Epsilon Calculus I

"In the ε-calculus it is hard to understand anything"[1]

Georg Moser

Department of Computer Science
University of Innsbruck

International Summer School for Proof Theory in First-Order Logic,
August. 22–27, 2017

[1] © Michel Parigot

Summary

Lemma (Embedding Lemma)

if π is a regular PC_ε-proof of A then there is an EC_ε-proof π^ε of A^ε with $\mathrm{sz}(\pi^\varepsilon) \leqslant 3 \cdot \mathrm{sz}(\pi)$ *and* $\mathrm{cc}(\pi^\varepsilon) \leqslant \mathrm{cc}(\pi)$

Theorem (First Epsilon Theorem)

suppose $E(e_1, \ldots, e_m)$ is a quantifier-free formula containing only the ε-terms $s_1, \ldots, s_m$, and $\mathrm{EC}_\varepsilon \vdash_\pi E(s_1, \ldots, s_m)$ Then there are ε-free terms t^i_j such that

$$\mathrm{EC} \vdash \bigvee_{i=1}^{n} E(t^i_1, \ldots, t^i_m)$$

where $n \leqslant 2^{3 \cdot \mathrm{cc}(\pi)}_{2 \cdot \mathrm{cc}(\pi)}$

Outline

The First Epsilon Theorem (without =)

Simplifications

- suppose $\mathrm{EC}_\varepsilon \vdash_\pi E$ and E contains no ε-terms
- we show that $\mathrm{EC} \vdash E$ by induction on the rank and degree of π. w.l.o.g. we assume π doesn't contain any free variables (replace free variables by new constants—may be resubstituted later)

Lemma

Let e be a critical ε-term of π of maximal degree among the critical ε-terms of maximal rank. Then there is π_e with end formula A so that $\mathrm{rk}(\pi_e) \leqslant \mathrm{rk}(\pi)$, $\deg(\pi_e) \leqslant \deg(\pi)$ *and* $o(\pi_e, \mathrm{rk}(e)) = o(\pi, \mathrm{rk}(e)) - 1$

Proof of Lemma.

Construct π_e as follows:

1. Suppose $A(t_1) \to A(e)$, ..., $A(t_n) \to A(e)$ are all the critical formulas belonging to e. For each critical formula ($i = 1, \ldots, n$)

$$A(t_i) \to A(e)$$

we obtain a derivation

$$\pi_i \vdash A(t_i) \to E$$

as follows:

- Replace e everywhere it occurs by t_i. Every critical formula $A(t) \to A(e)$ belonging to e turns into a formula of the form $B \to A(t_i)$
- Add $A(t_i)$ to the axioms. Now every such formula is derivable using the propositional tautology $A(t_i) \to (B \to A(t_i))$ and modus ponens
- Apply the deduction theorem for the propositional calculus to obtain π_i

Proof (cont'd).

2. Obtain a derivation π' of

$$\bigwedge \neg A(t_i) \to E$$

by:

- Add $\bigwedge \neg A(t_i)$ to the axioms. Now every critical formula $A(t_i) \to A(e)$ belonging to e is derivable using the propositional tautology $\neg A(t_i) \to (A(t_i) \to A(e))$.
- Apply the deduction theorem to obtain π'

3. Combine the proofs

$$\pi_i \vdash A(t_i) \to E$$

and

$$\pi' \vdash \bigwedge \neg A(t_i) \to E$$

to get $\pi_e \vdash E$ (case distinction) ■

Why is this correct?

We start with critical formulas of the form $A(t_i) \to A(e)$ ($i = 1, \ldots, n$)

Facts

- The proof π' does not contain any critical formulas belonging to e. Hence e is no longer a critical ε-term in π'. All other critical formulas (and the critical ε-terms they belong to) remain unchanged. Thus $o(\pi', \mathrm{rk}(e)) = o(\pi, \mathrm{rk}(e)) - 1$.
- In the construction of π_i, we substitute e by t throughout the proof. We will show that such uniform substitutions of a term by another are proof-preserving.
- Replacing e by t_i in $A(e)$ indeed results in $A(t_i)$, since e cannot occur in $A(x)$—else $e = \varepsilon_x A(x)$ would be a proper subterm of itself, which is impossible.
- If e appears in another critical formula $B(s) \to B(\varepsilon_y B(y))$, we have three cases.

