

Towards an Intuitionistic Foundation for Interactive Computation

(Workshop on Constructive Aspects of Logic and Mathematics)

Simon Kramer

University of Tsukuba, Japan

March 8, 2010



Outline

Introduction

- Motivation
- Goal
- Problem
- Solution
- Methodology

Non-interactive logics

- The Logic of Proofs (LP)
- The logic of non-arithmetic provability S4
- Intuitionistic Logic (IL)
- Typed programs

Conclusion

Bibliography

Purpose of this talk

Motivate the following diagram and explain its lower part:



Motivation

Interactive computation the [GSW06] new paradigm of computation

Purpose

Yes (they) the purpose of interactive computation ultimately is not the computation of result values

But (I) the purpose of interactive computation is **not** the possibly unending interaction *itself*.

(The interaction may well be unending, but it cannot be a self-purpose because if it were then all interactive programs would be quines.)

Goal

Reach consensus with you that:

1. values are only the means—not the ends—of interactive computation
2. **the purpose of interactive computation is interpreted communication between distributed agents—humans and/or machines—interacting via message passing.**
(message = *information token* in the sense of D. Scott)

Problem (continued)

- ▶ Due to the distribution of the different agents in a communication system, which may have different views of the system, the agents constitute different message *interpretation contexts*.
- ▶ Hence, identical messages may well be interpreted differently in different contexts, and thus have different meanings to different agents.
- ▶ [Re]producing intended message meaning across interpretation contexts is a highly critical and non-trivial problem.

Problem

So what is interpreted communication?

According to Shannon [Sha48]:

The fundamental problem of [uninterpreted] communication is that of reproducing at one point either exactly or approximately a message selected at another point.

In analogy, we declare:

*The fundamental problem of interpreted communication is that of [re]producing at one point either exactly or approximately the **intended meaning** of a message selected at another point.*

Problem (continued)

But what does **message meaning** mean more precisely?

We argue that

the meaning of a message in a given interpretation context is the propositional knowledge which the individual knowledge of that message induces in that context.

Problem (continued)

By **individual knowledge** we mean

knowledge in the sense of the transitive use of the verb “to know”, here to know a message, such as the plaintext of an encrypted message.

$$\mathcal{M} \ni M ::= a \mid B \mid \{\!\{M\}\!\}_a \mid (M, M)$$

- ▶ $\vdash_{\text{LiP}} a \mathbf{k} b$ (knowledge of agent names $a, b \in \mathcal{A}$)
- ▶ $\vdash_{\text{LiP}} a \mathbf{k} M \rightarrow a \mathbf{k} \{\!\{M\}\!\}_a$ (personal signature synthesis)
- ▶ $\vdash_{\text{LiP}} a \mathbf{k} \{\!\{M\}\!\}_b \rightarrow a \mathbf{k} M$ (universal signature analysis)
- ▶ $\vdash_{\text{LiP}} (a \mathbf{k} M \wedge a \mathbf{k} M') \leftrightarrow a \mathbf{k} (M, M')$ ([un]pairing)

Problem (continued)

- ▶ Hence, an agent-centric paraphrase of our previous problem statement is:

*The fundamental problem of communication is that of **inducing** at one point either an intended **knowledge** or an intended belief with a message selected at another point.*

- ▶ Again, result values are only the means—not the ends—of interactive computations.

Problem (continued)

By **propositional knowledge** we mean

knowledge in the sense of the use of the verb “to know” with a clause, here to know that a statement is true.

$$\underbrace{((\mathcal{S}, \{\equiv_a\}_{a \in \mathcal{A}}), \mathcal{V})}_{\text{frame}}, s \models \mathbf{K}_a(\phi) \text{ :iff}$$

for all $s' \in \mathcal{S}$, if $s \equiv_a s'$ then $((\mathcal{S}, \{\equiv_a\}_{a \in \mathcal{A}}), \mathcal{V}), s' \models \phi$

- ▶ $\models \mathbf{K}_a(\phi \rightarrow \phi') \rightarrow (\mathbf{K}_a(\phi) \rightarrow \mathbf{K}_a(\phi'))$ (Kripke's law)
- ▶ $\models \mathbf{K}_a(\phi) \rightarrow \phi$ (truth law)
- ▶ $\models \mathbf{K}_a(\phi) \rightarrow \mathbf{K}_a(\mathbf{K}_a(\phi))$ (positive introspection)
- ▶ $\models \neg \mathbf{K}_a(\phi) \rightarrow \mathbf{K}_a(\neg \mathbf{K}_a(\phi))$ (negative introspection)
- ▶ if $\models \phi$ then $\models \mathbf{K}_a(\phi)$ (necessitation)

