J. Symbolic Computation (1987) 3, 39–68

Thue Systems as Rewriting Systems†

RONALD V. BOOK

Department of Mathematics,
University of California at Santa Barbara,
Santa Barbara, California 93106, *USA*

This paper is a survey of recent results on Thue systems, where the systems are viewed as rewriting systems on strings over a finite alphabet. The emphasis is on Thue systems with the Church–Rosser property, where the notion of reduction is based on length-decreasing rewriting rules. The main effort is expended in outlining the properties of such systems, paying close attention to the issue of the possible decidability of properties and to the issue of the computational complexity of decidable properties. Since Thue systems may also be considered as presentations of monoids, the language of monoids (and groups) is used to describe some of these properties.

1. Introduction

Replacement systems arise in the study of formula manipulation systems such as theorem provers, program optimisers, and algebraic simplifiers. These replacement systems take such forms as term rewriting systems, tree manipulating systems, graph grammars, etc. The study of abstract data types is another area where such systems are useful. The principal problem in this context is the word problem: given a system and two objects, are the two objects equivalent? From a slightly different viewpoint the problem can be stated as follows: can one of these objects be transformed into the other by means of a finite number of applications of the rewriting rules in the given system? This leads naturally to the question of the decidability of the word problem for a given class of systems. In general it is desirable to be able to describe canonical representatives or unique normal forms for objects in the domain of the rewriting system. If unique normal forms are guaranteed to exist and there is an algorithm for computing the unique normal form of an object, then the word problem is decidable.

Recently there has been a great increase in interest in rewriting and replacement systems. Part of this increased interest stems from the advances made in symbolic computation in general and also in building systems for automated deduction and for computer algebra. In addition, there have been a number of new results that add to our understanding of the underlying theory and to certain applications, e.g. algorithms underlying computer algebra.

† This is the revised version of the text of an invited lecture presented at the First International Conference on Rewriting Techniques and Applications, Dijon, France, May 1985. (See Jouannaud, 1985.) The preparation of this paper was supported in part by the National Science Foundation under Grant DCR-8314977. A major portion of this paper was written while the author was at the Mathematical Sciences Research Institute, Berkeley, CA.

0747-7171/87/010039+30 $03.00/0

If one uses an algorithm to solve some problem, then it is important to consider whether or not the algorithm is efficient. In the study of combinatorial algorithms much effort is expended in attempting to determine whether or not specific problems actually have efficient algorithms, that is, whether or not specific problems are tractable or feasible. Sometimes the solution of a problem by use of rewriting systems allows one to determine bounds on the inherent complexity of the problem. Unfortunately, it is extremely difficult to obtain results about tractable problems of rewriting systems in general. It appears that such results can only be obtained by restricting attention to specific types of objects. In this paper we consider the rewriting of strings and the inherent computational complexity of problems that arise there.

The subject of this survey paper is Thue systems, as rewriting systems on strings over a finite alphabet. The emphasis is on Thue systems with the Church–Rosser property, where the notion of reduction is based on length-decreasing rewriting rules, and the main effort is expended in outlining the properties of such systems and the monoids they present. Of special concern are the results that describe the inherent computational complexity of problems that arise in this area. The intended audience is researchers studying rewriting techniques, automated deduction, computer algebra, and, more generally, symbolic computation. The purpose is to inform the audience of the results in this area that have been developed in the last eight to ten years; while this includes a number of results by the author, his students, and his colleagues, others have somewhat different views of the subject, e.g. see Jantzen (1984). It is hoped that the audience will be able to use the results surveyed here as counter-examples and also as suggestions for results that may be established about more general types of rewriting systems.

A Thue system is simply a set of ordered pairs (u, v) of strings (over some alphabet); the rewriting of a given string w is performed by (non-deterministically) replacing some occurrence of the string u in w by the string v or by replacing some occurrence of string v in w by string u. When dealing with Thue systems, there is an advantage that is not always available when dealing with more general types of rewriting systems: the multiplication in a free monoid (that is, concatenation) is associative. Thue (1914) was interested in the general problem of rewriting, considering systems of rules for rewriting combinatorial objects such as graphs or trees as well as strings, and he studied the word problem in this context. Thue systems have also been studied by computer scientists and by logicians interested in computability theory.

