Mode$\lambda$ Checking DEL for Guessing Games and Cryptography

Malvin Gattinger

ILLC, Amsterdam

October 3rd 2014

LiRA-Workshop
“The Logical Dynamics of Information, Agency and Interaction”
Outline

1. Guessing Games
   - Register Models
   - Syntax and Semantics
   - Axiomatization

2. Cryptography
   - Communication
   - Computation
   - Example: Diffie-Hellman

3. Model Checking
   - Live Demo
   - Monte Carlo Method

4. Conclusion
Guessing Games
What does it mean to know a number?

JAN: “I have a number in mind, in the range from one to ten. You may take turns guessing. Whoever guesses the number first wins.”

GAIA: “But how can we know you are not cheating?”

ROSA: “Please write down the number before we start guessing, so you can show it afterwards as a proof.”

JAN: “Okay.”

[Jan writes 6 on a piece of paper, hidden from Gaia and Rosa.]
What does it mean to know a number?
What does it mean to know a number?

Agents: Jan, Gaia, Rosa

\[
0
\]
\[
1 \leq p \leq 10 \text{ and } p \not\in \{6\}
\]

\[
1
\]
\[
p = 6
\]

Jan
Gaia
Rosa
Models

**Definition** (Guessing Game Models)
\[ \mathcal{M} = (W, R, V) \] where

- \((W, R)\) is a multi-agent S5 frame,
- \(V : w \mapsto (P_w, f_w, C^+_w, C^-_w)\) is a valuation:
  - \(P_w \subseteq P\) are the basic propositions true at \(w\),
  - \(f_w\) is a function that assigns to some propositions \(q \in Q\) triples \((n, m, X)\), meaning that the value of \(q\) is between \(n\) and \(m\) but not in \(X\). We also demand that
    - (i) whenever \(q \in P_w\) then \(n = m\) and \(X = \emptyset\)
    - (ii) whenever \(q \in P_v \cap P_w\) for \(v, w \in W\) then \(f_v(q) = f_w(q)\)
  - \(C^+_w, C^-_w \subseteq Q^2\) are in/equality constraints in the following sense:
    - \((p, q) \in C^+_w\) expresses that \(p\) and \(q\) have the same values and
    - \((p, q) \in C^-_w\) expresses that \(p\) and \(q\) have different values at \(w\).
Example

Agents: Jan, Gaia, Rosa
Updates (two examples)

**Register Creation** $p \leftarrow^i N$: Create secret variable $p$ for agent $i$ with value $N$.

- $p$ must be globally false before.
- Copy all worlds, let $p = N$ at the new worlds and let $p$ have any other value at the others.
- Connect the worlds for everyone but $i$.

**Announcement** $!p = q$: Tell everyone that $p = q$.

- $p = q$ must be true at the current world.
- Where $p$ and $q$ are false, add $p = q$ to the constraints.

Exact definitions: Action structures as in [BMS98] and [BEK06].
Syntax

**Definition** (Language)
The language $\mathcal{L}_{GG}$ consists of formulas, commands and expressions:

$$
\phi ::= \top | p | p = E | \neg \phi | \phi \land \phi | K_i \phi | G \phi | \langle C \rangle \phi
$$

$$
C ::= !p = E | !p \neq E | p \leftarrow N | C; C
$$

$$
E ::= p | N
$$
Assignments

**Definition** (Assignments and Agreement)
An assignment is a function \( h : \text{Prop} \rightarrow \mathbb{N} \).
It *agrees* with a world \((h \circ \models w)\) iff
- for all \( q \in Q \): \( f^0_w(q) \leq h(q) \leq f^1_w(q) \) and \( h(q) \not\in f^2_w(q) \)
- positive constraints \( C^+_w \): if \((p, q) \in C^+_w\) then \( h(p) = h(q) \)
- negative constraints \( C^-_w \): if \((p, q) \in C^-_w\) then \( h(p) \neq h(q) \).

**Example**
\[ h = \{ p \mapsto 6, p_1 \mapsto 5 \} \]
agrees with 0, but not with 3.
Definition (Truth with regard to assignments)

\[ M, w, h \models \top \] always

\[ M, w, h \models p \] iff \( p \in P_w \)

\[ M, w, h \models p_1 = p_2 \] iff \( h(p_1) = h(p_2) \)

\[ M, w, h \models p = N \] iff \( h(p) = N \)

\[ M, w, h \models \neg \phi \] iff not \( M, w, h \models \phi \)

\[ M, w, h \models \phi_1 \land \phi_2 \] iff \( M, w, h \models \phi_1 \) and \( M, w, h \models \phi_2 \)

\[ M, w, h \models K_i \phi \] iff \( wR_i w' \Rightarrow \forall h' \circlearrowleft w' : M, w', h' \models \phi \)

\[ M, w, h \models G \phi \] iff \( \forall w' \in W \forall h' \circlearrowleft w' : M, w', h' \models \phi \)

