Custard: Computing Norm States over Information Stores

Amit K. Chopra
School of Computing and Communications
Lancaster University
Lancaster, LA1 4WA, UK
a.chopra1@lancaster.ac.uk

Munindar P. Singh
Department of Computer Science
North Carolina State University
Raleigh, NC 27695-8206, USA
mpsingh@ncsu.edu

ABSTRACT

Norms provide a way to model the social architecture of a sociotechnical system (STS) and are thus crucial for understanding how such a system supports secure collaboration between principals, that is, autonomous parties such as humans and organizations. Accordingly, an important challenge is to compute the state of a norm instance at runtime in a sociotechnical system.

Custard addresses this challenge by providing a relational syntax for schemas of important norm types along with their canonical lifecycles and providing a mapping from each schema to queries that compute instances of the schema in different lifecycle stages. In essence, Custard supports a norm-based abstraction layer over underlying information stores such as databases and event logs. Specifically, it supports deadlines; complex events, including those based on aggregation; and norms that reference other norms.

We prove important correctness properties for Custard, including stability (once an event has occurred, it has occurred forever) and safety (a query returns a finite set of tuples). Our compiler generates SQL queries from Custard specifications. Writing out such SQL queries by hand is tedious and error-prone even for simple norms, thus demonstrating Custard’s practical benefits.

1. INTRODUCTION

A sociotechnical system (STS) involves social elements or principals, such as autonomous humans or organizations, and technical elements such as IT resources. We understand an agent as a software entity that acts on behalf of a principal in an STS.

Norms provide a standard of correctness for interactions among the principals, thereby capturing the social architecture of an STS [37]. Specifically, a norm captures how the principals ought to interact: it provides a social-level, yet computational, encoding of an integrity or security (for simplicity, including privacy) requirement regarding their collaboration. An example norm would be that a physician is prohibited by the hospital from disclosing identifying information about a patient. Such a norm helps characterize security at the social level independently of the implementation. Therefore, representing norms is crucial for an agent to determine how to act; and how to evaluate compliance and accountability of others.

We distinguish norm schemas from instances. A norm schema or specification describes a norm in general terms, such as a prohibition against disclosing information about a patient. A norm instance would specify the specific patient whose information has been received. Some instances of a norm may be violated and some satisfied. We consider important norm types from the literature, namely, commitment, authorization, prohibition, and power [4, 22, 26, 36]. Each of these norm types involves a canonical lifecycle [36], discussed in Figure 3, in which a norm instance may be created, expired, detached, discharged, or violated.

Norms as institutional facts are elements of social reality in the sense of Searle [31] and as such are realized through and reflected in brute facts [3], that is, low-level information. In our setting, brute facts are recorded in databases and event logs; often, these events correspond to messages sent and received. However, Searle’s claims about mental representation are inapplicable here [7, 16, 30, 32].

An important challenge in realizing norms, therefore, is how to compute norm instances from brute facts. To this end, we treat (1) norms on par with information schemas and (2) database relations as stores of norm instances in various lifecycle stages. For example, an information store may indicate which instances of a prohibition are expired and which are violated. In general, we would like to specify nested norms—for example, a commitment to inform patients of the violation of a prohibition on disclosing their private information. Figure 1 illustrates our approach in conceptual terms.

Our contributions are as below. First, we propose Custard, a language for specifying information-based norms, including commitments, authorizations, prohibitions, and powers. Custard is event-based: important stages in the lifecycle of a norm instance, specifically, its creation, detachment, expiration, discharge, and violation, are event instances and inferred from event instances recorded in the underlying information store. Custard supports complex event expressions involving logic operators, aggregation operators, relative time intervals within which events should occur, and nested norms. We give the semantics of Custard via queries in the tuple relational calculus (TRC) [15]. Effectively, for every norm specified in Custard, we define a query (expression) for each stage in the norm’s canonical lifecycle, which yields all instances of the norm in that stage. The benefit of using the TRC is that it maps well to underlying representations and paves the way for easy implementation in widely used query languages such as SQL.

Figure 1: Custard realizes norms over information stores. An agent can query a virtual norm store for norm instances; Custard computes and retrieves such instances based on events in the underlying information store.
Second, we formulate and prove two desirable properties for Custard. Stability is monotonicity over time: once an event instance has occurred, it stays occurred forever. For example, a prohibition instance violated at one moment remains violated at all future moments. Ensuring stability requires a correct treatment of time. Safety captures the idea that queries map to finite sets.

Third, because of Custard’s support for specifying the nonoccurrence of an event, aggregation, and expressive time intervals, the TRC queries for a norm turn out to be nontrivial. As Section 4 shows, even a simple Custard specification yields SQL queries that are complex and an order of magnitude longer. Writing such queries by hand would be highly tedious, time-consuming, and error-prone. To demonstrate the practical benefits of Custard, we implemented a compiler that generates SQL queries from Custard specifications.

