TOWARDS A PROOF THEORY OF ANALOGICAL REASONING

M. BAAZ

VIENNA UNIVERSITY OF TECHNOLOGY

Analogical Reasoning in Mathematics

Euler became famous by deriving

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} \tag{1}$$

Let us consider Eulers reasoning. Consider the polynomial of even degree

$$b_0 - b_1 x^2 + b_2 x^4 - \cdots + (-1)^n b_n x^{2n} \tag{2}$$

If it has the $2n$ roots $\pm\beta_1, \ldots, \pm\beta_n \neq 0$ then (2) can be written as

$$b_0 \left(1 - \frac{x^2}{\beta_1^2}\right)\left(1 - \frac{x^2}{\beta_2^2}\right)\cdots\left(1 - \frac{x^2}{\beta_n^2}\right) \tag{3}$$

By comparing coefficients in (2) and (3) one obtains that

$$b_1 = b_0 \left(\frac{1}{\beta_1^2} + \frac{1}{\beta_2^2} + \cdots + \frac{1}{\beta_n^2}\right). \tag{4}$$

Next Euler considers the Taylor series

$$\frac{\sin x}{x} = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n+1)!} \tag{5}$$

which has as roots $\pm\pi, \pm 2\pi, \pm 3\pi, \ldots$ Now by way of analogy Euler *assumes* that the infinite degree polynomial (5) behaves in the same way as the finite polynomial (2). Hence in analogy to (3) he obtains

$$\frac{\sin x}{x} = \left(1 - \frac{x^2}{\pi^2}\right)\left(1 - \frac{x^2}{4\pi^2}\right)\left(1 - \frac{x^2}{9\pi^2}\right)\cdots \tag{6}$$

and in analogy to (4) he obtains

$$\frac{1}{3!} = \left(\frac{1}{\pi^2} + \frac{1}{4\pi^2} + \frac{1}{9\pi^2} + \cdots\right) \tag{7}$$

which immediately gives

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}. \tag{1}$$

The structure of Eulers argument is the following.

(a) $(2) = (3)$	(mathematically derivable)
(b) $(2) = (3) \supset (4)$	(mathematically derivable)
(c) $(2) = (3) \supset (5) = (6)$	(analogical hypothesis)
(d) $(5) = (6) \supset (4)$	(modus ponens)
(e) $((2) = (3) \supset (4)) \supset ((5) = (6) \supset (7))$	(analogical hypothesis)
(f) $(5) = (6) \supset (7)$	(modus ponens)
(g) (7)	(modus ponens)
(h) $(7) \supset (1)$	(mathematically derivable)
(i) (1)	(modus ponens)

We will consider analogies based on

1 Generalizations wrt. invariant parts of the proofs (e.g., graphs of rule applications)

   1.1 Generalizations of conclusions

   1.2 Generalizations of premises

2 Generalizations wrt. semantical features

The calculus LK

logical axiom schema: $A \to A$

structural inferences:

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

$$\text{weakening left}\ \frac{\Gamma \to \Delta}{A, \Gamma \to \Delta} \qquad \text{weakening right}\ \frac{\Gamma \to \Delta}{\Gamma \to \Delta, A}$$

$$\text{exchange left}\ \frac{\Gamma_1, A, B, \Gamma_2 \to \Delta}{\Gamma_1, B, A, \Gamma_2 \to \Delta} \qquad \text{exchange right}\ \frac{\Gamma \to \Delta_1, A, B, \Delta_2}{\Gamma \to \Delta_1, B, A, \Delta_2}$$

$$\text{contraction left}\ \frac{A, A, \Gamma \to \Delta}{A, \Gamma \to \Delta} \qquad \text{contraction right}\ \frac{\Gamma \to \Delta, A, A}{\Gamma \to \Delta, A}$$

logical inferences:

$$\neg\text{:left}\ \frac{\Gamma \to \Delta, A}{\neg A, \Gamma \to \Delta} \qquad \neg\text{:right}\ \frac{A, \Gamma \to \Delta}{\Gamma \to \Delta, \neg A}$$

$$\vee\text{:left}\ \frac{A, \Gamma_1 \vdash \Delta_1 \qquad B, \Gamma_2 \vdash \Delta_2}{A \vee B, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} \qquad \vee\text{:right}_1\ \frac{\Gamma \to \Delta, A}{\Gamma \to \Delta, A \vee B}$$

$$\wedge\text{:left}_1\ \frac{A, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta} \qquad \vee\text{:right}_2\ \frac{\Gamma \to \Delta, B}{\Gamma \to \Delta, A \vee B}$$

$$\wedge\text{:left}_2\ \frac{B, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta} \qquad \wedge\text{:right}\ \frac{\Gamma_1 \vdash \Delta_1, A \qquad \Gamma_2 \vdash \Delta_2, B}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, A \wedge B}$$

