Cut Elimination as Error Correcting Device

Matthias Baaz
Vienna University of Technology

6.1202

Proof in logic is only a mechanical expedient to facilitate the recognition of tautology, where it is complicated.

6.1203

It would be too remarkable, if one could prove a significant proposition *logically* from another, and a logical proposition *also*. It is clear from the beginning that the logical proof of a significant proposition and the proof *in* logic must be two quite different things.

LK

Axioms:

$$A \to A.$$

Structural inferences:

$$\frac{\Gamma_1 \to \Delta_1, A \qquad A, \Gamma_2 \to \Delta_2}{\Gamma_1, \Gamma_2 \to \Delta_1, \Delta_2}\ cut$$

$$\frac{\Gamma \to \Delta}{A, \Gamma \to \Delta}\ w:l \qquad \frac{\Gamma \to \Delta}{\Gamma \to \Delta, A}\ w:r$$

$$\frac{\Gamma_1, A, B, \Gamma_2 \to \Delta}{\Gamma_1, B, A, \Gamma_2 \to \Delta}\ ex:l \qquad \frac{\Gamma \to \Delta_1, A, B, \Delta_2}{\Gamma \to \Delta_1, B, A, \Delta_2}\ ex:r$$

$$\frac{A, A, \Gamma \to \Delta}{A, \Gamma \to \Delta}\ c:l \qquad \frac{\Gamma \to \Delta, A, A}{\Gamma \to \Delta, A}\ c:r$$

LK

Logical inferences:

$$\frac{\Gamma \to \Delta, A}{\neg A, \Gamma \to \Delta}\ \neg : l \qquad\qquad \frac{A, \Gamma \to \Delta}{\Gamma \to \Delta, \neg A}\ \neg : r$$

$$\frac{A, \Gamma \to \Delta \qquad B, \Gamma \to \Delta}{A \vee B, \Gamma \to \Delta}\ \vee : l \qquad\qquad \frac{\Gamma \to \Delta, A}{\Gamma \to \Delta, A \vee B}\ \vee : r_1$$

$$\frac{A, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta}\ \wedge : l_1 \qquad\qquad \frac{\Gamma \to \Delta, B}{\Gamma \to \Delta, A \vee B}\ \vee : r_2$$

$$\frac{B, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta}\ \wedge : l_2 \qquad \frac{\Gamma \to \Delta, A \qquad \Gamma \to \Delta, B}{\Gamma \to \Delta, A \wedge B}\ \wedge : r$$

$$\frac{\Gamma \to \Delta, A \qquad B, \Gamma \to \Delta}{A \supset B, \Gamma \to \Delta}\ \supset : l \qquad\qquad \frac{A, \Gamma \to \Delta, B}{\Gamma \to \Delta, A \supset B}\ \supset : r$$

LK

$$\frac{C(e), \Gamma \rightarrow \Delta}{\exists x C(x), \Gamma \rightarrow \Delta}\ \exists : l \qquad \frac{\Gamma \rightarrow \Delta, C(r)}{\Gamma \rightarrow \Delta, \exists x C(x)}\ \exists : r$$

$$\frac{C(r), \Gamma \rightarrow \Delta}{\forall x C(x), \Gamma \rightarrow \Delta}\ \forall : l \qquad \frac{\Gamma \rightarrow \Delta, C(e)}{\Gamma \rightarrow \Delta, \forall x C(x)}\ \forall : r$$

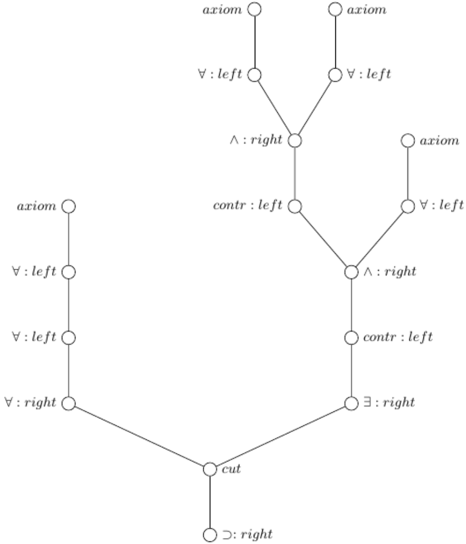
with the usual restrictions.