2. SAMPLING CUSTARD IN PRIVACY

We demonstrate the effectiveness of Custard by modeling a real-world privacy consent scenario being considered by Health Level Seven (HL7) [18], which is a leading standardization body for health information systems. A patient signs up with a cloud-based health vault provider to store and manage access to its private health information (PHI). This information may include records of the patient’s vital signs such as blood pressure and blood sugar, for example, as monitored by wearable devices and uploaded to the vault. The patient may authorize third parties, such as a health coach, to receive the PHI from the vault by indicating consent. A patient may revoke an authorization. The overseeing jurisdictional authority empowers the patient to grant or revoke such authorizations. In general, third parties authorized by the patient to access information are prohibited from forwarding the information they receive to yet other parties. Parties may be sanctioned for violating this prohibition.

Listing 1 shows an information schema for this healthcare setting. It describes a number of event specifications as relations, each annotated with its key and timestamp attributes. No two instances of an event (specification) may have identical bindings for the key; for every instance, the timestamp attribute records the time of occurrence of the instance. The key of one event may occur in another. For example, accID occurs in Allowed. Such foreign keys enable correlation: every Allowed instance can be correlated by a Signedup instance via the binding for accID in the former. In general, correlations may be effected via chaining of foreign keys. For example, a Revoked instance is correlated with an Allowed instance by discID, and, therefore, with Signedup via accID.

Notice that there can be at most one SentCred instance for an Allowed instance as their keys are identical. For every disclosure to a third party, there can be zero or more requests for data from that party to the vault provider (ReqData). For every request, there can be at most one access (Accessed). A third party may forward data that has accessed via a request to other parties zero or more times (Forwarded). Every Forwarded instance is correlated with a Signedup instance via a chain of correlations (forID to reqID to discID to accID).

We exclude methodologies for designing the appropriate information schemas from our present scope and expect such methodologies can build on known data and ontology modeling techniques.

Listing 1: Example schema for the healthcare scenario.

```
\(\begin{align*}
// Patient\ pID\ registers\ in\ jurisdiction\ jID \\
&\text{Registered}(pID, jID, resID, council) \\
&\text{key}\ resID\ time\ t
\end{align*}\)

\(\begin{align*}
// pID\ signs\ up\ with\ health\ vault\ provider\ hID \\
&\text{Signedup}(pID, hID, accID)
\end{align*}\)
```

We build on recent work that understands norm types such as commitment, authorization, prohibition, and power as directed social expectations between agents [36,37]. Figure 2 shows important elements of our conceptual model.

```
Listing 1: Example schema for the healthcare scenario.

key accID time t

// pID allows disclosure to third party tpID
Allowed(pID, hID, discID, accID, tpID, info) key discID time t

// pID revokes disclosure for tpID
Revoked(pID, hID, discID) key discID time t

// hID sends creds to tpID if disclosure allowed
SentCred(hID, tpID, discID, credentials) key discID time t

// tpID requests patient data from hID
ReqData(tpID, hID, reqID, discID, request) key reqID time t

// tpID gets access to the requested data
Accessed(tpID, hID, reqID, response) key reqID time t

// tpID forwards data to party otherID
Forwarded(tpID, otherID, forID, reqID, response) key forID time t

// hID sanctions tpID for mishandling information
Sanction(hID, tpID, discID, details) key discID time t
```

Figure 2: Simplified metamodel for norms (based on [36]).

In Figure 2, each (created) norm instance is a conditional expectation, whose antecedent states the condition under which the force of the norm, given by the consequent, applies. The expector and expectee represent the privileged and liable parties, respectively. Crucially, this formulation yields a basis for accountability in STSs: the expectee is accountable to the expector for the satisfaction of the expectation. Conversely, the expector has standing and may legitimately demand that the expectee give an account of the status of the expectation. As Example 1 illustrates, doing so helps understand accountability independently of implementation.

**EXAMPLE 1.** A commitment from a hospital to encrypt sensitive private health information (PHI) represents the patient’s expectation that the hospital will do just that—and that the patient has a basis for demanding an account from the hospital about whether his or her PHI has been encrypted. A failure to encrypt PHI would be a violation, for which the hospital may be sanctioned.

Viewing norms as expectations leads to interesting questions that have not received adequate attention in the literature. For example, when is an authorization violated? And, who is accountable to whom for the violation? We now discuss possible lifecycles for the norm types, as in Figure 3, and conventions about accountability.
2.1 Commitment

Our notion of commitment corresponds to the standard one in the literature [33]: the debtor commits to the creditor to bring about a condition (the consequent) if some condition (the antecedent) holds. We give an example from the foregoing scenario.

Example 2. When a patient signs up, the health vault provider commits to the patient that if the patient grants access to a third party, the vault provider will authorize that party within a day.

Listing 2 shows a commitment listing in Custard. DisclosureCom is a name for the schema. The commitment is from hID to tpID; it is created upon the occurrence of a Signedup instance; detached upon the occurrence of a correlated Allowed disclosure instance, provided that disclosure has not been revoked (this allows modeling situations where patients may change their minds); it is discharged when a correlated instance of DisclosureAuth (an authorization, see Listing 3) is created. The detach and discharge clauses represent the antecedent and the consequent, respectively. In an expression of the form $E[l, r]$, $[l, r]$ is a time interval; the expression says that $E$ should occur within this interval. To reduce clutter, we often omit $l$ and $r$ when they are 0 and $\infty$, respectively.