Viewed as rewriting systems on strings, Thue systems are also of interest to algebraists since they are presentations of monoids. A Thue system induces a congruence on the free monoid generated by the alphabet of the system. The collection of congruence classes forms a quotient monoid under the multiplication obtained by first multiplying (concatenating) strings in the free monoid and then taking the congruence class of the product. Of course, it is possible that this monoid is a group. While results concerning groups or monoids may not be considered to be of primary interest to the researcher in symbolic computation, it turns out that the language of such algebraic systems is quite useful in describing the power of certain restricted Thue systems, e.g. Thue systems that give rise to complete rewriting systems, and Thue systems with the Church–Rosser property.

In order to study Thue systems to learn more about general rewriting systems, one looks for an ordering on the strings and properties of the rewriting rules that enable unique normal forms to exist. There are many ways to do this and one might hope to find ways such that when a Thue system is both noetherian and confluent, then the word

problem is guaranteed to be tractable. Unfortunately, even for objects as conceptually simple as quotient monoids of finitely generated free monoids this is not possible in general. We survey a number of results that show just how badly this notion fails. This leads us to consider one case where a number of positive results are known and where there are results in the complexity theory literature that can be used to determine upper bounds on the complexity of certain specific problems. In this case the notion of "reduction" in the rewriting process depends on length.

Consider the partial order on free monoids determined by comparing lengths of strings. For a given Thue system T, a string x *reduces* to a string y if y can be obtained from x by applying a sequence of length-decreasing rules of T. The system T has the *Church–Rosser property* (or "is Church–Rosser") if for every x and y, x and y are congruent if and only if there exists a z such that both x and y reduce to z. Because the ordering is based on length, it is clear that for every string w there exists an "irreducible" string $\bar{w}$ such that w reduces to $\bar{w}$; when the Thue system is Church–Rosser, the string $\bar{w}$ is unique. In the case of a finite Thue system that is Church–Rosser, there is a linear-time algorithm to solve the word problem. Further, there is a polynomial-time algorithm to determine whether a Thue system is Church–Rosser.

This approach to the study of Thue systems and Thue congruences was initiated by Maurice Nivat and his colleagues and students in France. The principal contributions of that group were made in the late 1960s and early 1970s. The motivation of Nivat's school was based on the intertwining of algebra and formal language theory that has been characteristic of the achievements made by this school in theoretical computer science. Berstel (1977) has written a survey of the main results in this area obtained by that school through the mid-1970s. More recent work, particularly outside France, has been influenced not only by the work of Nivat's school but also by questions arising in the study of term-rewriting systems, symbolic computation, and computability theory. A variety of proof techniques and combinatorial algorithms has been developed and their applications have produced a number of interesting results and have stimulated some important work.

In section 3 certain results about string rewriting systems are described. Here the notion of reduction is not based on length; rather, it is assumed that the rewriting system generates a relation that is both noetherian and confluent. Such systems are called *complete* and have properties that are similar to complete term-rewriting systems. The results show that a system's being complete does not itself guarantee that the word problem will be easy to solve. In section 4 properties of arbitrary Thue systems and those with the Church–Rosser property are described. The properties that are featured include those that have played the most important role in recent developments. Several new results are described.

One important motivation for studying Thue systems with the Church–Rosser property (particularly for the school of Nivat) has been the specification of formal languages, more specifically, subclasses of the class of context-free languages. Certain fundamental results as well as recent results and interesting new classes are described in section 5.

As noted above, a Thue system can be viewed as a presentation of a monoid. In sections 6–9 we describe what is known about the classes of monoids and groups that have Church–Rosser presentations. The study of the algebraic properties of monoids with presentations as Thue systems that are Church–Rosser has been extremely fruitful. Some of the most interesting results in this area have been developed quite recently; of particular interest are the results by Otto (1985, 1986*a*, *b*, *c*). While properties of groups

and monoids may be peripheral to studying other types of rewriting systems, they are central to the subject of string rewriting since they provide excellent examples and yield a convenient language for illustrating the power of the underlying notions.