$$\frac{\Gamma_1 \to \Delta_1, A \qquad A, \Gamma_2 \to \Delta_2}{\Gamma_1, \Gamma_2' \to \Delta_1', \Delta_2}\ mix$$

where Δ_1' is Δ_1 after removing A and Γ_2' is Γ_2 after removing A.

$$\frac{\Gamma_1 \to \Delta_1, A \qquad A, \Gamma_2 \to \Delta_2}{\Gamma_1, \Gamma_2' \to \Delta_1', \Delta_2}\ mix^*$$

where Δ_1' is Δ_1 after removing only the As later contracted to the mix formula and Γ_2' is Γ_2 after removing only the As later contracted to the mix formula.



$$\rightarrow \forall x \forall y P(x, y) \supset \exists z(P(0, z) \wedge P(z, a) \wedge P(Sz, Sa)).$$

There is a proof underlying this representation by name iff a is replaced by $S^{2n}(0)$.

A second order unification problem is a finite set of equations in the language $T \cup \{Sub_1, \ldots, Sub_m\}$ plus free variables for elements of T. The free variables will be called the term variables. By introducing new term variables we can transform any such system into an equivalent one where all equations have form

$$\delta(a_i/\sigma) = \rho,$$

where δ, σ, ρ are terms of term variables.
Suppose a unary function symbol is chosen, say S. Then we call a numeral any term of the form $S^n(t)$, t a free variable or $t = 0$, $n \in \omega$.

Theorem

Let L contain a unary function symbol S, a constant 0 and a binary function symbol. Let τ_0 be a term variable. Then for every recursively enumerable set $X \subseteq \omega$ there exists a second order unification problem Ω such that $\Omega \cup \{\tau_0 = S^n(0)\}$ has a solution iff $n \in X$.

Proof

We use Matijasevič's theorem.

$$\exists y_1, \ldots, y_k D_X(x, y_1, \ldots, y_k),$$

where D_X is a conjunction of formulas of the form

$$\begin{array}{rcl} y_i & = & u, u < \omega \\ y_i & = & y_j + y_l \\ y_i & = & y_j * y_l \\ y_i & = & x \end{array}$$

$i, j, l \leq k$.

Proof cont.

1. The equation $s(\tau) = \tau(a/s(a))$, τ term variable, has solutions $\tau = S^n(a), n \in \omega$.
2. The equation $\tau(a/\sigma) = \rho$ plus the equations from 1. for term variables τ, σ, ρ have solutions:

$$S^p(a), S^q(a), S^m(a) \quad \text{for} \quad p + q = m.$$

3. The equations

$$\begin{aligned} S(\sigma_1) &= \sigma_1(a/S(a)) \\ S(\sigma_2) &= \sigma_2(a/S(a)) \\ S(\sigma_3) &= \sigma_3(b/S(b)) \\ \tau(a/\sigma_1, b/S(b), c/a \circ (b \circ c)) &= \sigma_2 \circ (\sigma_3 \circ \tau) \end{aligned}$$

with variables a, b, c and term variables $\sigma_1, \sigma_2, \sigma_3, \tau$ have solutions for $\sigma_1, \sigma_2, \sigma_3$ of the form $S^p(a), S^m(a), S^q(b)$ for $p * q = m$.
The proof is non-trivial only for claim 3.

