Emulating Hilbert's Epsilon in ZFC

Norman Megill

nm@alum.mit.edu http://metamath.org

August 12, 2005

Hilbert's epsilon calculus

Hilbert's epsilon calculus is described at `http://plato.stanford.edu/entries/epsilon-calculus/`. The term "$\varepsilon x \varphi$" denotes "some x satisfying wff φ."

The *Transfinite Axiom* is the basic axiom needed for the epsilon calculus:

$$\varphi \to [\varepsilon x \varphi / x]\varphi \tag{1}$$

where x is free in φ and $[A/x]\varphi$ denotes the proper substitution of class-term A for x in φ.

Motivation

Theorem provers such as HOL use the epsilon calculus extensively as a proving tool. Our goal is to be able to translate such proofs into a form that can be verified by a ZFC-only proof verifier.

Discussion: `http://ghilbert.org/choice.txt`

While the Transfinite Axiom represents a form of the Axiom of Choice, ZFC cannot express it directly. ZFC can, however, prove the same epsilon-free theorems as the epsilon calculus. **We will show a practical algorithm that can translate an epsilon-calculus proof (of an epsilon-free theorem) to a ZFC-only proof.**

The trivial case of Hilbert's epsilon

If there is exactly one element such that a property φ is true, we can express "the (unique) element such that φ" (usually called "iota") as "$\bigcup\{x|\varphi\}$," which emulates Hilbert's epsilon. Hilbert's Transfinite Axiom can be easily emulated using this ZFC theorem:

$$\exists! x\varphi \rightarrow [\bigcup\{x|\varphi\}/x]\varphi \tag{2}$$

To use it, just detach $\exists! x\varphi$ and add the antecedent φ to obtain the Transfinite Axiom instance. So, assuming $\exists! x\varphi$,

$$\varphi \rightarrow [\bigcup\{x|\varphi\}/x]\varphi \tag{3}$$

The ZFC axioms

$$\text{(Ext) } \forall z(z \in x \leftrightarrow z \in y) \to x = y \tag{4}$$

$$\text{(Rep) } \forall w \exists y \forall z(\forall y \varphi \to z = y) \to \exists y \forall z(z \in y \leftrightarrow \exists w(w \in x \wedge \forall y \varphi)) \tag{5}$$

$$\text{(Un) } \exists y \forall z(\exists w(z \in w \wedge w \in x) \to z \in y) \tag{6}$$

$$\text{(Pow) } \exists y \forall z(\forall w(w \in z \to w \in x) \to z \in y) \tag{7}$$

$$\text{(Reg) } \exists y\, y \in x \to \exists y(y \in x \wedge \forall z(z \in y \to \neg z \in x)) \tag{8}$$

$$\text{(Inf) } \exists y(x \in y \wedge \forall z(z \in y \to \exists w(z \in w \wedge w \in y))) \tag{9}$$

$$\begin{aligned} &\text{(AC) } \exists y \forall z \forall w((z \in w \wedge w \in x) \to \\ &\quad \exists v \forall u(\exists t((u \in w \wedge w \in t) \wedge (u \in t \wedge t \in y)) \leftrightarrow u = v)) \end{aligned} \tag{10}$$

Just for fun

A very short version of the Axiom of Infinity, using only elementary symbols ($\subset$ is proper subset):

$$\exists x\, x \subset \bigcup x \tag{11}$$

If we allow restricted quantifiers and $\exists!$, the Axiom of Choice with only one propositional connective:

$$\exists y \forall z \in x \forall w \in z \exists! v \in z \exists u \in y (z \in u \wedge v \in u) \tag{12}$$

Definitions for set theory (1 of 5)

We assume you know: virtual classes, subset, power class $\mathcal{P}x$, empty set $\varnothing$, universe V, unordered and ordered pairs, class builder, union and intersection (small and big), Cartesian (cross) product, binary relations.

Capital letters A, B, F, R are variables ranging over classes (which may be proper). Small letters x, y, z, w, f, g, etc. range over sets and are the individual variables of the first-order logic.

Define "R is a founded relation on (possibly proper) class A."

$$R \,\mathrm{Fr}\, A \overset{\text{def}}{\leftrightarrow} \forall x((x \subseteq A \wedge \neg x = \varnothing) \to \exists y \in x \forall z \in x \neg z \, R \, y) \quad (13)$$

Definitions for set theory (2 of 5)

Define "R well-orders A."

$$R\,\mathrm{We}\,A \overset{\text{def}}{\leftrightarrow} (R\,\mathrm{Fr}\,A \wedge \forall x \in A \forall y \in A (x\,R\,y \vee x = y \vee y\,R\,x)) \quad (14)$$

Define "A is a transitive class."

$$\mathrm{Tr}\,A \overset{\text{def}}{\leftrightarrow} \bigcup A \subseteq A \quad (15)$$