Listing 2: Captures Example 2.

<table>
<thead>
<tr>
<th>commitment DisclosureCom hID to tpID</th>
</tr>
</thead>
<tbody>
<tr>
<td>detach Allowed except Revoked</td>
</tr>
<tr>
<td>discharge created DisclosureAuth[0, Allowed+1]</td>
</tr>
</tbody>
</table>

Figure 3a shows the lifecycle of a created commitment instance. The instance is violated if the antecedent occurs but the consequent cannot; it expires if the antecedent cannot occur; and it is discharged if the consequent occurs. For simplicity, a commitment instance may be both expired and discharged: when its antecedent can no longer occur (as after a time out) but the consequent occurs.

2.2 Authorization

An agent authorizes another to bring about its consequent provided its antecedent holds.

Example 3. The health vault provider authorizes a party by sending it credentials assuring it that patient data will be available for access any time between one and ten days after its request.

Listing 3: An authorization in Custard.

<table>
<thead>
<tr>
<th>authorization DisclosureAuth tpID by hID</th>
</tr>
</thead>
<tbody>
<tr>
<td>create SentCred</td>
</tr>
<tr>
<td>detach ReqData</td>
</tr>
<tr>
<td>discharge Accessed [ReqData+1, ReqData+10]</td>
</tr>
</tbody>
</table>

In authorizations, we treat the authorizing party as the expectee and the authorized party as the expector. Thus, in Listing 3, the expector is tpID and the expectee is the vault. Specifically, tpID expects access to patient information if it has been authorized to obtain it. This agrees with the intuition that an authorization is the authorized party’s privilege, not a liability. The authorization instance would be violated if the patient had authorized disclosure to a specific party, but the vault provider blocks that party from accessing the patient’s information.

Although, in principle, an authorization may be violated as above, we make an architectural assumption and adopt a convention that the violation of an authorization is impossible [36]. Specifically, we assume that authorizations are regimented [20] by the agent, for example, via authentication and access control mechanisms. That is, access to a patient’s record is controlled via a mechanism that allows access by all who are authorized. Figure 3b captures the authorization lifecycle. It makes the violated event unreachable to capture the doctrine that authorizations cannot be violated.

2.3 Prohibition

An agent prohibits another from bringing about the consequent if its antecedent has occurred. In contrast with authorizations, we apply prohibitions to cases where events are either not easily regimented or not desired to be regimented. For example, it is in general impossible to regiment a system to make disclosure of confidential information impossible. We capture the undesirability of such behaviors by placing prohibitions on them. Example 4 demonstrates a prohibition followed by its formal encoding in Listing 4.

Example 4. The health vault provider prohibits any party who accesses patient information from forwarding that information to other parties.

Listing 4: A prohibition in Custard.

<table>
<thead>
<tr>
<th>prohibition DisclosureProh tpID by hID</th>
</tr>
</thead>
<tbody>
<tr>
<td>create discharged DisclosureAuth</td>
</tr>
<tr>
<td>violate Forwarded</td>
</tr>
</tbody>
</table>

Figure 3c captures the prohibition lifecycle. A prohibition is violated if the antecedent and the consequent have both occurred. In a prohibition, the expectee and expector are the prohibited and prohibiting parties, respectively.

2.4 Power

An agent empowers another to bring about certain states of affairs by simply “saying so” provided some conditions hold [5, 19]. We adopt Jones and Sergot’s distinction between power and authorization [20]. In our setting, power is the ability of an agent to modify norms among other agents whereas authorization is the ability to access resources [36]. In addition, as discussed above, we treat authorizations as regimented via technical mechanisms.
**Example 5.** The jurisdictional authority empowers the patient to authorize any party to receive the patient’s information from the vault provider by simply filling out the appropriate form.

Listing 5 captures Example 5. It says that a patient who is registered in a jurisdiction and who has signed up with a vault provider after becoming a resident has the power to authorize disclosure to other parties—and to revoke such authorizations.

Listing 5: A power in Custard.

```plaintext
creator ConsentPower pID by jID
detach Signedup[Registered]
discharge Allowed[Registered] and Revoke[Registered]
```

In a power instance, the empowered agent is the privileged party, that is, the expector. The empowering agent is the liable party, that is, the seeactor. For simplicity, we adopt the view that a power cannot be violated for the simple reason that “saying so” under the right conditions is enough to fully exercise the power. The effects of a power may be realized through other norms. In Example 5, the effect of the power is realized through the vault provider becoming committed to authorizing parties who are allowed by the patient to receive information. Of course, the vault provider may refuse to comply, thus violating the above-mentioned commitment. If the antecedent would never hold, then the power expires. Figure 3d captures the lifecycle of a power.