Proof cont.

a) Assume $p * q = m$. Then $S^p(a), S^m(a), S^q(b)$ and the following term are solution for the equations above

$$S^{p(q-1)}(a) \circ (S^{q-1}(b) \circ (S^{p(q-2)}(a) \circ (S^{q-2}(b)$$

$$\circ (\ldots (S^p(a) \circ (S(b) \circ (a \circ (b \circ c) \ldots))))))).$$

b) Suppose $S^p(a), S^m(a), S^q(b), t$ are a solution. We shall proceed by induction on the depth of t, denoted by $dp(t)$.

(i) $dp(t) = 0$. Then t is c, hence σ_2 is a and σ_3 is b. Thus $p * q = m = 0$.

(ii) $dp(t) > 0$. Then t is $t_1 \circ t_2$, where

$$t_1(a/S^p(a), b/S(b), c/a \circ (b \circ c)) = S^m(a)$$

i.e. $t_1 = S^{m-p}(a)$ and

$$t_2(a/S^p(a), b/S(b), c/a \circ (b \circ c)) = S^q(b) \circ t.$$

Proof cont.

Hence $dp(t_2) > 0$, so $t_2 = t_3 \circ t_4$

$$t_3(a/S^p(a), b/S(b), c/a \circ (b \circ c)) = S^q(b),$$

thus $t_3 = S^{q-1}(b)$. Further we have

$$t_4(a/S^p(a), b/S(b), c/a \circ (b \circ c)) = t$$

$$= t_1 \circ (t_3 \circ t_4) = S^{m-p}(a) \circ (S^{q-1}(b) \circ t_4)$$

By the induction hypothesis, since $dp(t_4) < dp(t)$,

$$p * (q - 1) = m - p$$

i.e. $p * q = m$. We are done.

Theorem

Let L be a language containing a unary function symbol S, a constant 0 and a binary function symbol. Then for every recursively enumerable set $X \subseteq \omega$ there exists a sequent $A \to A, P(a)$ and a skeleton with universal cuts S such that $n \in X$ iff $A \to A, P(S^n(0))$ has an LK-proof with skeleton S.

Proof.

The argument is based on the following observation: Construct a derivation such that $P(a) \vee P(d), P(s) \vee P(t)$ occur on the right side enforced by the end-sequent. Quantify both formulas by $\exists$-right (one after the other). Afterwards infer $\exists$-left with eigenvariable a such that the position of a has to be bound on the right side. The two formulas can be constructed iff

$$d(a/s) = t.$$

Cut the description of the contracted formula F with the description of $F \to A \supset A$ directly obtained from an axiom by $\supset: r$ and $weakening: l$. $\square$

A semi-unification problem is a set of pairs of terms $S = \{(s_1, t_1), \ldots, (s_n, t_n)\}$. A solution to S is a substitution Δ such that there are $\Sigma, \ldots, \Sigma_n$ such that $s_1\Delta = t_1\Delta\Sigma_1, \ldots, s_n\Delta = t_n\Delta\Sigma_n$.

Example

$\{(x, s(y))\}$: $\Delta = \{x \leftarrow s(y')\}$ but also $\{x \leftarrow s(0)\}$.
$\{(x, s(x))\}$: unsolvable.

Theorem

Semi-unification is undecidable.
If a solution exists, then there is a most general solution.

Theorem

For every skeleton with universal cuts it is decidable whether a proof according to this skeleton and block-wise inference of quantifiers for a given end-sequent exists. If there is a proof there is a most general proof.

$$
\begin{array}{ccccc}
A(\bar{t}) & \supset & \exists \bar{x} A(\bar{x}) & & (A, A') \\
| & & | & & \\
A & & A' & & \\
| & & | & & \\
A(t) & \supset & \exists x A(x) & & A = A'\sigma_x(y)
\end{array}
$$

Theorem

For every semi-unification problem there is a linear skeleton S with universal cuts and an end-sequent such that S with the end-sequent can be realized by a proof with block-wise inference of quantifiers iff the semi-unification problem is solvable.

