MODEL CHECKING COMBINED TEMPORAL LOGICS

[an overview of some current work]

Michael Fisher, **Savas Konur**, **Sven Schewe**

Department of Computer Science, University of Liverpool, UK

VPS Meeting, Birmingham, June 2009

The Problem

Pervasive Systems comprise many different facets are so are often difficult to describe formally/logically.

We want to represent not just the basic dynamic behaviour of a pervasive system, but also

- *real-time* aspects
- *uncertainty* and *environmental models*
- *collaboration* and *cooperation*
- *mobility*, *distribution* and *concurrency*
- *autonomous decision-making*
- the central involvement of both *humans* and *artifacts*
- *etc*...

Combining Logics

Since one framework is not able to describe all aspects of a pervasive system at once, we will often need to *combine* formalisms.

As we do *not* want to develop new verification techniques, we need to re-use current ones for the constituent logics.

So: can we combine logics to give a sophisticated basis for specification?

And: more importantly, can we use the verification methods from each of the component logics to construct a combined verification method?

A Plethora of Formal Logics

The *formal description* of pervasive systems can typically involve many different logical dimensions:

- dynamic communicating systems $\longrightarrow$ *temporal logics*
- systems managing information $\longrightarrow$ *logics of knowledge*
- autonomous systems $\longrightarrow$ *logics of goals, intentions*
- situated systems $\longrightarrow$ *logics of belief, contextual logics*
- timed systems $\longrightarrow$ *real-time temporal logics*
- uncertain systems $\longrightarrow$ *probabilistic logics*
- cooperative systems $\longrightarrow$ *cooperation/coalition logics*

Combinations of such logics are usually needed.

Sample Logical Operators

$\Diamond$ . . . . *at some point in the future*

$\bigcirc$ . . . . *at the next moment in time*

$\Diamond^{<5s}$ . . . . *at some point, within 5 seconds*

$K_{Michael}$ . . . . *Michael knows*

$K_{Michael}K_{Mark}$ . . . . *Michael knows that Mark knows*

$K_{Muffy}\neg K_{Michael}$ . . . . *Muffy knows that Michael doesn't know*

B . . . . *belief*

$B^{0.55}$ . . . . *belief with 55% probability*

G, D, I, W . . . . *goal, desire, intention, wish*

....

Agent Example

$$B_{me}^{>0.75} \Diamond G_{you} attack(you, me) \Rightarrow I_{me} \Diamond^{<5s} attack(me, you)$$

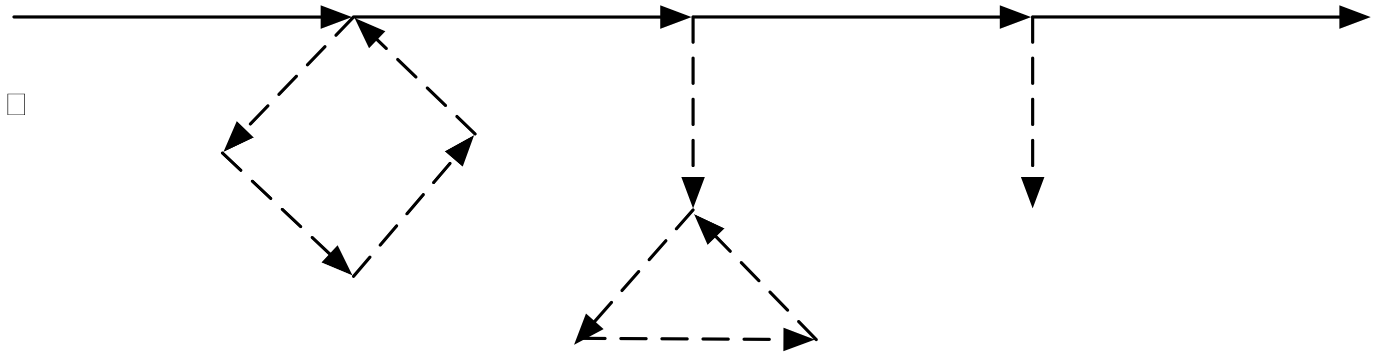
"If I believe, with over 75% probability that at some point in the future your goal will be to attack me, then I intend that within 5 seconds I will attack you."