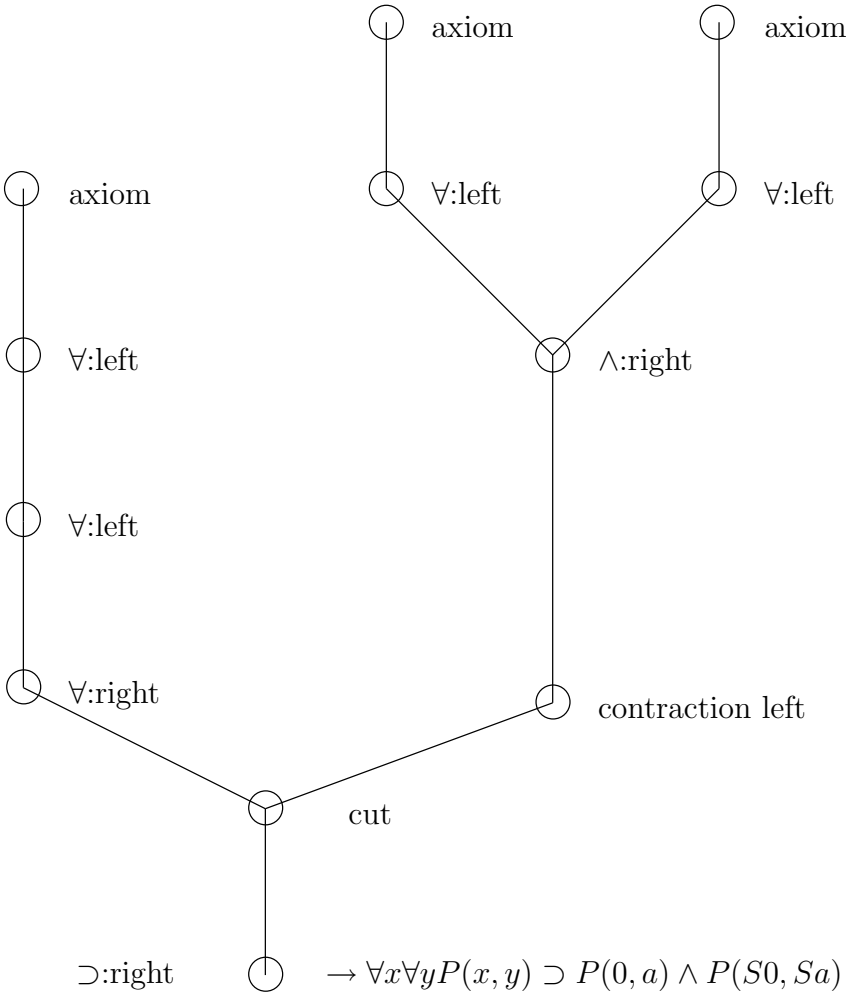
$$\supset\text{:left}\ \frac{\Gamma_1 \vdash \Delta_1, A \qquad B, \Gamma_2 \vdash \Delta_2}{A \supset B, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} \qquad \supset\text{:right}\ \frac{A, \Gamma \to \Delta, B}{\Gamma \to \Delta, A \supset B}$$

$$\exists\text{:left}\ \frac{C(e), \Gamma \to \Delta}{\exists \alpha C(\alpha), \Gamma \to \Delta} \qquad \exists\text{:right}\ \frac{\Gamma \to \Delta, C(r)}{\Gamma \to \Delta, \exists \alpha C(\alpha)}$$

$$\forall\text{:left}\ \frac{C(r), \Gamma \to \Delta}{\forall \alpha C(\alpha), \Gamma \to \Delta} \qquad \forall\text{:right}\ \frac{\Gamma \to \Delta, C(e)}{\Gamma \to \Delta, \forall \alpha C(\alpha)}$$

with the usual restrictions.

Skeleton/proof analysis



The above analysis and sequent determine an (extended) proof matrix:

$$\dfrac{\dfrac{\dfrac{P(t_1,t_2)\to P(t_1,t_2)}{\forall\beta P(s_1,s_2)\to P(t_1,t_2)}}{\forall\alpha\forall\beta P(r_1,r_2)\to P(t_1,t_2)}}{\forall\alpha\forall\beta P(r_1,r_2)\to\forall\gamma P(s,t)} \qquad \dfrac{\dfrac{\dfrac{P(r_3,r_4)\to P(r_3,r_4)}{\forall\gamma P(s,t)\to P(r_3,r_4)} \quad \dfrac{P(r_5,r_6)\to P(r_5,r_6)}{\forall\gamma P(s,t)\to P(r_5,r_6)}}{\forall\gamma P(s,t),\forall\gamma P(s,t)\to P(r_3,r_4)\wedge P(r_5,r_6)}}{\forall\gamma P(s,t)\to P(r_3,r_4)\wedge P(r_5,r_6)}$$

$$\dfrac{\forall\alpha\forall\beta P(r_1,r_2)\to\forall\gamma P(s,t) \qquad \forall\gamma P(s,t)\to P(r_3,r_4)\wedge P(r_5,r_6)}{\forall\alpha\forall\beta P(r_1,r_2)\to P(r_3,r_4)\wedge P(r_5,r_6)}$$

Then all substitutions producing proofs can be characterized by the following equations

$$r_1(\alpha) = s_1 = t_1 = s(e) \wedge r_2(\beta) = s_2(\beta) = t_2 = t(e) \wedge \\ \wedge s(\gamma_1) = r_3 \wedge t(\gamma_1) = r_4 \wedge s(\gamma_2) = r_5 \wedge t(\gamma_2) = r_6$$

(i.e., the do not occur in the matrix).

If we take into account the term structure of the end sequent, we can get rid of the restrictions and can substitute the above equations with

$$r_1(\alpha) = \alpha \quad r_2(\beta) = \beta \quad r_3 = 0 \quad r_4 = a \quad r_5 = S0 \quad r_6 = Sa.$$

Then, using the validity of $\exists\alpha\exists\beta(\alpha = s(e) \wedge \beta = t(e))$, the condition on derivability of our formula with the proof analysis reduces to

$$\exists st\exists\gamma_1\gamma_2 \left[s(\gamma_1) = 0 \wedge t(\gamma_1) = a \wedge s(\gamma_2) = S0 \wedge t(\gamma_2) = Sa\right].$$

If the above holds then $s(\gamma) = \gamma$ and $St(0) = t(S0) = Sa$. Thus, our formula is derivable with the considered analysis iff a is S^n0 for some n.

