A CHARACTERIZATION THEOREM FOR A SUBCLASS OF ETOL LANGUAGES +

A. Ehrenfeucht
Department of Computer Science
University of Colorado
Boulder, Colorado 80302 U.S.A.

G. Rozenberg
Institute of Mathematics
University of Utrecht
Utrecht-Uithof, The Netherlands

Report # CU-CS-028-73 August, 1973

All correspondence to:

G. Rozenberg
Institute of Mathematics
Utrecht University
Utrecht - Uithof
The Netherlands

+ This work supported by National Science Foundation Grant # GJ-660

INTRODUCTION.

This paper deals with a class of developmental languages. The theory of developmental systems and languages originated in the works of Lindenmayer (see [Lindenmayer]). This theory provided a useful theoretical framework within which the nature of cellular behavior in development can be discussed, computed and compared (see, e.g. [Herman and Rozenberg], [Lindenmayer] and [Lindenmayer and Rozenberg]). It turned out that developmental systems and languages are interesting and novel objects from the formal language theory point of view. Especially in comparison with Chomsky grammars and languages (see, e.g., [Ginsburg]) they provided a lot of insight into the basic problems of formal language theory.

An important subclass of developmental systems are the so called ETOL systems (see [Rozenberg, 1973]) which were devised to allow descriptions of development which take into account both the changing environment and the inaccuracy of our observations.

One of the basic open problems within the theory of ETOL systems (and in fact within the whole theory of developmental systems) are the characterization theorems which allow one, for example, to prove that some languages are not ETOL languages (i.e. languages generated by the ETOL systems).

This paper provides such a characterization for a subclass of ETOL languages. The characterization theorem (Theorem 7) binds together the number of occurrences (in the words of the given ETOL language) of letters from a given set of letters with the distribution of these letters.

The paper also discusses some applications of the main result.

PRELIMINARIES.

We assume the reader to be familiar with the basics of formal language theory (see, e.g., [Ginsburg], whose notation and terminology we shall mostly follow). In addition to this we shall use the following notation:

(i) N denotes the set of nonnegative integers and $N^+ = N - \{0\}$.

(ii) If x is a word over an alphabet Σ, then $|x|$ denotes the length of x and Min(x) denotes the set of letters which occur in x. For a in Σ, $\#_a(x)$ denotes the number of occurrences of the letter a in x and if B is a subset of Σ then $\#_B(x) = \sum_{a \in B} \#_a(x)$.

(iii) If A is a finite set then #A denotes its cardinality. If $B \subseteq A$ and $\#B = 1$ then B is called a <u>singleton in</u> A.

(iv) A <u>coding</u> is a letter to letter homomorphism. If h is a homomorphism from Σ^* into V^* and $L \subseteq V^*$ then $h^{-1}(L) = \{x \in \Sigma^* : h(x) = y$ for some y in L$\}$.

DEFINITIONS AND EXAMPLES.

In this section we define the notions needed for this paper and give some examples.

Definition 1. If L is a language over an alphabet Σ and B is a nonempty subset of Σ, then

(i) B is called nonfrequent (in L) if there exists a constant $C_{B,L}$ such that for every x in L, $\#_B(x) < C_{B,L}$; otherwise B is called frequent in L.

(ii) B is rare (in L) if for every positive integer k there exists a n_k in N^+ such that for every n larger than n_k, if a word x in L contains n occurrences of letters from B then each two such occurrences are distant not less than k.

Definition 2. An ETOL system is a construct $G = \langle V_N, V_T, P, \omega \rangle$ such that

V_N is a finite alphabet (of nonterminal letters or symbols),

V_T is a finite nonempty alphabet (of terminal letters or symbols),

such that $V_N \cap V_T = \emptyset$,

ω is an element of $(V_N \cup V_T)^+$ (called the axiom of G),

$\mathcal{P}$ is a finite nonempty family, each element of which is a finite nonempty set of the form $\{a \to \alpha$: a is in $V_N \cup V_T$ and α is in $(V_N \cup V_T)^*\}$ (where we assume that the symbol $\to$ is not in $V_N \cup V_T\}$. Each element P of $\mathcal{P}$ (called a table of G) satisfies the condition:

for every a in $V_N \cup V_T$ there exists at least one α in $(V_N \cup V_T)^*$ such that $a \to \alpha$ is in P. (If P is in $\mathcal{P}$ and $a \to \alpha$ is in P then $a \to \alpha$ is called a production for a in P, or just a production in P).

