Supple: Multiagent Communication Protocols with Causal Types

Akin Günay
Lancaster University
Lancaster, UK
akingunay@gmail.com

Amit K. Chopra
Lancaster University
Lancaster, UK
amit.chopra@lancaster.ac.uk

Munindar P. Singh
North Carolina State University
Raleigh, USA
singh@ncsu.edu

ABSTRACT
A (communication) protocol captures how agents collaborate by specifying the messages they exchange. In particular, since the information content of messages characterizes the interactions a protocol specifies, message types can improve collaboration by strengthening the specification of what each agent may legitimately expect from another agent. In addition, in implementations, typing information can enable improved verification of agents.

We introduce Supple, a protocol specification language that expresses message schemas with typed parameters. Supple enables definition of causal types for parameters that constrain how other parameters are computed in a protocol enactment. We give the formal semantics of Supple; characterize the liveness and safety of Supple specifications; and provide decision procedures for them.

KEYWORDS
Communication protocols; Agent communication

ACM Reference Format:

1 INTRODUCTION
Motivation Our setting is a decentralized multiagent system (MAS) of agents communicating via asynchronous messaging. Each agent is autonomous—acts on behalf of some real-world principal. The agents are heterogeneous—each is independently implemented or configured. Successful collaboration in such a setting requires precise specification of each agent’s expectations of the others, which is naturally accomplished via norms [13, 26, 31].

But how can agents realize their collaboration based on norms despite decentralization? A protocol captures how agents communicate separately from their internal decision making, e.g., in healthcare [17] and finance [19]. Prevalent protocol languages focus on control flow concerns such as message ordering and occurrence, facing an impedance mismatch with message meaning.

In contrast, we posit that to effectively support norms a protocol must precisely characterize the exchange of information pertinent to norms and avoid, which are extraneous to meaning [11, 25, 27]. Information-oriented languages [30, 34] address this challenge but suffer from weak type support. We introduce stronger type support, while retaining the asynchronous enactments.

Problem As our running example, we adopt an insurance auditing scenario. In healthcare, HIPAA (US) and NHS (UK) specify auditing protocols involving several stakeholders. In our scenario, the agents involved are a subscriber $S$, insurer $I$, and auditor $A$. $S$ buys policies from $I$ which it uses to make claims; $A$ requests reports from $I$ for auditing, which list the claims that were paid out but for less than the initial claimed amount.

A protocol language must deal with three collaboration failures. One, liveness failure: the insurer may lack the information needed to compute a report. Two, integrity failure: the report does not contain all and only the correct results. Three, safety failure: agents face a race situation where each attempts to produce authoritative results for the same request.

Our problem is how can a protocol language support statically verifying the absence of the above failures? And, how can we relate the structure of communication in a MAS to the structure of information exchanged between agents.

Approach Our proposed language, Supple, builds on the intuition that communication both produces and is constrained by information. Supple introduces causal types for parameters as first-class language elements that constrain how other parameters are computed in a protocol enactment. A causal type specifies the type of information on which a computation is performed, and the type of information the computation yields. For example, a causal type may specify a computation that can be applied to the claimed and paid amounts of an insurance policy to compute the total payable amount of the policy. The auditor may send a request for a report including a function of the above causal type to express the selection criteria for the claims to be considered in the report and the type of information to be reported for those claims.

Supple yields three main benefits. First, agents may enact the same protocol instantiated with different functions to produce different report types. Second, agents can be verified against those types. Third, protocols can be verified taking parameter types into account. For example, if a protocol enables the auditor to send a function of the above causal type to the insurer, it must enable the insurer to acquire the necessary information to apply the function during the enactment. Otherwise, the protocol is incorrect. Parameter types enable static checking of protocols to prevent such errors even though a function may be formulated at run time.

Literature Existing protocol specification approaches inadequately specify what information may be exchanged through a protocol, leading to ad hoc methods to ensure correctness. Several approaches capture control flow: UML sequence diagrams [6], session types [23], WS-CDL [35], RASA [21], and 2CL [5], but none captures information flow. FIPA [15] adds ontology annotations to messages but doesn’t relate information across messages. Günay et al. [16], assign meanings to messages but don’t specify the underlying
message content precisely. Chopra et al.’s [10] Splee incorporates queries into protocols, e.g., to specify that the winner in an English auction protocol is the highest bidder, but treats them as untyped descriptive annotations outside of Splee’s formalization. Supple shares some motivations with business artifacts and data-centric models [8, 24], which combine information abstractions with process. Montali et al. [22] address verification of commitment-based MAS with queries. However, these works typically do not address decentralization, creating a multiagent system as a single machine.

Baldoni et al. [4] formalize agent types to check compatibility with commitment protocols. Damiani et al. [14] formalize type soundness of MAS in terms of agents and artifacts [7]. Supple focuses on the complementary concern of specifying a protocol independently of agent reasoning to promote loose coupling among agents. In decentralized MAS, a protocol must handle loosely coupled, asynchronous communication whereas the above approaches require a shared memory that indirectly induces tight coupling between the agents.

**Contributions** Supple provides (1) a language for enriched protocol specification; (2) a novel definition of safe and live protocols; and (3) associated verification algorithms. Supple’s novelty lies in introducing type abstractions for information in interaction whereas existing work does not consider information modeling of interactions. Supple’s significance lies in advancing interaction-orientation: by specifying interactions in more detail, we can verify protocols and agents without relying upon internal details. Exposing implementations is anathema to engineering practice in any setting and especially inapplicable in decentralized MAS.