**2.5 Aggregation**

Norms can naturally involve aggregation, as Example 6 illustrates. Such norms capture key performance indicators in business settings as well as levels of interaction by various agents.

**Example 6.** The vault provider commits to the patient to declare a third party as “out of compliance” if in the year following the patient authorizing the party to receive information, it violates the prohibition to forward information to others more than twice.

Listing 6 captures Example 6. The aggregation syntax is based on the standard one in databases: specify the attribute to aggregate over (forID), the expression in which the attribute appears (violated DisclosureProh), how to group the tuples of the expression (by discID), and the attribute that holds the aggregated value (numViol).

The aggregate event occurs when the count of forID over the specified interval is greater than two.

Listing 6: A norm involving aggregation in Custard.

```plaintext
commitment SanctionCom hID to pID
detach count forID of violated DisclosureProh as numViol group by discID > 2
| Signedup, Signedup+365 |
discharge Sanction detached SanctionCom+10 where details = "Out of compliance"
```

**3. TECHNICAL FRAMEWORK**

Let $D = \{D_1, \ldots, D_n\}$ be a set of domains where $\mathcal{T} \in D$ is the domain of time instants; in particular, $\mathcal{T} = \mathbb{N} \cup \{\infty\}$, where $\mathbb{N}$ is the set of natural numbers and $\infty$ is an infinitely distant time instant. Below, A and R are the sets of agent names and the real numbers, respectively. Table 1 defines the syntax of Custard.

Expres yields complex events. The foregoing Custard listings use a surface syntax in which we (1) write and, or, and except for $\cap$, $\cup$, and $\ominus$ respectively; (2) omit lower and upper instants in time intervals when they are, respectively, 0 and $\infty$; (3) omit the detach clause for unconditional norms; and (4) label norms to simplify writing nested commitments. For instance, Listing 2 equals the following Spec expression: commitment(hID, pID, SignedUp[0,∞], Allowed[0,∞], Revoked[0,∞], created authorization([tpID, hID, SentCred[0,∞], ReqData[0,∞], Accessed[ReqData+1, ReqData+10]])[0,Allowed+1]).

**3.1 Semantics**

As Definition 1 describes, an information schema is a nonempty set of event schemas, each modeled as a relation with a key and a distinguished timestamp column. Informally, these correspond to Base events in our syntax (Table 1). The relation for each event schema records (positive) events. That is, no event that has occurred ever goes away.

Below, we assume that the timestamp does not feature in a key since it has no semantic force as such. $\mathcal{N}$ is a set of event names.

**Definition 1.** For convenience, we identify a domain with its set of possible values. (Treating each attribute as unique with its own domain simplifies the notation without loss of generality.)

An information schema $I$ over $D$ is a partial mapping from event names to attributes and keys; it includes precisely the events of interest. That is, $I : \mathcal{N} \rightarrow D \times \mathcal{N}$. Specifically, $I(E) = (A, K)$, where $A \subseteq D$, $\mathcal{T} \in A \setminus K$, and $K \subseteq A$. For brevity, we write $E = (A, K)$ below.

Definition 2 gives the intension, the set of possible extensions, of an event schema with respect to a universe. A universe captures the possible combinations of attribute values under consideration.

**Definition 2.** Let $E = (\{A_1, \ldots, A_m\}, K)$. The universe over $E$, $U_E = A_1 \times \ldots \times A_m$.

The intension of $E$ is the powerset of $U_E$ restricted to sets that satisfy the key constraint of the event schema. That is, any two $E$ instances that agree on the key attributes must agree on every attribute (that is, they are the same instance). That is, $[E] = \{Y | |Y| \subseteq U_E \text{ and } (\forall u_i, u_j \in Y : u_i[K] = u_j[K], then u_i = u_j)\}$, where $|$ indicates projection to the specified set of attributes.

An extension of $E$ is any member of its intension.

Let $I_E$ be the set of event schemas defined in an information schema $I$. Definition 3 states that a model of an information schema determines an extension for each of its event schemas.

**Definition 3.** A model $M$ of an information schema $I$, maps each of $I$’s event schemas to its extension. Let $E = (A, K) \in I_E$. Then the extension of $E$ in $M$ is any member of $E$’s intension: that is, $[E]^M \in [E]$. (We omit $M$ when it is understood.)
The model defines \([E_v]\) for Base event \(E_v\). The semantic postulates below lift \([\_]\) to all expressions in Custard via the TRC. In the TRC, quantification is over tuples; for a tuple \(\tau, \tau.a\) gives the value of attribute \(a\) of \(\tau\). Below, \(t\) is the distinguished timestamp attribute of all event schemas; \(\{c, d\} \subseteq T\); \(F, \ldots\) are expressions of type Event; \(X, Y, \ldots\) are expressions of type Expr; \(l\) and \(r\) are Time expressions; \(\oplus\) is either \(\ast\) or \(\ominus\); \(\odot\) is any Comp operator; \(N\) is a Norm expression; \(g\) is a GSpec expression.

