Observations about the proof theory of cyberlogic

Giselle Reis

July, 2019

In this document we analyze a first proposal of a sequent calculus for cyberlogic, which follows closely the rules in [2], and show why cut-elimination fails. The calculus below was implemented in the Abella proof assistant [1], and the problem was encountered while trying to complete the cut-admissibility proof.

The first proposal of a sequent calculus for cyberlogic is shown in Figure 1. We read the operators $\rhd_K$ as an *attestation* of authority K, and $:\rhd_K$ as a *direct attestation* of authority K. The judgment $K \vdash A$ represents the fact that authority K has an external evidence for A.

$$\frac{}{\Gamma, A \longrightarrow A}\ \mathsf{init} \qquad \frac{\Gamma \longrightarrow :\rhd_K A}{\Gamma \longrightarrow \rhd_K A}\ \mathsf{gen}$$

$$\frac{\Gamma, A, B \longrightarrow C}{\Gamma, A \wedge B \longrightarrow C}\ \wedge_l \qquad \frac{\Gamma \longrightarrow A \quad \Gamma \longrightarrow B}{\Gamma \longrightarrow A \wedge B}\ \wedge_r$$

$$\frac{\Gamma \longrightarrow A \quad \Gamma, B \longrightarrow C}{\Gamma, A \Rightarrow B \longrightarrow C}\ \Rightarrow_l \qquad \frac{\Gamma, A \longrightarrow B}{\Gamma \longrightarrow A \Rightarrow B}\ \Rightarrow_r$$

$$\frac{\Gamma, A[t/x] \longrightarrow C}{\Gamma, \forall x.A \longrightarrow C}\ \forall_l \qquad \frac{\Gamma \longrightarrow A[\alpha/x]}{\Gamma \longrightarrow \forall x.A}\ \forall_r$$

$$\frac{\Gamma, A[\alpha/x] \longrightarrow C}{\Gamma, \exists x.A \longrightarrow C}\ \exists_l \qquad \frac{\Gamma \longrightarrow A[t/x]}{\Gamma \longrightarrow \exists x.A}\ \exists_r$$

$$\frac{\Gamma, A \longrightarrow :\rhd_K C}{\Gamma, \rhd_K A \longrightarrow :\rhd_K C}\ \rhd_l \qquad \frac{\Gamma \longrightarrow A}{\Gamma \longrightarrow \rhd_K A}\ \rhd_r$$

$$\frac{\Gamma, \rhd_K A \longrightarrow C}{\Gamma, :\rhd_K A \longrightarrow C}\ :\rhd_l \qquad \frac{K \vdash A}{\Gamma \longrightarrow :\rhd_K A}\ :\rhd_r$$

Figure 1: Proposed sequent calculus for cyberlogic

Observe that the rule gen is not admissible. The proof, by induction on the derivation, breaks on the cases for $\rhd_l$ and $:\rhd_r$ (an axiom). It seems that the case for $\rhd_l$ cannot be recovered: we need to find a proof of $\Gamma, \rhd_K B \longrightarrow \rhd_K A$ assuming that $\Gamma, B \longrightarrow \rhd_K A$. The case for $:\rhd_r$ would work using cut but, as we see below, cut it not admissible.

Observe also that identity expansion does not hold (i.e., we cannot reduce the init rule to the atomic case), because of the case $:\rhd_K A \longrightarrow :\rhd_K A$.

We tried to show that cut is admissible for this system, i.e.:

Conjecture 1. *If* $\Gamma \longrightarrow A$ *and* $\Gamma, A \longrightarrow C$*, then* $\Gamma \longrightarrow C$*.*

The proof proceeds by a triple structural induction on:

1. the size of the cut-formula A
2. the structure of the proof of $\Gamma, A \longrightarrow C$
3. the structure of the proof of $\Gamma \longrightarrow A$

The last induction is needed for those connective whose right rule is not invertible.

Unfortunately, the proof seems to break with two incompatible cases:

- **Case 1:**

$$\dfrac{\dfrac{\overset{\mathcal{D}}{\Gamma \longrightarrow :\rhd_K A}}{\Gamma \longrightarrow \rhd_K A}\,\mathsf{gen} \qquad \dfrac{\overset{\mathcal{E}}{\Gamma, A \longrightarrow \rhd_K C}}{\Gamma, \rhd_K A \longrightarrow \rhd_K C}\,\rhd_l}{\Gamma \longrightarrow \rhd_K C}\,\mathsf{cut}$$

  This proof can be transformed into:

$$\dfrac{\overset{\mathcal{D}}{\Gamma \longrightarrow :\rhd_K A} \qquad \dfrac{\dfrac{\overset{\mathcal{E}}{\Gamma, A \longrightarrow \rhd_K C}}{\Gamma, \rhd_K A \longrightarrow \rhd_K C}\,\rhd_l}{\Gamma, :\rhd_K A \longrightarrow \rhd_K C}\,:\rhd_l}{\Gamma \longrightarrow \rhd_K C}\,\mathsf{cut}$$

  Even though the left branch of the cut is smaller, the right one is bigger, therefore, we need to rely on the IH concerning the size of the cut-formula. Structurally speaking, the cut-formula $:\rhd_K A$ is the same size of $\rhd_K A$, but we can define a weight measure such that $:\rhd_K < \rhd_K$ and this way, this case works.