In section 10 we provide a very brief description of results on Thue systems that are not Church–Rosser but have properties similar to those of Church–Rosser systems.

In the last ten years a wide variety of proof techniques has been applied by those studying problems of Thue systems. The rich collection of results that have been obtained shows that this aspect of the theory of rewriting systems is not purely algebra or logic or formal language theory. Techniques from each of these areas are useful in such studies and one can expect to find results about Thue systems that speak to problems in each of these areas. It is hoped that the results obtained in this area, particularly the results concerning the inherent computational complexity of various problems, will lead to similar results in the study of more general types of rewriting systems.

It is assumed that the reader is acquainted with the basic facts of the theory of formal languages (e.g. regular sets, context-free languages) and of computational complexity theory, say at the undergraduate level in the USA.

2. Strings and Thue Systems

In this section we provide formal definitions of Thue systems, Thue congruences, etc. We introduce the notion of length as the metric on strings. This will lead to the property that "reduction" of strings is a noetherian relation when length serves as the basis for defining reduction.

For any set Σ of symbols, Σ^* is the free monoid generated by Σ under the operation of concatenation with the empty word e as identity. If $w \in \Sigma^*$, then the *length* of w, denoted $|w|$, is defined as follows: $|e| = 0$, $|a| = 1$ for $a \in \Sigma$, and $|wa| = |w| + 1$ for $w \in \Sigma^*$ and $a \in \Sigma$. The *concatenation* of words u and v is written as uv.

If $A, B \subseteq \Sigma^*$, then the *concatenation* of A and B, denoted AB, is defined to be $\{xy | x \in A, y \in B\}$. If $A \subseteq \Sigma^*$, then define $A^0 = \{e\}$, $A^1 = A$, and $A^{n+1} = A^n A$ for $n \geqslant 0$. If $A \subseteq \Sigma^*$, then define $A^* = \cup_{i \geqslant 0} A^i$. It is clear that if $A \subseteq \Sigma^*$, then A^* is the submonoid of Σ^* generated by A and $A^* = \{x_1 \ldots x_n | n \geqslant 1, \text{ each } x_i \in A\} \cup \{e\}$. Recall that if Σ is a finite alphabet, then the *regular* subsets of Σ^* form the smallest class containing the finite subsets and closed under union, concatenation, and *.

Let Σ be an alphabet. A *Thue system* T on Σ is a subset of $\Sigma^* \times \Sigma^*$ and each element (u, v) of T is a *rewriting rule*. The *Thue congruence* $\overset{*}{\leftrightarrow}_{(T)}$ *generated by* T is the transitive, reflexive closure of the relation $\leftrightarrow_{(T)}$ defined as follows: for $(u, v) \in T$ and $x, y \in \Sigma^*$, $xuy \leftrightarrow_{(T)} xvy$ and $xvy \leftrightarrow_{(T)} xuy$. Two strings $w, z \in \Sigma^*$ are *congruent* (mod T) if $x \overset{*}{\leftrightarrow}_{(T)} y$ and, for $w \in \Sigma^*$, the *congruence class of* w (mod T) is $[w]_{(T)} = \{z \in \Sigma^* | z \overset{*}{\leftrightarrow}_{(T)} w\}$.

The subscript (T) will be omitted whenever ambiguity is not introduced.

By the "word problem" for T, we mean the following problem:

INSTANCE: strings x and y;
QUESTION: are x and y congruent (mod T)?

For a given Thue system, we would like to know whether the word problem for that system is decidable and, if so, what inherent complexity it has.

A *rewriting system* R on Σ is also a subset of $\Sigma^* \times \Sigma^*$. An element (u, v) of R is considered to be ordered in the sense that an occurrence of string u may be rewritten as v but not vice versa. The *derivation relation* $\overset{*}{\Rightarrow}_{(R)}$ *generated by* R is the transitive, reflexive closure of the relation $\Rightarrow_{(R)}$ defined as follows: for $(u, v) \in R$ and $x, y \in \Sigma^*$, $xuy \Rightarrow_{(R)} xvy$.