Corollary

It is undecidable whether a linear skeleton with universal cuts can be realized by a proof.

Proof. First note that the semi-unification problem can be reduced to a semi-unification problem $\{(s_1^*, t), \ldots, (s_p^*, t)\}$ with $s_i^* = f(\cdots f(a_{i_1}, a_{i_2}) \ldots s_i) \ldots a_{i_p})$ and $t = f(\cdots f(t_1, t_2), \ldots t_p)$, where a_{i_j} are new free variables.

Let $A_\Omega(a_1, \ldots, a_n) \equiv P(t) \wedge ((P(s_1^*) \wedge \ldots \wedge P(s_p^*)) \supset Q)$, where all free variables are among $a_1, \ldots, a_n$ and do not occur in Q. We sketch the construction of a proof analysis as follows:

$$
\begin{array}{ll}
 & \quad \Big\{ \text{propositional inferences} \\
(a) & A_\Omega(a_1, \ldots, a_n)\delta \to A_\Omega(a_1, \ldots, a_n)\delta \\
(a+1) & \underline{(\forall x_1) \ldots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to A_\Omega(a_1, \ldots, a_n)\delta} \\
 & \quad \Big\{ \begin{array}{l}\text{propositional inferences including} \\ \text{propositional cuts from } (a+1)\end{array} \\
(b) & (\forall x_1) \ldots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to P(t)\delta \\
(b+1) & \underline{(\forall x_1) \ldots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to (\forall y_1) \ldots (\forall y_m) R(y_1, \ldots, y_m)} \\
 & \quad \Big\{ \begin{array}{l}\text{propositional inferences including} \\ \text{propositional cuts from } (a+1)\end{array} \\
(c) & P(s_1^*)\delta, \ldots, P(s_p^*)\delta, (\forall x_1) \ldots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to Q \\
 & \quad \Big\{ \begin{array}{l}p\ (\forall_B\text{-left})\text{-inferences, exchanges} \\ \text{and contractions from } (c)\end{array} \\
(d) & (\forall z_1) \ldots (\forall z_s) R'(z_1, \ldots, z_s), (\forall x_1) \ldots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to Q \\
(e) & (\forall x_1) \ldots (\forall x_n) A_\Omega(x_1, \ldots, x_n), (\forall x_1) \ldots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to Q \\
(e+1) & (\forall x_1) \ldots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to Q
\end{array}
$$

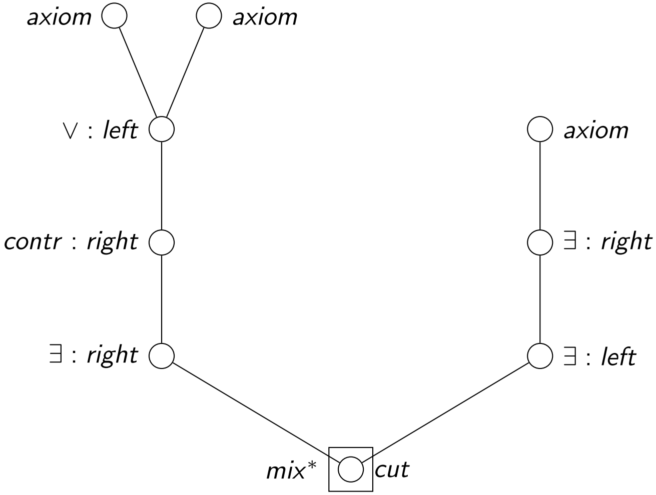
Here, $(a+1)$ is obtained from (a) by ($\forall_B$:left), $(b+1)$ from (b) by ($\forall_B$:right), (e) from $(b+1)$ and (d) by cut, and $(e+1)$ from (e) by contraction. Note that $(\forall y_1) \ldots (\forall y_m) R(y_1, \ldots, y_m) \equiv (\forall z_1) \ldots (\forall z_s) R'(z_1, \ldots, z_s)$ by the cut rule and hence δ is forced to be a semi-unifier. The label $(a+1)$ is ancestor of *both* sides of the cut, the skeleton is therefore *not* in tree form. (The length of the skeleton is linear in n.)
□

Theorem

There is a procedure which transforms any proof skeleton P into a cut-free proof skeleton P' with the same bottom node. If there is a proof realizing P for a given end-sequent there is a proof realizing P'.