Combinations: Temporalization

Imagine we have two logics to combine, $\mathcal{A}$ (a temporal one) and $\mathcal{B}$.

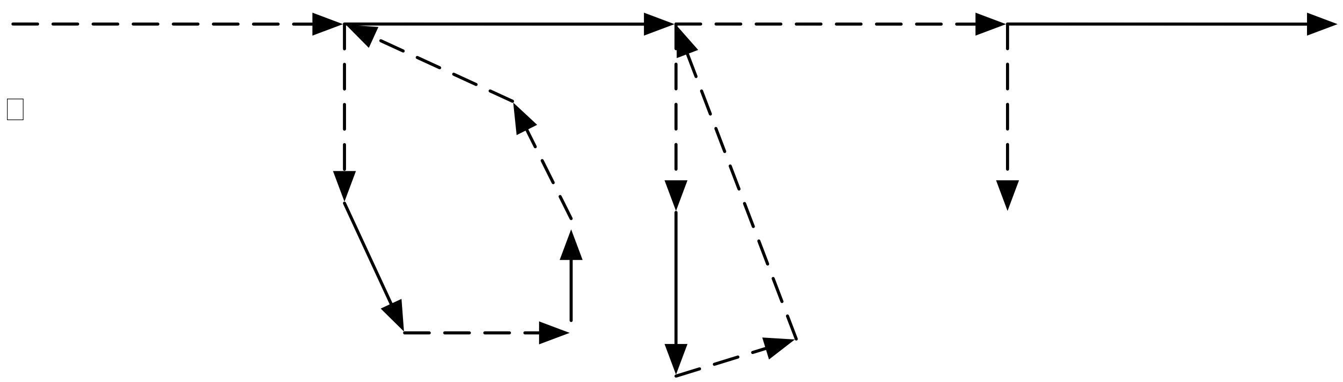
The *temporalization* is $\mathcal{A}(\mathcal{B})$ where a pure subformula of $\mathcal{B}$ can be treated as an atom within $\mathcal{A}$.

This combination is *not* symmetric — $\mathcal{A}$ is the main logic, but at each world/state described by $\mathcal{A}$ we might have a formula of $\mathcal{B}$ describing a "$\mathcal{B}$-world".



Combinations: Fusion

The *fusion* A $\oplus$ B is more symmetric than temporalization in that, at any state/world we can either take an "A-step" or a "B-step".