We use the following auxiliary definitions. The function \(att\) produces the nontimestamp attributes of an event schema; and \(cmmn\) the common nontimestamp attributes of two event schemas. The predicate \(eq\) takes two tuples and a set of attributes and returns true if and only if the tuples are equal for each of those attributes; \(nul\) takes a tuple and a set of attributes and returns true if and only if each attribute’s value is null in that tuple; and \(holds\) takes a constraint and a tuple and returns true iff the tuple satisfies the constraint.

The function \(sumf\) works like the conventional sum operator in database theory: it takes four inputs, a relation \(S\), an attribute \(col\) (in \(S\)) which needs to be summed, a set of columns \(g\) to group \(S\) by, and an attribute colsum whose value will be the sum and produces a set of tuples with the attributes \(g\) and colsum. That is, it produces a relation whose attributes are \(g\) and \(colsum\) whose values are what it computes. We would need analogous functions \(maxf\), \(minf\), \(countf\), and \(avgf\) for tackling the corresponding constructs in Custard. The functions \(maxf\) and \(mint\) compute max and min of timestamps.

\[D_1. \quad [E[c, d]](\tau) = \{\tau | \tau \in [E[c, d]] \land c \leq \tau.t < d\}.\]

All events in \(E\) that occur after \((\subseteq c)\) before \(d\).

\[D_2. \quad [E[F \oplus c, d]](\tau) = \{\tau | \exists (\exists r' \in [E] \land r' \in [F] \land \text{eq}(\tau, r', F) \land \text{cmmn}(E, F) \land \tau.t \land c \leq \tau.t < d\}.\]

Select \(E\) if \(F\) occurs and \(E\) occurs after \((\text{before})\), depending upon what \(\odot\) is \(c\) moments of \(F\)’s occurrence before \(d\).

\[D_3. \quad [E[c, F \oplus d]](\tau) = \{\tau | \exists r' \in [E] \land r' \in [F] \land \text{eq}(\tau, r', \text{cmmn}(E, F)) \land \tau.t \land c \leq \tau.t < d\}.\]

Select \(E\) if \(F\) occurs and \(E\) occurs after \((\text{before})\) before \(d\) moments have passed since \(F\)’s occurrence (or at least \(d\) moments before \(F\)’s occurrence, depending upon what \(\odot\) is).

\[D_4. \quad [E[F \oplus c, G \oplus d]](\tau) = \{\tau | \exists r' \in [E[F \oplus c, \infty]] \land \tau \in [E[G \oplus d]]\}.\]

Combines \(D_2\) and \(D_3\).

We give definitions for aggregate events involving sum. We skip the analogous definitions for the other Func expressions (min, max, count, avg) for brevity.

\[D_5. \quad \text{[sum col of } E \text{ as colsum group by } g \text{]} = \{\tau | \exists r' \in \text{sumf}([E[l, d], \text{col}, \text{colsum}, g] \land \tau.colsum \lor n \land \text{eq}(\tau, r', g \lor \{\text{colsum}\}) \land \tau.t = d).\]

Compute all \(E\) instances between \(l\) and \(d\) and sum them up grouped by \(g\) over column \(col\). If the sum for some \(g\) is \(\triangleright\), then the event has occurred with a timestamp of \(d\).

\[D_6. \quad \text{[sum col of } E \text{ as colsum group by } g \text{]} = \{\tau | \exists r' \in \text{sumf}([E[l, d], \text{col}, \text{colsum}, g] \land \tau.colsum \lor n \land \text{eq}(\tau, r', g \lor \{\text{colsum}\}) \land \exists (\exists r' \in [F] \land \text{eq}(\tau, r', F) \land \text{att}(F)) \land \tau.t = \tau'.t \land d).\]

Analogous to \(D_5\) except that \(D_5\) has a different timestamp of\(E\) event.

\[D_7. \quad (X \times Y) = \{\tau | \exists r' \in [X] \land \exists r'' \in [Y] \land \text{eq}(\tau, r', att(X)) \land \text{eq}(\tau, r'', att(Y)) \land \tau.t = \text{max}(\tau'.t, \tau''.t]\}.\]

Select \((X, Y)\) pairs where both have occurred; the timestamp of this composite event is the greater of the two.

\[D_8. \quad [X \sqcup Y] = \{\tau | \exists r' \in [X] \land \exists r'' \in [Y] \land \text{eq}(\tau, r', att(X)) \land \text{eq}(\tau, r'', att(Y)) \land \tau.t = \text{min}(\tau'.t, \tau''.t)]\}

Select \((X, Y)\) pairs where both have occurred; the timestamp of this composite event is the smaller of the two, if both have occurred, or equal to the timestamp of the one that has occurred.