One says that "z can be derived from w" if $w \overset{*}{\Rightarrow}_{(R)} z$; in this case, z is a *descendant* of w and w is an *ancestor* of z. The reader should note that the rules of a rewriting system may be applied only in the direction given by that system, while the rules of a Thue system may be applied in either direction. A string x is *irreducible* (mod R) if there is no string y such that $x \Rightarrow_{(R)} y$. Let $IRR(R)$ denote the set of all strings that are irreducible (mod R).

Notice that if R is a finite rewriting system on Σ, then the set $IRR(R)$ is a regular subset of Σ^*, and one can effectively construct from R a regular expression that specifies $IRR(R)$. This fact is very useful.

For a rewriting system R, let R^{-1} denote the system $\{(v, u) | (u, v) \in R\}$. The union of R and R^{-1} is a Thue system, and the Thue congruence generated by $R \cup R^{-1}$ is the transitive, reflexive closure of $\Rightarrow_{(R)} \cup \Rightarrow_{(R^{-1})}$. By "the word problem for R" we mean the word problem for the Thue system $R \cup R^{-1}$.

Let R be a rewriting system on Σ. Then R is

(a) *noetherian* if there is no infinite chain $x_1 \Rightarrow_{(R)} x_2 \Rightarrow_{(R)} \ldots$;
(b) *locally confluent* if for all $w, x, y \in \Sigma^*$, $w \Rightarrow x$ and $w \Rightarrow y$ imply that there exists $z \in \Sigma^*$ such that $x \overset{*}{\Rightarrow} z$ and $y \overset{*}{\Rightarrow} z$;
(c) *confluent* if for all $w, x, y \in \Sigma^*$, $w \overset{*}{\Rightarrow} x$ and $w \overset{*}{\Rightarrow} y$ imply that there exists $z \in \Sigma^*$ such that $x \overset{*}{\Rightarrow} z$ and $y \overset{*}{\Rightarrow} z$;
(d) *Church–Rosser* if for all $x, y \in \Sigma^*$, $x \overset{*}{\leftrightarrow}_{(R \cup R^{-1})} y$ implies that there exists $z \in \Sigma^*$ such that $x \overset{*}{\Rightarrow} z$ and $y \overset{*}{\Rightarrow} z$;
(e) *complete* if it is both noetherian and confluent.

Notice that if R is a noetherian rewriting system on Σ, then for every $w \in \Sigma^*$ there exists a $z \in \Sigma^*$ such that $w \overset{*}{\Rightarrow}_{(R)} z$ and z is irreducible (mod R). If R is a complete rewriting system on Σ, then for every $w \in \Sigma^*$ there exists a unique $z \in \Sigma^*$ such that $w \overset{*}{\Rightarrow}_{(R)} z$ and z is irreducible (mod R).

If T is a Thue system on alphabet Σ, then the *monoid* $\mathbf{M}_T$ *presented by* T is defined as follows: (i) the elements are $[x]$, $x \in \Sigma^*$, (ii) the multiplication is $[x] \cdot [y] = [xy]$, $x, y \in \Sigma^*$, and (iii) the identity is $[e]$. The pair $[\Sigma; T]$ is a *monoid presentation of* $\mathbf{M}_T$. If Σ is finite, then $\mathbf{M}_T$ is *finitely generated*, and if both Σ and T are finite, then $\mathbf{M}_T$ is *finitely presented*. A *monoid presentation* $[\Sigma; T]$ *admits a (finite) complete rewriting system* if there exists a (finite) complete rewriting system R over Σ such that the congruences determined by T and R coincide, that is, both $[\Sigma; T]$ and $[\Sigma; R]$ present precisely the same quotient monoid of Σ^*. A *monoid* $\mathbf{M}$ *admits a (finite) complete rewriting system* if there exists a monoid presentation of $\mathbf{M}$ that admits a (finite) complete rewriting system.

If T_1 and T_2 are Thue systems on Σ such that for all $x, y \in \Sigma^*$, $x \overset{*}{\leftrightarrow}_{(T_1)} y$ implies $x \overset{*}{\leftrightarrow}_{(T_2)} y$, then T_1 *refines* T_2. If T_1 refines T_2 and T_2 refines T_1, then T_1 and T_2 are *equivalent*.