\[ M, w, h \models \langle! p = E\rangle \phi \] iff \( M, w, h \models p = E \) and \( M^! p=E, w, h \models \phi \)

\[ M, w, h \models \langle! p \neq E\rangle \phi \] iff \( M, w, h \models p \neq E \) and \( M^! p\neq E, w, h \models \phi \)

\[ M, w, h \models \langle p \triangleright N\rangle \phi \] iff \( M, w, h \models G\neg p \) and

\[ M_{p\leftarrow N}, w, (h \cup \{(p, N)\}) \models \phi \]

\[ M, w, h \models \langle A_1; A_2\rangle \phi \] iff \( M, w, h \models \langle A_1\rangle\langle A_2\rangle \phi \)
Semantics

**Definition (World Level Truth)**

\[ \mathcal{M}, w \models \phi \iff \forall h \text{ with } w \rightarrow h : \mathcal{M}, w, h \models \phi. \]

A formula \( \phi \) is *valid* iff for all \( \mathcal{M}, w \) we have \( \mathcal{M}, w \models \phi \). We then write \( \models \phi \).

This leaves some formulas undecided on the world level. But we still have:

**Theorem**

For all \( \mathcal{M}, w, i \) and \( \phi \) we have either \( \mathcal{M}, w \models K_i \phi \) or \( \mathcal{M}, w \not\models K_i \phi \).
Reduction Axioms (some of them)

P5) \( ⟨!p = E⟩ \widehat{K}_i φ \leftrightarrow (p = E \land \widehat{K}_i(⟨!p = E⟩ φ)) \)

P6) \( ⟨!p = E⟩ Gφ \leftrightarrow (p = E \land G(p = E \rightarrow ⟨!p = E⟩ φ)) \)

R3a1) \( ⟨p \leftarrow N⟩(p = N) \leftrightarrow (G\neg p) \)

R3a1') \( ⟨p \leftarrow N⟩(p = M) \leftrightarrow \bot \) where \( M \neq N \)

R3a2) \( ⟨p \leftarrow N⟩(q = M) \leftrightarrow (G\neg p \land (q = M)) \) where \( p \neq q \)

R3b1) \( ⟨p \leftarrow N⟩(p = p) \leftrightarrow (G\neg p) \)

R3b1') \( ⟨p \leftarrow N⟩(p = q) \leftrightarrow (G\neg p \land (q = N)) \) where \( p \neq q \)

R3b2) \( ⟨p \leftarrow N⟩(q = p) \leftrightarrow (G\neg p \land (q = N)) \) where \( p \neq q \)

R3b2') \( ⟨p \leftarrow N⟩(q = r) \leftrightarrow (G\neg p \land (q = r)) \) where \( p \neq q \) and \( p \neq r \)

R6) \( ⟨p \leftarrow N⟩(K_i φ) \leftrightarrow (G\neg p \land K_i(G\neg p \rightarrow ⟨p \leftarrow N⟩ φ)) \)

R7) \( ⟨p \leftarrow N⟩(K_j φ) \leftrightarrow (G\neg p \land K_j φ) \) where \( j \neq i \)

R8) \( ⟨p \leftarrow N⟩(Gφ) \leftrightarrow G(⟨p \leftarrow N⟩ φ) \)
Axiomatization

**Theorem** (Soundness)
All reduction axioms are valid.

**Definition** (Proof System)
We write $\vdash \phi$ iff $\phi$ is provable using propositional tautologies, standard rules for the S5 modalities $K_i$ and the global modality $G$ and the reduction axioms.

**Theorem** (Completeness)
For all $\phi \in \mathcal{L}_{GG}$, if $\models \phi$, then $\vdash \phi$. 
Cryptography
Communication

“Let me tell you a secret ...”

Goal: Model the intended audience, but also eavesdropping.

- New proposition: \( w \models L_i \) means Agent \( i \) is listening at \( w \).
- Two new commands: \( \langle \text{Open}_i \rangle \) and \( \langle \text{Close}_i \rangle \).
- Announcements are only heard by the current listeners.
“If I know that $p = 5$ then I also know that $p + p = 10$.”

Goal: Give agents some (realistic) computational power. For now: Primality-Testing and modular arithmetic, which are both assumed to be feasible in Cryptography.