The interpretation of \(X \odot Y\) is that \(X\) should have occurred but the (corresponding) \(Y\) should not have occurred. But what is the time of nonoccurrence of an event? Consider \(X \odot E[l, d]\). Here, \(E[l, d]\) (corresponding to \(X\)) has not occurred if \(E\) (corresponding to \(X\)) has not occurred between \(l\) and \(d\). Thus if \(E\) occurs before \(l\), say at \(b\), then the time of the nonoccurrence of \(E[l, d]\) is \(b\); if \(E\) does not occur before \(d\), then the time of nonoccurrence of \(E[l, d]\) is \(d\), which could be \(\infty\). The time of occurrence of the \(X \odot E[l, d]\) is the maximum of the timestamps of \(X\) and \(E[l, d]\).

\[D_9. \quad [X \times E[l, d]] = \{\tau | \exists r' \in [X] \land \text{eq}(\tau, r', att(X)) \land \tau.t = \text{max}(\tau'.t, \tau'.t)\}\}

The definition of \(X \times E[c, F \oplus d]\) follows along the same lines except to account for the difference that the right timepoint refers to an event \(F\) instead of being a constant. As before, we want \(X\) if \(E\) occurs too soon (before \(c\)). In addition, we want \(X\) if \(E\) occurs too late, in this case, after \(f \oplus d\), where \(f\) is the value of \(F\)’s timestamp. We will give this nonoccurrence of \(E\) the timestamp \(f \oplus d\). But what if \(E\) itself has not occurred? Then, we would not have a value for \(F\). But in this case, we would not want \(X\) anyway because without the occurrence of \(F\), it is not possible to determine the appropriateness of the occurrence of \(E\).

\[D_{10}. \quad [X \odot Y \sqcup Z] = \{\tau | \exists r' \in [X] \land \exists r'' \in [F] \land \text{eq}(\tau, r', att(X)) \land \text{eq}(\tau', r'', \text{cmmn}(E, F)) \land \tau.t = \text{max}(\tau'.t, \tau''.t)\}\}

The definition of \(X \times Y \sqcup Z\) is \([X \times Y] \sqcup (X \odot Z)\).

\[D_{11}. \quad [X \times (Y \times Z)] = \{\tau | \exists r' \in [X] \land \exists r'' \in [Y] \land \exists r''' \in [Z] \land \text{eq}(\tau, r', att(X)) \land \text{eq}(\tau', r'', att(Y)) \land \text{eq}(\tau'', r'', att(Z))\}\}

Below, we write \(N(c, r, u)\) where the definition applies uniformly to all kinds of norms. For brevity, we omit the expectee and expecter agents.
D16. \[ \text{[created } N(c, r, u) \text{]} = [c]. \] An norm instance is created when its create event occurs.

D17. \[ \text{[detached } N(c, r, u) \text{]} = [c \land r]. \] A norm instance is detached when its create and detach events both occur.

D18. \[ \text{[expired } N(c, r, u) \text{]} = [c \lor r]. \] A norm instance is expired when its create event has occurred but its detach fails to occur within the specified interval.

D19. \[ \text{[discharged commitment(c, r, u)]} = [(c \land u) \cup (r \land u)]. \] A commitment is discharged when its discharge event has occurred along with either its create or detach event.

D20. \[ \text{[discharged authorization(c, r, u)]} = [c \land r \land u]. \] An authorization is discharged when its discharge event has occurred along with its create and detach event.

D21. \[ \text{[discharged power(c, r, u)]} = [c \land r \land u]. \] A power is discharged when its discharge event has occurred along with its create and detach event.

D22. \[ \text{[discharged prohibition(c, r, u)]} = [(c \land r) \lor u]. \] A prohibition is discharged when its create and detach events occur but the violate event fails to occur.

D23. \[ \text{[violated commitment(c, r, u)]} = [(c \land r) \lor u]. \] A commitment is violated when its create and detach events occur but the discharge event fails to occur.

D24. \[ \text{[violated authorization(c, r, u)]} = \emptyset \] (the empty set). No authorization can be violated.

D25. \[ \text{[violated power(c, r, u)]} = 0. \] No power can be violated.

D26. \[ \text{[violated prohibition(c, r, u)]} = [c \land r \land u]. \] A prohibition is violated when its create, detach, and violate events all occur.

3.2 Properties

Stability is the idea that once an event is determined to have occurred, then at all future time instants, it should continue to be determined to have occurred. In other words, an event that has occurred cannot later unoccur. For example, a message that been sent cannot later be undeleted. In essence, we would have switched the status of the event from occurred to not occurred.

Second, let us consider aggregation operators. A sum event determined to have occurred at an instant may at future instants be determined to have not occurred as additional events occur. For example, if the sum over a number of events was required to be greater than some value, it may hit that value after observing, say, five events. However, future events may lower the sum (if the attribute which is being summed can take negative values) and cause it to dip below the required value.

We have built the semantics so that stability is guaranteed for all events and the above-described scenarios do not occur. We can treat all observations up to a time as forming a model. Thus as a computation progresses and additional events occur, a model corresponding to additional observations would extend a prior model.

**DEFINITION 4.** Let L and M be two models for information schema I. Then M expands on L if and only if for each event in \( L \), \( [E]^L \subseteq [E]^M \).

Theorem 1 states that the result obtained by evaluating an expression would persist through expansions of models, thereby ensuring stability of Custard.

