# basic protocol formalism

February 6, 2018

Our data types will be required to be finite:

$$\tau ::= \mathbb{Z}_q \mid \mathsf{bool} \mid \tau \times \tau \mid \dots.$$

Additionally, assume some message spaces $I$ and $O$. (A possible choice for this is to have each party be indexed by a natural number, and let $I$ and $O$ be of the form $\Sigma_{i \in \mathcal{I}} F(i)$, where $\mathcal{I}$ is a finite set of natural numbers, and $F$ is a function from natural numbers to message types $\tau$.)

Then, a process with state space $S$ is defined to be a pair $S \times (S \to I \to \mathcal{D}(S \times O))$.

We may ask if two processes $P$, $Q$ are behaviorally equivalent by first forming their disjoint union, where states of the disjoint union are pairs, and the handler pattern matches on the state to decide which handler to run. Then, we ask if the initial state of $P$ is bisimilar to the initial state of $Q$.

For a state $s$ in some process, write $s \xrightarrow{m} \mu$ to mean $\mu := \delta(s, m)$, where $\delta$ is the handler for that process. Then, we say that a relation $\sim$ over states is a *bisimulation* if for any $s \sim t$,

$$\forall m, \forall C \in S/\sim, \text{ if } s \xrightarrow{m} \mu \text{ and } t \xrightarrow{m} \eta \text{ then } \forall m', \mu(m', C) = \eta(m', C),$$

where $\mu(m', C)$ is the probability that $\mu$ outputs a pair $m'', s'$ such that $m'' = m'$ and $s' \in C$.

Note that this above notion can be checked symbolically, even in the presence of a large number of equivalence classes. Represent each equivalence class by a number in $\mathbb{N}$, and represent $\sim$ by a function $f : S \to \mathbb{N}$. Then, we may say that $f$ induces a bisimulation if

$$\forall s, t \text{ such that } f(s) = f(t), \forall m, \text{ if } s \xrightarrow{m} \mu \text{ and } t \xrightarrow{m} \eta \text{ then } \bar{\mu} \equiv \bar{\eta},$$

where $\bar{\mu}(m, n)$ is the probability that $\mu$ outputs a pair $(m', s)$ such that $m = m'$ and $f(s) = n$, and $\equiv$ is equality of distributions. Given such an $f$, $s$ is bisimilar to $t$ if $f(s) = f(t)$. A well-chosen $f$ will be such that the constraint $f(s) = f(t)$ will make it easy to prove that $\bar{\mu} \equiv \bar{\eta}$.