2 BACKGROUND

We introduce information-based protocols by example. BSPL [28] specifies protocols declaratively, constraining message via causality and integrity, and omitting control structures (e.g., sequencing, branching, iteration). Listing 1 shows a BSPL protocol, CreatePolicy, to create an insurance policy between an insurer (I) and a subscriber (S). It declares three public parameters, pID (the protocol’s key), premium, and date. A tuple of bindings for the public parameters implies a complete enactment of the protocol. A protocol’s roles and public parameters represent its interface for purposes of composition. Given a protocol, the bindings of public parameters adorned “in” must be supplied from the enactment of some other protocol; of those adorned “out” must be generated by enacting the protocol; and of those adorned “nil” must neither be supplied nor generated. A message schema is the special case of an atomic protocol. All parameters of CreatePolicy are “out”, meaning that their bindings are generated by enacting CreatePolicy.

**Listing 1: A protocol to create an insurance policy.**

```
CreatePolicy
role I, S
parameter out pID key, out premium, out date
I \rightarrow S: offer\{out pID, out premium\}
I \rightarrow S: reject\{in pID, in premium, out date\}
I \rightarrow S: create\{in pID, in premium, in agreed, out date\}
```

CreatePolicy declares four message schemas. The ordering of message schemas in a protocol listing is irrelevant to their operational ordering in an enactment. The message offer is directed from the insurer to the subscriber to offer a new policy. Its two parameters are adorned “out”, meaning that their bindings must be produced by the insurer when emitting an offer message. In accept, the parameters pID and premium are adorned “in”, meaning that the subscriber must know the bindings of these parameters from prior messages (e.g., offer) to emit accept. Each protocol and message must have a key. The key parameters of a protocol are also key parameters of its messages. Bindings of all parameters are unique for each binding of the key parameters. Note that date is adorned “out” in reject and create. Hence, in any enactment of CreatePolicy, either only reject or only create can be emitted to ensure integrity.

Figure 1 shows two valid enactments of CreatePolicy with bindings of the message parameters. In Figure 1a, the subscriber accepts the insurer’s offer and in Figure 1b, the subscriber rejects the offer.

![Figure 1: Valid enactments of CreatePolicy.](image)

Listing 2 illustrates protocol composition. ReportPolicy references CreatePolicy via its public parameters, and adds two messages. Here, rID identifies report instances, and forms a composite key with pID to associate multiple policies with a report. The auditor’s request for a report is captured as request, where amount indicates the minimum premium amount the insurer should report. BSPL enforces no constraints besides integrity on parameter bindings. Hence, although amount is meant as a criterion to filter the reported policies, ReportPolicy does not capture this intuition: ReportPolicy’s enactments may include a report for any known pID.

**Listing 2: Reporting insurance policies to an auditor.**

```
ReportPolicy
role I, A
parameter out rID key, out pID key, out amount, out info
CreatePolicy\{I, S, out pID key, out premium, out date\}
I \rightarrow A: request\{out rID, out amount\}
I \rightarrow A: report\{in rID, in pID, in amount, in premium, out info\}
```

3 TYPES IN SUPPLE

The failure of Listing 2 to capture the desired constraint on report highlights the need for a protocol language that provides language support for information dependencies more generally than BSPL. Specifically, BSPL supports “out”-“in” causal dependencies. However, it ignores “in”-“out” dependencies that would be needed to correctly link the requested minimum premium amount in request with the information in report. In the section, we introduce
the notion of causal types, which enables specifying "in"→"out" dependencies.

3.1 Atomic and Composite Causal Types

In Supple, each parameter with its adornment constitutes a distinct causal type and may have a binding conforming to its type. For example, in Listing 1, we interpret out pID and in pID, and out premium and in premium as distinct causal types.

Whereas a data type in traditional languages defines how a value may be interpreted by an application (e.g., premium is money in Euros), a type in Supple defines the flow of information in a protocol. We disregard data types since they are well-known (assume they are strings throughout) and reserve the term "type" for causal types.

In Supple, the possible bindings of a type whose adornment is "out" include any possible binding (i.e., any string). For instance, the parameter premium can be bound to any string by the insurer when emitting offer, since the type of the parameter is out premium.

Conversely, the possible bindings of a type for which the adornment is "in", depend on the existing bindings of the types, which share the same parameter component, in all enactments. For instance, the possible bindings of parameter premium in accept depend on the existing bindings of the premium parameters in all messages.

A type is atomic when it consists of a single pair of adornment and parameter components. A type may be a composite of multiple atomic types. Protocols (and messages) have composite types over their parameters' types. For example, offer's type in Listing 1 is the composite type (out pID, out premium) with respect to the types of its parameters (i.e., pID and premium). Note that an atomic type is a special case of a composite type. We omit parentheses where appropriate, as in out premium, reduce clutter.

3.2 Causal Type of a Computation

Our main focus is the notion of the causal type of a computation, which we denote as $T : I \rightarrow O$, where $T$ is a name, and $I$ and $O$ are composite types. $I$ defines the type of information on which the computation is performed and $O$ defines the type of information the computation yields. For instance, a computation whose type is $c : (in pID, in premium) \rightarrow (out c.pID, out c.premium, out c.info)$ is performed on the information, whose type is (in pID, in premium), yielding the information, whose type is (out c.pID, out c.premium, out c.info). Note that in pID and out c.pID (and similarly in premium and out c.premium) are different types.

The causal type of a computation enforces certain constraints on the type of information the computation yields with respect to the type of information on which the computation is applied.

**Constraint 1:** The atomic types that form a composite type $I$ must have "in" as their adornment because $I$ defines the type of information on which the computation is performed. Hence, this type of information must be known to the agent at runtime, which is signified by the "in" adornment.