Case I

Case: e occurs only in s

Replacing e by t_i results in a critical formula

$$B(s') \to B(\varepsilon_y B(y))$$

The new critical critical formula belongs to the same ε-term as the original formula.

Hence $o(\pi_i, \mathrm{rk}(e)) = o(\pi, \mathrm{rk}(e)) - 1$ ■

Case II

Case: e may occur in $B(y)$ and perhaps also in s, but contains neither s nor $\varepsilon_y B(y)$, in other words, the affected critical formula has the form

$$B'(s'(e), e) \to B'(\varepsilon_y B'(y, e), e)$$

Replacing e by t_i results in a different critical formula

$$B'(s'(t_i), t_i) \to B'(\varepsilon_y B'(y, t_i), t_i)$$

belonging to the ε-term $\varepsilon_y B'(y, t_i)$ which has the same rank as

$$e' = \varepsilon_y B'(y, e)$$

Further note that the ε-term e' is of higher degree than e. By our assumptions, this implies that $\mathrm{rk}(\varepsilon_y B'(y, e)) < \mathrm{rk}(e)$. Thus also $\mathrm{rk}(\varepsilon_y B'(y, t_i)) < \mathrm{rk}(e)$

Thus, again $o(\pi_i, \mathrm{rk}(e)) = o(\pi, \mathrm{rk}(e)) - 1$ ∎

Case III

Case: e does contain s or $\varepsilon_y B(y)$, then e is of the form

$$e'(s) \quad \text{or} \quad e'(\varepsilon_y B(y))$$

and $B(a)$ is really of the form $B'(e'(a))$ where $e'(a)$ is an ε-term of the same rank as e.

Then $\varepsilon_y B(y)$ has the form $\varepsilon_y B'(e'(y))$, to which the ε-expression $e'(y)$ is subordinated. But then $\varepsilon_y B'(e'(y))$ has higher rank than $e'(y)$, which has the same rank as e. By assumption this cannot happen. ∎

Lemma (revisited)

Let e be a critical ε-term of π of maximal degree among the critical ε-terms of maximal rank. Then there is π_e with end formula A so that $\mathrm{rk}(\pi_e) \leqslant \mathrm{rk}(\pi)$, $\deg(\pi_e) \leqslant \deg(\pi)$ and $o(\pi_e, \mathrm{rk}(e)) = o(\pi, \mathrm{rk}(e)) - 1$

Proof.

Finally the lemma follows: In all of the cases considered one ε-critical term of $\mathrm{rk}(e)$ was removed and other ε-critical terms of $\mathrm{rk}(e)$ remained equal. Thus $o(\pi_e, \mathrm{rk}(e)) = o(\pi, \mathrm{rk}(e)) - 1$ holds. ∎

Proof of Simplified First Epsilon Theorem.

- By induction on $\mathrm{rk}(\pi)$.
- If $\mathrm{rk}(\pi) = 0$, there is nothing to prove (no critical formulas).
- If $\mathrm{rk}(\pi) > 0$ and the order of π wrt. $\mathrm{rk}(\pi)$ is m, then m-fold application of the lemma results in a derivation π' of rank $< \mathrm{rk}(\pi)$.

∎

Theorem (First Epsilon Theorem)

suppose $E(e_1, \dots, e_m)$ is a quantifier-free formula containing only the ε-terms $s_1, \dots, s_m$, and $\mathrm{EC}_\varepsilon \vdash_\pi E(s_1, \dots, s_m)$ Then there are ε-free terms t^i_j such that

$$\mathrm{EC} \vdash \bigvee_{i=1}^{n} E(t^i_1, \dots, t^i_m)$$

where $n \leqslant 2^{3 \cdot \mathrm{cc}(\pi)}_{2 \cdot \mathrm{cc}(\pi)}$

Proof.

