Notre Dame Journal of Formal Logic
Volume VI, Number 2, April 1965

CHURCH'S THEOREM ON THE DECISION PROBLEM[1]

THOMAS E. PATTON

I. *Introduction*. This expository paper borrows from three main sources to present a proof of Church's theorem in the form

(1) *The set of valid quantificational formulas is not effective.*

A set C of formulas is called *effective* if there is a clerical routine which, for any given formula F, correctly answers Yes or No to the question whether $F \varepsilon C$. (Sets and relations of numbers will be called effective in parallel fashion.) But effectiveness, being an intuitive notion, must be replaced by a suitable formal analogue if we are to have a claim which admits of mathematical proof. The notion of *recursiveness* has been cast in this role, in what seems a paradigm of successful explication. Using this technical term and another soon to be explained, then, we arrive at

(2) *The set of Gödel numbers of valid quantificational formulas is not recursive.*

While (2) is provable, however, in order to infer (1) we need an additional premise, a version of Church's Thesis, namely,

(3) *All effective sets of numbers are recursive.*

But by using (3) and its analogue for relations, it turns out that a proof of (1) is possible which saves labor by not using (2) at all. This general strategy, whose source is Quine [6], will be the one followed here. The plan is (a) to exhibit a nonrecursive set of numbers, (b) to establish a link between recursiveness and quantificational validity, and then (c) in terms of this link, to show that the denial of (1) implies that the set presented in (a) is recursive. This proof, while owing its spirit to Quine, won't follow him in details, however. For phase (a), we borrow the same diagonal argument as Quine does from Kleene [3], but here adapt it to a definition of recursiveness, adapted from Smullyan [7], which lends itself particularly well to the purposes of phase (b).[2]

II. *Recursive enumerability and recursiveness* will be treated in terms of the *elementary arithmetic* (**EA**). An **EA** may be defined as a finite set of

Received March 9, 1963

formulas, as defined below, called *axioms*, and an ordered finite set of symbols called *digits*. Formulas are written using digits, right arrows, commas, other symbols called *variables*, and others called *predicates*. Calling a finite string of symbols composed of digits and/or variables a *term*, an *atomic formula* is a predicate followed by a finite number of terms with commas between them. A *formula*, finally, is either,an atomic formula or else two formulas with the right arrow between them. (Formulas with two or more arrows are to be read as having association to the right.)

An **EA** is called *n-adic* if it has just n digits (except that an **EA** with just one digit is called *unary*.) We will construe the digits of an n-adic **EA** as names of the first n positive integers. Then if $d_0, d_1, \ldots, d_k$ are each one of the digits of an n-adic **EA**, the string $d_k \ldots d_1 d_0$, which is called an *n-adic numeral*, will be construed as naming the number $d_0 + nd_1 + n^2 d_2 + \ldots + n^k d_k$. For the special case of a unary **EA**, we note that a string of k digits thus comes to name the positive integer k.

One formula is said to follow from another by *instantiation*, and is called an *instance* of the other, if it is obtainable from the other by uniformly putting numerals for all variables. Also, a formula F is said to follow from two others by *modus ponens* if the two others are an atomic formula G and the formula '$G \rightarrow F$'. A *proof* in an **EA** S is then defined as a sequence of formulas each of which is either an axiom of S or follows by instantiation from a previous formula of the sequence or follows by *modus ponens* from two such previous formulas. The sequence is called a proof of its last formula, which is called a *theorem* of S.

A predicate P of an n-adic **EA** S is said to *represent* a set Q of numbers (positive integers) if for every number x, $x \varepsilon Q$ iff P followed by the n-adic numeral of S that names x is a theorem of S. Predicates are said to represent relations of numbers, seen as ordered m-tuples of numbers, in parallel fashion. We call a set Q of numbers *recursively enumerable* if a predicate of some unary **EA** represents Q. The set Q is called *recursive*, finally, if both Q and its complement $\widetilde{Q}$ are recursively enumerable. Again, parallel definitions are given for relations of numbers.[3]

As an example, consider the unary **EA** whose digit is the arabic numeral '*1*' and whose axioms, in which '*E*' is a predicate, '*x*' is a variable, and '*11*', '*x*', and '*x11*' are terms, are the formulas

(4) $$E11$$
$$Ex \rightarrow Ex11$$

If we subjoin to(4) the following two formulas, which arise by instantiation and *modus ponens* respectively, the sequence that results is a proof in this **EA** of the theorem '*E1111*':

(5) $$E11 \rightarrow E1111$$
$$E1111$$

Where X is a unary numeral, the formula '*EX*' is provable here, plainly, iff X names an even number—hence the set of even numbers, which '*E*' represents, is recursively enumerable. This set is also recursive, for the predicate '*0*' represents the set of odd numbers, its complement, in the unary **EA** with axioms '*01*' and '$0x \rightarrow 0x11$'.