The notion of equivalence of Thue systems has to do with the congruence on the free monoid generated by the alphabets of the two systems. The alphabets must be the same, and the systems are equivalent if and only if they generate the same congruence on the corresponding free monoid. It is clear that if T_1 and T_2 are equivalent Thue systems, then the monoids $\mathbf{M}_{T_1}$ and $\mathbf{M}_{T_2}$ are identical and, hence, isomorphic.

3. Complete Rewriting Systems and the Word Problem

In general, the word problem for finite Thue systems, for finite rewriting systems, and for finitely presented monoids is undecidable. This is easily seen as a reduction from the Correspondence Problem of Post. Thus, we turn to restrictions on such systems.

If a rewriting system R is noetherian, then for every string w the congruence class of w (mod $R \cup R^{-1}$) contains at least one irreducible element; such an irreducible element may be considered to be a *normal form* for that class. If a rewriting system R is confluent, then for every string w the congruence class of w (mod $R \cup R^{-1}$) contains at most one irreducible element. If a rewriting system R is complete, then for every string w the congruence class of w (mod $R \cup R^{-1}$) contains exactly one irreducible element which can be considered to be a *unique* normal form. Thus, the word problem for a complete rewriting system is decidable, since for two objects x, y, one computes the normal forms $\bar{x}, \bar{y}$ and then compares $\bar{x}$ and $\bar{y}$: x and y are congruent (mod R) if and only if $\bar{x}$ and $\bar{y}$ are identical. Many problems arising in automated deduction, computer algebra, and other aspects of symbolic computation can be stated as a combination of one or more word problems; therefore, one attempts to find complete rewriting systems in order to solve these problems, that is, there are problems that "seek a rewriting system" for their solution.

Thus, it would be useful to determine when a rewriting system is complete. There are two results that are of particular interest.

THEOREM 3.1 (Newman, 1942; Huet, 1980). *Let R be a rewriting system. Suppose that R is noetherian. If R is locally confluent, then R is confluent.*

THEOREM 3.2 (Nivat & Benois, 1972). *Let R be a finite rewriting system on alphabet Σ. Suppose that R is noetherian. Then it is decidable whether R is locally confluent. Hence, it is decidable whether R is confluent.*

The proof of Theorem 3.2 involves the generation of "critical pairs" (see Buchberger, 1985). Since R is finite, only finitely many critical pairs can be generated. Thus, it can be tested whether every critical pair resolves (i.e. whether the two strings in a critical pair have a common irreducible descendant). This is sufficient since R is locally confluent if and only if every critical pair resolves.

If a rewriting system R is not complete, one wishes to determine whether there exists an equivalent system that is complete or whether the monoid presented by R is isomorphic to a monoid presented by a complete rewriting system. Bauer & Otto (1984) have noted that a result of Ó'Dúnlaing (1981, 1983*a*) can be used to obtain the following fact.

THEOREM 3.3. *The following problems are undecidable:*

(*a*) *INSTANCE: a finite monoid presentation* $[\Sigma; T]$;
QUESTION: does $[\Sigma; T]$ *admit a finite complete rewriting system?*

(*b*) *INSTANCE: a finite monoid presentation* $[\Sigma; T]$;
QUESTION: does the monoid presented by $[\Sigma; T]$ *admit a finite complete rewriting system?*

Consider the monoid $\mathbf{M}_T$ with presentation $[\Sigma; T]$ where $\Sigma = \{a, b\}$ and $T = \{(aba, bab)\}$. Since *aba* and *bab* have the same length, the word problem for $\mathbf{M}_T$ is decidable non-deterministically using at most linear space and, hence, deterministically in time $O(2^{cn})$ for some $c > 0$. Kapur & Narendran (1985*a*) have shown that there is no finite complete rewriting system R over $\Sigma = \{a, b\}$ that is equivalent to $T = \{(aba, bab)\}$, that is, the monoid presentation $[\Sigma; T]$ does not admit a finite complete rewriting system. However, Bauer & Otto (1984) have found another presentation of the monoid $\mathbf{M}_T$ that

does admit a finite complete rewriting system; this is done by adding one generator so that the new system presents a quotient monoid on $\{a, b, c\}^*$, and this monoid is isomorphic to $\mathbf{M}_T$. However, the new system is not equivalent to T. Bauer & Otto summarize in the following way.