Theorem (Orevkov, Krajicek and Pudlak)**.** *For every r.e. set E, there is a skeleton S_E with universal or existential cuts and a sequent $\Pi_E \to \Gamma_E, A_E(a)$ such that*

$$\Pi_E \to \Gamma_E, A(s^n(a)) \text{ is provable with } S_E$$
$$\Updownarrow$$
$$n \in E.$$

Theorem. *Let S cutfree and $\Pi(a) \to \Gamma(a)$ be given. If there is a proof at all, there is a most general proof*

$$\frac{T}{\Pi(t) \to \Gamma(t)}$$

such that any other proof has the form

$$\frac{T\sigma}{\Pi(t\sigma) \to \Gamma(t\sigma)}.$$

Second Order Unification

Let L be a set of function symbols, $a_1, \ldots, a_m$ variables. Let $\underline{T} = (T, Sub_1, \ldots, Sub_m)$ be the algebra of terms where T is the set of terms in L, $a_1, \ldots, a_m$ and for $i = 1, \ldots, m$

$$Sub_i(\delta, \sigma) := \delta\{\sigma/a_i\}$$

are substitutions as binary operations on T. A *second order unification* is a finite set of equations in the language $T \cup \{Sub_1, \ldots, Sub_m\}$ plus free variables for elements of T.

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 E there exists a second order unification problem Ω_E such that $\Omega_E \cup \{\tau_0 = S^n(0)\}$ has a solution iff $n \in E$.*

Idea

$$\dfrac{\dfrac{\Pi \to \Gamma, P(a) \vee P(t), P(u) \vee P(v)}{\exists\text{-r}}}{\begin{array}{c}\text{exchange}\\ \exists\text{-r such that } a \text{ is not free anymore}\\ \text{contraction}\\ \text{cut with weakened formula}\end{array}} \qquad \begin{array}{c} T \\ A, \Pi \to \Gamma \end{array}$$

$$\Rightarrow v = t\{u/a\}$$

LK$_B$

Replace

$$\frac{\Pi\rightarrow\Gamma, A(a)}{\Pi\rightarrow\Gamma, \forall x A(x)} \quad \text{by} \quad \frac{\Pi\rightarrow\Gamma, A(a_1, \ldots, a_n)}{\Pi\rightarrow\Gamma, \forall x_1, \ldots, x_n A(x_1, \ldots, x_n)}$$

$$\frac{A(t), \Pi\rightarrow\Gamma}{\forall x A(x), \Pi\rightarrow\Gamma} \quad \text{by} \quad \frac{A(t_1, \ldots, t_n), \Pi\rightarrow\Gamma}{\forall x_1, \ldots, x_n A(x_1, \ldots, x_n), \Pi\rightarrow\Gamma}$$

$$\frac{\Pi\rightarrow\Gamma, A(t)}{\Pi\rightarrow\Gamma, \exists x A(x)} \quad \text{by} \quad \frac{\Pi\rightarrow\Gamma, A(t_1, \ldots, t_n)}{\Pi\rightarrow\Gamma, \exists x_1, \ldots, x_n A(x_1, \ldots, x_n)}$$

$$\frac{A(a), \Pi\rightarrow\Gamma}{\exists x A(x), \Pi\rightarrow\Gamma} \quad \text{by} \quad \frac{A(a_1, \ldots, a_n), \Pi\rightarrow\Gamma}{\exists x_1, \ldots, x_n A(x_1, \ldots, x_n), \Pi\rightarrow\Gamma}$$

n arbitrary

Theorem. *Let S contain only existential and universal cuts and let*

$$\Pi(a) \to \Gamma(a)$$

be given. If there is a proof at all, there is a most general proof

$$\frac{T}{\Pi(t) \to \Gamma(t)}$$

such that any other proof has the form

$$\frac{T\sigma}{\Pi(t\sigma) \to \Gamma(t\sigma)}.$$

Semiunification

A semiunification problem is given by a set of pairs of terms $(s_1, t_1), \ldots, (s_n, t_n)$. A solution to the semiunification problem is a substitution δ such that there exist substitutions $\sigma_1, \ldots, \sigma_n$ such that

$$s_1\delta = t_1\delta\sigma_1, \ldots, s_n = t_n\delta\sigma_n;$$

a solutions will be also called a semiunifier. A *most general semiunifier* is a semiunifier δ_0 such that for every semiunifier δ there exists a substitution δ' such that $\delta = \delta_0\delta'$ (i.e., $\delta(x) = \delta'(\delta_0(x))$).

Theorem. *If a semiunification problem has a semiunifier then it has a most general one.*

Example.

- $\{(x, s(x))\}$ *unsolvable*
- $\{(y, s(x))\}$
  solution e.g., $\delta = \{s(s(x))/y\}$
  most general solution $\delta_{mg} = \{s(x')/y\}$

Semiunification is undecidable!

$\underline{\forall x A(x) \supset A(t)}$

$$\begin{array}{ccccc} A' & & & & A'' \\ \downarrow & & \sigma & & \downarrow \\ A(a) & & & & A(t) \end{array} \qquad (t \text{ arbitrary})$$

Second-order unification problem
$A'' = A'\{x/a\}$ σ solution

$\underline{\forall x_1, \ldots, x_n A(x_1, \ldots, x_n) \supset A(t_1, \ldots, t_n)}$

$$\begin{array}{ccccc} A' & & & & A'' \\ \downarrow & & \sigma & & \downarrow \\ A(a_1, \ldots, a_n) & & & & A(t_1, \ldots, t_n) \end{array}$$

Semiunification problem
$\{(A'', A')\}$ σ solution

Theorem. *It is undecidable whether there is a proof with (non tree-like)* $\mathbf{LK}_B$*-skeleton* S *with universal/existential cuts for any instance of* $\Pi(a) \to \Gamma(a)$.