**Constraint 2:** If there is an atomic type $t$ in $I$ whose parameter component is $p$ (e.g., pID), and there is an atomic type $t'$ in $O$ whose parameter component includes $p$ prefixed with $T$ (e.g., c.pID), then (1) $t'$ must have an "out" adornment, and (2) the bindings of $t'$ that are computed must be a subset of the existing bindings of $t$ when the computation is performed. That is $t'$ is a dependent type on $t$. This "in"→"out" dependency, which is not captured in BSPL, enables us to specify the causal type of computations that perform information filtering, which we explore in Section 3.3.

**Constraint 3:** If there is an atomic type $t'$ in $O$ whose parameter component is $p$ without the prefix $T$ (e.g., info without the prefix $c$), but there is no atomic type $t$ in $I$ whose parameter component is $p$, then $t'$ must have an "out". This kind of a type enables us to specify the production of new information as the result of a computation and may be used to create mappings or aggregations, which we explore in Section 3.3.

These constraints allow only certain adornments of atomic types in $I$ and $O$, which we can infer from the names of the atomic types. Hence, we simplify the notation of causal types as follows. Using Constraint 1, we drop "in" adornments from the atomic types in $I$. Using Constraint 2, we drop "out" adornments and use of $T$ as a prefix of atomic types in $O$. Using Constraint 3 we drop "out" adornments of atomic types in $O$. As a result, in the rest of the paper, instead of $c : (in pID, in premium) \rightarrow (out c.pID, out c.premium, out c.info)$ we write $c : (pID, premium) \rightarrow (pID, premium, info)$.

Listing 3 shows a Supple protocol that uses the causal type $c : (pID, premium) \rightarrow (pID, premium, info)$ for a computation in our scenario. The parameter $c$, whose type is $c : (pID, premium) \rightarrow (pID, premium, info)$ with the adornment "out" is used in the message request to indicate the type of computation that the auditor requests. When emitting request, the auditor can bind the parameter $c$ to any computation conforming to its type. The adornment of $c$ in report is "in", meaning that the insurer must know the computation that is bound to $c$ in order to send an instance of a report.

Supple is indifferent to the meaning of parameter bindings. Hence, the binding of $c$ can be anything (e.g., a query or constraint) that the agents can interpret as a computation. Type conformance verification methods are out of our scope but program analysis techniques or run-time verifiers [29] can possibly support verification.

**Listing 3:** Capturing causal types of computations.

```
ReportPoliciesViaConstraint {}
role I, A
 parameter out rID key, out [c]
type c : (pID, premium) → (pID, premium, info)
CreatePolicy(I, S, out pID key, out premium, out date)
A → I: request [out rID, out c]
I → A: report [in rID, in c, out [c]]
```

Supple introduces [ ] notation to refer to the yielding composite type (i.e., $O$ in $T : I \rightarrow O$) of a computation. For example, in Listing 3, report includes [c], which corresponds to the composite type (out c.pID, out c.premium, out c.info).

3.3 Causal Computation Patterns

We introduce major patterns that occur in a variety of applications.

3.3.1 Filter. Filter selects a subset of a parameter's known bindings according to the criteria defined in a computation. For example, the auditor may request the insurer report exactly the policies that satisfy some premium criteria (e.g., below a specified amount). Listing 4 shows ReportPremium, in which the parameter $c$ is used to define computations to represent such criteria. Listing 5 shows such a computation specified as a (simplified SQL), which can be
assigned to \( c \) by the auditor for requesting only the policies with premiums between 50 and 100.

**Listing 4: Reporting premiums of selected policies.**

```plaintext
ReportPremium {
    role l, A
    parameter out rID key, out [c]
    type c: (pID, premium) → (pID, premium)
}
```

In Filter, the computation yields a dependent type of its input. Let \( K \) and \( P \) be the types of key and non-key parameters, respectively. Filter is represented by the following type definition:

\[
(K, P) \rightarrow (K, P)
\]

**Listing 5: Example query in SQL to filter policies.**

```sql
SELECT CreatePolicy.pID AS pID
CreatePolicy.premium AS premium
WHERE 50 < CreatePolicy.premium < 100
```

3.3.2 **Map.** Map transforms bindings of a tuple of parameters yielding new bindings for another tuple of parameters. For instance, the auditor may request the insurer to report its debt for each claim, which is the difference between the claimed and the paid amounts. Listing 6 defines *ReportClaimDebt* referring to *MakeClaim*, which makes a claim for an existing policy (identified by \( pID \)), and produces bindings of \( cID \) (claim’s key), \( claimed \), and \( paid \) amounts. In *ReportClaimDebt*, the insurer’s debt for each claim (i.e., \( cDebt \)) is computed using \( claimed \) and \( paid \) according to the computation that is bound to \( c \) (i.e., the claimed and paid amounts of each claim in each policy are mapped to the debt for the corresponding claim). Note that the outcome of \( c \) includes \( pID \), which is needed to associate the computed debt for a claim with the corresponding policy.

**Listing 6: Reporting insurer’s debt per claim.**

```plaintext
ReportClaimDebt {
    role l, A
    parameter out rID key, out [c]
    type c: (pID, cID, claimed, paid) → (pID, cID, cDebt)
    CreatePolicy(l, S, out pID key, out premium, out date)
    MakeClaim(S, l, in pID key, out cID key, out claimed, out paid)
    A ← l: request [out rID, out c]
    A ← A: report [in rID, in c, out [c]]
}
```

Let \( K \) be a the type of key parameters, and \( P \) and \( R \) be the types of non-key parameters. Map corresponds to the type:

\[
(K, P) \rightarrow (K, R)
\]

3.3.3 **Reduce.** Reduce yields bindings for a parameter by aggregating another parameter’s bindings. For instance, the auditor may want to know the total debt of an insurer for each policy, a solution to which Listing 7 illustrates. In *ReportPolicyDebt*, the insurer’s debt per policy is computed using the computation bound to \( c \), which assigns the insurer’s debt per policy to \( pDebt \) according to \( cDebt \) referring to *ReportClaimDebt*. Here, the key \( cID \) is not involved in the yielding type of \( c \), since the reduced debt information is associated only with policies (and reports).