Remark. In the sequel we shall consider only reduced ETOL systems, i.e., ETOL systems $G = \langle V_N, V_T, P, \omega \rangle$ such that each letter from $V_N \cup V_T$ occur in some word in L(G).

Definition 3. Let $G = \langle V_N, V_T, P, \omega \rangle$ be an ETOL system.

(i) If $V_N = \emptyset$ then G is called a TOL system. (In this case we write G as $\langle V_T, P, \omega \rangle$).

(ii) If for every P in P and for every a in $V_N \cup V_T$ there exists exactly one α such that $a \to \alpha$ is in P, then G is called deterministic. (We use the letter D to denote the deterministic restriction, and so, e.g., a DTOL system means a deterministic TOL system).

Definition 4. Let $G = \langle V_N, V_T, P, \omega \rangle$ be an ETOL system.

(i) Let $x \in (V_N \cup V_T)^*$, say $x = b_1 \ldots b_t$ for some $b_1, \ldots, b_t$ in $(V_N \cup V_T)$, and let $y \in (V_N \cup V_T)^*$. We say that x directly derives y (in G), denoted as $x \underset{G}{\Rightarrow} y$, if there exist P in P and a sequence $\pi_1, \ldots, \pi_t$ of productions from P such that, for every i in $\{1, \ldots, t\}$, $\pi_i = b_i \to \alpha_i$ and $y = \alpha_1 \ldots \alpha_t$. (In this case we also write $x \underset{P}{\Rightarrow} y$, and we say that x directly derives y (in G) using P).

(ii) As usual $\overset{+}{\underset{G}{\Rightarrow}}$ denotes the transitive closure, and $\overset{*}{\underset{G}{\Rightarrow}}$ the reflexive and transitive closure of the relation $\underset{G}{\Rightarrow}$. If $x \overset{*}{\underset{G}{\Rightarrow}} y$ for some x, y in $(V_N \cup V_T)^*$ then we say that x derives y (in G).

(iii) If $x_0 \underset{T_1}{\Rightarrow} x_1 \underset{T_2}{\Rightarrow} x_2 \underset{T_3}{\Rightarrow} \cdots \underset{T_p}{\Rightarrow} x_p$, for some $p \geq 1$ and some $T_1, \ldots, T_0$ in P then we also write $x_0 \xrightarrow[G]{T_1 \ldots T_p} x_p$, and if G is deterministic then we write $x_p = T_1 \ldots T_p(x_0)$. The sequence $D = (x_0, x_1, \ldots, x_p)$ is called a derivation of x_p from x_0 in G and the sequence $\tau = T_1, \ldots, T_p$ is called an associated sequence of D. If $x_0 = \omega$ then D is called a derivation of x_p in G (in this case we also write $x_0 \overset{P}{\underset{G}{\Longrightarrow}} x_p$). If G is deterministic then the pair (D,τ) is called a description of x_p (in G).

Remark. If G is an arbitrary ETOL system and $D = (x_0,\ldots,x_p)$ is a derivation of x_p in G with an associated sequence τ, then, in general, the pair (D,τ) does not provide us with the information needed to determine which particular productions were used to rewrite particular occurrences of letters in x_i (for $0 \leq i \leq p-1$). However, we shall assume that the pair (D,τ) provides such an information, but this should not lead to confusion. (Such a convention saves us a lot of combersome notation).

Definition 5. Let $G = \langle V_N, V_T, P, \omega \rangle$ be an ETOL system. The language of G, denoted as L(G), is defined by $L(G) = \{x \in V_T^* : \omega \overset{*}{\underset{G}{\Longrightarrow}} x\}$.

Definition 6. A nonempty language K different from $\{\Lambda\}$ is called an ETOL (TOL, DTOL, etc.) language if, and only if, there exists an ETOL (TOL, DTOL, etc.) system G such that $L(G) = K$.

We end this section with some examples of ETOL systems and languages.

Example 1.

$G = \langle\{S, A, B, C, D\}, \{a, b\}, \{\{S \to AB, S \to CD, A \to A, B \to B, C \to C, D \to D, a \to a, b \to b\}, \{A \to A^2, B \to B, C \to C, D \to D, S \to S, a \to a, b \to b\}, \{C \to C^3, A \to A, B \to B, D \to D, S \to S, a \to a, b \to b\}, \{A \to a, B \to b, C \to b, D \to a, S \to S, a \to a, b \to b\}\}, S\rangle$ is an ETOL system such that $L(G) = \{a^{2^n} b : n \geq 0\} \cup \{b^{3^n} a : n \geq 0\}$.