THEOREM 3.4. *The property of allowing a finite complete rewriting system depends on the specific presentation of the monoid.*

Thus, to show that a finitely presented monoid with a decidable word problem does not allow a finite complete rewriting system, it is necessary to show that no finite presentation of this monoid admits such a system. Also, notice that Theorem 3.4 shows that the two parts of Theorem 3.3 are in fact different questions.

We are left with a fundamental question: does every monoid with a decidable word problem admit a finite complete rewriting system? Bauer & Otto state the question in this way, but it is well known in more general forms (see Huet, 1980; Huet & Oppen, 1980). Much recent work in automated deduction has been directed at the corresponding problem for groups, and it seems that the question for monoids ought to be closely tied to the question for groups. There is one recent contribution to the question for monoids that must be noted.

A *two-level rewriting system* R over Σ is a pair $\langle R_1, R_2 \rangle$, where R_1 and R_2 are rewriting systems over Σ with the following rule of application of rewriting rules: the only admissible sequences of applications of rules in R starting from a string $w \in \Sigma^*$ are such that all applications of rules from R_1 come before any application of a rule from R_2.

Bauer (1984, 1985) has studied "n-level" rewriting systems and has established the following result.

THEOREM 3.5. *Let* $\mathbf{M}$ *be a finitely presented monoid. Suppose that the word problem for* $\mathbf{M}$ *is decidable. Then there exists a finite 2-level rewriting system* R *on some finite alphabet* Δ *such that the monoid with presentation* $[\Delta; R]$ *is isomorphic to* $\mathbf{M}$ *and* R *is complete. That is, every finitely presented monoid with a decidable word problem admits a finite complete 2-level rewriting system.*

Now consider the computational complexity of the word problem. Once one knows that a problem is decidable, the next step is to classify its inherent complexity. If a problem is tractable, then a good algorithm exists for its solution, an algorithm that can be guaranteed to perform well when properly implemented—in current usage, an algorithm is tractable if its running time is bounded above by a polynomial in the size of the input. Thus, one would like to know when the existence of a complete rewriting system guarantees that the word problem is tractable. More generally, if a monoid $\mathbf{M}$ admits a finite complete rewriting system, what can be said about the computational complexity of the word problem for $\mathbf{M}$? One way to approach this problem is to consider the derivational complexity of rewriting systems.

Suppose that R is a rewriting system on Σ such that the word problem for the monoid with presentation $[\Sigma; R]$ is decidable. Define a function f as follows: for $x, y \in \Sigma^*$, $f(x, y)$ is the minimum number of steps in a sequence of transformations under R that begin with x and end with y (or vice versa) if such a sequence exists, and is "no" otherwise. The function f is the *derivational complexity* of the rewriting system R.

One might think that the derivational complexity of a rewriting system defines the

computational complexity of the word problem. In fact, this is not the case. Madlener & Otto (1985) have considered this situation in the case that the derivational complexity is a primitive recursive function. For each $n > 0$, let E_n be the class of functions in the nth level of the Grzegorczyk hierarchy.

THEOREM 3.6. *For each $m \geq 4$, there is a finitely presented group $\mathbf{G}(m)$ with an E_3-decidable word problem such that $\mathbf{G}(m)$ has a presentation with derivational complexity in E_m but no finite group presentation of $\mathbf{G}(m)$ has derivational complexity in E_{m-1}.*

Bauer & Otto (1984) use the techniques of Madlener & Otto (1985) to obtain results about the derivational complexity of finite complete rewriting systems.

THEOREM 3.7. *For each $m \geq 2$, there exists a finite complete rewriting system R_m with the following properties:*

(*a*) *there is an algorithm to solve the word problem for R_m that has its running time bounded above by a function in E_1;*
(*b*) *the derivational complexity of R_m is in E_m but is not bounded above by any function in E_{m-1}.*

Further, the hope that a finite complete rewriting system may be guaranteed to have a word problem that is computationally feasible has been dashed. Bauer & Otto (1984) have established the following result.