**Listing 7: Reporting insurer’s debt per policy.**

```plaintext
ReportPolicyDebt {
    role l, A
    parameter in aiD key, in q, in c, out [c]
    type c: (rID, pID, cID, cDebt) → (rID, pID, pDebt)
    ReportClaimDebt(l, A, out rID key, out pID key, out cID key, out cDebt)
    A ← l: aggregate [in aiD, in c, out [c]]
}
```

Let \( K_1 \) and \( K_2 \) be the types of key parameters, and \( P \) and \( R \) be the types of non-key parameters. Reduce corresponds to:

\[
(K_1, K_2, P) \rightarrow (K_2, R)
\]

### 3.4 A Comprehensive Example

Listing 8 gives a comprehensive example that applies all of the patterns introduced above, illustrating how the results of a computation may be used in another. In the example, the auditor requests from the insurer reports on (1) its policies, using filter via \( c_1 \); (2) its debts for those policies, using map via \( c_2 \); and, (3) its total debt over those debts using reduce via \( c_3 \).

**Listing 8: Chaining computation results.**

```plaintext
Report {
    role l, A
    parameter out rID key, out [c]
    type c1: (pID, premium) → (pID, premium)
    type c2: (pID, claimed, paid) → (pID, debt)
    type c3: (pID, debt) → (totalDebt)
    CreatePolicy(l, S, out pID key, out premium, out date)
    MakeClaim(S, l, in pID key, out claimed, out paid)
    A ← l: reqPolicies [out rID, out c1]
    A ← A: resPolicies [in rID, in c1, out [c1]]
    A ← A: reqDebts [in rID, in [c1], out c2]
    A ← A: resDebts [in rID, in [c2], out [c2]]
    A ← A: reqSum [in rID, in [c2], out c3]
    A ← A: resSum [in rID, in c3, out [c3]]
}
```

### 4 FORMAL MODEL AND VERIFICATION

Supple’s syntax enhances BSPL with causal types that constrain bindings of parameters at runtime. The requisite computations may be specified in any language that the concerned agents can interpret. Computations may be specified at design time to accommodate restricted situations such as in contracts or regulations.

Below, superscripts + and * denote zero or more, and one or more repetitions, respectively. Delimiters [ ] and { } identify optional expressions. Cardinality constraints are left informal for readability.

**Table 1: Supple’s syntax.**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Name [role Role* parameter [Parameter [key] ]]+ [Type:Reference*]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference</td>
<td>Name(Role* Parameter*)</td>
</tr>
<tr>
<td>Role</td>
<td>Role : Name[Parameter*]: [Attachment]</td>
</tr>
<tr>
<td>Type</td>
<td>type Name: (Parameter*): (Parameter*)</td>
</tr>
<tr>
<td>Attachment</td>
<td>(Parameter*): (Parameter*): (ComputationSpec)</td>
</tr>
<tr>
<td>Parameter</td>
<td>Adornment (Name</td>
</tr>
<tr>
<td>Adornment</td>
<td>in</td>
</tr>
</tbody>
</table>

A protocol declaration involves a name, two or more roles, one or more parameters, zero or more type definitions, and one or more protocol and message references. A protocol reference consists of either (1) a name, one or more roles, and one or more parameters.
of the referred protocol or (2) a (message) name, exactly two roles, one or more parameters, and an optional computation attachment. A type definition consists of a parameter name, and two tuples of parameters. A computation attachment consists of two tuples of parameters and a computation specification. A parameter either consists of an adornment and a name or a name enclosed in double brackets. The latter refers to the outcome of a bound computation from which individual parameters can be accessed using the $\cdot$ notation. An adornment is either $\cdot\text{in}$, $\cdot\text{out}$, or $\cdot\text{nil}$.

### 4.1 Semantics

Supple pertains to the specification of causal types. As a result, message instances in Supple must satisfy the type of their schema, meaning that each binding matches the type of the bound parameter. Below, $\sigma$ denotes a finite list, which can be treated in places as a set, and $\sigma\downarrow\rho$ denotes projection of $\sigma$ on to the elements of $\rho$.

**Definition 4.1.** A protocol $P$ is a tuple $(\eta, x, \bar{p}, \bar{k}, \bar{q}, F, T)$, where $n$ is the protocol’s name and $x, \bar{p}, \bar{k} , \bar{q}$ are lists of roles, public parameters, key parameters, and private parameters, respectively, such that $x \subseteq x, \bar{p} \subseteq F$ is a finite set of references, such that $\forall f \in F: f = (\eta_f, x_f, \bar{p}, \bar{k}_f, \bar{q}_f)$ is a public projection of a protocol $P = (\eta, x, \bar{p}, \bar{k}, \bar{q}, F, T)$ satisfying $\eta_f \subseteq x, \bar{p}_f \subseteq \bar{p} \cup \bar{q}$, and $f_T \subseteq \bar{p} \cup \bar{k}$. $T$ is a finite set of causal types, such that $\forall T: t = (p, x, \bar{p}, \bar{q})$ satisfying $p \in \bar{p} \cup \bar{q}, x, \bar{p} \subseteq \bar{p} \cup \bar{q}, \text{and} \bar{w}_T \subseteq \bar{p} \cup \bar{q}$.