Define the epsilon relation.

$$E \overset{\text{def}}{=} \{\langle x, y\rangle | x \in y\} \quad (16)$$

Define "A is an ordinal class."

$$\mathrm{Ord}\,A \overset{\text{def}}{\leftrightarrow} \mathrm{Tr}\,A \wedge E\,\mathrm{We}\,A \quad (17)$$

Define the class of all ordinals.

$$\mathrm{On} \overset{\text{def}}{=} \{x | \mathrm{Ord}\,x\} \quad (18)$$

Definitions for set theory (3 of 5)

Define "A is a limit ordinal."

$$\text{Lim}\, A \overset{\text{def}}{\leftrightarrow} \text{Ord} A \wedge \neg A = \varnothing \wedge A = \bigcup A \tag{19}$$

Define the successor of a class A.

$$\text{suc}\, A \overset{\text{def}}{=} A \cup \{A\} \tag{20}$$

Define the domain of a class.

$$\text{dom}\, A \overset{\text{def}}{=} \{x | \exists y \, x \, A \, y\} \tag{21}$$

Define the range of a class.

$$\text{ran}\, A \overset{\text{def}}{=} \{y | \exists x \, x \, A \, y\} \tag{22}$$

Define the restriction of a class.

$$(A \upharpoonright B) \overset{\text{def}}{=} A \cap (B \times V) \tag{23}$$

Definitions for set theory (4 of 5)

Define the image of a class.

$$(A\text{``}B) \overset{\text{def}}{=} \operatorname{ran}(A \restriction B) \tag{24}$$

Define the value of a function. (Applies to any class F).

$$(F\text{`}A) \overset{\text{def}}{=} \bigcup\{x|(F\text{``}\{A\}) = \{x\}\} \tag{25}$$

Define "A is a relation."

$$\text{Rel}\, A \overset{\text{def}}{\leftrightarrow} A \subseteq (V \times V) \tag{26}$$

Define "class A is a function."

$$\text{Fun}\, A \overset{\text{def}}{\leftrightarrow} \text{Rel}\, A \land \forall x \exists z \forall y (x\, A\, y \to y = z) \tag{27}$$

Define "class A is a function with domain B."

$$A\, \text{Fn}\, B \overset{\text{def}}{\leftrightarrow} \text{Fun}\, A \land \text{dom}\, A = B \tag{28}$$

Definitions for set theory (5 of 5)

Define a recursive definition generator on On with characteristic function F and initial value A.

$$\begin{aligned} \mathrm{rec}(F, A) \overset{\text{def}}{=} & \bigcup\{f|\exists x \in \mathrm{On}(f \,\mathrm{Fn}\, x \wedge \forall y \in x(f`y) = \\ & (\{\langle g, z\rangle|((g = \varnothing \wedge z = A) \\ & \vee(\neg(g = \varnothing \vee \mathrm{Lim}\,\mathrm{dom}\, g) \wedge z = (F`(g`\bigcup \mathrm{dom}\, g))) \\ & \vee(\mathrm{Lim}\,\mathrm{dom}\, g \wedge z = \bigcup \mathrm{ran}\, g))\}`(f \restriction y)))\} \end{aligned} \tag{29}$$

Define the cumulative hierarchy of sets function R_1.

$$R_1 \overset{\text{def}}{=} \mathrm{rec}(\{\langle x, y\rangle|y = \mathcal{P}x\}, \varnothing) \tag{30}$$

Define the rank function.

$$\mathrm{rank} \overset{\text{def}}{=} \{\langle x, y\rangle|y = \bigcap\{z \in \mathrm{On}|x \in (R_1`\mathrm{suc}\, z)\}\} \tag{31}$$

The Main Theorem!

Recall our goal: we want to emulate Hilbert's epsilon $\varepsilon x \varphi$.

We define two class variables A and B, where y is not free in φ:

$$A = \{x | (\varphi \wedge \forall y ([y/x]\varphi \rightarrow (\text{rank}`x) \subseteq (\text{rank}`y)))\} \quad (32)$$

$$B = \bigcup \{x \in A | \forall y \in A \, \neg y \, R \, x\} \quad (33)$$

Then the following theorem of ZFC emulates Hilbert's Transfinite Axiom, with the additional antecedent "R We A":

$$R \text{ We } A \rightarrow (\varphi \rightarrow [B/x]\varphi) \quad (34)$$

Class B emulates Hilbert's epsilon!

(Note: In English, A is the collection of all sets of minimum rank with property φ. B is the smallest member of A w.r.t. some well-ordering relation R.)