Some recursively enumerable sets are not recursive, however, and this crucial fact must now be established. First of all, for the balance of this section, let us assume that every unary **EA** is written using just the six symbols '*1*', '*F*', '*x*', the right arrow, the comma, and the prime. This economy won't decrease the number of sets representable in unary **EA**'s, for we may add primes to '*F*' and '*x*' when additional predicates and variables are needed. Now consider all concatenations of one or more **EA** formulas written in these six symbols. By dint of clerical routine, we may put these in *lexicographical* order, in which shorter concatenations precede longer ones, with the order being alphabetical when the length is the same. This allows us to assign to each concatenation, as its *Gödel number*, its rank in the ordering. We next remark that both unary **EA**'s and proofs within them may here be seen, harmlessly if artificially, as concatenations of formulas. In fact, every such concatenation uniquely determines a unary **EA** and a unary **EA** proof.

As a last bit of notation, for any number m, let $g(m)$ be the concatenation of formulas whose Gödel number is m and let $F(m)$ be the formula that consists of '*F*' followed by m tokens of the digit '*1*'. Now consider the relation K borne by a number m to a number n iff $g(m)$ is a proof of $F(n)$ in the **EA** $g(n)$. From the analogue of (3) for relations, we see that K is recursive, since K is plainly effective. Let us next show that the set D of numbers n such that $F(n)$ is provable in $g(n)$ is recursively enumerable. From the fact that K is recursive and *a fortiori* recursively enumerable, we know that some predicate R represents K in some unary **EA**. But this **EA** becomes one in which a new predicate P represents the set D if we simply add the axiom '$Ry,x \rightarrow Px$'.

D is not recursive, however, for suppose that it is. Then $\widetilde{D}$, being recursively enumerable, is represented in some unary **EA** by a predicate which, since typographical alterations are possible, may be taken to be '*F*'. Hence where s is the Gödel number of this **EA**,

$$(n)\ [n \notin D \Longleftrightarrow F(n) \textit{ is provable in } g(s)] \tag{6}$$

But it follows from the definition of D that

$$(n)\ [n \in D \Longleftrightarrow F(n) \textit{ is provable in } g(n)] \tag{7}$$

Letting n be s in (6) and (7), we obtain a contradiction.[4]

III. *Quantificational arithmetics.* In order to establish a link between recursiveness and quantificational logic, we next prove a normal form theorem about unary **EA**'s. A unary **EA** formula will be called *normal* if each of its terms is either a single variable or a numeral. Moreover, each unary **EA** formula has what we will call a normal version. This is obtainable from the given formula by a series of transformations based on the following rule, in which C is the formula at hand at any stage: if C has a term that contains a variable x and a string y, either another variable or a numeral, delete y, replace x by a new variable z, and add 'Ax,y,z' to C as an antecedent. For example, the upper of the two formulas below is transformed into the lower by three applications of this rule:

(8a) $Gy111 \rightarrow Hx11y$

(8b) $Az_2,y,z_3 \rightarrow Ax,11,z_2 \rightarrow Ay,111,z_1 \rightarrow Gz_1 \rightarrow Hz_1$

We next define a unary **EA** to be *normal* if each of its axioms is either normal or else is the formula '$Sx1,x$'. (We assume from now on that the unary **EA** digit is '1'.) Moreover, every unary **EA** will be said to have a *normal version*, comprising normal versions of its axioms (typographically altered to avoid the predicates 'S' and 'A' if these occur), the axiom '$Sx1,x$', and the two axioms

(9) $Sy,x \rightarrow Ax,1,y$

$Ax,y,z \rightarrow Sw,y \rightarrow Su,z \rightarrow Ax,w,u$

We now show that a unary **EA** predicate represents the same set or relation in a normal version as in the **EA** itself, which implies

(10) *Every recursively enumerable set or relation is represented in a normal version of some unary* **EA**.