- **Case 2:**

$$\dfrac{\overset{\mathcal{D}}{\Gamma \longrightarrow :\rhd_K A} \qquad \dfrac{\overset{\mathcal{D}}{\Gamma, \rhd_K A \longrightarrow C}}{\Gamma, :\rhd_K A \longrightarrow C}\,:\rhd_l}{\Gamma \longrightarrow C}\,\mathsf{cut}$$

> This proof can be transformed into:
>
> $$\dfrac{\dfrac{\overset{\mathcal{D}}{\Gamma \longrightarrow :\triangleright_K A}}{\Gamma \longrightarrow \triangleright_K A}\,\textsf{gen} \qquad \overset{\mathcal{D}}{\Gamma, \triangleright_K A \longrightarrow C}}{\Gamma \longrightarrow C}\,\textsf{cut}$$
>
> Normally, this transformation should work since the size of the cut-formula is the same, but the proof of the right branch of the cut has decreased. But remember that we needed to make $:\triangleright_K < \triangleright_K$ for the previous case to work, so now we can no longer apply the inductive hypothesis.

If gen was not a rule, the case of cut on a $\triangleright_K$ formula would work just fine (see lines 170 to 188 in `cyber.thm`). The case of cut on a $:\triangleright_K$ formula would fail (lines 193 to 209). Since $:\triangleright_r$ is not an "invertible rule" (even if it is an axiom, we cannot use this fact to do a cut transformation), we need to induct on the left premise of the cut. This induction fails on two cases: $\triangleright_l$ and $:\triangleright_r$. That means we cannot reduce the cut for:

$$\dfrac{\dfrac{\overset{\mathcal{D}}{\Gamma, B \longrightarrow :\triangleright_K A}}{\Gamma, \triangleright_K B \longrightarrow :\triangleright_K A}\,\triangleright_l \qquad \dfrac{\overset{\mathcal{E}}{\Gamma, \triangleright_K B, \triangleright_K A \longrightarrow C}}{\Gamma, \triangleright_K B, :\triangleright_K A \longrightarrow C}\,:\triangleright_l}{\Gamma, \triangleright_K B \longrightarrow C}\,\textsf{cut}$$

$$\dfrac{\dfrac{K \vdash A}{\Gamma \longrightarrow :\triangleright_K A}\,:\triangleright_r \qquad \dfrac{\overset{\mathcal{E}}{\Gamma, \triangleright_K A \longrightarrow C}}{\Gamma, :\triangleright_K A \longrightarrow C}\,:\triangleright_l}{\Gamma \longrightarrow C}\,\textsf{cut}$$

Indeed, without gen we cannot prove $\triangleright_K :\triangleright_K A \longrightarrow \triangleright_K A$, but with cut this is possible:

$$\dfrac{\dfrac{\dfrac{}{:\triangleright_K A \longrightarrow :\triangleright_K A}\,\textsf{init}}{\triangleright_K :\triangleright_K A \longrightarrow :\triangleright_K A}\,\triangleright_l \qquad \dfrac{\dfrac{}{\triangleright_K A \longrightarrow \triangleright_K A}\,\textsf{init}}{:\triangleright_K A \longrightarrow \triangleright_K A}\,:\triangleright_l}{\triangleright_K :\triangleright_K A \longrightarrow \triangleright_K A}\,\textsf{cut}$$

I could not find yet a formula which is provable using cut and not provable using *all* the rules of the system above.

The following implications concerning attestation connectives hold:

$$\begin{array}{rcl} :\triangleright_K A & \Rightarrow & \triangleright_K A \\ A & \Rightarrow & \triangleright_K A \end{array}$$

The following ones do not hold:

$$\begin{array}{rcl} \rhd_K A & \nRightarrow & :\rhd_K A \\ A & \nRightarrow & :\rhd_K A \\ \rhd_K A & \nRightarrow & A \\ :\rhd_K A & \nRightarrow & A \end{array}$$

In particular, the implication $\rhd_K \rhd_K\ A \Rightarrow \rhd_K\ A$, listed in the white paper as a logical equivalence, does not hold.

References

[1] D. Baelde, K. Chaudhuri, A. Gacek, D. Miller, G. Nadathur, A. Tiu, and Y. Wang. Abella: A System for Reasoning about Relational Specifications. *Journal of Formalized Reasoning*, 7(2):1–89, 2014.

[2] V. Bernat. First-Order Cyberlogic Hereditary Harrop Logic. Technical report, SRI International, 2006. `http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/Bernat-cyberlogic1.ps`.