$T$ formalizes causal types of the form $T: I \rightarrow O$ that we introduce in Section 3.2. Specifically, in a type $(p, x, \bar{p}, \bar{q}) \in T, \bar{p}, \bar{u}, \bar{w}_T$ correspond to $I, T, \bar{O},$ respectively. For convenience, we treat causal types as shared by all references of a protocol.

**Definition 4.2.** A message schema $\cdot\text{as is atomic protocol} (m, \{s, r, \bar{p}, \bar{q} \}$ with roles $s$ and $r$, and no references.

**Definition 4.3.** A message instance $m[s, r, \bar{p}, \bar{q}]$ associates a message schema $\cdot\text{as a list of values, where } \bar{p} \subseteq \bar{p}$.

**Definition 4.4.** A universe of discourse (UoD) is a pair $(\mathcal{R}, \mathcal{M})$ where $\mathcal{R}$ is a set of roles, and $\mathcal{M}$ is a set of message names, each with its parameters, and sender and receiver roles from $\mathcal{R}$.

**Definition 4.5.** The history of a role $x$, $H^x$, is a sequence of message instances $m_1, m_2, \ldots$, each emitted or received by $x$.

A role’s history captures the local view of the role with respect to the message instances that are sent and received by the role.

**Definition 4.6.** A causal type parameter that is bound to a computation, $x$ knows the bindings of every parameter in $\bar{q}$, before emitting the message with the outcome of the computation that is bound to $p$—which satisfies Constraint 1 in Section 3.2; and (6) ensures that for every parameter $p$ in $\bar{w}$, if there is a parameter $u$ in $\bar{u}$ whose base name is equal to $p$, then the bindings of $p$ must be a subset of the known bindings of $u$—which satisfies Constraint 2 in Section 3.2. In (6) base returns the unqualified name of a parameter (i.e., base($p$) = $p$, and base($p, q$) = $q$). Note that Definition 4.6 satisfies Constraint 3 from Section 3.2 implicitly via (2) and (3), which ensure that $\cdot\text{out}$ adorned parameters are bound preserving integrity.

**Definition 4.6.** A message instance $m[s, r, \bar{p}, \bar{q}]$ with key parameters $\bar{k} \subseteq \bar{p}$ is viable at role $x$’s history $H^x$ iff these hold:

1. $r = x$ (reception) or $s = x$ (emission)
2. $\forall m[s, r, \bar{p}, \bar{q}] \in H^x$ if $\bar{k} \subseteq \bar{p}$ and $\bar{w}_t \downarrow \bar{k} = \bar{w}_t \downarrow \bar{p}$ then $\bar{w}_t \downarrow \bar{p} \subseteq \bar{w}_t \downarrow \bar{q}$ (messages respect keys)
3. $\forall p \in \bar{p}: p \in \bar{p_1}$ iff $(\exists m[s, r, \bar{p}, \bar{q}] \in H^x \& p \in \bar{p}_1 \& \bar{k} \subseteq \bar{p})$
4. $\forall p \in \bar{p}: p \in \bar{p_1}$ iff $p \in \bar{p_1}$ and $\forall \bar{w}_t \in \bar{u}_t, \exists \bar{w}_t \subseteq \bar{w}_t \subseteq \bar{w}_t \cup \bar{u}_t$
5. $\forall p \in \bar{p}: p \in \bar{p_1}$ iff $(\exists p, \bar{u}, \bar{w} \in T \& \forall \bar{w}_t \in \bar{u}_t, \exists \bar{w}_t \subseteq \bar{w}_t \subseteq \bar{w}_t \cup \bar{u}_t)$
6. $\forall p \in \bar{p}: p \in \bar{p_1}$ and $\forall \bar{w}_t \in \bar{u}_t, \exists \bar{w}_t \subseteq \bar{w}_t \subseteq \bar{w}_t \cup \bar{u}_t$

An enactment of a protocol is a vector of its roles’ histories.

**Definition 4.7.** Let $(\mathcal{R}, \mathcal{M})$ be a UoD. A history vector over $(\mathcal{R}, \mathcal{M})$ is $[H^1, \ldots, H^{|R|}]$, such that $\forall s, r: 1 \leq s, r \leq |R| \Rightarrow H^s$ is a history, and $\forall m[s, r, \bar{p}, \bar{q}] \in H^s$.

**Definition 4.8.** A history vector is viable if and only if each of its histories is empty or it arises from the addition of the emission or reception of a viable message by any role to a viable history vector.

**Definition 4.9.** Let $(\mathcal{R}, \mathcal{M})$ be a UoD. The universe of enactments $\mathcal{U}_\mathcal{R}_\mathcal{M}$ for $(\mathcal{R}, \mathcal{M})$ is the set of viable history vectors with exactly $|\mathcal{R}|$ dimensions over the instances of messages in $\mathcal{M}$.

**Definition 4.10.** The extension of a message schema $\eta; r \mapsto m: \bar{p} \subseteq \bar{p}$ for the UoD $(\mathcal{R}, \mathcal{M})$ is $\{s \mapsto r: m \bar{p}(\bar{k})\}_{\mathcal{R}, \mathcal{M}} = \{H^s \in \mathcal{U}_\mathcal{R}_\mathcal{M} \& \exists \bar{w}_t, i: H^s_i = m[s, \bar{p}, \bar{q}] \& \exists \bar{w}_t, i: H^s_i = m[s, \bar{p}, \bar{q}]\}$.

