Message logic for service commitments

Murdoch J. Gabbay

IC3 Winter Retreat

7 January 2025

Message Logic is . . .

. . . a simple logic designed to talk about message-passing in distributed systems, as presented in this technical report (https://zenodo.org/records/14251398).



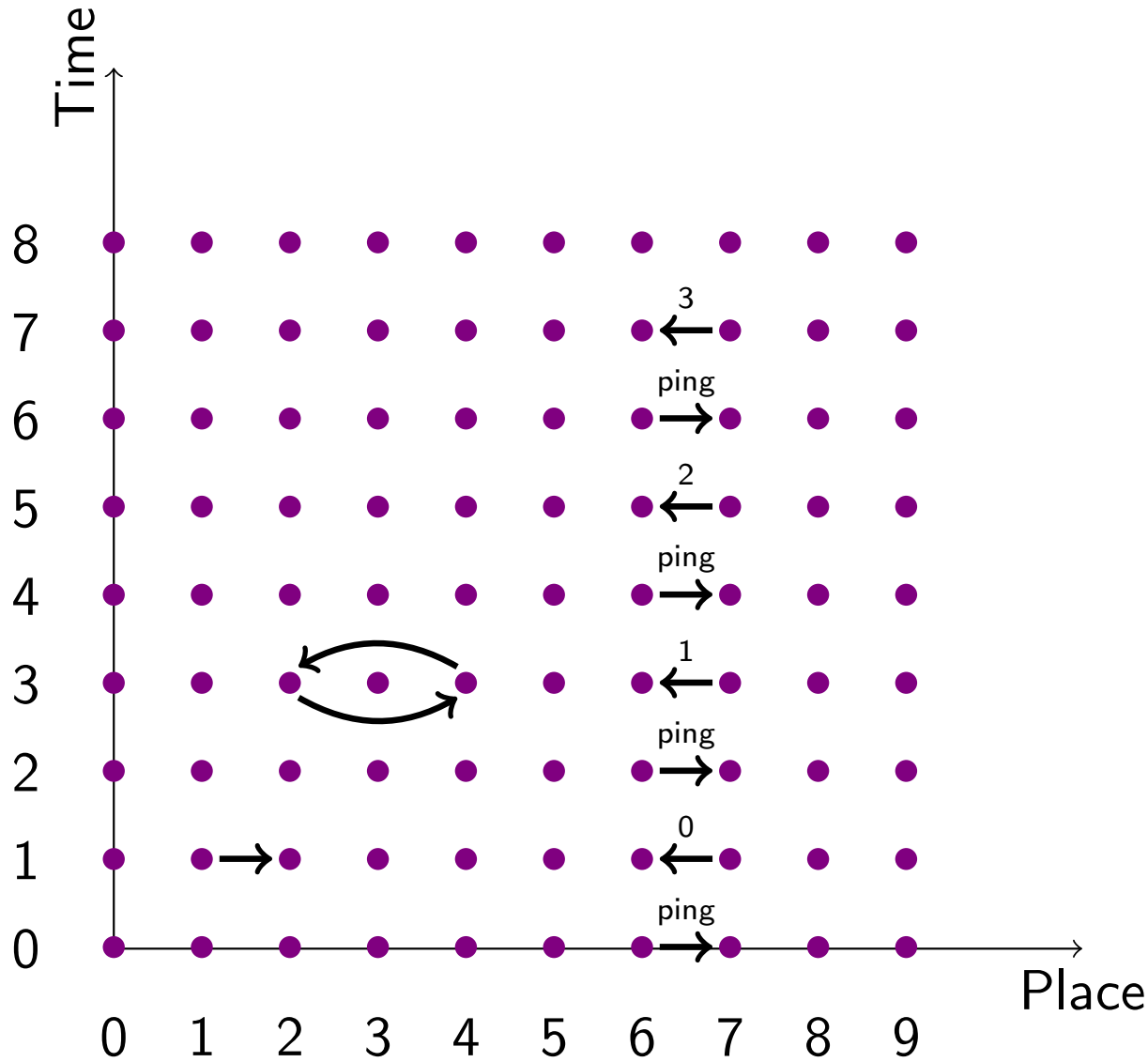
It turns out to be surprisingly interesting. In this short talk I'll try to give a flavour of why. (I might not get through all the slides in 12 minutes, but that's OK.)

Thanks to Heliax and to the organisers for making it possible for me to be here.

Message Logic universe is simple

1. Assume a fixed set of participants (or points, or places) $p, p' \in \text{Place}$.
   In practice Place will be finite.
2. Assume a set of discrete times $n \in \text{Time} \subseteq \mathbb{N}_{\geq 0}$.
   Time is discrete, universal (no local clocks), and may be finite.
3. Assume a set of data $d \in \text{Data}$. We don't really care what data is; it's just message payloads.
4. Assume messages $(n, p) \xrightarrow{d} (n, p')$ that carry arbitrary data d and pass instantly and reliably from p to p' at time n.
   So: no bandwidth limit; no latency; no message loss.

So: times, places, and messages. Let's see a picture:


Time
8
7
6
5
4
3
2
1
0
3
ping
2
ping
1
ping
0
ping
Place
0 1 2 3 4 5 6 7 8 9

A typical service commitment

Forwarding commitment $\mathrm{F}(x, z, t, r, l)$:

> *For the next t ms, I will forward to z at least $(100 * r)\%$ of the messages I receive from x, within l ms.*

For y at time n to commit to the above, is for y to promise to behave such that $\mathrm{F}(x, z, t, r, l)$ will be valid (= true) at y at time n.