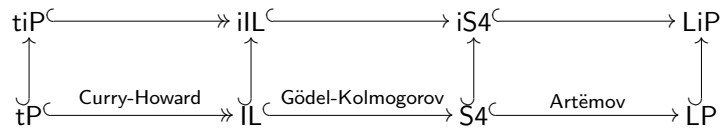
Solution

- ▶ Our problem statement contains an inceptive solution and defining principle for interactive computation, namely **induction of knowledge**.
- ▶ Our task is thus to make this principle precise.
- ▶ This in turn leads us to defining the concept of an **interactive proof** whose effect is to induce the knowledge of its proof goal in the intended interpretation context.

Methodology

An interactive generalisation of a classical construction that consists in a

- ▶ “horizontal” transitive *embedding* of programs into proofs
- ▶ “vertical” embedding of each non-interactive structure into its interactive counterpart:



Methodology (continued)

3. *interactive Intuitionistic Logic* (iIL) via an embedding into iS4 in analogy with the Gödel-Kolmogorov embedding of Intuitionistic Logic IL into S4 [Art07]
4. *typed interactive programs* (tiP) via a morphism from iIL in analogy with the Curry-Howard isomorphism between IL and typed programs tP [dG95].

In sum, **the purpose of interactive proofs is the transfer of propositional knowledge** (i.e., [to-be-]known facts) via the transfer of certain individual knowledge (i.e., [to-be-]known proofs) in multi-agent systems.

Methodology (continued)

More precisely, we shall define:

1. a classical modal logic (LiP) of *interactive proofs* that
 - 1.1 are agent-centric generalisations of non-interactive proofs
 - 1.2 induce the knowledge of their proof-goal with their intended interpreting agent(s) such that the induced knowledge is knowledge in the sense of the standard modal logic of knowledge S5 [FHMV95]
2. a classical modal logic (iS4) of *interactive provability* via an embedding into LiP in analogy with Artëmov's embedding of the standard modal logic of non-arithmetic provability S4 into his Logic of Proofs LP [Art01, Art07]

The Logic of Proofs (LP)

0. the axioms of classical propositional logic
1. $\vdash_{LP} (p:F) \rightarrow (p+q):F$ (sum left)
2. $\vdash_{LP} (q:F) \rightarrow (p+q):F$ (sum right)
3. $\vdash_{LP} (p:(F \rightarrow G)) \rightarrow ((q:F) \rightarrow (p \cdot q):G)$ (application)
4. $\vdash_{LP} (p:F) \rightarrow F$ (reflection)
5. $\vdash_{LP} (p:F) \rightarrow !p:(p:F)$ (proof checker)
6. $\{F \rightarrow G, F\} \vdash_{LP} G$ (*modus ponens*)
7. $\vdash_{LP} c:A$, for an axiom A and a proof constant c (constant specification).

LP versus LiP

In contrast to LP:

LiP gives **an epistemic explication of proofs**, i.e., an explication of proofs in terms of the *epistemic impact* that they effectuate with their intended interpreting agents (i.e., the knowledge of their proof goal).

Hence, we beg to differ with Artëmov and Nogina, who, like Aristotle and Plato, define (propositional) knowledge as justified true belief, but unlike Aristotle and Plato, admit as admissible justifications only (mathematical) proofs [AN05].

The logic of non-arithmetic provability S4

0. the axioms of classical propositional logic
1. $\vdash_{S4} \Box(F \rightarrow G) \rightarrow (\Box F \rightarrow \Box G)$ (Kripke's law)
2. $\vdash_{S4} \Box F \rightarrow F$ (reflexivity)
3. $\vdash_{S4} \Box F \rightarrow \Box \Box F$ (transitivity)
4. $\{F \rightarrow G, F\} \vdash_{S4} G$ (*modus ponens*)
5. $F \vdash_{S4} \Box F$ (necessitation).