**THEOREM 1.** Let L and M be models where M expands on L. Let X be any Expr expression. Then, \( [X]^L \subseteq [X]^M \).

**Proof Sketch.** The proof is by induction on the syntax. Specifically, an expression X maps to a tree of height h where the leaf nodes are Base events and the root is the expression itself.

The expressions at the leaves represent the base case for the induction. The model defines \( [Ev] \) if Ev is a Base event. We obtain \( [Ev]^L \subseteq [Ev]^M \) immediately from our assumption regarding Base events. Consider an expression at height k \((0 < k < h)\) and assume that the property holds for its children. The expression must correspond to one of the postulates in D11-D26. We must show that the stability property holds for them.

D11. From the inductive hypothesis, we know that \( [E]^L \subseteq [E]^M \). It follows from D11 that \( [E[c, d]^L \subseteq [E[c, d]^M \). Reasoning for D22-D23 is analogous.

D28. If \( \tau \in \text{[sum col of } E \text{ as colsum group by } \gamma \text{ by } \gamma_{[l, d]}^L] \), then from the fact that \( \tau.t = d \), we know all relevant E instances, that is, those that happen in \( [E[l, d]^L \) have been considered. Further, \( [E[l, d]^L = [E[l, d]^M \). Therefore, stability holds. D28 is analogous.

D29. Follows from \( [X]^L \subseteq [X]^M \) and \( [Y]^L \subseteq [Y]^M \). D29 is analogous.

D30. Two subcases. One, \( \tau \in \text{[X \lor E[l, d] \lor] \) and \( \tau \) occurs at some time \( k \) but \( E \) does not occur in \([0, d] \). In this case, stability of the sum event follows from the fact that \([E[l, d]]^L = [E[l, d]]^M \). Two, \( \tau \in \text{[X \lor E[l, d] \lor] \) because \( X \) and \( E[0, l] \) have both occurred. In this case, stability of the sum event follows from the fact that \([E[l, d]]^L = [E[l, d]]^M \) and \( [X]^L \subseteq [X]^M \). D30 is analogous.

D31. Follows from the fact that \([X]^L \) is stable.

D32-D35. An expression of these forms reduces to an expression where the right hand side of every \( \lor \) operand is a base event, lifecycle event, or aggregation event qualified by a time interval. Such expressions are stable. Their combinations with other expressions is also stable.

D36. Follows from the fact that \([c]^L \) is stable. D37-D40 are analogous.

Safety is a well-known correctness criterion for database queries [15]. Definition 6 describes safety as the idea that the result of any query evaluated over a finite database is finite. Here, a query is an expression that we evaluate using a database.
**Definition 5.** Let $M$ be a model over information schema $I$. Then $M$ is a finite model if and only if for each event $E$ occurring in $I_E$, $[E]^M$, is finite.

**Definition 6.** Let $Q$ be an Expr expression. Then, $Q$ is safe if and only if given any finite model $M$ of $I$, the extension of $Q$ relative to $M$, $[Q]^M$, is finite.

Negation-like operators such as $\ominus$ have the potential to compromise safety if their usage is not restricted adequately. For example, imagine that we had a unary negation operator $\ominus u$, and the create clause for some commitment were simply $\ominus uE$ (assume $E$ is Base). This would amount to considering created infinitely many commitment instances, one for each $E$ instance that is not present in $[E]$. A technique that is commonly employed to avoid such conclusions is to guard such negation-like operators, as we do in Custard: $\ominus$ is a binary operator, the extension of whose left operand circumscribes the extension of its right operand. Theorem 2 and its proof sketch below capture the foregoing discussion.

**Theorem 2.** Let $Q$ be any Expr expression in Custard. Then $Q$ is safe.

**Proof sketch.** The proof is by induction on the height of the syntax tree. The expressions at the leaves represent the base case. We know that they have finite extensions because a finite model defines finite extensions for Base events. Assume finiteness for every expression at height $k$ and show finiteness for every expression at height $k + 1$. For brevity, we illustrate only the crucial cases, which involve $\ominus$, as motivated above. Suppose an expression at $k + 1$ is $X \ominus E[l, d]$. By the inductive hypothesis, we know that both $X$ and $E[l, d]$ have finite extensions. According to the definition of $[X \ominus E[l, d]] (D_\alpha)$, there are two subcases to consider, corresponding to the disjunction. In both cases, though, we are selecting tuples from finite extensions of $X$ and $E$ (specifically, from $E[0, d]$ and $E[0, l]$). Hence, $[X \ominus E[l, d]]$ is finite. The other cases involving $\ominus$ are analogous.

### 4. Implementation

We implemented a Custard compiler in Java using the Eclipse XText language definition and parsing library (version 2.8.3). The compiler reads in one or norm schemas along with an information schema, such as the one in Listing 1, and outputs (1) SQL table creation statements corresponding to the information schema and (2) SQL queries, one for each lifecycle event for each specified norm schema. We adopt the widely used MySQL dialect of SQL. Listing 7 shows some of the table creation statements generated for the information schema in Listing 1.