Two key auxilliary theorems

Well-ordering theorem (derived from the Axiom of Choice): for any set x, there exists a set y s.t. y well-orders x.

$$\exists y\, y\, \mathsf{We}\, x \tag{35}$$

Scott's trick collects all sets that have a certain property and are of smallest possible rank. The following amazing theorem shows that the resulting collection exists, i.e. is a set.

$$\{x|(\varphi \wedge \forall y([y/x]\varphi \rightarrow (\mathsf{rank}`x) \subseteq (\mathsf{rank}`y)))\} \in V \tag{36}$$

where y is not free in φ. In other words, the class A on the previous slide is a set, which is crucial for the well-ordering theorem to work!

The algorithm - case 1

Suppose the set A in Theorem 34 has a constructible well-ordering (rather than just the existence implied by Theorem 35). For example, A might be a subset of the natural numbers. In that case, we simply substitute the well-ordering in place of R and detach R We A. The result is the necessary instance of Hilbert's Transfinite Axiom. I.e. if we can find an R s.t. we can prove R We A, then (from Th. 34)

$$\varphi \rightarrow [B/x]\varphi \tag{37}$$

Note that the trivial case of unique existence, discussed at the beginning of this talk, is also covered by case 1, although Theorem 2 may be preferred for simplicity.

The algorithm - case 2

Suppose the set A in Theorem 34 does not have a constructible well-ordering. We substitute a temporary dummy variable, say w, for R in Theorem 34. In each step in the epsilon-calculus proof referencing the Transfinite Axiom, we replace the Transfinite Axiom by Theorem 34 with a temporary dummy variable, say w, for R, and carry along in the proof the extra antecedent $w\,\mathrm{We}\,A$ in each step containing a reference to B (the object that emulates Hilbert's epsilon). Note that B will have w as a free variable, so this antecedent cannot be eliminated. But since the final theorem is epsilon-free, at the end we can existentially quantify $w\,\mathrm{We}\,A$ then detach it with the Well-Ordering Theorem 35.

The algorithm - case 2 - continued

Epsilon-calculus proof	**ZFC proof**
$\vdots$	$\vdots$
$\varphi \to [\varepsilon x \varphi / x]\varphi$	w We $A \to (\varphi \to [B(w)/x]\varphi)$
$\vdots$	$\vdots$
(manipulate $\varepsilon x \varphi$)	(manipulate $B(w)$)
$\vdots$	$\vdots$
($\varepsilon x \varphi$-free result)	w We $A \to$ ($B(w)$-free result)
	$\exists w\, w$ We $A \to$ ($B(w)$-free result)
	($B(w)$-free result)
$\vdots$	$\vdots$

Appendix - Equation references

The following list provides the hyperlinks to the formal proofs for most of the theorems.

Eq. 2—http://us.metamath.org/mpegif/reuuni4.html
Eq. 4—http://us.metamath.org/mpegif/ax-ext.html
Eq. 5—http://us.metamath.org/mpegif/ax-rep.html
Eq. 6—http://us.metamath.org/mpegif/ax-un.html
Eq. 7—http://us.metamath.org/mpegif/ax-pow.html
Eq. 8—http://us.metamath.org/mpegif/ax-reg.html
Eq. 9—http://us.metamath.org/mpegif/ax-inf.html
Eq. 10—http://us.metamath.org/mpegif/ax-ac.html
Eq. 11—http://us.metamath.org/mpegif/inf5.html
Eq. 12—http://us.metamath.org/mpegif/ac2.html

Eq. 13—http://us.metamath.org/mpegif/df-fr.html

Eq. 14—http://us.metamath.org/mpegif/dfwe2.html

Eq. 15—http://us.metamath.org/mpegif/df-tr.html

Eq. 16—http://us.metamath.org/mpegif/df-eprel.html

Eq. 17—http://us.metamath.org/mpegif/df-ord.html

Eq. 18—http://us.metamath.org/mpegif/df-on.html

Eq. 19—http://us.metamath.org/mpegif/df-lim.html

Eq. 20—http://us.metamath.org/mpegif/df-suc.html

Eq. 21—http://us.metamath.org/mpegif/df-dm.html

Eq. 22—http://us.metamath.org/mpegif/dfrn2.html

Eq. 23—http://us.metamath.org/mpegif/df-res.html

Eq. 24—http://us.metamath.org/mpegif/df-ima.html

Eq. 25—http://us.metamath.org/mpegif/df-fv.html

Eq. 26—http://us.metamath.org/mpegif/df-rel.html

Eq. 27—http://us.metamath.org/mpegif/dffun3.html

Eq. 28—http://us.metamath.org/mpegif/df-fn.html

Eq. 29—http://us.metamath.org/mpegif/dfrdg2.html

Eq. 30—http://us.metamath.org/mpegif/df-r1.html

Eq. 31—http://us.metamath.org/mpegif/df-rank.html

Eq. 34—http://us.metamath.org/mpegif/hta.html

Eq. 35—http://us.metamath.org/mpegif/weth.html

Eq. 36—http://us.metamath.org/mpegif/scottexs.html