Due to the axioms (9) and '$Sx1,x$', in every normal version of a unary **EA**, the predicates 'S' and 'A' represent the Successor and Addition relations. Thus if, say, (8a) is an axiom in a unary **EA**, its instances are also derivable in any normal version of this **EA**, while no instance of this form is derivable in the normal version unless derivable in the given **EA**. Finally, every unary **EA** theorem has a proof in which all instantiations precede all steps by *modus ponens*, the effect of which proof may be had in any normal version.

Quantificational arithmetics (**QA**'s) will now be introduced, in order to define a *counterpart* **QA** for any normal version of a unary **EA**. Let E be a normal unary **EA** formula whose longest numeral term has $k+1$ digits. The counterpart **QA** formula CE is then defined to be the universal closure with respect to all variables but '1' of a conditional whose antecedent is the conjunction '$Sx_1 1. \ldots . Sx_k x_{k-1}$, and whose consequent is obtained from E by putting in parentheses by right association, changing '$\rightarrow$' to '$\supset$', putting 'x_i' for each numeral term with $i+1$ digits, and deleting commas. As an example,

(11) $Fx,11 \rightarrow Gy,111,x \rightarrow Hy,1$

$(x)(y)(x_1)(x_2)[(Sx_1 1.Sx_2 x_1) \supset (Fxx_1 \supset (Gyx_2 x \supset Hy1))]$

Let us now define CS, the **QA** counterpart to a normal version S of a unary **EA** as a set of axioms that comprises the **QA** counterparts to the normal axioms of S and, corresponding to the axiom '$Sx1,x$', the formula '$(x)(\exists y)Syx$'. The theorems of CS will be these axioms and such **QA** counterparts to formulas of S as are quantificationally derivable from them. By an *atomic instance* we will mean an atomic **EA** formula, like $F(m)$ of the previous section, whose terms are all numerals. In the remainder of this section, then, we show that

(12) *An atomic instance E is provable in a normal version S of a unary* **EA** *iff CE is provable in the* **QA** *counterpart CS.*

As illustration, the following two axioms, along with axioms (9) and '$Sx1,x$', form a typographical variant of a normal version of the unary **EA** of Section II whose axioms were (4).

(13a) $F11$

(13b) $Ax,11,y \rightarrow Fx \rightarrow Fy$

Letting this system be S, the **QA** counterpart CS contains the axiom '$(x)(\exists y)Syx$', the **QA** counterparts to (9), and the axioms

(14a) $(x_1)(Sx_1 1 \supset Fx_1)$

(14b) $(x)(y)(x_1)[Sx_1 1 \supset (Axx_1 y \supset (Fx \supset Fy))]$

As an interpretation in the positive integers of a system CS, let us assign the number *1* to the free variable '*1*', the Successor and Addition relations to the predicates 'S' and 'A' respectively, and to each other predicate let us assign the set or relation that it represents in the normal version S. Then all the axioms of CS, and hence all CS theorems, become true on this interpretation. We see this easily for the axiom '$(x)(\exists y)Syx$' and the **QA** counterparts to (9). The other CS axioms become synonymous with their opposite numbers in S, as exemplified by (13) and (14), which are made true by this interpretation. The axiom '$F11$', for example, here states that the number 2 is in the set represented in S by 'F', which its own presence as an axiom of S guarantees to be true. But given an atomic instance, say, $F(m)$, suppose that its **QA** counterpart $CF(m)$ is provable in CS. Then $CF(m)$, as above interpreted, becomes the true statement that the number m is in the set that 'F' represents in S, or, by definition, that $F(m)$ is provable in S.

In proving (12), we next establish the converse of this, that an atomic instance is provable in a normal version S only if its **QA** counterpart is provable in CS. First, it is plain that if a normal unary **EA** formula D is an instance of another such formula E, then CD follows from CE in any **QA**. For example, taking (13b) and (14b) as E and CE, let D and CD be the respective formulas

(15a) $A11,11,1111 \rightarrow F11 \rightarrow F1111$

(15b) $(x_1)(x_2)(x_3)[(Sx_1 1.Sx_2 x_1 .Sx_3 x_2) \supset (Ax_1 x_1 x_3 \supset (Fx_1 \supset Fx_3))]$

Here as in every such case, the main antecedent of the matrix of CE is a conjunct of its correspondent in CD.