**Definition 4.11.** Let $P = (n, \bar{p}, \bar{q}, F, T)$ be a protocol. The universe of discourse of the protocol $(\mathcal{R}, \mathcal{M})$ is $\mathcal{U}_\mathcal{P}(\mathcal{R}, \mathcal{M}) = (\{s \mapsto r: m \bar{p}(\bar{k})\}_{\mathcal{R}, \mathcal{M}})$, where $\mathcal{U}_\mathcal{P}(\mathcal{R}, \mathcal{M}) = \{s \mapsto r: m \bar{p}(\bar{k})\}_{\mathcal{R}, \mathcal{M}}$.

**4.2 Liveness and Safety**

Liveness and safety are key correctness properties of protocols. A protocol is live if every enactment of the protocol can be completed by producing bindings for all public parameters. A protocol is safe if no key constraint is violated in any enactment.
Definition 4.13. A protocol $P$ is live if and only if each history vector in $UoD(P)$ can be extended by finitely many message emissions and receptions to a history vector in $UoD(P)$ that is complete.

Definition 4.14. A protocol $P$ is safe iff all key constraints apply across all histories in each history vector in $(P')_{UoD(P)}$.

Liveness and safety in Supple go beyond those of BSPL. In Supple, liveness requires, if there is causal type parameter that is bound to a computation, the role who performs the computation, must know the bindings of the parameters on which the computation is performed. For instance, consider LivenessFailure in Listing 9, which is a variant of ReportClaimDebt in Listing 6.


LivenessFailure {  
role I, A, S  
parameter out rID key, out [c2]  
type c1: (pID, cID, claimed, paid)→(pID, cID, cDebt)  
type c2: (pID, cID, complaint)→(pID, cID, cDebt)  
// CreatePolicy and MakeClaim as before  
A → I: auditReportRequest [out rID, out c1]  
I → A: auditReport [in rID, in c1, out [c1]]  
S → A: complaintSubmission [out rID, out complaint]  
A → I: complaintReportRequest [in rID, out c2]  
I → A: complaintReport [in rID, out c2, out [c2]]  
}

LivenessFailure includes an additional causal type $c2$ and new messages complaintSubmission, complaintReportRequest, and complaintReport to capture the scenario where a subscriber makes a complaint about a policy to the auditor, and the auditor requests a report from the insurer about that policy that is subject to the complaint. The type definition of $c2$ requires complaint to be available to the insurer. However, complaint appears only in complaintSubmission, which is sent from the subscriber to the auditor. Thus, the insurer can never send a complaintReport in any enactment where it receives a complaintReportRequest message. Note that some enactments of LivenessFailure can be completed, e.g., enactments where the auditor sends a auditReportRequest, which does not refer to $c2$. This protocol would be live if complaint were included as an $\rho$ in parameter in complaintReportRequest.

Safety of a protocol means that each of its enactments ensures integrity of the information exchanged. Safety may be violated if two or more roles (1) in BSPL, may bind the same parameter; or (2) as added by Supple, concurrently perform the computation that is bound to a causal type parameter. For instance, SafetyFailure in Listing 10, where the auditor requests the total claimed amount for a policy from both insurer and subscriber, is unsafe.

Listing 10: Safety failure.

SafetyFailure {  
role I, A, S  
parameter out rID key, out [c]  
type c: (pID, cID, cClaim)→(pID, pClaim)  
// CreatePolicy and MakeClaim as before  
A → I: reqTotalClaimI [out rID, out c]  
A → S: reqTotalClaimS [in rID, in c]  
I → A: repTotalClaimI [in rID, in c, out [c]]  
S → A: repTotalClaimS [in rID, in c, out [c]]  
}

Both $reqTotalClaimI$ and $reqTotalClaimS$ use the same computation, bound to $c$, to determine the total claims for a policy. However, because of asynchrony, the same information is not available to all parties and applying the same computation may produce different results, thus violating integrity. For example, in Figure 2, which shows a possible enactment omitting the binding of $c$ for readability, the auditor sends $reqTotalClaimI$ and $reqTotalClaims$ to the insurer and subscriber, respectively. The insurer computes the total claim amount for the policy, where $pID$ is equal to $p1$, before receiving the submitClaim message of the subscriber. Hence, the insurer sends $repTotalClaimI$ with $pClaim$ of 0 to the auditor. In the meantime, the subscriber submits a claim for 15 to the insurer and, therefore, responds to the auditor’s request by sending $repTotalClaims$ with $pClaim$ of 15. As a result, the auditor receives inconsistent bindings of $pClaim$, which violates integrity for the binding $p1$ of key $pID$.

4.3 Verification of Supple Protocols

To verify correctness, we derive the following propositional logic expressions from a Supple protocol (1) $C$: its causal structure, indicating how information flows via its messages; (2) $S$: its unsafety, i.e., that two messages that produce bindings for the same parameter both occur; and (3) $L$: its liveness failure, i.e., some parameters remain unbound even tough every agent sends every viable message, and the infrastructure delivers all messages. Safety and liveness hold when $C \land S$ and $C \land L$, respectively, are unsatisfiable.

Algorithm 1 specifies how we create the causal structure of a protocol as a propositional logic expression as a conjunction of subexpression. For readability, we define the subexpressions separately in Definitions 4.15–4.19.

