THE SEMANTICS OF EVIDENCE

Robert L. Constable
Cornell University
Ithaca, NY 14853

ABSTRACT

The usual meaning of a sentence in the predicate calculus is its truth value. In this paper we show that there is associated with every statement a set of elements comprising *evidence* for it. A statement is true in a model exactly when there is evidence for it. Proofs can be regarded as expressions which denote evidence. A statement is *constructively true* when the evidence can be computed from its proofs. Proofs are useful in practical computations when evidence for statements is needed. They are especially valuable in relating computations to the problems they solve.*

I. INTRODUCTION

If I correctly state the winning lottery number before it has been publicly announced, many people will be more interested in my evidence for the assertion than in its truth. Even for routine utterances we are interested in the evidence. "How do you know?" we ask. In formal logic the "truth" of a sentence can be defined following Tarski [22] who put the matter this way for the case of a universal statement: $\forall x.B(x)$ is true in a model **m** if the model assigns to B some propositional function **m**(B) which has value true for every element of the *universe of discourse* D of the model. That definition ignores evidence. We want to give a precise definition of evidence and relate it to truth as defined by Tarski.

In mathematics there is a persistent interest in evidence even though the official definition of truth does not refer to it. So if I claim that there is a regular 17-gon, then you may wish to see one . The ancient Greeks would require that I <u>construct</u> one or in some way actually exhibit it. As another interesting example, suppose that I claim that there are two irrational numbers, say x and y, such that x^y is rational. I might prove that they exist this way. Consider $\sqrt{2}^{\sqrt{2}}$, it is either rational or irrational. If it is rational, take $x=\sqrt{2}$, $y=\sqrt{2}$. If it is irrational, take $x=\sqrt{2}^{\sqrt{2}}$ and $y=\sqrt{2}$. Then $x^y=(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}=\sqrt{2}^2=2$. So in either case there are the desired x, y. But notice that the evidence for existence here is <u>indirect</u>. I have not actually exhibited x by this method, even

*This research was supported in part by NSF grants MCS-81-04018 and (joint Cornell-Edinburgh) MCS-83-03336. Technical Report 85-684, 1985

ideas to classical logics as well. Later we will make connection to constructive logic via the so-called propositions-as-types principle due to Curry, Howard, Lauchli, and de Bruijn (for references see [10, 11]). This principle can be seen as formalyzing the notion of evidence in *type theory*, see also Martin-Lof [18], Constable et al. [10].

II. THE LOGIC

Syntax

We present a standard kind of predicate calculus, see [15]. The formulas of our logic are built using the binary propositional connectives &,|,¬,⇒ (and, or, not, implies) and the quantifiers $\forall x$, $\exists x$ *(all and some)*. There are *predicate* constants $A, A(x), A(x,y), \ldots, B, B(x), B(x,y) \ldots, C, C(x), C(x,y)$. Each predicate has an *arity* which is its number of argument positions, e.g. an arity n predicate with variables in the argument positions appears in formulas as $B(x_1,\ldots,x_n)$ showing that the argument positions are given by the x_i. There are also *terms*, usually denoted t_1, t_2,... These are built from variables x, y, z,... and constants $c_1, c_2, c_3, \ldots$. Constants also have an arity; an arity n constant c is used to build a term of the form $c(t_1,\ldots,t_n)$ where t_i are terms.

A *formula* of the logic is defined as follows.

(i) *false* is a formula

(ii) if B is a predicate constant of arity n, and $t_1,\ldots,t_n$ are terms, then $B(t_1,\ldots,t_n)$ is a formula

(iii) if A,B are formulas, then so are

$(A \& B)$

$(A | B)$

$(A \Rightarrow B)$

(iv) if B is a formula, then so are

$(\exists x.B)$ *and* $(\forall x.B)$.

For example, over the set of natural numbers, $\{0,1,2,\ldots\}$, $x=y$ and $x<y$ are arity 2 predicates on N and $+(x,y)$ and $*(x,y)$ are arity 2 terms on N, then $\forall x.\exists y.(+(x,y)\ *(x,y))$ is a formula. Formulas in (i) and (ii) are atomic. Those in (iii) are *compound* with principle operator &,|, or ⇒ (in that order). Those in (iv) are quantified formulas, and their principle operators, is $\forall x$ or $\exists x$.

The quantifiers $\forall x$, $\exists x$ are called *binding operators* because they bind occurrences of the variable x in the formulas to which they are applied. In $\forall x.B$ and in $\exists x.B$, the formula part B is called the *scope* of the quantifier. Any occurrence of x *in* B is bound. It is bound by the quantifier of smallest scope that causes it to be bound.