Finally, calling an **EA** formula with no variables an *instance*, we show that the effect of *modus ponens* for normal unary instances may be had for their **QA** counterparts in any **QA**. As we saw before, instantiations may always precede *modus ponens* steps in **EA** proofs, so this completes the argument for (12). Such a *modus ponens* step is typified well enough by the inference from '$B11,111 \rightarrow C11$' and '$B11,111$' to '$C11$', whose respective **QA** counterparts are

(16a) $$(x_1)(x_2)[(Sx_1 1.Sx_2 x_1) \supset (Bx_1 x_2 \supset Cx_1)]$$

(16b) $$(x_1)(x_2)[(Sx_1 1.Sx_2 x_1) \supset Bx_1 x_2]$$

(16c) $$(x_1)(Sx_1 1 \supset Cx_1)$$

Plainly, (16a), (16b), and the axiom '$(x)(\exists y)Syx$' imply (16c).

IV. *Church's theorem*. We now prove (1) from (3), (10), (12), and the nonrecursiveness of D, itself shown using (3). First, we note that by Gödel's completeness theorem, to ask whether a **QA** formula G is provable in a **QA** a conjunction of whose axioms is A is in effect to ask whether '$A \supset G$' is a valid quantificational formula. Hence any clerical routine that disproved (1) would also provide clerical answers to all questions of the former kind.

Supposing such a routine R to exist, let us now ask, for some arbitrary number m, whether $m \varepsilon D$. By (10), since D is recursively enumerable, D is represented, by a predicate which may be assumed to be 'F', in a normal version S of some unary **EA**. Letting A be a conjunction of the axioms of the **QA** counterpart CS, we may apply R to '$A \supset CF(m)$'. If the answer is Yes, which tells us that $CF(m)$ is provable in CS, we infer by (12) that $F(m)$ is provable in S, hence that $m \varepsilon D$. Similarly, we learn from a No answer that $m \notin D$.

What has just been described, however, is a clerical routine that qualifies D as an effective set. This is impossible, by (3) and the nonrecursive character of D. We must conclude, therefore, that no such routine as R exists, which establishes (1).

NOTES

1. I am indebted to the referee who read an earlier version of this paper and made numerous helpful suggestions.

2. Quine defines recursiveness in the general manner of Kleene [3], pp. 227, 266-276, and makes the connection with quantificational logic through a "schematic function theory" that he develops for this purpose. In the present paper, recursiveness is defined in the general manner of Post [5], as modified in Smullyan [7], and no recourse is made to a theory of functions like Quine's.

3. These definitions are taken from Smullyan [7], pp. 3-10, with one significant change—recursive enumerability is there defined in terms of dyadic (*2*-adic) rather than unary **EA**'s. The choice of a base in this definition makes no extensional difference, however, as is shown in Smullyan [7], pp. 35, 36, and in Patton [4].

4. The relation K and this diagonal argument are adapted from the Quine [6] adaptation from Kleene [3], pp. 282, 283.

BIBLIOGRAPHY

1 A. Church, "A Note on the Entscheidungsproblem", *Journal of Symbolic Logic,* Volume 1 (1936).

2 D. Hilbert and P. Bernays, *Grundlagen der Mathematik*, Volume 2, Springer, Berlin, 1939, Edwards, Ann Arbor, 1944.

3 S. C. Kleene, *Introduction to Metamathematics*, Van Nostrand, Princeton, 1952.

4 T. E. Patton, "On *n*-adic Representation of Numbers", *Journal of Symbolic Logic*, Volume 28 (1963).

5 E. L. Post, "Recursively Enumerable Sets of Positive Integers and Their Decision Problems", *Bulletin of the American Mathematical Society*, Volume 50 (1954).

6 W. V. Quine, "A Proof of Church's Theorem", mimeographed, 1954.

7 R. M. Smullyan, *Theory of Formal Systems*, Princeton University Press, Princeton, 1961.

8 A. M. Turing, "On Computable Numbers, with an Application to the Entscheidungsproblem", *Proceedings of the London Mathematical Society*, Series 2, Volume 42 (1936-7).

University of Pennsylvania
Philadelphia, Pennsylvania