Important: *mix** has to be employed.

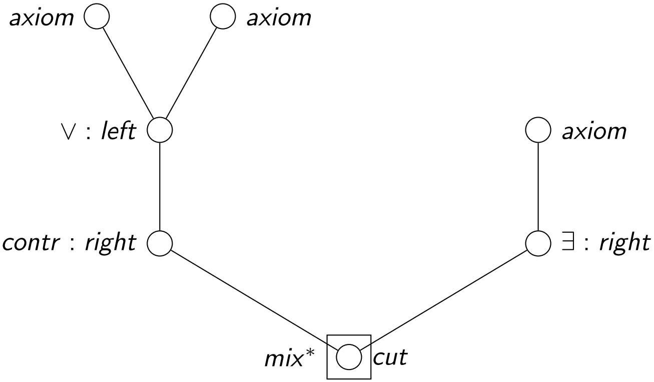
Consider $P(c) \vee P(d) \to \exists x P(x)$ (all trees have this formula as bottom node), the box denotes the *mix**:



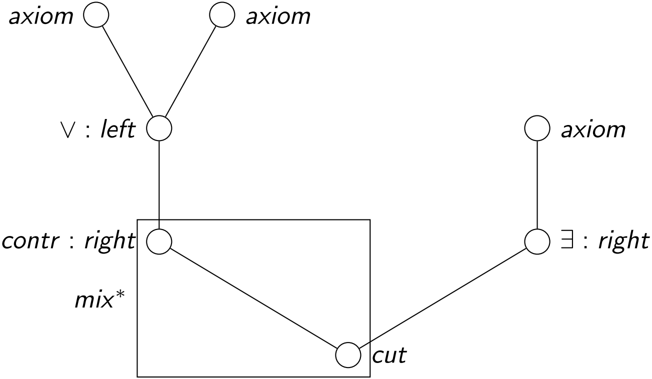
(a)

$$\Downarrow$$

(b)

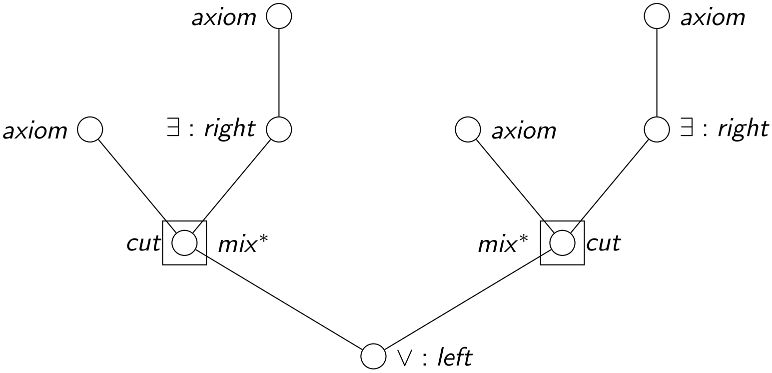


$\Downarrow$



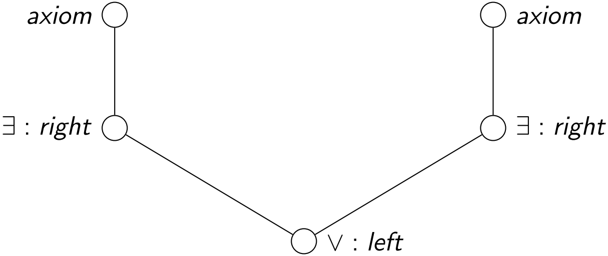
(c)

$$\Downarrow$$



(d)

$$\Downarrow$$



(*e*)

