Bull. Korean Math. Soc.
Vol. 8 (1971), pp. 1-7.

On constructing an unsolvable Thue system on two letters

Joseph T. Ryan

ABSTRACT

This paper presents in detail the construction of an unsolvable Thue system on two letters. The approach employed consists of first constructing a Thue system Γ on n letters whose decision problem is recursively unsolvable. Then along the lines suggested by Davis [1], a combinatorial system Γ^* whose alphabet consists of two letters is constructed whose decision problem is recursively solvable if and only if that for Γ is.

Introduction

In general, a decision problem inquires as to the existence of effective computational procedures for deciding the truth or falsity of individual statements belonging to a prescribed "class" of declarative statements. Such problems are solved by either showing that an effective algorithm exists or proving that no algorithm exists. If no algorithm exists, then the problem is called *unsolvable*. The existence of unsolvable decision problems has philosophical significance as well as relevance to the theory of digital computers.

The purpose of this paper is to present a constructive proof of the following theorem:

THEOREM *There exists a Thue system whose alphabet consists of two letters and whose decision problem is recursively unsolvable.*

The impetus for this problem comes from Davis [1], who suggests that it is possible to construct a combinatorial system on two letters whose decision problem is recursively solvable if and only if the decision problem of an appropriately constructed combinatorial system on in letters is recursively solvable. Using Davis' framework, both the notions of Gödel numbers and the Universal Turing Machine are useful in this regard.

The necessary terminology and a reasonably concise set of notation are developed in the next section. The last section of this paper presents the constructive proof of the existance of an unsolvable Thue system on two letters.

Terminology and Notation

A *combinatorial system* Γ consists of a single non-empty word called the *axiom* of Γ and a finite set of productions called the productions of Γ. Here, a *production* is defined simply as the binary predicate

$$R^{g,\ h,\ k,}_{\bar{g},\ \bar{h},\ \bar{k},}(X, Y) \longleftrightarrow \bigvee_P \bigvee_Q [(X=gPhQk) \wedge (Y=\bar{g}P\bar{h}Q\bar{k})]$$

The *alphabet* of Γ consists of all letters that occur either in the axiom of Γ or in the $g, h, k, \bar{g}, \bar{h}, \bar{k}$ which define the productions of Γ (symbolized $gPhQk \longrightarrow \bar{g}P\bar{h}Q\bar{k}$). A finite sequence (possible of length 0) of these letters will be called a *word*. The emply word of length 0 is written Λ and the productions of the form

$$\Lambda Pg Q\Lambda \longrightarrow \Lambda P\bar{g}Q\Lambda$$

are called *semi-Thue producations* associated with $g, \bar{g}$. A *semi-Thue system* is a combinatorial system all of whose productions are semiThue productions.

A *Thue system* is a semi-Thue system with the property that the inverse of each of its productions is also one of its productions. If we are given a finite number of pairs of strings J_i, K_i; $i=1,\ 2,\ \cdots,\ m,$ we note that the productions in a Thue system Γ consist of all of the productions

$$PJ_iQ \longrightarrow PK_iQ$$

and

$$PK_iQ \longrightarrow PJ_iQ$$

where $i=1, 2, \cdots, m$.

By a *proof* in Γ is meant a finite sequence $X_1, X_2, \cdots, X_r$ of words such that X_1 is the axiom of Γ and

$$X_{i-1} \longrightarrow X_i$$

with respect to one of the productions of Γ and for all $i=2, 3, \cdots, r$. In each of these, X_i is called a *step* in the proof. W is a *theorem* of Γ (written $\vdash_\Gamma W$) if W is the final step of at least one proof in Γ. The set of all of the Gödel numbers of all of the theorems of the combinatorial system Γ will be written T_Γ. Thus, $\vdash_\Gamma w$ if and only if $gn(W) \in T_\Gamma$ where $gn(W)$ is the Gödel number of W.

The decision problem for a combinatorial system Γ is said to be *recursively solvable or unsolvable* according as T_Γ is or is not a recursive set, respectively.

For the purpose of using "Turing machine" arguments in the development of the proof, the following notational conventions and results presented by Davis [1] are also required.