- suppose now the endformula E does contain ε-term
- ε-elimination method produces Herbrand disjunction of E by construction

∎

Theorem (Extended First Epsilon Theorem)

If $\exists x_1 \dots \exists x_k E(x_1, \dots, x_k)$ is a purely existential formula containing only the bound variables $x_1, \dots, x_k$, and $\mathrm{PC}^{\varepsilon} \vdash \exists x_1 \dots \exists x_k E(x_1, \dots, x_k)$ then there are terms t_{ij} such that

$$\mathrm{EC} \vdash \bigvee_{i=1}^{n} E(t_1^i, \dots, t_m^i)$$

where $n \leqslant 2^{3 \cdot \mathrm{cc}(\pi)}_{2 \cdot \mathrm{cc}(\pi)}$

Proof.

- consider $\mathrm{PC}^{\varepsilon} \vdash_{\pi} \exists x_1 \dots \exists x_k E(x_1, \dots, x_k)$
- employing embedding we obtain $\mathrm{EC}_{\varepsilon} \vdash E(s_1, \dots, s_k)$, where $s_1, \dots, s_k$ are terms (containing ε's)
- finally, we employ the First Epsilon Theorem

∎

Lower Bounds

Observations

- the upper bound on the length of the Herbrand disjunction depends only on the critical count of the initial proof
- in contrast, usually the bound depends on the length and cut complexity of the original proof
- in both cases the relationship is non-elementary
- its well-known that proofs with cut have non-elementary speedup over cut-free proofs

Question

what about lower-bounds of the ε-elimination procedure

Lower Bounds

Definition

- an $\vee$-expansion (of $E \equiv E(s_1, \dots, s_m)$) is a finite disjunction

$$E' \equiv E_1 \vee \cdots \vee E_l$$

  $E_i \equiv E(s_1^i, \dots, s_m^i)$ for terms s_j^i
- the Herbrand complexity $\mathrm{HC}(E)$ of a purely existential formula $E \equiv \exists x_1 \dots \exists x_n E'(x_1, \dots, x_n)$ is the length of the shortest valid $\vee$-expansion of $E'(x_1, \dots, x_n)$

Theorem

there is a sequence of formulas E_k so that

1. *for each k, $\exists$ $\mathrm{PC}_{\varepsilon}$-proof π_k of E_k with $\mathrm{cc}(\pi_k) \leq c \cdot k$, but*
2. $\mathrm{HC}(E_k) \geq 2_k^1$.

Proof Sketch of Part 1

Definition

$\mathrm{Hyp}_1 := \forall x\, R(x, 0, S(x))$

$\mathrm{Hyp}_2 := \forall y \forall x \forall z \forall z_1 (R(y, x, z) \wedge R(z, x, z_1) \to R(y, S(x), z_1))$

$C_k := \exists z_k \dots \exists z_0 (R(0, 0, z_k) \wedge R(0, z_k, z_{k-1}) \wedge \cdots \wedge R(0, z_1, z_0))$

$E_k :=$ (purely existential) prefix form of $\mathrm{Hyp}_1 \wedge \mathrm{Hyp}_2 \to C_k$

$R(n, m, k)$ expresses that $n + 2^m = k$, and C_k expresses that 2_k^1 is defined

Lemma

for every k, $\mathrm{PC}_{\varepsilon} \vdash_{\pi_k} E_k$, where $\mathrm{cc}(\pi_k) = c \cdot k$

this establishes part one of the theorem

Proof Sketch of Part 2

Definition

consider Herbrand sequents of the sequent $\mathrm{Hyp}_1, \mathrm{Hyp}_2 \Rightarrow C_k$

1. each of these sequents has the from $\Gamma_1, \Gamma_2 \Rightarrow \Delta$ such that each formula in
   - Γ_1 is instance of $R(x, 0, S(x))$
   - Γ_2 is instance of $R(y, x, z) \land R(z, x, z_1) \to R(y, S(x), z_1)$
   - Δ is instance of $R(0, 0, z_k) \land R(0, z_k, z_{k-1}) \land \cdots \land R(0, z_1, z_0)$
2. $\max\{|\Gamma_1|, |\Gamma_2|, |\Delta|\} \leqslant \mathrm{HC}(E_k)$