Proposition. *Let the language contain a binary function symbol f. For every semi-unification problem $\Omega = \{(s_1, t_1), \ldots, (s_p, t_p)\}$, there is a proof analysis P_Ω and a sequent $\Pi_\Omega \to \Lambda_\Omega$, s.t. there is an $\mathbf{LK}_B^{\Pi\Sigma}$-proof realizing P_Ω with end sequent $\Pi_\Omega \to \Lambda_\Omega$ iff Ω is solvable.*

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

Let $A_\Omega(a_1, \ldots, a_n) \equiv P(t) \wedge ((P(s_1^\star) \wedge \cdots \wedge P(s_p^\star)) \supset Q)$, 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:

$$\left.\begin{array}{r} \\ (a) \\ (a+1) \end{array}\right| \begin{array}{c} \\ A_\Omega(a_1, \ldots, a_n)\delta \to A_\Omega(a_1, \ldots, a_n)\delta \\ \underline{(\forall x_1) \cdots (\forall x_n) A_\Omega(x_1, \ldots, x_n)\delta \to A_\Omega(a_1, \ldots, a_n)\delta} \end{array} \quad \left|\begin{array}{l} \\ \text{propositional inferences} \end{array}\right.$$

$$\left.\begin{array}{r} \\ (b) \\ (b+1) \end{array}\right| \begin{array}{c} \\ (\forall x_1) \cdots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to P(t)\delta \\ \underline{(\forall x_1) \cdots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to (\forall y_1) \cdots (\forall y_n) R(y_1, \ldots, y_n)} \end{array} \quad \left|\begin{array}{l} \\ \text{propositional inferences including} \\ \text{propositional cuts from } (a+1) \end{array}\right.$$

$$\left.\begin{array}{r} \\ (c) \\ \\ (d) \\ (e) \\ (e+1) \end{array}\right| \begin{array}{c} \\ P(s_1^\star)\delta, \ldots, P(s_p^\star)\delta, (\forall x_1) \cdots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to Q \\ \\ (\forall z_1) \cdots (\forall z_s) R'(z_1, \ldots, z_s), (\forall x_1) \cdots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to Q \\ (\forall x_1) \cdots (\forall x_n) A_\Omega(x_1, \ldots, x_s), (\forall x_1) \cdots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to Q \\ (\forall x_1) \cdots (\forall x_n) A_\Omega(x_1, \ldots, x_n) \to Q \end{array} \quad \left|\begin{array}{l} \\ \text{propositional inferences including} \\ \text{propositional cuts from } (a+1) \\ \\ p\ (\forall_B\text{-left})\text{-inferences, exchanges} \\ \text{and contractions from } (c) \end{array}\right.$$

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 $(\forall y_1) \cdots (\forall y_m) R(y_1, \ldots, y_m) \equiv (\forall z_1) \cdots (\forall z_s) R'(z_1, \ldots, z_s)$ 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.) $\square$

More complex cuts

Generalizations are not obtainable from the skeletons and potential end-sequents alone

$$S \xrightarrow[\text{cut-elimination}]{} \underset{\text{cut-free}}{S'} \xrightarrow[\text{inversion of cut-elimination}]{} S$$

Propositional Calculi

Proposition. *For every Hilbert-system and every skeleton S, there is a most general proof with a most general result if there is a proof at all in accordance with S.*

However, admit in classical logic schemata/rules of the kind

$$\frac{A(\top) \quad A(\bot)}{A(B)}$$

$$\text{or } A \leftrightarrow B \supset (C(A) \leftrightarrow C(B))$$

$$\text{or } \frac{A \leftrightarrow B}{C(A) \leftrightarrow C(B)}$$

Then the following holds:

Theorem. *Let $TAUT_n$ be tautologies with $\leq n$ variables.*

$$\forall n \exists k \forall A \in TAUT_n \vdash^k A$$

Idea

First derive uniformly all tautologies without variables (assume that $\top$ and $\bot$ are present).
Let ΔA be defined by replacing all innermost

$$\top \wedge \top, \top \wedge \bot, \ldots, \top \supset \top, \top \supset \bot, \ldots \text{ in } A \text{ by } \top, \bot, \ldots, \top, \bot, \ldots$$

Consider the sequence

$$\begin{array}{c} A \leftrightarrow \underbrace{(\Delta A \leftrightarrow \cdots (\Delta^{k-1} A \leftrightarrow \Delta^k A) \cdots)}_{\star} \\ \updownarrow \\ \Delta A \leftrightarrow \Delta^2 A \leftrightarrow (\cdots (\top \leftrightarrow \top) \cdots) \\ \updownarrow \\ \underbrace{\Delta A \leftrightarrow \Delta^2 A \leftrightarrow \top \cdots)}_{\star} \end{array}$$

Therefore $(A \leftrightarrow \star) \leftrightarrow \star$, i.e., A

Now introduce variables by the case distinction $(\star \leftrightarrow \top) \vee (\star \leftrightarrow \bot)$.

Summary

Analogies based on generalizations wrt. invariant parts of the proofs are very sensitive to details of the description of the invariant parts. Natural candidates are general proofs obtained from the inversion of cut-elimination.

$F_5 = 4294967297$ is compound:

$$\begin{aligned}
5 \cdot 2^7 + 1 &\equiv 0 \pmod{5 \cdot 2^7 + 1} \\
5 \cdot 2^7 &\equiv -1 \pmod{5 \cdot 2^7 + 1} \\
5^4 \cdot 2^{7 \cdot 4} &\equiv 1 \pmod{5 \cdot 2^7 + 1} \\
5^4 + 2^4 &= 5 \cdot 2^7 + 1 \\
5^4 &\equiv -2^4 \pmod{5 \cdot 2^7 + 1} \\
1 \equiv 5^4 \cdot 2^{7 \cdot 4} &\equiv \underbrace{-2^4 \cdot 2^{7 \cdot 4}}_{-2^{2^5}} \pmod{\underbrace{(5 \cdot 2^7 + 1)}_{641}}
\end{aligned}$$

The result can be derived immediately by direct division.

$$2^{2^5} + 1 = 641 \cdot 6700417$$

Definition. *A* calculation in $\mathcal{K}$ *is a finite tree of closed quantifier-free formulas different from* $\mathbf{T}$*, valid in* $\mathcal{K}$*. The bottom formula is the* result *of the calculation. If* $A_1, \ldots, A_m$ *are direct predecessors of* A *in the calcuation then* $\langle A_1, \ldots, A_m \mid A \rangle$ *is a calculation step.*