If Z is a Turing machine, then for each n, we associate with Z an n-ary function

$$\Psi_Z^{(n)}(x_1, x_2, \cdots, x_n) \Bigg|_{x_1=m_1, x_2=m_2, \cdots, x_m=m_m}$$

which is defined as the number of 1's in the tape expression for the $n$tuple $(m_1, m_2, \cdots, m_m)$ when there exists a computation of Z for the n-tuple $(m_1, m_2, \cdots, m_m)$. We write

$$\Psi_Z^{(1)}(x) = \Psi_Z(x)$$

Associated with each simple Turing machine Z and integer m, there is a semi-Thue system $\tau_m(Z)$ with the following properties:

(1) The axiom of $\tau_m(Z)$ is $hq_1\overline{m}h$ where q_1 denotes the first internal configuration of Z and $\overline{m}$ is the tape expression given by

$$\overline{m}=\underbrace{1\,1\ldots1}_{m+1}$$

(2) The productions and alphabet of $\tau_m(Z)$ depend only on Z and not on the number m.

(3) $\tau_m(Z)$ is monogenic

(4) $\vdash \tau_m(Z)hq'h$ if and only if $m \in P_Z$

We associate a semi-Thue system $\sigma(Z)$ as follows:

(1) The alphabet of $\sigma(Z)$ is that of $\tau_m(Z)$.

(2) The axiom of $\sigma(Z)$ is $hq'h$.

(3) The productions of $\sigma(Z)$ are the inverses of those of $\tau_m(Z)$.

Approach

This section briefly outlines the method of construction. We will first construct a Z_0 such that

$$P_{Z_0}=K$$

where K is not recursive and where we agree to write P_{Z_0} for the domain of the function $\Psi_{Z_0}(x)$. Here we note that

$$x \in K \longleftrightarrow \bigvee_y T(x, x, y)$$

where $T(x, x, y)$ is a predicate which states that x is the Gödel number of a Turing machine Z and that y is the Gödel number of a computation with respect to Z beginning with, say, the instantaneous description, $q_1(x)$.

With the Turing machine Z_0, we associate the Thue system $\rho(Z_0)$ which is obtained from $\sigma(Z)$ by adjoining to the productions of $\sigma(Z)$ the inverses of these productions.

If we let Γ be the Thue system thus constructed, we simply construct a combinatorial system Γ^* using a construction algorithm suggested by the proof of the following theorem presented by Davis [1]:

THEOREM *For every combinatorial system Γ, we can constrvct a combinatorial system Γ^* whose alphabet consists of two letters and whose decision* *problem is recursively solvable if and only if that for Γ is. Moreover, if Γ is a semi-Thue system, a Thue system, a normal system, or a Post system, respec-tively, then so is Γ^*.*

Actual Construction

we note immediately that if Z_0 is such that

$$\Psi_{Z_0}=\min_y T(x, x, y),$$

then x belongs to the domain of Ψ_{Z_0} if and only if $\bigvee_y T(x, x, y)$. But if we define K such that

$$x \in K \longleftrightarrow \bigvee_y T(x, x, y)$$

that is, if

$$K=\{x \mid \bigvee_y T(x, x, y)\}$$

then K is recursively enumerable.

But we know that if Z_0 is such a Turing machine and z_0 is its Gödel number then the domain of the function $\Psi_{Z_0}(x)$ is the same as the domain of $\min_y T(z_0, x, y)$. Moreover,

$$\Psi_{Z_0}(x)=\bigcup\{\min_y T(Z_0, x, y)\}$$

Also if $T(Z_0, x, y)$ is true for a given x, then the Gödel number of the final instantaneous description α of this computation is

$$(L\{\min_y T(z_0, x, y\})Gl(\min_y T(z_0, x, y)\}.$$

where if $x=gn(M)$, then $L(x)$ is the number of symbols occuring in M and n Gl x is read "nth Gödel number of x."