Lemma

if $T = (\Gamma_1, \Gamma_2 \Rightarrow \Delta)$ is a minimal Herbrand sequent of $\mathrm{Hyp}_1, \mathrm{Hyp}_2 \Rightarrow C_k$, then $|\Gamma_1| \geqslant 2^1_k$

this establishes the lower bound on $\mathrm{HC}(E_k)$

The Second Epsilon Theorem

Theorem

If A is a formula of $L(\mathrm{PC})$ and $\mathrm{PC}_\varepsilon \vdash A$, then $\mathrm{PC} \vdash A$.

Proof Sketch

- assume $A = \exists x \forall y \exists z\, B(x, y, z)$ and $\mathrm{PC}_\varepsilon \vdash A$
- then $\mathrm{PC}_\varepsilon \vdash \exists x \exists z\, B(x, f(x), z) =: A^H$
- apply the extended first epsilon theorem to A^H: $\exists$ ε-free terms r_i, s_i

$$\mathrm{EC} \vdash \bigvee_i B(r_i, f(r_i), s_i)$$

- replace the $f(r_i)$ by fresh free variables a_i such that $\mathrm{EC} \vdash \bigvee_i B(r_i', a_i, s_i')$
- deduce A in PC from above disjunction, essentially applying quantifier shiftings ∎

Epsilon Calculus with Equality

Definitions

- $\mathrm{AxEC}^=$: AxEC + all substitution instances of

$$s = s$$
$$s = t \to f(\vec{u}, s, \vec{v}) = f(\vec{u}, t, \vec{v})$$
$$s = t \to (P(\vec{u}, s, \vec{v}) \to P(\vec{u}, t, \vec{v}))$$

- $\mathrm{AxEC}^=_\varepsilon$: $\mathrm{AxEC}^=$ + all substitution instances of critical formulas
- $\mathrm{AxPC}^=$: AxPC plus all all substitution instances of the following identity schema, where A is an arbitrary formula

$$s = s \qquad s = t \to (A(s) \to A(t))$$

- $\mathrm{AxPC}^=_\varepsilon$: $\mathrm{AxPC}^=$ + all substitution instances of critical formulas
- a proof in $\mathrm{PC}^=$ ($\mathrm{EC}^=$, $\mathrm{EC}^=_\varepsilon$, $\mathrm{PC}^=_\varepsilon$) is defined as expected and if A is provable in say $\mathrm{EC}^=_\varepsilon$ we write $\mathrm{EC}^=_\varepsilon \vdash_\pi A$

Lemma

For any formula $A(a)$ in $L(\mathrm{PC}^=)$, there is an $\mathrm{EC}^=_\varepsilon$-proof π^ε of

$$s = t \to A^\varepsilon(s) \to A^\varepsilon(t)$$

Proof.

by induction on A:

- suppose $A(a) \equiv P(r_1, \dots, r_k) \equiv (P(r_1, \dots, r_k))^\varepsilon$, where any of r_i may contain a and is expressed as $r_i(a)$. Then

$$\mathrm{EC}^=_\varepsilon \vdash s = t \to r_i(s) = r_i(t)$$

  for each i, hence the claim holds
- suppose $A \equiv \neg B$, $A \equiv B \land C$, $A \equiv B \lor C$, $A \equiv B \to C$, then the claim follows from IH (and propositional logic)
- suppose $A(a) \equiv \exists x B(x, a)$ or $A(a) \equiv \forall x B(x, a)$, wlog. we consider the first case

Proof (cont'd).