Example. *Consider the class of Boolean Algebras* $\mathcal{B}$ *with signature* $\langle \mathbf{Val}(.), =, \mathbf{1}, -, \cap, \cup, \rightarrow \rangle$*.* $\mathbf{Val}(x)$ *is defined by* $x = \mathbf{1}$*.*

The following trees of formulas are calculations in $\mathcal{B}$*:*

$$\frac{\mathbf{Val}(\mathbf{1} \rightarrow \mathbf{1})}{\mathbf{Val}((\mathbf{1} \rightarrow \mathbf{1}) \cup (\mathbf{1} \rightarrow \mathbf{1}))}$$

$$\frac{\dfrac{\mathbf{Val}(\mathbf{1} \cup -\mathbf{1})}{\mathbf{Val}((\mathbf{1} \rightarrow \mathbf{1}) \cup -\mathbf{1})}}{\mathbf{Val}((\mathbf{1} \rightarrow \mathbf{1}) \cup (\mathbf{1} \rightarrow \mathbf{1}))}$$

Definition. *Let*

$$\langle \bar{A}_1, \ldots, \bar{A}_m \rangle \Rightarrow \langle A_1, \ldots, A_m \rangle$$

iff there exists a σ *s.t.* $\bar{A}_i\sigma = A_i$ *for* $\bar{A}_i \neq \mathbf{T}$. *Let* $\langle A_1, \ldots, A_m \mid A \rangle$ *be a calculation step of a calculation in* $\mathcal{K}$.

Then $\langle \bar{A}_1, \ldots, \bar{A}_m \mid \bar{A} \rangle$ *is an* abstraction *of* $\langle A_1, \ldots, A_m \mid A \rangle$ *iff*

1. $\langle \bar{A}_1, \ldots, \bar{A}_m \mid \bar{A} \rangle \Rightarrow \langle A_1, \ldots, A_m \mid A \rangle$
2. $\mathcal{K} \models \forall x_1 \cdots x_r (\bigwedge_{\bar{A}_i \neq \mathbf{T}} \bar{A}_i \rightarrow \bar{A})$ *s.t.* $x_1, \ldots, x_r$ *are all the free variables in* $\langle \bar{A}_1, \ldots, \bar{A}_m \mid \bar{A} \rangle$.

$\langle \bar{A}_1, \ldots, \bar{A}_m \mid \bar{A} \rangle$ *is* proper *iff* $\bar{A} \neq A$. $\langle \bar{A}_1, \ldots, \bar{A}_m \mid \bar{A} \rangle$ *is* general *iff it is proper and there is no abstraction* $\langle A'_1, \ldots, A'_m \mid A' \rangle$ *s.t.* $\langle A'_1, \ldots, A'_m \mid A' \rangle \Rightarrow \langle \bar{A}_1, \ldots, \bar{A}_m \mid \bar{A} \rangle$ *but not* $\langle \bar{A}_1, \ldots, \bar{A}_m \mid \bar{A} \rangle \Rightarrow \langle A'_1, \ldots, A'_m \mid A' \rangle$.

Example.

$$\frac{\mathbf{Val}(\mathbf{1} \to \mathbf{1})}{\mathbf{Val}((\mathbf{1} \to \mathbf{1}) \cup (\mathbf{1} \to \mathbf{1}))}$$

original calculation step	*general abstractions*
$\langle \mathbf{Val}(\mathbf{1} \to \mathbf{1}) \rangle$	$\langle \mathbf{Val}(x \to x) \rangle$
$\langle \mathbf{Val}(\mathbf{1} \to \mathbf{1}) \mid \mathbf{Val}((\mathbf{1} \to \mathbf{1}) \cup (\mathbf{1} \to \mathbf{1})) \rangle$	$\langle \mathbf{1} \mid \mathbf{Val}((x \to x) \cup y) \rangle$ $\langle \mathbf{1} \mid \mathbf{Val}(y \cup (x \to x)) \rangle$ $\langle \mathbf{Val}(x) \mid \mathbf{Val}(x \cup y) \rangle$ $\langle \mathbf{Val}(y) \mid \mathbf{Val}(y \cup x) \rangle$

Example.

$$\dfrac{\dfrac{\mathbf{Val}(\mathbf{1} \cup -\mathbf{1})}{\mathbf{Val}((\mathbf{1} \to \mathbf{1}) \cup -\mathbf{1})}}{\mathbf{Val}((\mathbf{1} \to \mathbf{1}) \cup (\mathbf{1} \to \mathbf{1}))}$$

original calculation step	*general abstractions*
$\langle \mathbf{Val}(\mathbf{1} \cup -\mathbf{1}) \rangle$	$\langle \mathbf{Val}(x \cup -x) \rangle$
$\langle \mathbf{Val}(\mathbf{1} \cup -\mathbf{1}) \mid \mathbf{Val}((\mathbf{1} \to \mathbf{1}) \cup -\mathbf{1}) \rangle$	$\langle \mathbf{1} \mid \mathbf{Val}((x \to x) \cup y) \rangle$ $\langle \mathbf{Val}(x \cup y) \mid \mathbf{Val}((z \to x) \cup y) \rangle$
$\langle \mathbf{Val}((\mathbf{1} \to \mathbf{1}) \cup -\mathbf{1}) \mid \mathbf{Val}((\mathbf{1} \to \mathbf{1}) \cup (\mathbf{1} \to \mathbf{1})) \rangle$	$\langle \mathbf{1} \mid \mathbf{Val}((x \to x) \cup y) \rangle$ $\langle \mathbf{1} \mid \mathbf{Val}(y \cup (x \to x)) \rangle$ $\langle \mathbf{Val}(x \cup -y) \mid \mathbf{Val}(x \cup (y \to z)) \rangle$

