

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 $SZ(\pi^\varepsilon) \leq 3 \cdot SZ(\pi)$ and $CC(\pi^\varepsilon) \leq CC(\pi)$

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 $EC_\varepsilon \vdash_\pi E(s_1, \dots, s_m)$ Then there are ε -free terms t_j^i such that

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

where $n \leq \frac{2^{3 \cdot CC(\pi)}}{2 \cdot CC(\pi)}$

Outline

- Summary of Yesterday's Lecture
- The First Epsilon Theorem (without $=$)
- Lower Bounds
- The Second Epsilon Theorem
- Epsilon Calculus with Equality

The First Epsilon Theorem (without =)

Simplifications

- suppose $EC_\varepsilon \vdash_\pi E$ and E contains no ε -terms
- we show that $EC \vdash E$ 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 $\text{rk}(\pi_e) \leq \text{rk}(\pi)$, $\text{deg}(\pi_e) \leq \text{deg}(\pi)$ and $o(\pi_e, \text{rk}(e)) = o(\pi, \text{rk}(e)) - 1$

Proof of Lemma.

Construct π_e as follows:

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

$$A(t_i) \rightarrow A(e)$$

we obtain a derivation

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

as follows:

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

Proof (cont'd).

2 Obtain a derivation π' of

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

by:

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

3 Combine the proofs

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

and

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

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

Why is this correct?

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

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 $o(\pi', \text{rk}(e)) = o(\pi, \text{rk}(e)) - 1$.
- 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 $B(s) \rightarrow B(\varepsilon_y B(y))$, we have three cases.

Case I

Case: e occurs only in s

Replacing e by t_i results in a critical formula

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

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

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

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

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

Replacing e by t_i results in a different critical formula

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

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 $\text{rk}(\varepsilon_y B'(y, e)) < \text{rk}(e)$. Thus also $\text{rk}(\varepsilon_y B'(y, t_i)) < \text{rk}(e)$

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

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 $\text{rk}(\pi_e) \leq \text{rk}(\pi)$, $\text{deg}(\pi_e) \leq \text{deg}(\pi)$ and $o(\pi_e, \text{rk}(e)) = o(\pi, \text{rk}(e)) - 1$

Proof.

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

Proof of Simplified First Epsilon Theorem.

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

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 $EC_\varepsilon \vdash_\pi E(s_1, \dots, s_m)$ Then there are ε -free terms t_j^i such that

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

where $n \leq 2^{\frac{3 \cdot \text{cc}(\pi)}{2 \cdot \text{cc}(\pi)}}$

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 $\text{PC}^\varepsilon \vdash \exists x_1 \dots \exists x_k E(x_1, \dots, x_k)$ then there are terms t_{ij} such that

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

where $n \leq 2^{\frac{3 \cdot \text{cc}(\pi)}{2 \cdot \text{cc}(\pi)}}$

Proof.

- consider $\text{PC}^\varepsilon \vdash_\pi \exists x_1 \dots \exists x_k E(x_1, \dots, x_k)$
- employing embedding we obtain $\text{EC}_\varepsilon \vdash E(s_1, \dots, s_k)$, 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 **V-expansion** (of $E \equiv E(s_1, \dots, s_m)$) is a finite disjunction

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

$$E_i \equiv E(s_1^i, \dots, s_m^i) \text{ for terms } s_j^i$$

- the **Herbrand complexity** $\text{HC}(E)$ 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

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

Proof Sketch of Part 1

Definition

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

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

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

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

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

Lemma

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

this establishes part one of the theorem

Proof Sketch of Part 2

Definition

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

- 1 each of these sequents has the form $\Gamma_1, \Gamma_2 \Rightarrow \Delta$ such that each formula in
 - Γ_1 is instance of $R(x, 0, S(x))$
 - Γ_2 is instance of $R(y, x, z) \wedge R(z, x, z_1) \rightarrow R(y, S(x), z_1)$
 - Δ is instance of $R(0, 0, z_k) \wedge R(0, z_k, z_{k-1}) \wedge \dots \wedge R(0, z_1, z_0)$
- 2 $\max\{|\Gamma_1|, |\Gamma_2|, |\Delta|\} \leq \text{HC}(E_k)$

Lemma

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

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

The Second Epsilon Theorem

Theorem

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

Proof Sketch

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

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

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



Epsilon Calculus with Equality

Definitions

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

$$s = s$$

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

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

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

$$s = s \quad s = t \rightarrow (A(s) \rightarrow A(t))$$

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

Lemma

For any formula $A(a)$ in $L(PC^=)$, there is an EC_ε^- -proof π^ε of

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

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

$$EC_\varepsilon^- \vdash s = t \rightarrow r_i(s) = r_i(t)$$

for each i , hence the claim holds

- suppose $A \equiv \neg B$, $A \equiv B \wedge C$, $A \equiv B \vee C$, $A \equiv B \rightarrow C$, 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 $EC_{\varepsilon}^{\equiv} \vdash_{\pi_0^{\varepsilon}} s = t \rightarrow (B^{\varepsilon}(b, s) \rightarrow B^{\varepsilon}(b, t))$,
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

$$s = t \rightarrow (B^{\varepsilon}(e(s), s) \rightarrow B^{\varepsilon}(e(s), t))$$

- consider the impliciation

$$B^{\varepsilon}(e(s), t) \rightarrow B^{\varepsilon}(e(t), t) \tag{1}$$

note that (1) is a critical axiom

- finally, we get the proof π^{ε} of $s = t \rightarrow (B^{\varepsilon}(e(s), s) \rightarrow B^{\varepsilon}(e(t), t))$
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 $\text{PC}_\varepsilon^- \vdash \exists x_1 \dots \exists x_k E(x_1, \dots, x_k)$ then there are terms t_{ij} such that

$$\text{EC}^- \vdash \bigvee_i E(t_{i1}, \dots, t_{ik})$$

Proof Sketch.

- let π denote the PC_ε^- -proof of $\exists x_1 \dots \exists x_k E(x_1, \dots, x_k)$
- combining embedding and the lemma, we obtain a EC_ε^- -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 $\text{cc}(\pi^\varepsilon)$, which in turn depends linearly on $\text{cc}(\pi)$ 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)

$\text{AxEC}_\varepsilon^-$: AxEC^- + all substitution instances of critical formulas + all substitution instances of

$$s = t \rightarrow \varepsilon_x A(x, \vec{u}, s, \vec{v}) = \varepsilon_x A(x, \vec{u}, t, \vec{v})$$

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 $EC_\varepsilon^\equiv \vdash_\pi E(s_1, \dots, s_m)$ Then there are ε -free terms t_j^i such that

$$EC^\equiv \vdash \bigvee_{i=1}^n E(t_{i1}, \dots, t_{ik})$$

where $n \leq$ *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 $cc(\pi)$, 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!