Example 2.

$G = \langle \{a\}, \{\{a \to a^2\}, \{a \to a^3\}\}, a \rangle$ is a TOL system such that $L(G) = \{a^{2^n \cdot 3^m} : n, m \geq 0\}$.

AUXILLIARY RESULTS.

In this section we shall show how the properties of being rare and being unfrequent are connected with each other in TOL languages. As our main result (Theorem 1) is trivially true for finite languages, in the sequel we shall deal with infinite languages only. Thus, if we shall write "a language" we shall mean an infinite one.

The following construct will turn out to be a useful one for this paper.

Definition 7. Let $G = \langle \Sigma, \mathcal{P}, \omega \rangle$ be a TOL system. A DTOL system associated with G, denoted as Assoc(G), is defined by Assoc(G) $= \langle \Sigma, \overline{\mathcal{P}}, \omega \rangle$ where a table $\overline{P}$ is in $\overline{\mathcal{P}}$ if, and only if, there exists a table P in $\mathcal{P}$ such that $\overline{P} \subseteq P$.

We leave to the reader the obvious proof of the following result.

Lemma 1. If G is a TOL system, then L(Assoc(G)) $\subseteq$ L(G).

In the first part of this section we shall deal with sets of letters which are singletons. This will turn out to be sufficient for the proof of our main result (Theorem 1).

First of all we have the following result.

Lemma 2. Let $G = \langle \Sigma, \mathcal{P}, \omega \rangle$ be a TOL system and B a singleton in Σ. If B is rare in L(G), then B is also rare in L(Assoc(G)).

Proof.

This result follows directly from Lemma 1.

The next result shows that the property of being nonfrequent in L(G) is invariant under the operation of taking Assoc(G), for all TOL systems G and all singletons B.

Lemma 3. If $G = \langle \Sigma, P, \omega \rangle$ is a TOL system and B is a singleton in Σ, then B is nonfrequent in L(G) if, and only if, B is nonfrequent in L(Assoc(G)).

Proof.

Let $G = \langle \Sigma, P, \omega \rangle$ be a TOL system and B a singleton in Σ, say $B = \{\sigma\}$. We shall prove that if B is nonfrequent in L(G), then it is also nonfrequent in L(Assoc(G)) and if B is frequent in L(G), then it is also frequent in L(Assoc(G)). (This is obviously equivalent to the statement of the lemma).

By Lemma 1, $L(Assoc(G)) \subseteq L(G)$ and so if B is nonfrequent in L(G) it is also nonfrequent in L(Assoc(G)).

Now, let us assume that B is frequent in L(G).

Let x be a nonempty word in L(G) such that $x \neq \omega$, let $D = (\omega = x_0, x_1, \ldots, x_p = x)$ be a deriviation of x in G and let $T_1, T_2, \ldots, T_p$ be an associated sequence of G. For each i in $\{0, 1, \ldots, p-1\}$ and for each a in $Min(x_i)$, let (a, i) denote fixed (but an arbitrary) occurrence of a in x_i such that it "contributes" in the derivation D with an associated sequence $T_1, \ldots, T_p$ at least as many occurrences of σ to x as any other occurrence of a in x_i. For each i in $\{0, 1, \ldots, p-1\}$ and for each a in $Min(x_i)$, let $\pi(a, i)$ denote the production (from T_i) applied to (a, i) in the derivation D. Finally for each i in $\{0, 1, \ldots, p-1\}$ let $\overline{T}_i$ denote a subset of T_i such that, for every a in $Min(x_i)$ the only production for a in $\overline{T}_i$ is $\pi(a, i)$, and if a is not in $Min(x_i)$ then the only production for a in $\overline{T}_i$ is some fixed production from T_i.

Now let $\overline{D} = (\omega = \overline{x}_0, \overline{x}_1, \ldots, \overline{x}_p)$ be a derivation in Assoc(G) such that, for each i in {1,..., p}, $\overline{x}_i = \overline{T}_i(\overline{x}_{i-1})$. By construction of $\overline{D}$, $\#_B(\overline{x}) \geq \#_B(x)$.