□ in LiP (using **guarded quantification**):

$$\text{CP}_{(\{a_1, \dots, a_n\}, b)}^C(\phi) := \exists m_1(a_1 \mathbf{k} m_1 \wedge \dots \wedge \exists m_n(a_n \mathbf{k} m_n \wedge (m_1, \dots, m_n) :_b^C \phi)$$

LP versus LiP (continued)

Axioms for interactive proofs:

- ▶ $\vdash_{\text{LiP}} (M :_a^C (\phi \rightarrow \phi')) \rightarrow ((M' :_a^C \phi) \rightarrow (M, M') :_a^C \phi')$ (generalised Kripke law)
- ▶ $\vdash_{\text{LiP}} (M :_a^C \phi) \rightarrow (a \mathbf{k} M \rightarrow \phi)$ (conditional reflection)
- ▶ $\vdash_{\text{LiP}} (M :_a^C \phi) \rightarrow \bigwedge_{b \in \mathcal{CU}\{a\}} \{\{M\}\}_a :_b^{CU\{a\}} (M :_a^C \phi)$ (peer review)

and a semantics such that interactive proofs are **proofs of knowledge** in the following sense:

$$\models (M :_a^C \phi) \rightarrow \bigwedge_{b \in \mathcal{CU}\{a\}} \{\{M\}\}_a :_b^{CU\{a\}} (a \mathbf{k} M \wedge K_a(\phi))$$

S4 versus LP

Theorem (Artëmov)

S4 is the forgetful projection of LP, where the forgetful projection of an LP-formula F is the S4-formula obtained from F by replacing 'p:' in F by '□'.

In other words, the projection embeds S4 into LP such that for all occurrences of '□' in all S4-formulas there is an actually constructible proof-polynomial p such that ' p :' realises '□' in the corresponding LP-formulas.

Intuitionistic Logic (IL)

1. $\vdash_{IL} (F \rightarrow (G \rightarrow H)) \rightarrow ((F \rightarrow G) \rightarrow (F \rightarrow H))$
2. $\vdash_{IL} F \rightarrow F$
3. $\vdash_{IL} F \rightarrow (G \rightarrow F)$
4. $\{F \rightarrow G, F\} \vdash_{IL} G$.

Theorem (Gödel-Kolmogorov)

Let F designate a propositional formula, and let $e(F)$ designate the Gödel-Kolmogorov embedding of IL into S4, i.e., the formula obtained by prefixing every sub-formula of F (including F) with \Box . Then,

$\vdash_{IL} F$ if and only if $\vdash_{S4} e(F)$ [Art07, Page 931].

Typed programs

Simply typed Combinatory Logic [HS08]:

1. $\vdash_{tCL} S:((F \rightarrow (G \rightarrow H)) \rightarrow ((F \rightarrow G) \rightarrow (F \rightarrow H)))$
2. $\vdash_{tCL} I:(F \rightarrow F)$
3. $\vdash_{tCL} K:(F \rightarrow (G \rightarrow F))$
4. $\{p:(F \rightarrow G), q:F\} \vdash_{tCL} (p \cdot q):G$,




whence follows the famous Curry-Howard isomorphism [dG95] between typed programs and IL.

Conclusion




Our research:

- ▶ an intuitionistic foundation for interactive computation via a Curry-Howard isomorphism from interactive intuitionistic logic defined via a classical modal logic of interactive proofs.
- ▶ an interactive analog of
 - ▶ the Gödel-Kolmogorov-Artëmov definition of intuitionistic logic as embedded into a classical modal logic of proofs
 - ▶ the Curry-Howard isomorphism between intuitionistic proofs and typed programs.

Bibliography

-  S. Artemov and E. Nogina.
Introducing justification into epistemic logic.
Journal of Logic and Computation, 15(6), 2005.
-  S. Artemov.
Explicit provability and constructive semantics.
Bulletin of Symbolic Logic, 7(1), 2001.
-  S. Artemov.
Handbook of Modal Logic, volume 3 of *Studies in Logic and Practical Reasoning*, chapter Modal Logic in Mathematics.
Elsevier, 2007.



Bibliography

-  Ph. de Groote, editor.
The Curry-Howard Isomorphism.
Number 8 in Cahiers du centre de logique. Academia-Erasme,
Louvain-la-Neuve (Belgique), 1995.
-  R. Fagin, J.Y. Halpern, Y. Moses, and M.Y. Vardi.
Reasoning about Knowledge.
MIT Press, 1995.
-  D. Goldin, S.A. Smolka, and P. Wegner, editors.
Interactive Computation: The New Paradigm.
Springer, 2006.

質問

質問がありますか。

Bibliography

-  J.R. Hindley and J.P. Seldin.
Lambda-Calculus and Combinators.
CUP, second edition, 2008.
-  C.E. Shannon.
A mathematical theory of communication.
Bell System Technical Journal, 27, 1948.

Contact

Email:
simon.kramer@a3.epfl.ch

Homepage:
<http://www.cipher.risk.tsukuba.ac.jp/~kramer/>