Definition. *The* generalization *of a calculation in $\mathcal{K}$ is defined as follows:*

1. *If there are no general abstractions for a calculation step corresponding to a node and its immediate predecessors, then assign the matrix of the original formula to the node and remove all nodes in the sub-tree above.*

2. *For every node and its immediate predecessors in the (pruned) calculation tree select a general abstraction of the corresponding calculation step and assign the formulas of the abstraction to the nodes.*

3. *If* $\mathbf{T}$ *is assigned to a node, then remove this node and the sub-tree above.*

4. *Unify all pairs of formulas that have been assigned to the same node; this unification is processed simultaneously.*

Theorem. *Let C be a calculation in $\mathcal{K}$.*

1. *There are finitely many generalizations $G_1, \ldots, G_m$ of C with results*

$$\begin{array}{rcl} A_{11}, \ldots, A_{1n_1} & \triangleright & A_1 \\ & \vdots & \\ A_{m1}, \ldots, A_{mn_m} & \triangleright & A_m \end{array}$$

   s.t. $\mathcal{K} \models \forall x_1 \cdots x_r(\bigwedge A_{ij} \to A_i)$, for all $1 \leq i \leq m$, $1 \leq j \leq n_i$.

2. *C can be obtained from G_i by instantiation and addition of sub-calculations.*

Example.

$$\frac{\mathbf{Val}(\mathbf{1} \to \mathbf{1})}{\mathbf{Val}((\mathbf{1} \to \mathbf{1}) \cup (\mathbf{1} \to \mathbf{1}))}$$

$\mathbf{Val}((x \to x) \cup y)$	$\sigma = \epsilon$	$\mathbf{Val}((x \to x) \cup y)$
$\mathbf{Val}(y \cup (x \to x))$	$\sigma = \epsilon$	$\mathbf{Val}(y \cup (x \to x))$
$\dfrac{\dfrac{\mathbf{Val}(x \to x)}{\mathbf{Val}(\bar{x})}}{\mathbf{Val}(\bar{x} \cup y)}$	$\sigma = \{\bar{x} \mapsto (x \to x)\}$	$\dfrac{\mathbf{Val}(x \to x)}{\mathbf{Val}((x \to x) \cup y)}$
$\dfrac{\dfrac{\mathbf{Val}(x \to x)}{\mathbf{Val}(\bar{x})}}{\mathbf{Val}(y \cup \bar{x})}$	$\sigma = \{\bar{x} \mapsto (x \to x)\}$	$\dfrac{\mathbf{Val}(x \to x)}{\mathbf{Val}(y \cup (x \to x))}$

Example.

$$\dfrac{\dfrac{\mathbf{Val}(\mathbf{1} \cup \mathbf{-1})}{\mathbf{Val}((\mathbf{1} \to \mathbf{1}) \cup \mathbf{-1})}}{\mathbf{Val}((\mathbf{1} \to \mathbf{1}) \cup (\mathbf{1} \to \mathbf{1}))}$$

$\mathbf{Val}((x \to x) \cup y)$	$\sigma = \epsilon$	$\mathbf{Val}((x \to x) \cup y)$
$\mathbf{Val}(y \cup (x \to x))$	$\sigma = \epsilon$	$\mathbf{Val}(y \cup (x \to x))$
$\dfrac{\dfrac{\mathbf{Val}((x \to x) \cup y)}{\mathbf{Val}(\bar{x} \cup -\bar{y})}}{\mathbf{Val}(\bar{x} \cup (\bar{y} \to z))}$	$\sigma = \{\bar{x} \mapsto (x \to x), y \mapsto -\bar{y}\}$	$\dfrac{\mathbf{Val}((x \to x) \cup -\bar{y})}{\mathbf{Val}((x \to x) \cup (\bar{y} \to z))}$
$\dfrac{\dfrac{\dfrac{\mathbf{Val}(x \cup -x)}{\mathbf{Val}(x' \cup y')}}{\mathbf{Val}((\bar{z} \to x') \cup y')}}{\mathbf{Val}(\bar{x} \cup -\bar{y})}}{\mathbf{Val}(\bar{x} \cup (\bar{y} \to z))}$	$\sigma = \{x' \mapsto x, y' \mapsto -x, \bar{y} \mapsto x, \bar{x} \mapsto (\bar{z} \to x)\}$	$\dfrac{\dfrac{\mathbf{Val}(x \cup -x)}{\mathbf{Val}((\bar{z} \to x) \cup -x)}}{\mathbf{Val}((\bar{z} \to x) \cup (x \to z))}$

We formalize Euler's calculation in $\langle \mathbf{Z}, \mathbb{N} \mid +, \cdot, -, \exp, r, \widehat{\mathbb{N}} \rangle$. where

$+$	$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$
$\cdot$	$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$
$-$	$\mathbf{Z} \to \mathbf{Z}$
exp	$\mathbf{Z} \times \mathbb{N} \to \mathbf{Z}$, $\exp(x, y)$ is also denoted as x^y
r	$\mathbf{Z} \times \mathbf{Z} \times \mathbb{N} \to \mathbf{Z}$, where $r(x, y, z)$ is defined by $\sum_{k=0}^{z-1} \binom{z}{k} x^k y^{z-k-1}$ i.e. $(x+y)^2 = x^2 + r(x, y, z) \cdot y$, for $z \geq 0$
$\widehat{\mathbb{N}}$	$\mathbb{N}$, contains constants for all natural numbers