Algorithm 1: Generation of the causal structure of a protocol $P$ as a propositional logic expression.

input : $P = (n, \bar{x}, \bar{p}, \bar{k}, \bar{q}, F, T)$  
output: $C^P$ // expression of $P$’s causal structure  
$C^P$ ← message-reception-exp // Definition 4.15  
$C^P$ ← information-transmission-exp // Definition 4.16  
$C^P$ ← information-reception-exp // Definition 4.17  
$C^P$ ← information-minimality-exp // Definition 4.18  
$C^P$ ← message-ordering-exp // Definition 4.19  
return $C^P$

Given a protocol $P = (n, \bar{x}, \bar{p}, \bar{k}, \bar{q}, F, T)$, Algorithm 1 uses the following sets of propositional symbols. (1) A finite set $P$ of $p_e$ symbols for each parameter $p \in \bar{p}$ and for each role $x \in \bar{x}$, which model observation of $p$ by $x$. (2) A finite set $M$ of $m_e$ symbols for each message $m \in F$ and for each role $x \in \bar{x}$, which model observation of $m$ by $x$. (3) A finite set of $e_i$ symbols for each $(e_i, e_j)$ pair in $F$ union $M$, which model observation of $e_i$ before $e_j$. For
we write $b_{c, r}$ in predicate form as $\text{before}(e_i, e_j)$. (4) A
finite set of $e_i, e_j$ symbols for every $(e_i, e_j)$ pair in $\mathcal{P} \cup \mathcal{M}$, which
model observation of $e_i$ together with $e_j$. For readability, we write
two or more messages, only one of these messages is emitted. Hence, integrity of parameter bindings cannot be
violated. This means that for any pair of messages $m^1$ and $m^2$ in a
protocol and with corresponding $\text{out} \gamma$ adorned parameters $p_{i}^O$ and $p_{j}^O$, respectively where $p_{i}^O \cap p_{j}^O \neq \emptyset$, we must not infer the
clause $m^1_{s} \land m^2_{s}$ from the causal structure of a protocol.

Definition 4.22. Given a protocol’s list of messages $\mathcal{F}$, let $\bar{J}$ be
the list of every message pair $(m^1, m^2)$ for which $p_{i}^O$ and $p_{j}^O$ are
the respective $\text{out} \gamma$ adorned parameters and $p_{i}^O \cap p_{j}^O \neq \emptyset$. The
Unsafety expression of the protocol is:

$$\bigvee_{(m^1, m^2) \in \bar{J}} (m^1_{s} \land m^2_{s})$$

Let $\mathcal{P}$ be a protocol, $\mathcal{C}^\mathcal{P}$ be the causal structure of $\mathcal{P}$, and $\mathcal{S}^\mathcal{P}$ be
the unsafety expression of $\mathcal{P}$ as in Definition 4.22. We decide on
$\mathcal{P}$’s safety by checking the unsatisfiability of $\mathcal{C}^\mathcal{P} \land \mathcal{S}^\mathcal{P}$.

Theorem 4.23. A protocol $\mathcal{P}$ is safe iff $\mathcal{C}^\mathcal{P} \land \mathcal{S}^\mathcal{P}$ is not satisfiable.

### 4.3.1 Correctness of Causal Structure Generation

Let $\mathcal{P}$ be a protocol for which Algorithm 1 generates the causal structure $\mathcal{C}^\mathcal{P}$.

Theorem 4.20. (Correspondence) For every viable history vector of $\mathcal{P}$, there is a model of $\mathcal{C}^\mathcal{P}$, and vice versa.

Proof Sketch. We use induction in the forward direction. An
empty $H$ corresponds to an empty $\mathcal{C}^\mathcal{P}$ without any propositions.
Inductively, for every viable message $m$ that extends $H$, we can
extend $\mathcal{C}^\mathcal{P}$ for $m$’s emission using the above information transmission
clauses, and for $m$’s reception using the reception clause. Conversely, given $\mathcal{C}^\mathcal{P}$, we can construct $H$, simply appending messages instances that correspond to the message emission and reception propositions to the histories of the corresponding roles.

Theorem 4.21. (Termination) Algorithm 1 always terminates.

### 4.3.2 Safety

A protocol’s safety requires that, if any parameter is adorned $\text{out} \gamma$ in two or more messages, only one of these messages is emitted. Hence, integrity of parameter bindings cannot be
violated. This means that for any pair of messages $m^1$ and $m^2$ in a
protocol and with corresponding $\text{out} \gamma$ adorned parameters $p_{i}^O$ and $p_{j}^O$, respectively where $p_{i}^O \cap p_{j}^O \neq \emptyset$, we must not infer the
clause $m^1_{s} \land m^2_{s}$ from the causal structure of a protocol.

For example, considering only premium for brevity, for message
$r \mapsto A: \text{resPolicies[in ID, in c1, out c2]} \gamma$ and $c1$ of type (pID, premium)$\mapsto$(pID, premium), Definition 4.17 yields $\neg \text{resPolicies}_A \vee
\text{before(premium}_A, \text{resPolicies}_A \land \text{with(premium}_A, \text{resPolicies}_A))$:

Definition 4.18. (Information Minimality) For every role $x$ in $\bar{x}$ and
parameter $p$ in $\bar{p}$, $p$ is either not observed or $p$ is observed together with a message $m$ in $\mathcal{F}$ ($\mathcal{F}' \subseteq \mathcal{F}$ comprises messages $r \mapsto r \mapsto m \bar{p}_m(k_m)\gamma \in \mathcal{F}$ where $x = s$ or $x = r$, and $p \in \bar{p}$):

$$\bigwedge_{x \in \bar{x}} \bigwedge_{p \in \bar{p}} (\neg p_x \vee \bigvee_{m \in \mathcal{F}'} (\text{with}(p_x, m_x)))$$

Definition 4.19. (Ordering) For every pair of messages $m^1$ and $m^2$ in $\mathcal{F}$ that are emitted by $x$ in $\bar{x}$, $x$ may observe them in some order, but not together ($\mathcal{F}' \subseteq \mathcal{F}$ comprises messages $r \mapsto r \mapsto m \bar{p}_m(k_m)\gamma \in \mathcal{F}$, where $x = s$ or $x = r$):

$$\bigwedge_{m^1, m^2 \in \mathcal{F}'} (\neg m^1_x \vee \neg m^2_x \vee \text{before}(m^1_x, m^2_x) \vee \text{before}(m^2_x, m^1_x))$$
Proof Sketch. If \( C_P \land S_P \) is satisfiable, by Theorem 4.20, we can construct a history vector that contains two messages that bind the same "out" parameter. Conversely, if \( C_P \land S_P \) is not satisfiable, by Theorem 4.20, we cannot construct a history vector in which more than one message binds the same "out" parameter. \( \square \)

4.3.3 Liveness. A protocol is live if every enactment of the protocol can be completed (i.e., every public parameter is bound). Below, we give a procedure for determining liveness. Definition 4.24 captures that some public parameter is observed by no role in the protocol.