**Listing 7:** Generated SQL Create Table statements.

```
CREATE TABLE SentCred (  
  hID VARCHAR(10), tpID VARCHAR(10), discID VARCHAR(10), credentials VARCHAR(10),  
  t DATETIME,  
  PRIMARY KEY(discID)  
 );

CREATE TABLE ReqData (  
  hID VARCHAR(10), tpID VARCHAR(10), discID VARCHAR(10), reqID VARCHAR(10), request VARCHAR(10),  
  t DATETIME,  
  PRIMARY KEY(reqID)  
 );

CREATE TABLE Accessed (  
  hID VARCHAR(10), tpID VARCHAR(10), reqID VARCHAR(10), request VARCHAR(10),  
  t DATETIME,  
  PRIMARY KEY(reqID)  
 );
```

For the authorization specification in Listing 3, the compiler generates four SQL queries corresponding to the created, expired, detached, and discharged instances (recall that in our model, authorizations cannot be violated). Listing 8 shows the SQL query that returns the created instances of the authorization at time NOW (the current time). That is, it shows $\lfloor$created DisclosureAuth$\rfloor$NOW—rendered into SQL. Although, in the current implementation all queries are automatically evaluated for NOW, we are working on an extension where the user could input a time value. This would allow the user to run retrospective queries such as How many instances of this authorization were created two months ago? and hypothetical queries such as Given the current state of the database, augmented with some hypothetical events, how many instances of DisclosureCom commitments will be violated?

**Listing 8:** Generated SQL for created instances of DisclosureAuth.

```
SELECT hID, tpID, discID, credentials, reqID, request, t  
FROM (SELECT hID, tpID, discID, credentials, t  
  FROM SentCred) AS Query0  
WHERE t < NOW();
```

Listing 8 contains a nested SQL query. The query is simple and could be easily rewritten without nesting. Listing 9, which shows the SQL query for the discharged instances of the authorization, is far more complex, and contains several levels of unavoidable nesting. Such a query would be practically impossible to write by hand—which demonstrates the significant practical benefits of Custard.

**Listing 9:** Generated SQL for the discharged instances. The SQL DATETIME values ‘1000-01-01 00:00:00’ and ‘9999-12-31 23:59:59’ correspond to the 0th and the infinitely distant time instants, respectively, in our implementation. The unit of time is day.

```
SELECT hID, tpID, discID, credentials, reqID, request, t  
FROM (SELECT hID, tpID, reqID, request, t AS t3  
  FROM (SELECT hID, tpID, reqID, request, discID, request  
    AS request,  
    GREATEST(Query22.t, Query34.t5) AS t  
    FROM Accessed AS Query22  
  ) AS Query23  
  NATURAL JOIN (SELECT hID, tpID, reqID, request, t AS t5  
    FROM (SELECT hID, tpID, reqID, request, discID, request  
      AS request,  
      GREATEST(Query24.t, Query36.t7) AS t  
      FROM Accessed AS Query24  
    ) AS Query25  
  ) AS Query26  
) AS Query27  
WHERE t < NOW();
```
WHERE for example, reasoning about operations on norms, richer content, 39,40,43]. These representations often emphasize different aspects, representations of commitments and, more generally, norms [4, 25, model expansions) is novel to Custard. The formulation and proof of stability (over them in terms of the TRC, which yields cleaner and more direct set-
aggregation schemas and evaluating norm instances over information

WHERE they in information-based language for commitments. Whereas Custard in terms of the TRC, which yields cleaner and more direct set-
aggregation. Custard's novelty lies not only in that it raises norm speci-
fications to the level of information schemas but also in how it de-
vantages to address particular needs of real-life problems, such as
enhancements to address particular needs of real-life problems, such as

WHERE Custard represents an initial effort to represent norms in an information-oriented framework. It opens up many interesting directions of work. These include improvements to Custard to accommodate valuable ideas from the literature as well as enhancements to address particular needs of real-life problems, such as in healthcare or business.

The following are some particularly important and interesting di-
rections for future research. One, formalizing norms in higher-level database logics, such as 4QL, which are beginning to be applied in settings of collaborative agents [14] as well as defeasible reasoning. Two, extending Custard to enable capturing settings where there is uncertainty associated with the occurrence of events [38] and therefore the states of the norm instances. Three, developing an enhanced agent-oriented API to support runtime monitoring of norms and their incorporation in the agent deliberation cycle. Four, creating a catalog of norm patterns that arise in real-life settings and attempting to encode them in Custard. This exercise would point to directions in which Custard would need to be extended. Five, developing a tool-supported methodology for writing Custard specifications, including well-formedness criteria for specifications, for example, relating to the specification of time intervals and keys. Six, relating Custard specifications to alignment for ensuring that multiple Custard stores remain adequately synchronized.

Acknowledgments

We thank the anonymous reviewers for their helpful comments on a previous version of this paper. Munindar Singh thanks the US Department of Defense for partial support under the Science of Security Tablet.
REFERENCES