The calculation of Euler in the modified language:

$$\dfrac{\dfrac{\dfrac{\dfrac{5\cdot 2^7+1=\overbrace{5\cdot 2^7+1}^{D}}{5\cdot 2^7=-1+D}\quad 4=2\cdot 2}{5^4\cdot 2^{7\cdot 4}=1+\overbrace{r(-1,D,4)}^{E}\cdot D}\quad \dfrac{\dfrac{5^4+2^4=D}{5^4=-2^4+D}}{5^4\cdot 2^{7\cdot 4}=-2^4\cdot 2^{7\cdot 4}+2^{7\cdot 4}\cdot D}}{1+E\cdot D=-2^4\cdot 2^{7\cdot 4}+2^{7\cdot 4}\cdot D}}{2^{7\cdot 4+4}+1=(-E+2^{7\cdot 4})\cdot D}\qquad 7\cdot 4+4=2^5}{2^{2^5}+1=(-E+2^{7\cdot 4})\cdot D}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{x_1 = x_1}{x_2 + y_2 = z_2}}{x_2 = -y_2 + z_2}}{x_4 \cdot y_4^{a_4} = (-1) + v_4} \quad \dfrac{x_3 = y_3(\star)}{b_4 = 2 \cdot c_4}}{x_4^{b_4} \cdot y_4^{a_4 b_4} = 1 + r(-1, v_4, b_4) \cdot v_4}}{x_8 = y_8} \Pi \dfrac{\dfrac{\dfrac{\dfrac{x_5 = y_5(\star)}{x_6 + y_6 = z_6}}{x_6 = -y_6 + z_6}}{x_7 = -y_7 + z_7}}{x_7 \cdot w_7 = -(y_7 \cdot w_7) + w_7 \cdot z_7}}{x_8 = z_8}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{y_8 = z_8}{u_9 + v_9 \cdot w_9 = -(x_9^{y_9} \cdot x_9^{z_9}) + a_9 \cdot w_9}}{x_9^{y_9 + z_9} + u_9 = (-v_9 + a_9) \cdot w_9}}{x_{11}^{u_{11}} + v_{11} = w_{11}} \quad \dfrac{x_{10} = y_{10}(\star)}{u_{11} = y_{11}}}{x_{11}^{y_{11}} + v_{11} = w_{11}}$$

$x_1 \mapsto \hat{D}$	$c_4 \mapsto x$	$z_7 \mapsto \hat{D}$	$a_9 \mapsto 2^{uy}$
$x_2 \mapsto v \cdot 2^u$	$v_4 \mapsto \hat{D}$	$x_8 \mapsto v^y \cdot 2^{uy}$	$x_{10} \mapsto r + u \cdot y$
		$y_8 \mapsto 1 + \overbrace{r(-1, \hat{D}, y)}^{\hat{E}} \cdot \hat{D}$	
$y_2 \mapsto 1$	$x_5 \mapsto v^y + 2^r$		$y_{10} \mapsto 2^n$
$z_2 \mapsto \hat{D}$	$y_5 \mapsto \hat{D}$	$z_8 \mapsto -2^r \cdot 2^{uy} + 2^{uy} \cdot \hat{D}$	$x_{11} \mapsto 2$
$x_3 \mapsto y$	$x_6 \mapsto v^y$	$u_9 \mapsto 1$	$u_{11} \mapsto r + u \cdot y$
$y_3 \mapsto 2 \cdot x$	$y_6 \mapsto 2^r$	$v_9 \mapsto \hat{E}$	$v_{11} \mapsto 1$
$x_4 \mapsto v$	$z_6 \mapsto \hat{D}$	$w_9 \mapsto \hat{D}$	$w_{11} \mapsto -\hat{E} + 2^{uy} \cdot \hat{D}$
$y_4 \mapsto 2$	$x_7 \mapsto \hat{D}$	$x_9 \mapsto 2$	
$a_4 \mapsto u$	$y_7 \mapsto 2^r$	$y_9 \mapsto r$	
$b_4 \mapsto y$	$w_7 \mapsto 2^{uy}$	$z_9 \mapsto u \cdot y$	

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{v\cdot 2^u+1=\overbrace{v\cdot 2^u+1}^{\hat{D}}}}{v\cdot 2^u=-1+\hat{D}}\quad y=2\cdot x}{v^y\cdot 2^{uy}=1+\overbrace{r(-1,\hat{D},4)}^{\hat{E}}\cdot\hat{D}}\quad\dfrac{\dfrac{}{v^y+2^r=\hat{D}}}{v^y=-2^r+\hat{D}}}{v^y\cdot 2^{uy}=-2^r\cdot 2^{uy}+2^{uy}\cdot\hat{D}}}{1+\hat{E}\cdot\hat{D}=-2^r\cdot 2^{uy}+2^{uy}\cdot\hat{D}}}{2^{r+uy}+1=(-\hat{E}+2^{uy})\cdot\hat{D}}\qquad r+u\cdot y=y_{11}}{2^{y_{11}}+1=(-\hat{E}+2^{uy})\cdot\hat{D}}$$

The result of the generalization is

$$y=2\cdot x, v^y+2^r=\hat{D}, r+u\cdot y=y_{11}\ \triangleright\ 2^{y_{11}}+1=(-\hat{E}+2^{uy})\cdot\hat{D}$$

Theorem. *F_n can be shown to be compound using Eulers method iff the following equations can be solved.*

$$v^{2x} + 2^r = v \cdot 2^{n+2} + 1 \quad \text{and} \quad (n+2) \cdot 2x + r = 2^n$$

with $v \neq 0, v \neq 2^{2^n-(n+2)}$.

Proof. If follows from the result of the generalization that $y = 2x$, $v^y + 2^r = v \cdot 2^u + 1$, $r + u \cdot y = 2^{y_{11}}$. To apply the generalization to Euler's factorization substitute 2^n for y_{11}. Moreover it is known that all divisors of F_n are of the form $v \cdot 2^{n+2} + 1$, hence $u \mapsto n + 2$. $v \neq 0, v \neq 2^{2^n-(n+2)}$ eliminates the in-genuine divisors. □

Summary

Analogies based on generalizations wrt. the underlying semantics are mathematically strong because they represent an universal bookkeeping of all possible parameters. Theoretically, they are in general not even calculable.