Thus, for every nonempty word x in L(G), such that $x \neq \omega$, there exists a word $\overline{x}$ in L(Assoc(G)) such that $\#_B(\overline{x}) \geq \#_B(x)$. Hence if B is frequent in L(G), it must be also frequent in L(Assoc(G)).

Thus Lemma 3 holds.

Lemma 4. Let $G = \langle \Sigma, P, \omega \rangle$ be a DTOL system. If B is a singleton in Σ and B is rare in L(G), then B is nonfrequent in L(G).

Proof.

Let $G = \langle \Sigma, P, \omega \rangle$ be a DTOL system and let B be a singleton in Σ, say $B = \{\sigma\}$, such that B is rare in L(G). We shall prove the lemma by showing that if B is frequent in L(G), then it cannot be rare in L(G).

Thus, let us assume that B is frequent in L(G).

Let $\#\Sigma = \ell$ and let $F = \max \{|\gamma| :$ there exists a in Σ such that $a \xRightarrow[G]{\ell!(\ell-1)+\ell+1} \gamma\}$.

Let n be a positive integer such that $n > |\omega|$.

Let z be a word in L(G) such that z contains at least n occurrences of the letter σ. Let $D = (\omega = z_0, \ldots, z_p = z)$ be a derivation of z in G and let (D, τ) be a description of z in G, where $\tau = T_1 \ldots T_p$. For i in $\{0, \ldots, p-1\}$, the level i of (D, τ) is called productive if there exists a letter a in $Min(x_i)$ such that $T_{i+1} \ldots T_p(x_i)$ contains at least two occurrences of σ; otherwise the level i is called unproductive.

Note that:

(i) $\#_B(z) > |\omega|$ and so at least one level of (D,τ) is productive, and

(ii) if the level i is unproductive and $(i+1) \leq p-1$, then also the level $(i+1)$ is unproductive.

Let i_0 be the largest nonegative integer such that the level i_0 is productive.

The tail of (D,τ), denoted as tail (D,τ), is a pair $(\overline{D}, \overline{\tau})$ where $\overline{D} = (x_{i_0+1}, x_{i_0+2}, \ldots, x_p)$ and $\overline{\tau} = T_{i_0+2} T_{i_0+3} \ldots T_p$, $(p-(i_0+1)$ is said to be the length of the tail).

If the length of tail (D,τ) is smaller than $((\ell-1) \cdot \ell! + \ell+1)$ then z contains at least two occurrences of σ distant no more than F (because i_0 is a productive level of (D,τ) and so there exists a letter, say d, in $\mathrm{Min}(x_{i_0})$ which contributes at least two occurrences of σ in z, but at the same time the whole subword of z contributed by any occurrence of d in x_{i_0} is no longer than F).

So let us assume that the length of tail (D,τ) is larger than or equal to $((\ell-1) \cdot \ell! + \ell+1)$.

For each i in $\{0, \ldots, p-1\}$, let $\mathrm{Min}_B(x_i)$ denote the set of all letters in $\mathrm{Min}(x_i)$ which contribute in (D,τ) an occurrence of σ in z.

Let us consider the sequence $\#\mathrm{Min}_B(x_{i_0+1})$, $\#\mathrm{Min}_B(x_{i_0+2}), \ldots, \#\mathrm{Min}_B(x_p)$. Obviously, if $i_0+1 \leq g < j \leq p$, then $\#\mathrm{Min}_B(x_g) \geq \#\mathrm{Min}_B(x_j)$. But $\#\Sigma = \ell$ and so for no more than ℓ elements i in the sequence $\#\mathrm{Min}_B(x_{i_0+1}), \ldots, \#\mathrm{Min}(x_p)$ we have $\#\mathrm{Min}_B(x_i) > \#\mathrm{Min}(x_{i+1})$.

Let j_0, j_1 be arbitrary two levels such that $i_0+1 \leq j_0 < j_1 \leq p$ and $\#Min_B(x_{j_0}) = \#Min_B(x_{j_1}) = \ldots = \#Min_B(x_{j_1-1}) < \#Min_B(x_{j_1})$. We shall show now that if $(j_1-j_0) > \ell!$, then there exists two levels f_0, f_1 such that $j_0 \leq f_0 < f_1 \leq j_1$ and if $c \in Min_B(x_{f_0})$, then $T_{f_0+1} \ldots T_{f_1-1}(c) = \beta_1 \, c \, \beta_2$, where $\beta_1, \beta_2 \in (Min(x_{f_1}) - Min_B(x_{f_1}))^*$.

