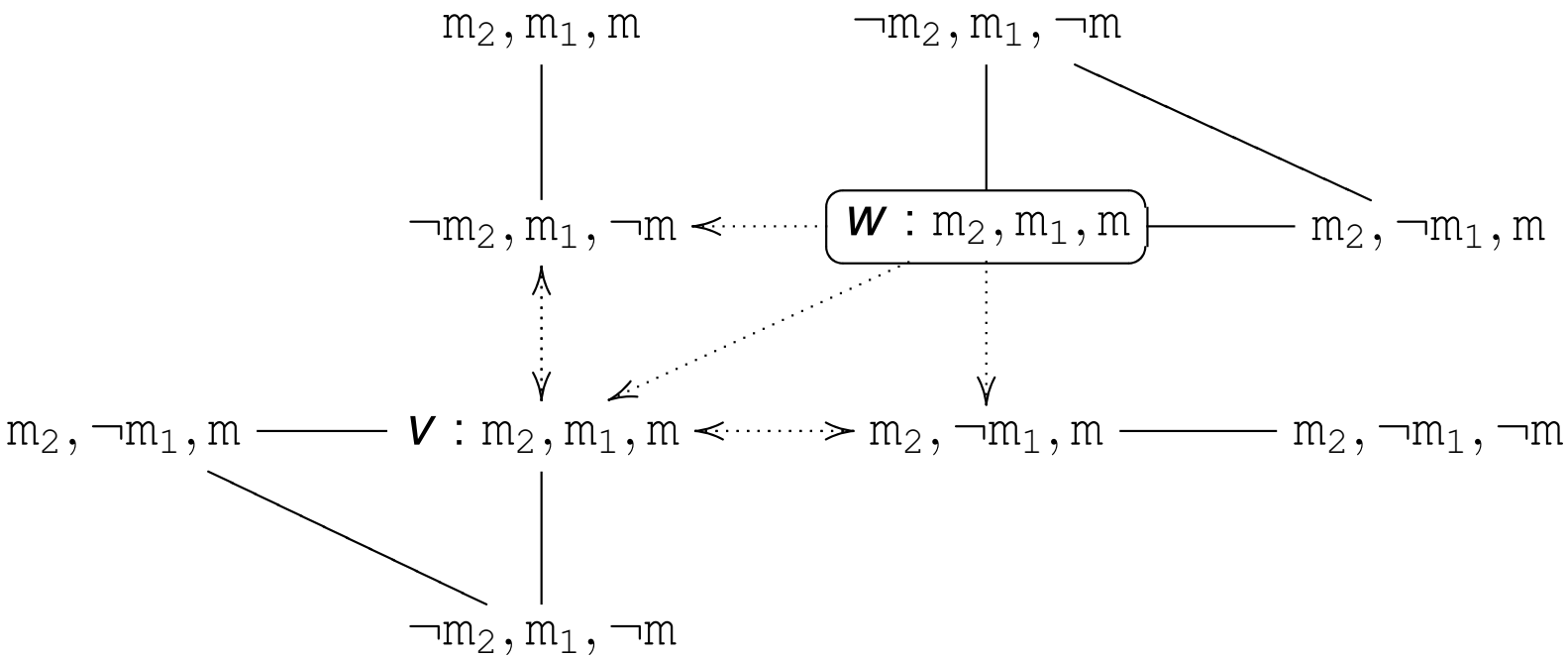
Website example



$$\mathcal{P} = \{PK m_1, PK m_2, \neg PK m\} \qquad \{(M, w), \mathcal{P}\} \models \mathrm{Cmp} \wedge \mathrm{Cmp}'$$