- by definition
$$(\exists x B(x,a))^\varepsilon \equiv B^\varepsilon(\varepsilon_x B^\varepsilon(x,a),a)$$
and by IH, we conclude $\mathrm{EC}^=_\varepsilon \vdash_{\pi_0^\varepsilon} s = t \to (B^\varepsilon(b,s) \to B^\varepsilon(b,t))$, where b is a fresh free variable
- instantiation of b by $\varepsilon_x B^\varepsilon(x,s) =: e(s)$ yields a proof π_1^ε of
$$s = t \to (B^\varepsilon(e(s),s) \to B^\varepsilon(e(s),t))$$
- consider the impliciation
$$B^\varepsilon(e(s),t) \to B^\varepsilon(e(t),t) \quad (1)$$
note that (1) is a critical axiom
- finally, we get the proof π^ε of $s = t \to (B^\varepsilon(e(s),s) \to B^\varepsilon(e(t),t))$ using (1) plus propositional logic ∎

Theorem (Extended First Epsilon Theorem (with =))

If $\exists x_1 \dots \exists x_k E(x_1,\dots,x_k)$ is a purely existential formula containing only the bound variables $x_1, \dots, x_k$, and $\mathrm{PC}^=_\varepsilon \vdash \exists x_1 \dots \exists x_k E(x_1,\dots,x_k)$ then there are terms t_{ij} such that
$$\mathrm{EC}^= \vdash \bigvee_i E(t_{i1},\dots,t_{ik})$$

Proof Sketch.

- let π denote the $\mathrm{PC}^=_\varepsilon$-proof of $\exists x_1 \dots \exists x_k E(x_1,\dots,x_k)$
- combining embedding and the lemma, we obtain a $\mathrm{EC}^=_\varepsilon$-proof π^ε of $E(s_1,\dots,s_k)$, where $s_1, \dots, s_k$ are terms (containing ε's)
- ε-elimination method (depending only on critical axioms of π^ε) produces Herbrand disjunction of E by construction
- n depends on $\mathrm{cc}(\pi^\varepsilon)$, which in turn depends linearly on $\mathrm{cc}(\pi)$ and the size of formulas used in identity schemas ∎

Epsilon Calculus with Equality (2)

Definition ("Grundtyp")

An ε-term $\varepsilon_x A(x)$ is an ε-matrix if the only terms that occur in $\varepsilon_x A(x)$ are free variables, each of which occurs exactly once.

Definition (alternative)

$\mathrm{AxEC}^=_\varepsilon$: $\mathrm{AxEC}^=$ + all substitution instances of critical formulas + all substitution instances of
$$s = t \to \varepsilon_x A(x,\vec{u},s,\vec{v}) = \varepsilon_x A(x,\vec{u},t,\vec{v})$$
where $\varepsilon_x A(x,\vec{b},a,\vec{c})$ is an ε-matrix

Remark

the restriction to ε-matrices for ε-equality axioms is sometimes omitted in the literature, which has severe effects (perhaps Matthias' talk)

Theorem (Alternative First Epsilon Theorem (with =, 2nd version))

suppose $E(e_1,\dots,e_m)$ is a quantifier-free formula containing only the ε-terms $s_1, \dots, s_m$, and $\mathrm{EC}^=_\varepsilon \vdash_\pi E(s_1,\dots,s_m)$ Then there are ε-free terms t^i_j such that
$$\mathrm{EC}^= \vdash \bigvee_{i=1}^n E(t_{i1},\dots,t_{ik})$$
where $n \leqslant$ subject to further work

Observations.

- the presence of ε-equality axioms makes the ε-elimination more involved
- a bound on n can be read off, however depending not only on the $\mathrm{cc}(\pi)$, but also on the number of ε-equality axioms and also on their size
- published proofs [HB39, Zac17] are faulty

Conclusion and Future Work

Final Remarks

- ε-theorems and Herbrand's theorem: proof theory without sequents
- the bound on the length of the Herbrand disjunction depends only on the critical count of the initial proof

Future Work

1. ϵ-elimination in the presence of ε-equality axioms is (formally) open
2. semantics is (wide) open
3. sequent calculus formulation admitting cut-elimination is open
4. ϵ-calculus for intuitionistic logic is open
5. computational interpretation is (wide) open

Thank You for Your Attention!