Let's unpack that:

1. 'For the next t ms, I promise': this commitment is made *at a time and a place*.
2. '(100*r)%': we have *sets* and *cardinalities*.
3. 'y will forward to z', 'y receives from x ': it's all about *messages coming in and out* at places ...
4. 'within l ms': ...and at times.
5. Validity is judged by an *omniscient observer*, standing outside the model.

Message Logic (syntax)

Let's build a logic to express validity of service commitments.

Syntax of terms and predicates first:

$$t ::= (a \in \mathsf{VarSymb}) \mid (d \in \mathsf{Data}) \mid \mathsf{f}(t) \mid \texttt{here} \mid \texttt{now} \mid \{a \mid \phi\}$$

$$\phi ::= \bot \mid \prod^{r} a : \phi.\phi \mid \mathsf{P}(t) \mid @_t\phi \mid \texttt{in}_p(t) \mid \texttt{out}_p(t) \mid \texttt{BOU}(\phi) \mid \texttt{EOU}(\phi)$$

A term t is either a variable symbol a, or a datum d, or $\mathsf{f}(t)$ a function-symbol f applied to a term t, or `here` (a place), or `now` (a time), or a compehension term $\{a \mid \phi\}$ (denotes the set of d such that $\phi[a{:=}d]$).

I'll discuss predicates below.

A flavour of the denotation (1 of 2)

The logic is modal: terms and predicates take values in a context of a time $n \in \text{Time}$ and a place $p \in \text{Place}$. Thus:

$$[\![d]\!]_{n,p} = d \quad \text{and} \quad [\![\texttt{here}]\!]_{n,p} = p \quad \text{and} \quad [\![\texttt{now}]\!]_{n,p} = n$$

and

$$\frac{(n,p') \overset{[\![t]\!]_{n,p}}{\rightarrow} (n,p)}{n,p \vDash \texttt{in}_{p'}(t)} \qquad \frac{(n,p) \overset{[\![t]\!]_{n,p}}{\rightarrow} (n,p')}{n,p \vDash \texttt{out}_{p'}(t)}$$

$$\frac{[\![t]\!]_{n,p}, p \vDash \phi \quad ([\![t]\!]_{n,p} \in \text{Time})}{n,p \vDash @_t \phi}$$

A flavour of the denotation (2 of 2)

I call this *Pragmatic Implication:*

$$\frac{\begin{array}{l} A = \{x \in \text{Data} \mid n, p \vDash \phi[a{:=}x]\} \\ B = \{x \in \text{Data} \mid n, p \vDash \phi[a{:=}x] \wedge \psi[a{:=}x]\} \\ (\#B/\#A \geq r) \end{array}}{n, p \vDash \prod^{r} a : \phi.\psi}$$

$\prod^{r} a : \phi.\psi$ means that for $(100 * r)\%$ of the d such that $\phi[a{:=}d]$ holds, $\psi[a{:=}d]$ also holds. E.g.

Nearly all swans are white.

could be expressed as

$$\prod^{0.999} a : \text{swan}(a).\text{white}(a).$$

Pragmatic implication is a kind of dependent product. It's not a probability! It may be related to theories of logic where truth-values are distances in a metric space.

Pragmatic implication, applied

It's expressive; e.g. we can derive propositional and predicate logic. For example:

- $\phi \Rightarrow \psi \;=\; \prod^1 a' : \phi.\psi$ (where $a' \notin fv(\phi)$).
- $\forall a.\phi \;=\; \prod^1 a : \top.\phi$.
- $\neg\phi \;=\; \prod^0 a' : \phi.\top$ (where $a' \notin (\phi)$).

We can express a promise that at time m, participant y for the next t ms will forward to z at least $(100 * r)\%$ of the messages it receives from x, within l ms as:

$$m, y \vDash \prod^r (n, d) : (\mathtt{now} \leq n < \mathtt{now} + t) \wedge @_n \mathtt{in}_x(d). \\ \exists n' : n \leq n' < n + l.@_{n'} \mathtt{out}_z(d).$$

Commitments are like axioms, but unlike axioms

Commitments and axioms are both predicates. But an axiom is an assumption, whereas a commitments is an aspiration.

When we assert an axiom, by definition models of that axiom are of interest, and non-models are not. Group theory is the study of models of the theory of groups: if a structure is a semiring but not a group, then it's not a group. That's it!

In contrast, service commitments are not always kept, and we consider non-models so we can reason about things going wrong. Arguably, we assert commitments so we can study their *non-models*!

Nobody worries about how to make sure a group stays a group, or how to recover from a group becoming a semigroup. But sysadmins ask such questions all the time, about service commitments.

Sometimes, commitments *should* fail

Sometimes breaking a service commitment would be judged as *right*.

I may promise to tell my wife the truth, and then tell her she's beautiful when she wakes up in the morning and her hair's a mess.

Paradoxically, my wife loves — and trusts — me *more*, not less, for having committed to honesty and then broken that commitment.

I may promise to forward network messages . . . but what if I know the message payload has a virus, so I drop it? Am I wrong to break my promise, or wrong to keep it?

What if the entire network goes down? It's still breaking a service commitment (no messages get forwarded), but who can blame me?

Noting what's new

Pragmatic implication seems to be new. There may be an interesting categorical (e.g. topos-like) theory to it.

The ontology is interesting. We have facts (things that are true), axioms (things that are true by assumption), and commitments (things that aspire to be true, but might not be, possibly in interesting ways).

Offers are bids to negotiate to enter into a commitment. More on these in another talk.

Evaluating validity of commitments happens in two ways: by participants at a time and a place deciding whether a p is trustworthy; and omnisciently, checking the model directly.

Future work

More on this in the technical report.



This was supposed to be a small exercise, but the more I dug, the more subtleties I found.

Perhaps Message Logic can be a useful conceptual tool. I welcome suggestions for ways to apply it: let's talk!