$(a) - (c)$ cannot be realized ($P(c)$ and $P(d)$ are forced to be contracted). (d) is realized by

$$\dfrac{\dfrac{P(c) \to P(c) \qquad \dfrac{P(c) \to P(c)}{P(c) \to \exists x P(x)}}{P(c) \to \exists x P(x)} \qquad \dfrac{P(d) \to P(d) \qquad \dfrac{P(d) \to P(d)}{P(d) \to \exists x P(x)}}{P(d) \to \exists x P(x)}}{P(c) \vee P(d) \to \exists x P(x)}$$

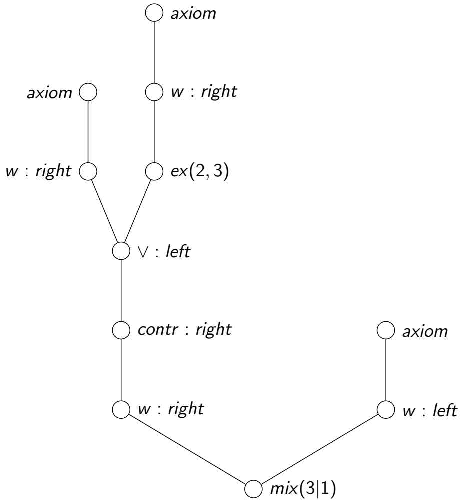
(e) is realized by

$$\dfrac{\dfrac{P(c) \to P(c)}{P(c) \to \exists x P(x)} \qquad \dfrac{P(d) \to P(d)}{P(d) \to \exists x P(x)}}{P(c) \vee P(d) \to \exists x P(x)}$$

Theorem

It is decidable for a cut-free skeleton S whether there is a proof realizing S for a given end-sequent. If there is a proof there is a most general proof.

Different cut-elimination strategies correct different proof skeleta



$$Q \lor P, R \to P, R$$

6.1265

Logic can always be conceived to be such that every proposition is its own proof.

$$\exists x A(x) \sim A(\varepsilon_x A(x))$$

$$\forall x A(x) \sim A(\varepsilon_x \neg A(x))$$

ε-translation of $\exists x \exists y \exists z A(x, y, z)$:

$A(\varepsilon_x A(x, \varepsilon_y A(x, y, \varepsilon_z\ A(x, y, z)),\ \varepsilon_z\ A(x, \varepsilon_y\ A(x, y,\ \varepsilon_z\ A(x, y, z)),$
$z)),\ \varepsilon_y\ A(\varepsilon_x\ A(x, \varepsilon_y\ A(x, y, \varepsilon_z\ A(x, y, z)),\ \varepsilon_z\ A(x, \varepsilon_y\ A(x, y, \varepsilon_z$
$A(x, y, z)), z)),\ y, \varepsilon_z\ A(\varepsilon_x\ A(x, \varepsilon_y\ A(x, y, \varepsilon_z\ A(x, y, z)),\ \varepsilon_z\ A(x, \varepsilon_y$
$A(x, y, \varepsilon_z\ A(x, y, z)), z)), y, z)),\ \varepsilon_z\ A(\varepsilon_x\ A(x, \varepsilon_y\ A(x, y, \varepsilon_z$
$A(x, y, z)), \varepsilon_z\ A(x,\ \varepsilon_y\ A(x, y,\ \varepsilon_z\ A(x, y, z)), z)),\ \varepsilon_y\ A(\varepsilon_x\ A(x, \varepsilon_y$
$A(x, y,\ \varepsilon_z\ A(x, y, z)),\ \varepsilon_z\ A(x, \varepsilon_y\ A(x, y,\ \varepsilon_z\ A(x, y, z)), z)),\ y, \varepsilon_z$
$A(\varepsilon_x\ A(x, \varepsilon_y\ A(x,\ y,\ \varepsilon_z\ A(x,\ y,\ z)),\ \varepsilon_z\ A(x, \varepsilon_y\ A(x, y, \varepsilon_z$
$A(x, y, z)), z)), y, z)), z)).$