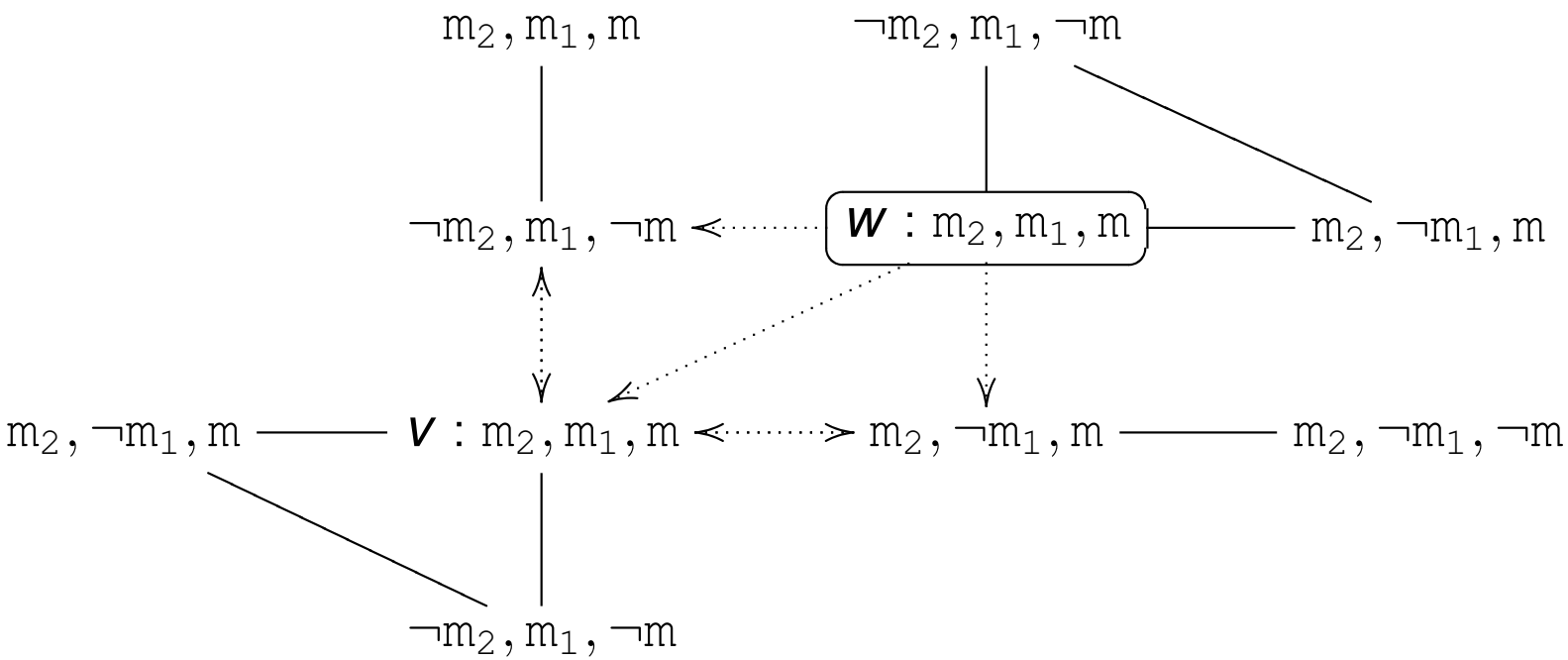
Website example

The law/policy maker asks *sender* to make the policy stricter:



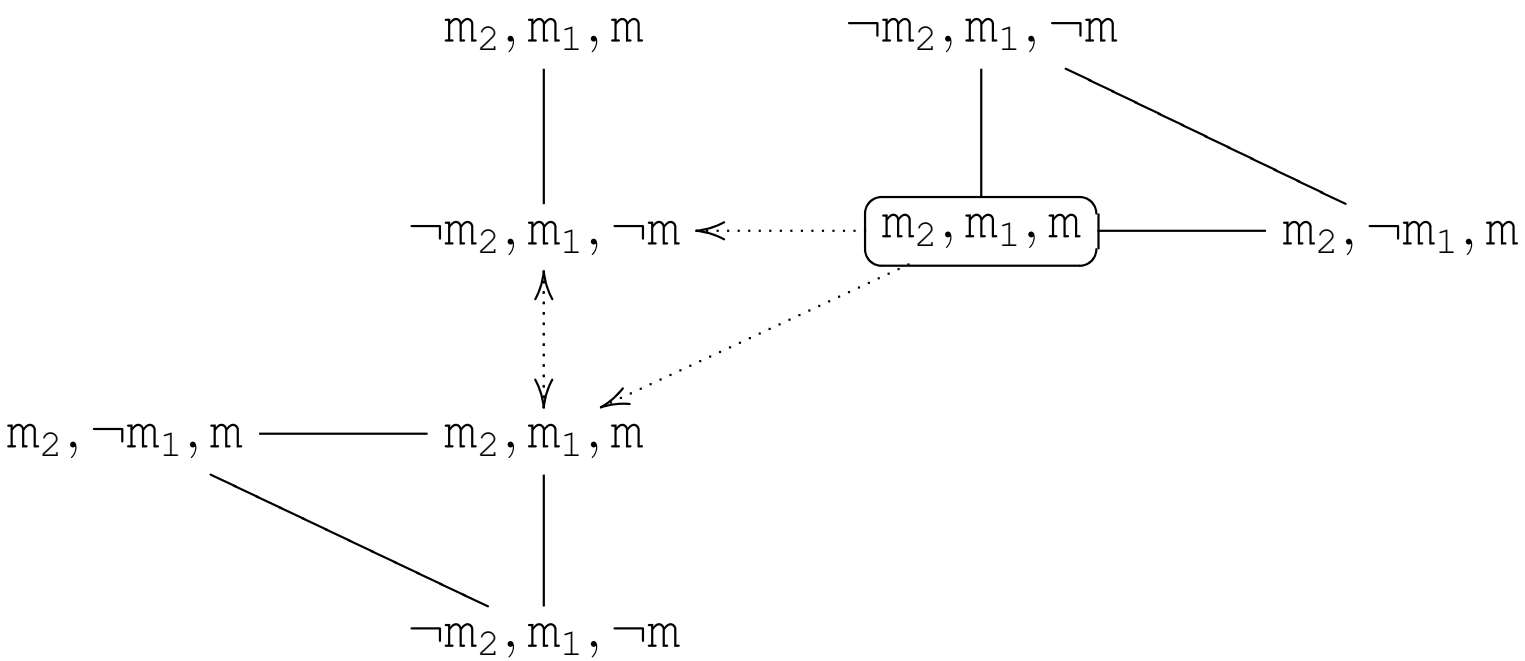
Enforce $\mathcal{P}' = \{PK\mathrm{m}_1, \neg PK\mathrm{m}_2, \neg PK\mathrm{m}\}$!

Website example



$$\mathcal{P}' = \{PK\mathrm{m}_1, \neg PK\mathrm{m}_2, \neg PK\mathrm{m}\} \qquad \{(M, w), \mathcal{P}'\} \models \neg \mathrm{Cmp}'$$

Website example



$\mathcal{P}' = \{PK\mathrm{m}_1, \neg PK\mathrm{m}_2, \neg PK\mathrm{m}\}$ $\quad$ $\{(M, w), \mathcal{P}'\} \models [s\ prom\ \neg K\mathrm{m}_2]\mathrm{Cmp}'$

Plan

Conclusion

- We defined a privacy policy as a set of epistemic norms specifying what a *recipient* is permitted and forbidden to know.
- This allowed us to derive the permitted and prohibited messages in a given situation with much flexibility.
- Our logic is decidable with reasonable complexity and allows to
  1. check compliance with respect to a privacy policy,
  2. change the privacy policy,
  3. determine which action needs to be done to enforce a privacy policy.

Thank you

Thank you !