This is proved as follows.

Note that, for every s in $\{j_0, \ldots, j_1-2\}$, every occurrence of a letter from $Min_B(x_s)$ in x_s contributes exactly one occurrence of a letter from $Min_B(x_{s+1})$ in x_{s+1} and (because G is deterministic) two different occurrences in x_s of the same letter from $Min(x_s)$ contribute exactly the same words into x_{s+1}. Thus we have a one-to-one correspondence between letters in $Min_B(x_s)$ and $Min_B(x_{s+1})$, and we can talk about a permutation π_s (taking $Min_B(x_s)$ into $Min_B(x_{s+1})$ and extended by identity on all other symbols of Σ). Thus we deal with a finite group of permutations with at most $\ell!$ elements (recall that $\#\Sigma = \ell$). Hence (see Lemma 8 in the Appendix), because $(j_1-j_0) > \ell!$, there must be two levels f_0, f_1 such that $j_0 \leq f_0 < f_1 \leq j_1$ and the permutation $\pi_{f_0} \pi_{f_0+1} \cdots \pi_{f_1-1}$ is the identity permutation. Thus our claim holds.

But then we can "shorten" the derivation D by the "piece from the level f_0 to the level f_1" and obtain a derivation $D_1 = (\omega = x_0, x_1, \ldots, x_{f_0}, x^{(1)}_{f_1+1}, \ldots, x^{(1)}_p)$ with an associated sequence $\tau_1 = T_1 \ldots T_{f_0} T_{f_1+1} \ldots T_p$, which are such that $\#_B(x^{(1)}_p) \geq \#_B(x_p)$ and the length of the tail of (D_1, τ_1) is smaller than the length of the tail of (D, τ).

Now we iterate the whole procedure (based on the length of the tail of the currently considered pair (D_i, τ_i)) and eventually we obtain a pair

(D_u, τ_u), for some $u \geq 1$, such that D_u is a derivation in G of the word $x_p^{(u)}$ with $\#_B(x_p^{(u)}) \geq \#_B(x_p)$ and the length of the tail of (D_u, τ_u) is smaller than $((\ell-1) \cdot \ell! + \ell + 1)$. (Note that the length of the longest tail without repetitions cannot be longer than $((\ell-1) \cdot \ell! + \ell + 1)$). But then (repeating the argument used before in this proof) $x_p^{(u)}$ contains at least two occurrences of σ distant no more than F.

Consequently, we have proved that there exists a positive integer $k_B (k_B = F)$ such that for every n in N^+ there exist an m_n in N^+ and a word x in L(G) such that $m_n > n$, $\#_B(x) = m_n$ and x contains at least two occurrences of σ distant less than k_B. Thus B is not rare in L(G).

Hence assuming that B is frequent in L(G) we get that B is not rare in L(G) and this proves Lemma 4.

Thus for an arbitrary TOL language L and for an arbitrary singleton rare in L we have the following result.

<u>Lemma 5</u>. If $G = \langle \Sigma, P, \omega \rangle$ is a TOL system, B is a nonempty subset of Σ and B is rare in L(G), then B is nonfrequent in L(G).

<u>Proof</u>.

Let L be a TOL language generated by a TOL system $G = \langle \Sigma, P, \omega \rangle$ and let B be a nonempty subset of Σ such that B is rare in L.

Obviously, each subset of B is also rare in L and in particular each singleton in B is rare in L(where L = L(G)).

Thus, if C is a singleton in B, then, by Lemma 2, C is rare in L(Assoc(G)). But then (recall that Assoc(G) is a DTOL system) from Lemma 4 it follows that C is nonfrequent in L(Assoc(G)), and consequently, by Lemma 3, C is nonfrequent in L(G) = L.

Thus (because B is a finite union of singletons in B) B itself is non-frequent in L and Lemma 5 holds.

THE RESULT AND ITS APPLICATIONS.

In this section we prove our main result which is a characterization of a subclass of ETOL languages. As an application we prove some languages to be non-ETOL languages.

To generalize Lemma 5 to arbitrary ETOL systems we need the following result proved in [Rozenberg & Ehrenfeucht].

Lemma 6. Every ETOL language is a coding of a TOL language.

Now let us notice that the operation of coding preserves the properties of being rare and nonfrequent in the following sense (the easy proof of the next result is left to the reader).