Definition 4.24. (Lack of Public Parameter Observation) Let \( \bar{p} \) be the list of a protocol’s public parameters and \( X_p \) be the set of roles in the protocol who are either sender or receiver of at least one message in the protocol, which includes \( p \) as a parameter.

\[
\exists p \in \bar{p} \forall x \in X_p \left( \neg p_x \right)
\]

However, some parameters may not be observed if an agent chooses to not communicate. For purposes of determining liveness, we therefore assume that if some messages are viable given an agent’s history, the agent sends one such message. Definition 4.25 captures this constraint.

Definition 4.25. (Emission of a Viable Message) Let \( m \) be a message, \( \bar{p}_m \) and \( \bar{p}_m^o \) be the list of "in" and "out" adorned parameters of \( m \), and \( s \) be the sender of \( m \).

\[
\exists p \in \bar{p}_m \left( \forall p_o \in \bar{p}_m^o \left( \neg p_o \right) \lor \neg p \right)
\]

Further, some parameters may not be observed if messages are lost. For purposes of determining liveness, we therefore assume that every emitted message is received. Definition 4.26 captures this constraint.

Definition 4.26. (Nonlossy Communication) Let \( m \) be a message with sender role \( s \) and receiver role \( r \).

\[
\exists m \in F \left( \neg m_s \lor \neg m_r \right)
\]

Let, \( L_P \) be the corresponding expressions in Definitions 4.24, 4.25, and 4.26, respectively, for protocol \( P \). We decide on the liveness of \( P \) by checking the unsatisfiability of \( C_P \land L_P \).

Theorem 4.27. A protocol \( P \) is live if \( C_P \land L_P \) is not satisfiable.

Proof Sketch. If \( C_P \land L_P \) is satisfiable, by Theorem 4.20, we can construct a viable history vector that cannot be extended via message emission (maximality) or reception (lossless transmission), and yet is incomplete. Conversely, if \( P \) is live, we know that each history vector of \( P \) is either complete or can be finitely extended to a complete history vector. Hence, \( C_P \land L_P \) is not satisfiable. \( \square \)

5 Discussion

Supple introduces a new abstraction of types in protocols, on which there is little work, and supporting checking of important properties. As noted in Section 1, these contributions coincide with the growing interest in data-aware specifications. Also, as noted in Section 1, existing work when it applies types does so only for static ontology annotations on fields and doesn’t consider information modeling of interactions, let alone the advanced typing techniques we introduce.

Our overarching contribution lies in elucidating an important aspect of information-based protocols via causal types. Supple extends information-based protocol specification approaches with causal types for constraining the information that is communicated in a protocol. Supple treats causal type parameters as first-class information parameters, which enables the agents (1) to define computations during enactment of a protocol, and (2) to communicate them and their results as they communicate any other information. Supple formalizes causal types and incorporates them into verification of a protocol’s safety and liveness. At the technical level, Supple provides a flexible and formal method to define constraints on the exchanged information in a protocol.

Recent protocol languages, besides BSPL, incorporate information. HAPN [34] complements state machine-based representation of protocols with guards and effects. A major conceptual difference is that HAPN supports system parameters, whose bindings are produced exogenously to the interaction, indicating shared state between agents and incorporation of internal decision-making in the specification of public interactions. In Supple, by contrast, interaction state as captured by parameter bindings is neither global nor includes any agent’s internal state. SPY [23] adds assertions to session types to constrain communicated values. However, neither HAPN nor SPY support causal types as in Supple.

Winikoff and Cranefield [33] study the testability of BDI agent programs and identify challenges in scalability. Supple could facilitate addressing those challenges in a MAS setting in two ways. First, decoupling agents through interactions would reduce the verification problem to verifying each agent separately. Second, the existence of a strong type discipline can reduce the burden on testing by eliminating certain kinds of interaction errors early.

An interesting future direction is to develop the rest of our vision by mapping norms [3, 9, 12] and concomitant computations to Supple to enable grounding norms in communications [2, 20]. Supple gives the example of auctions: the auctioneer’s commitment to seller to declare the highest bidder as winner yields a query attachment (i.e., a computation in Supple) that aggregates over all bids receives to produce a binding for winner. Supple can facilitate realizing secure collaboration [32] by enabling interaction based on norms, for example, to generate information protocols that undergird the implementation of information sharing and privacy policies [1].

Notice that as protocol languages support increasingly sophisticated constraints, they would enable aspects of norms to be regimented [18]. For example, the Spelle query attachment would prevent auctioneers from communicating false winners. Returning to Supple, it would prevent the insurer from sending reports that do not meet the computation specified by the auditor. Norm languages could be potentially be enhanced with annotations to indicate possibilities for regimentation.

Acknowledgments. We thank the anonymous reviewers for their helpful comments. Günay and Chopra were supported by EPSRC grant EP/N027965/1 (Turtles). Singh thanks the US Department of Defense for partial support under the Science of Security Labrad. 788
REFERENCES