The main logical problem of legal reasoning lies in the conflict of the following:

(i) Arguments should be demonstrably sound.

(ii) Decisions have to be achieved within a priori limited time and space.

The solution is provided by minimalist systems such as English Common Law and maximalist systems such as continental legal systems. In minimalist systems, completeness is achieved by the admitted generation of legal norms from juridical decisions (stare decis), which logically represent preconditions of the decisions (ratio decidendi) in the sense of incomplete reasoning. In maximalist systems extensive interpretations treat the inherent incompleteness of the system. The system obtains stability by the application of teleological interpretations, which restrict the derivable conclusions in conflicting situations.

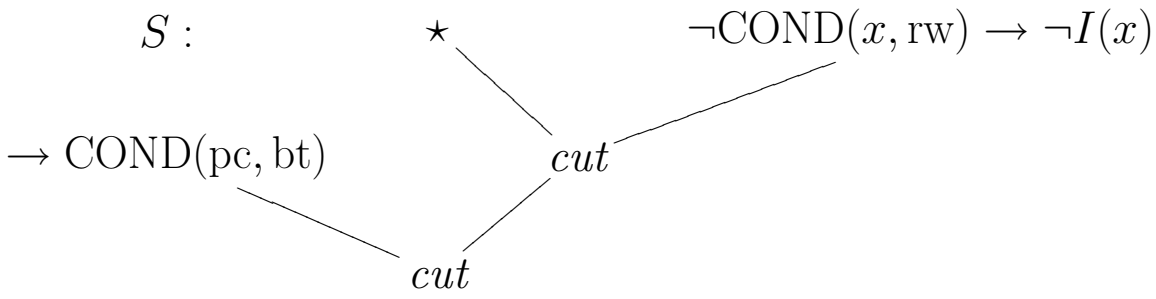
Wambaugh's test

"First frame carefully the supposed proposition of law. Let him then insert in the proposition a word reversing its meaning. Let him then inquire, whether, if the court had conceived this new proposition to be good, and had had it in mind, the decision would have been the same. If the answer be affirmative, then, however excellent the original proposition may be, the case is not a precedent for that proposition, but if the answer be negative the case is a precedent for the original proposition and possibly for the other proposition also. In short, when a case turns only on one point the proposition or doctrine of the case, the reason for the decision, the *ratio decidendi*, must be a general rule without which the case must have been decided otherwise."

Example (Brown versus Zürich Insurance (1997))**.** *The plaintiff claimed compensation for a car which was denied given the established principle that a car is not insured if it is not in roadworthy condition and the fact that the plaintiff's car had bald tires. The formalization of this decision look as follows.*

pc	*plaintiff's car*
bt	*bald tires*
rw	*roadworthy*
$I(x)$	*x is insured*
$\mathrm{COND}(x, y)$	*x is in condition y*

$$\dfrac{\dfrac{\mathrm{COND}(\mathrm{pc},\mathrm{bt}) \to \neg\mathrm{COND}(\mathrm{pc},\mathrm{rw}) \qquad \neg\mathrm{COND}(\mathrm{pc},\mathrm{rw}) \to \neg I(\mathrm{pc})}{\mathrm{COND}(\mathrm{pc},\mathrm{bt}) \to \neg I(\mathrm{pc})} \qquad \to \mathrm{COND}(\mathrm{pc},\mathrm{bt})}{\neg I(\mathrm{pc})}$$



$$T = \{\to \mathrm{COND}(\mathrm{pc},\mathrm{bt}), \neg\mathrm{COND}(x,\mathrm{rw}) \to \neg I(x)\}$$
$$E = \{\neg I(\mathrm{pc})\}$$
$$\Gamma = \{\mathrm{pc}\}$$

$$\dfrac{\to X \qquad \dfrac{X \to Y \qquad Y \to \neg I(\mathrm{pc})}{X \to \neg I(\mathrm{pc})}}{\neg I(\mathrm{pc})}$$

$$\sigma = \{\mathrm{COND}(\mathrm{pc},\mathrm{bt})/X, \neg\mathrm{COND}(\mathrm{pc},\mathrm{rw})/Y\}$$
$$(S, T, E, \Gamma) \vdash \mathrm{COND}(x,\mathrm{bt}) \to \neg\mathrm{COND}(x,\mathrm{rw})$$

Summary

Proof theoretic methods are useful to determine weakest preconditions which are essential to formal juridical reasoning, but less to mathematics. Not much is known about the structure of the set of all preconditions. Here mathematics begins.

Some References

[1] Krajicek, J. and Pudlak, P.: The number of proof lines and the size of proofs in first order logic. Arch. Math. Logic 27 (1988) 69–84

[2] Cross, R. and Harris, J. W.: Precedent in English law, 4th edition, Claredon Law Series, Oxford University Press 1991

[3] Baaz, M. and Zach, R.: Algorithmic structuring of cut-free proofs. Computer Science Logic. 6th Workshop, CSL'92. San Miniato. Selected papers (Springer, Berlin, 1993) 29–42

[4] Baaz, M.: Note on the existence of most general semiunifiers. In P. Clote and J. Krajicek, eds., Proof Theory and Computational Complexity, pages 20-29. Oxford Univ. Press, 1993

[5] Baaz, M. and Zach, R.: Short proofs of tautologies using the schema of equivalence. Computer Science Logic. 7th Workshop, CSL'93. Swansea. Selected papers (Springer, Berlin, 1994) 33–35

[6] Baaz, M. and Zach, R.: Generalizing theorems in real closed fields. Annals of Pure and Applied Logic **75** (1995) 3–23

[7] Baaz, M.: Note on Formal Analogical Reasoning in the Juridical Context. Computer Science Logic. 19th Workshop, CSL 2005. Oxford. Lecture Notes in Computer Science 3634 (Springer 2005) 18–26