Lemma 7. Let L be a language over an alphabet Σ, K be a language over an alphabet V and h be a coding from V^* into Σ^* such that $h(K) = L$. Let B be a nonempty subset of Σ. Then

(i) if B is rare in L, then $h^{-1}(B)$ is rare in K, and

(ii) if C is nonfrequent in K, then h(C) is nonfrequent in L.

Now we can easily prove our main result.

Theorem 1. If L is an ETOL language over an alphabet Σ, B is a nonempty subset of Σ and B is rare in L, then B is nonfrequent in L.

Proof.

This result follows directly from Lemmata 5, 6, and 7.

It should be obvious to the reader that Theorem 1 may be used to prove that certain languages are not ETOL languages.

For example we have the following useful result.

Theorem 2. Let ψ be a function from N^+ into N^+ such that $\lim_{n \to \infty} \psi(n) = \infty$ and let U be an arbitrary infinite subset of N^+. Then, the language $K(\psi, U) = \{ba^{m_1} ba^{m_2} \ldots ba^{m_k} : k \in U, m_1, \ldots, m_k \in N^+$ and $m_i = \psi(i)$ for $1 \leq i \leq k\}$ is not an ETOL language.

Proof.

Let ψ, U and $K(\psi, U)$ satisfy the statement of Theorem 2.

If we assume that $K(\psi, U)$ is an ETOL language, then the singleton $\{b\}$ must be nonfrequent in $K(\psi, U)$ (because $\{b\}$ is obviously rare in $K(\psi, U)$). But $\{b\}$ is frequent in $K(\psi, U)$; a contradiction.

Thus $K(\psi, U)$ is not an ETOL language, and Theorem 2 holds.

As an application of Theorem 2 we shall give a constructive proof of a previously known result. It was proved in [Rozenberg, 1973] that the class of ETOL languages is strictly included in the class of Λ-free context-free programmed languages (for the definition of this class see, e.g., [Rozenberg, 1972], whose "graph notation" for context-free programmed grammars we shall use in the proof of our next result). This proof was, however, "nonconstructive", based on different closure properties of discussed classes of languages. In fact until now it was an open problem to find a Λ-free context-free programmed language which is not an ETOL language. We can solve this problem now.

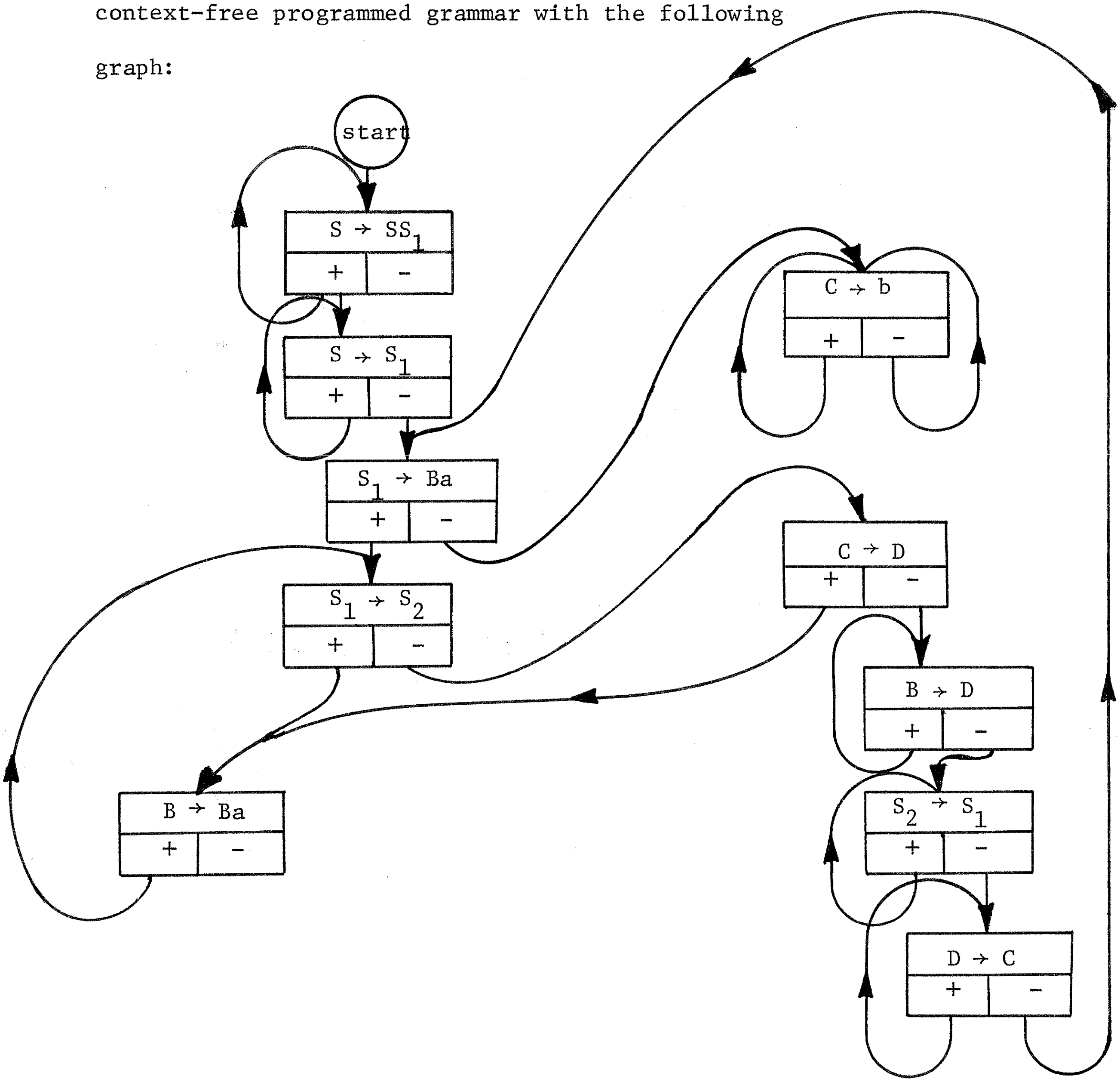
Theorem 3. There exists a Λ-free context-free programmed language which is not an ETOL language.