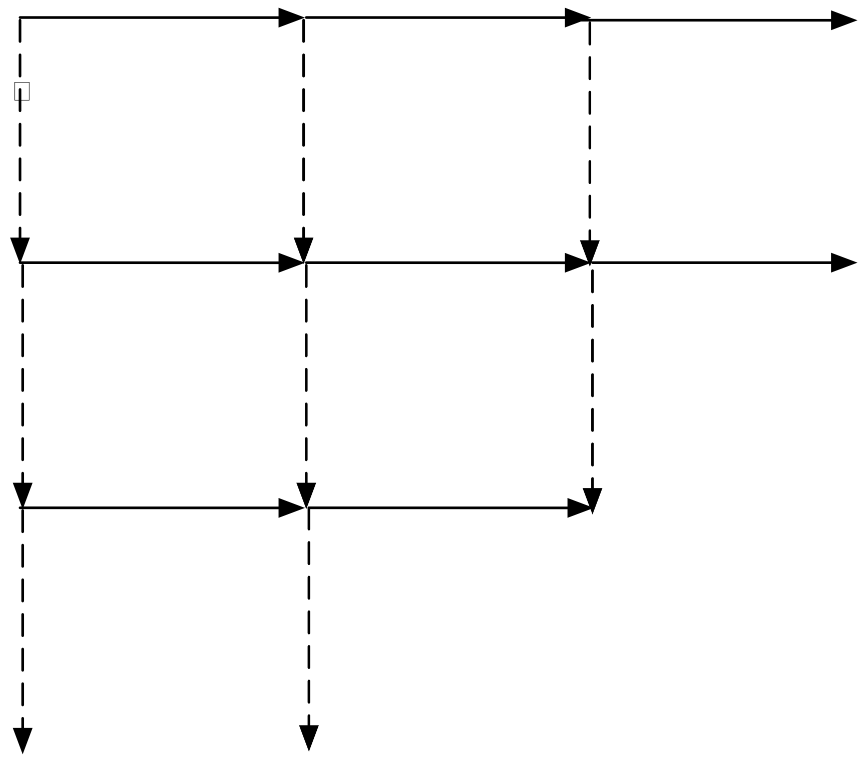


It is important to note that the two logical dimensions are essentially independent.

N.B: the formula $OP_A OP_B \varphi \Leftrightarrow OP_B OP_A$ *is not* valid.

Combinations: Product

The product combination, $\mathrm{A} \otimes \mathrm{B}$, is similar to the fusion, but with a much tighter integration of the logics.



Operators of the constituent logics tend to be *commutative*. Thus, formulae such as $OP_{\mathrm{A}}OP_{\mathrm{B}}\varphi \Leftrightarrow OP_{\mathrm{B}}OP_{\mathrm{A}}$ *are* valid.

Problems

There has been a *lot* of work on combinations of logics, almost all of it concerning axiomatizability, decidability, and deductive methods.

For example:

- If the constituent logics are decidable, then the fusion and temporalization of the logics is decidable.
- Because of the tight interaction between dimensions, the product of two decidable logics can often become undecidable, e.g $K \otimes K \otimes K$, $PTL \otimes PTL$.

Similarly, deduction within combined logics can become much harder.

Model Checking

However: Model checking combined logics is easier.

Franceschet, Montanari, and de Rijke have tackled the model checking problem for combined logics.

Result: for basic modal/temporal logics, model checking of temporalization, fusion or product logics is not very much more difficult than checking the constituent logics.

N.B: their result is for logics with simple Kripke semantics of the form $\langle W, \mathcal{R}, V \rangle$

What are we doing? (1)

We would like to combine more complex (temporal) logics, specifically, *real-time* and *probabilistic* temporal logics.

Real-time (e.g. TCTL) and probabilistic (PCTL) temporal logics also contain probability/clock-constraint mappings.

Can we extend the results/techniques of Franceschet et. al. to $\mathrm{PCTL}(\mathrm{L})$, $\mathrm{TCTL}(\mathrm{L})$, $\mathrm{PCTL} \oplus \mathrm{L}$ and $\mathrm{TCTL} \oplus \mathrm{L}$ where L is a standard (modal) logic?

And what is the complexity of these combinations?

What about $\mathrm{TCTL}(\mathrm{PCTL})$, $\mathrm{PCTL}(\mathrm{TCTL})$, $\mathrm{TCTL}(\mathrm{TCTL})$, $\mathrm{PCTL}(\mathrm{PCTL})$, $\mathrm{TCTL} \oplus \mathrm{TCTL}$, $\mathrm{PCTL} \oplus \mathrm{PCTL}$, $\mathrm{TCTL} \oplus \mathrm{PCTL}$, $\mathrm{TCTL} \otimes \mathrm{TCTL}$, $\mathrm{PCTL} \otimes \mathrm{PCTL}$, and $\mathrm{TCTL} \otimes \mathrm{PCTL}$?

What are we doing? (2)

In some case combined logics already exist, e.g. PTCTL.

What is comparison between PTCTL and $\mathrm{TCTL} \otimes \mathrm{PCTL}$?

Can we simulate PTCTL by $\mathrm{TCTL} \otimes \mathrm{PCTL}$?

Or even by $\mathrm{TCTL} \oplus \mathrm{PCTL}$ with additional constraints?

What about $\mathrm{TCTL}_1 \otimes \mathrm{TCTL}_1$ versus TCTL_2?

What combinations are really useful for pervasive systems??