critical formulas $A(t) \supset A(\varepsilon_x A(x))$

The translation of a first-order proof P to epsilon calculus results in a tautology

$$\bigwedge(A_i(t) \supset A_i(\varepsilon_x A_i(x)) \supset P_\varepsilon$$

Hilbert's Ansatz (Example)

$$A(t) \supset A(\varepsilon_x A(x)) \wedge A(s) \supset A(\varepsilon_x A(x)) \supset B(x)$$

$$A(t) \supset B(t)$$

$$A(s) \supset B(s)$$

$$\neg A(t) \wedge \neg A(s) \supset B(\varepsilon_x A(x))$$

$$\text{result:}\ \ B(t) \vee B(s) \vee B(\varepsilon_x A(x))$$

An ε-term e is *nested* in an ε-term e' if e is a proper subterm of e'. An ε-term e is *subordinate* to an ε-term $e' = \varepsilon_x A(x)$ if e occurs in e' and x is free in e.

The *rank* counts the subordination levels and the *degree* the length of the maximal inclusion chain.

Theorem (extended first epsilon theorem)

An epsilon proof of the translation of an existential formula can be stepwise transformed into a Herbrand disjunction.

Proof.

Induction according to the maximal rank and within the maximal rank according to the maximal degree. □

Epsilon elimination is a small error tolerant device

Theorem

Every epsilon proof of the translation of an existential formula with exactly one counter-valuation can be transformed into a disjunction where there is also at most one counter-valuation.

Proof.

Include the disjunctive normal form (one disjunction of negated and unnegated atoms) in the transformation process. □

Example

$$(A(s) \supset A(\varepsilon_x A(x)) \wedge A(t) \supset A(\varepsilon_x A(x))) \supset D(\varepsilon_x A(x))$$

$$D(x) \sim B(x) \vee \neg A(x) \vee \neg A(s) \vee \neg A(t)$$

the only counter valuation

$$A(s) = t \quad A(t) = t \quad A(\varepsilon_x A(x)) = t \quad B(\varepsilon_x A(x)) = f.$$

Consequently,
$C(\varepsilon_x A(x)) \supset (A(s) \supset A(\varepsilon_x A(x)) \wedge A(t) \supset A(\varepsilon_x A(x))) \supset D(\varepsilon_x A(x))$ is a tautology, where $C(\varepsilon_x A(x))$ is

$$\neg A(s) \vee \neg A(t) \vee \neg A(\varepsilon_x A(x)) \vee B(\varepsilon_x A(x)).$$

Consequently,
$(A(s) \supset A(\varepsilon_x A(x)) \wedge A(t) \supset A(\varepsilon_x A(x))) \supset (C(\varepsilon_x A(x)) \supset D(\varepsilon_x A(x)))$ is a tautology.

Example

Consequently,

$$B(s) \vee \neg A(s) \vee \neg A(s) \vee \neg A(t) \vee$$

$$B(t) \vee \neg A(t) \vee \neg A(s) \vee \neg A(t) \vee$$

$$B(\varepsilon_x A(x)) \vee \neg A(\varepsilon_x A(x)) \vee \neg A(s) \vee \neg A(t)$$

is valid but for the following counter valuation

$$f : A(s) = t \quad A(t) = t \quad A(\varepsilon_x A(x)) = t$$

$$B(s) = f \quad B(t) = f \quad B(\varepsilon_x A(x)) = f$$

5.511

How can the all-embracing logic which mirrors the world use such special catches and manipulations? Only because all these are connected into an infinitely fine network, to the great mirror.