2. $\mathbf{m} \models_s (A\&B)$

   iff $\mathbf{m} \models_s A$ *and* $\mathbf{m} \models_s B$

3. $\mathbf{m} \models_s (A|B)$

   iff $\mathbf{m} \models_s A$ *or* $\mathbf{m} \models_s B$

4. $\mathbf{m} \models_s (A\Rightarrow B)$

   iff $\mathbf{m} \models_s A$ *implies* $\mathbf{m} \models_s B$

5. $\mathbf{m} \models_s \forall x.B$

   iff $\mathbf{m} \models_{s'} B$ *for all* $s' = s[x_i=a]$ with a in D.

6. $\mathbf{m} \models_s \exists x.B$

   iff $\mathbf{m} \models_{s'} B$ *for some* $s' = s[x_i:=a]$ for a in D.

Semantics of Evidence

The following set constructors are needed in the semantics of evidence. Given sets A and B, let $A \times B$ denote their cartesian product, let $A+B$ denote their disjoint union, and let $A \rightarrow B$ denote all the functions from A to B. Given $B(x)$ a family of sets indexed by A, let

$$\prod_{x \in A} B(x)$$

denote the set of functions f from A into,

$$\sum_{x \in A} B(x)$$

such that $f(a)$ belongs to $B(a)$. (We mean by

$$\sum_{x \in A} B(x)$$

the disjoint union of the family of sets.) Notice that these are all ordinary set operations.

Now we define $\mathbf{m}[A](s)$, the evidence for formula A in model $\mathbf{m}$ and state s

1. $\mathbf{m}[\mathit{false}](s) =$ *the empty set*
2. $\mathbf{m}[c(t_1,\ldots,t_n)](s) = \{T\}$ *if* $\mathbf{m} \models_s c(x_1,\ldots,x_n)$
   empty otherwise for c a predicate constant.
3. $\mathbf{m}[A\&B](s) = \mathbf{m}[A](s) \times \mathbf{m}[B](s)$
4. $\mathbf{m}[A|B](s) = \mathbf{m}[A](s) + \mathbf{m}[B](s)$
5. $\mathbf{m}[A\Rightarrow B](s) = \mathbf{m}[A](s) \rightarrow \mathbf{m}[B](s)$

can be explained in terms of computable evidence, then the entire theory can be explained this way.

Predicate logics without the law of excluded middle or its equivalents are in some sense *constructive*, sometimes they are called *Intuitionistic logics* after Brouwer [6]. Arithmetic based on this logic and the Peano axioms is called *Heyting arithmetic* after the Intuitionist A.Heyting [14]. These topics are treated throughly in Kleene [15], Dummett [12] and Troelstra [23]. Analysis built on such a logic extended to higher order is sometimes called *constructive analysis*, see Bishop [3]. These topis are discussed in Troelstra [23] and Bridges [5].

Programming

The PRL programming systems built at Cornell in the early 1980's [2,18] are based on the idea that formal constructive logic, because of its computational semantics, provides a new kind of very high level programming language. This idea was first explored in Constable [8] and Bishop [4]. It was later developed by Bates and put into practice by Bates and Constable [2]. The semantics of evidence discussed here is quite close to the actual implementation ideas in Nuprl [17].

Acknowledgements

I want to thank Ryan Stansifer and Todd Knoblock for helpful comments and Donette Isenbarger, Elizabeth Maxwell, and Margaret Schimizzi for preparing the manuscript.

References

[1] Aczel, P. The type theoretic interpretation of constructive set theory. *Logic Colloquium '77*, A. MacIntyre, L. Pacholaki, and J. Paris (Eds.), North-Holland, Amsterdam, 1978, 55-66.

[2] Bates, J.L. and R .L. Constable. Proofs as programs. *TOPLAS*, 7:1, Jan. 1985, 113-136.

[3] Bishop, E. *Foundations of Constructive Analysis*. McGraw Hill, New York, NY, 196.

[4] Bishop, Errett. Mathematics as a numerical language. In *Intuitionism and Proof Theory*, Myhill, J. et al., (Eds.), North-Holland, Amsterdam, 1970, 53-71.

[5] Bridges, E and Bridges, D.S. *Constructive Analysis*. Springer-Verlag, NY, 1985.

[6] Brouwer, L.E.J. On the significance of the principle of excluded middle in mathematics, especially in function theory. *J. fur die reine und angewandte Math*, 154 (1923), 1-7. In *From Frege to Gödel*, J. van Heijenoort, (Ed.), Harvard University Press, Cambridge, MA, 1967, 334-345.

[8] Constable, R.L. Constructive mathematics and automatic program writers. In *Proc. of IFIP Congress*, Ljubljana, 1971 , 229-233.

[9] Constable, R.L. and O'Donnell, M.J. *A Programming Logic*. Winthrop, Cambridge, 1978.