- New propositions: $\text{Prime}E$, $\text{Coprime}EE$
- New expressions: $E + E \mod E$, $E \times E \mod E$, $E^E \mod E$
The full language

**Definition (Language)**
The language $\mathcal{L}_{ECL}$ consists of the following formulas, commands and expressions.

$$\phi ::= \top \mid p \mid L_i \mid p = E \mid \neg \phi \mid \phi \land \phi \mid K_i \phi \mid G \phi \mid \langle C \rangle \phi$$

$$\mid \text{Prime } E \mid \text{Coprime } E \ E$$

$$C ::= p \leftarrow i \ E \mid \text{Open}_i \mid \text{Close}_i \mid \!p \mid \!p = N \mid \!p = p$$

$$\mid \!p \neq N \mid \!p \neq p \mid ?\phi$$

$$E ::= p \mid N \mid E + E \mod E \mid E \times E \mod E \mid E^E \mod E$$
The Diffie-Hellman Key Exchange

(Whitfield Diffie and Martin Hellman [DH76])

1. Alice and Bob agree on a prime $p$ and a base $g < p$ such that $g$ and $p - 1$ are coprime.
2. Alice picks a secret $N$ and sends $g^N \mod p = A$ to Bob.
3. Bob picks a secret $M$ and sends $g^M \mod p = B$ to Alice.
4. Alice calculates $k = B^N \mod p$.
5. Bob calculates $k = A^M \mod p$.
6. They now have a shared key $k = (g^M)^N = (g^N)^M \mod p$.

If the Diffie-Hellman problem is hard, Eve does not know $k$.

NB: The protocol is only secure against passive eavesdroppers.
Let $\mathcal{M}_{DH}$ be the blissful ignorance model for Alice, Bob and Eve. Let $\mathbf{DH}_{g,p,N,M}$ be the command:

\begin{align*}
\text{Coprime } g (p - 1) ; \\
q_1 &\leftarrow^a N ; r_1 &\leftarrow^a (g^{q_1} \mod p) ; \text{Open}_b ; !r_1 ; \text{Close}_b ; \\
q_2 &\leftarrow^b M ; r_2 &\leftarrow^b (g^{q_2} \mod p) ; \text{Open}_a ; !r_2 ; \text{Close}_a ; \\
s_1 &\leftarrow^a r_2^{q_1} \mod p ; s_2 &\leftarrow^b r_1^{q_2} \mod p
\end{align*}

Let $\psi_{DH} := (s_1 = s_2) \land (K_as_1 \land K_bs_2) \land (\neg K_es_1 \land \neg K_es_2)$. Then we have:

$$\mathcal{M}_{DH}, w \models \langle \mathbf{DH}_{g,p,N,M} \rangle \psi_{DH}$$
Model Checking
Example 1
Creating a secret number for Alice and telling Bob about it.

Example 2
Order matters: “Hey Bob! Hey Alice!” ≠ “Hey Alice! Hey Bob!”
Monte Carlo Method

\[ M, w \models \phi \text{ iff for some randomly picked } h \leftarrow w : M, w, h \models \phi \]

For many formulas we do not have to check all possible assignments.
Example: Is \( K_a(p = q) \) is true at \( 0 \)?

No, and checking one assignment at \( 1 \) suffices.

NB: There are also cases where this almost always goes wrong.
Normal VS. Monte-Carlo Methods

How long does it take to check $\mathcal{M}_{\text{DH}}, w \models \langle \text{DH}_{g,p,N,M} \rangle_{\psi_{\text{DH}}}$?

<table>
<thead>
<tr>
<th>register size</th>
<th>Normal</th>
<th>Monte Carlo</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^8$</td>
<td>1.07</td>
<td>2.74</td>
</tr>
<tr>
<td>$2^9$</td>
<td>1.36</td>
<td>2.82</td>
</tr>
<tr>
<td>$2^{10}$</td>
<td>2.13</td>
<td>3.41</td>
</tr>
<tr>
<td>$2^{11}$</td>
<td>3.59</td>
<td>3.24</td>
</tr>
<tr>
<td>$2^{12}$</td>
<td>5.17</td>
<td>2.8</td>
</tr>
<tr>
<td>$2^{13}$</td>
<td>11.56</td>
<td>3.28</td>
</tr>
<tr>
<td>$2^{14}$</td>
<td>22.66</td>
<td>3.57</td>
</tr>
<tr>
<td>$2^{15}$</td>
<td>44.44</td>
<td>4.1</td>
</tr>
<tr>
<td>$2^{16}$</td>
<td>81.26</td>
<td>3.52</td>
</tr>
</tbody>
</table>
Conclusion
Conclusion

- To know a number is to distinguish a true value from all others
- Register models for DEL:
  - reduce “Knowledge of” to “Knowledge that”
- Axiomatization for GG
- Explicit communication and computation in ECL
- Example: Diffie-Hellman
- Implemented both frameworks in Haskell
- Efficient but probabilistic Monte Carlo method

Future ideas: axiomatize full ECL, improve implementation, non-S5, other protocols, automated attack finding, ...
References

Johan van Benthem, Jan van Eijck, and Barteld Kooi.
Logics of communication and change.

Alexandru Baltag, Lawrence S. Moss, and Slawomir Solecki.
The logic of public announcements, common knowledge, and private suspicions.

Whitfield Diffie and Martin Hellman.
New directions in cryptography.
Thank you.

http://is.gd/eclonline