Proof.

Let $L = \{(ba^n)^n : n \in N^+\}$.

By Theorem 2 (put ψ to be the identity function on N^+ and $U = N^+$, then $K(\psi, U) = L$) L is not an ETOL language.

But the reader can easily check that L is generated by the Λ-free context-free programmed grammar with the following graph:



Hence L is a Λ-free context-free programmed language, whereas it is not an ETOL language. Thus Theorem 3 holds.

REFERENCES.

Ehrenfeucht, A. and Rozenberg, G., Nonterminals versus homomorphisms in defining languages for some classes of rewriting systems, submitted for a publication.

Ginsburg, S., The mathematical theory of context-free languages, McGraw-Hill, 1966.

Herman, G. and Rozenberg G., Developmental systems and languages, to be published by North-Holland Publ. Company.

Lindenmayer, A., Mathematical models for cellular interactions in development, Journal of Theoretical Biology, 1968, v. 18, 280-315.

Lindenmayer, A. and Rozenberg, G., Developmental systems and languages, Proceedings of the Fourth ACM Symposium on Theory of Computing, 1972.

Rozenberg, G., Direction controlled programmed grammars, Acta Informatica, 1972, v. 1, 242-252.

Rozenberg, G., Extension of tabled OL systems and languages, International Journal of Computer and Information Sciences, 1973, to appear

APPENDIX.

Lemma 8. If G is a finite group consisting of s elements and $g_1 \cdot g_2 \cdot \ldots \cdot g_k$ is a product of k elements of the group for some $k > s$, then for some i_0 in $\{1,\ldots,k-1\}$ and a positive integer r such that $(i_0+r) \leq k$ we have $g_{i_0} \cdot g_{i_0+1} \cdot \ldots \cdot g_{i_0+r} = e_G$ where e_G is the identity in G.

Proof.

Let G, s and k satisfy the statement of the lemma.

Then g_1, $g_1 \cdot g_2$, $g_1 \cdot g_2 \cdot g_3, \ldots, g_1 \cdot g_2 \cdot \ldots \cdot g_k$ are k elements of G and, as $k > s$, for some i_0 in $\{1,\ldots, k-1\}$ and for some positive integer r such that $(i_0+r) \leq k$ we have $g_1 \cdot \ldots \cdot g_{i_0} = g_1 \cdot \ldots \cdot g_{i_0} \cdot g_{i_0+1} \cdot \ldots \cdot g_{i_0+r}$ and consequently $g_{i_0+1} \cdot \ldots \cdot g_{i_0+r} = e_G$. Thus Lemma 8 holds.

ACKNOWLEDGMENT.

The authors are indebted to J. Malitz for his comments on the original manuscript.