Further, since $Z_0(x)$ is computable, there exists a Turing machine Z_0 such that

$$\Psi_{Z_0}{}^{(2)}(z_0, x)=\bigcup\{\min_y(z_0, x, y)\}.$$

But this is defined to be the Universal Turing machine. Thus, if we associate with Z_0 the Thue System $T(Z_0)$ as follows: $T(Z_0)$ is obtained from $\sigma(Z_0)$ by adjoining to the productions of $\sigma(Z_0)$ the inverses of these productions. That is, the alphabet and axiom of $T(Z_0)$ are those of $\sigma(Z_0)$ whereas the productions of $T(Z_0)$ consist of those of $\sigma(Z_0)$ and those of $\gamma_m(Z_0)$

where $\sigma(Z_o)$ and $\Upsilon_m(Z_o)$ are set up in the following manner:

Υ_m: *alphabet*: The alphabet of $\Upsilon_m(Z_o)$ consists of the alphabet of Z_o the internal configurations of Z_o and the additional symbols h, q, q'.

axiom: The axiom of $\Upsilon_m(Z_o)$ is $hq_1S_1^{m+1}h$; that is, $hq_1\overline{m}h$.

productions: (1) with each quadruple of Z_o of the form $q_iS_jS_kq_l$ of Z_o we include the associated production $Pq_iS_jQ \longrightarrow Pq_lS_kQ$.

(2) with each quadruple of Z_o of the form $q_iS_jRq_l$ and each S_k in the alphabet of Z_o we include the productions:

$$Pq_iS_jS_kQ \longrightarrow PS_jq_lS_kQ$$

$$Pq_iS_jhQ \longrightarrow PS_jq_lS_ohQ$$

(3) with each quadruple of Z_o of the form $q_iS_jLq_l$ and each S_k in the alphabet of Z_o, we include the productions

$$PS_kq_iS_jQ \longrightarrow Pq_lS_kS_jQ$$

$$Phq_iS_jQ \longrightarrow Phq_lS_oS_jQ$$

(4) with each internal configuration q_i of Z_o and each S_j in the alphabet of Z_o for which no quadruple of Z_o begins with q_iS_j, we include the production

$$Pq_iS_jQ \longrightarrow PqS_jQ$$

(5) Finally, we include with each S_i in the alphabet of Z_o the productions

$$PqS_iQ \longrightarrow PqQ$$

$$PqhQ \longrightarrow Pq'hQ$$

$$PS_iq'Q \longrightarrow Pq'Q$$

$\sigma(Z_o)$: *alphabet*: Same as $\Upsilon_m(Z_o)$

axiom: $hq'h$

Productions: The inverses of the productions of $\Upsilon_m(Z_o)$ If we now let $\Upsilon \equiv T(Z_o)$. Then

$$\bigvee_y T(x, x, y) \longleftrightarrow x \in K \qquad \text{and}$$

$$K = P_{Z_o} = \{x \mid \vdash hq_1\bar{x}h\} = \{x \mid gn(hq_1\bar{x}h) \in \Upsilon_T$$

Let

$$T(Z_0)=\Gamma$$

and set

$$a_i^*=1b^{i+1}1$$

also let

$$W=a_{i_1}a_{i_2}a_{i_3}\cdots a_{i_p}$$

and set

$$W^*=a_i^*\cdots a_{i_p}^*$$

We also let $\Lambda^*=\Lambda$. Now let the axiom of Γ be called A and let its productions be

$$q_iPhQk_i\longrightarrow\bar{q}_iP\bar{h}_i^*Q\bar{k}_i^*,\quad i=1,\cdots,\quad m.$$

Then Γ^* is taken to be the combinatorial system whose axiom is A^* and whose productions are

$$q_i^*Ph_i^*Qk_i^*\longrightarrow\bar{q}_i^*P\bar{h}_i^*Q\bar{k}_i^*;\quad i=1,\quad\cdots,\quad m.$$

Γ^* is a Thue system on two letters and is unsolvable. Thus, we have constructed an unsolvable Thue system on two letters.

References

1. Martin Davis. ***Computability and Unsolvability***, McGraw-Hill Book Co., New York, 1958.

The Total System Corporation,* Honolulu, Hawaii

---

* Besides serving as President, The Total Systems Corporation, Mr. Ryan is also a Senior Staff Consultant to the Control Data Corporation in the areas of logic design and systems analysis.