THEOREM 3.8. *For every $n \geq 3$, there is a finite complete rewriting system R_n such that the word problem for R_n is decidable by an algorithm whose running time is bounded above by a function in E_n but not by any function in E_{n-1}.*

In the remaining sections we consider Thue systems where the notion of reduction is based on length, that is, where reduction depends on applying length-reducing rules. Based on this notion of reduction, we consider Thue systems that are Church–Rosser and develop properties of these systems and the monoids they present. One important theme for future work is to identify those properties that are decidable when reduction is based on length and are still decidable when reduction is based on some other ordering (possibly a Knuth–Bendix ordering). Another important theme is the study of the complexity of problems of monoids and of Thue systems when reduction is based on length. In particular, we are concerned with properties that are tractable. A number of results have already been obtained in this case, and some of them will be surveyed here. When reduction is not based on length, then Theorem 3.8 suggests that one should not expect to find that decidable problems are tractable, i.e. decidable in polynomial time.

4. Length as a Basis for Reduction

In this section and the remaining sections, we concentrate on a special case of Thue systems and rewriting systems. We use the notion of length as a metric on strings as a basis for the notion of "reduction". While a Thue system may have rewriting rules that change length as well as rewriting rules that are length-preserving, we obtain a rewriting system corresponding to the Thue system by using the partial order on the set of strings obtained by considering length reduction. The derivation relation in this rewriting system

is then referred to as the "reduction" relation. This approach appears to have been pursued for the first time by Nivat. A survey of the work of Nivat and his colleagues and students was presented by Berstel (1977).

Let Σ be an alphabet and let T be a Thue system on Σ. If $x, y \in \Sigma^*$, $x \leftrightarrow y$, and $|x| > |y|$, then define $x \to y$; this is the *reduction* relation. Let $\overset{*}{\to}$ be the reflexive, transitive closure of the relation $\to$; abusing the terminology, we also call this relation *reduction*. The corresponding rewriting system is

$$R = \{(u, v) \mid |u| > |v|, (u, v) \in T \text{ or } (v, u) \in T\}.$$

We say that a string $z \in \Sigma^*$ is *irreducible* (mod T) if there is no y such that $z \to y$, and we let $IRR(T)$ denote the set of all strings that are irreducible (mod T). A string $z \in \Sigma^*$ is *minimal with respect to* $\overset{*}{\leftrightarrow}_{(T)}$ if there is no y such that $|y| < |z|$ and $y \overset{*}{\leftrightarrow} z$.

For a Thue system T we write $\overset{*}{\to}$ instead of $\overset{*}{\Rightarrow}$ in order to distinguish the situation where decreasing length is the basis for reduction from the situation where R is obtained from T in the manner described in section 2. We lose no generality by assuming that for every Thue system T, if $(u, v) \in T$, then $|u| \geqslant |v|$; this assumption will be made throughout the remainder of this paper unless explicitly noted to the contrary.

Henceforth, we will refer to a Thue system being Church–Rosser when the rewriting system described above is Church–Rosser. Since the reduction relation is noetherian, such a system is complete. Thus, every congruence class has a unique irreducible string.

If T is a Thue system, then the reduction relation $\overset{*}{\to}$ is noetherian, and so for every string w there exists an irreducible string z such that $w \overset{*}{\to} z$. It is easy to see that one can compute (by exhaustive search) all such z, but this is much too costly. Hence it would be desirable to have an efficient algorithm for computing an irreducible descendant of a given string. Such an algorithm exists.

THEOREM 4.1 (Book, 1982). *Let T be a finite Thue system on finite alphabet Σ. There is a linear-time algorithm that on input a string $w \in \Sigma^*$ will compute an irreducible string z such that $w \overset{*}{\to} z$.*

SKETCH OF THE PROOF. At most $|w|$ such reductions can be applied. Proceed by scanning w from left-to-right and applying reductions whenever possible. Each time a reduction is applied one must consider the possibility that a portion of the previously scanned string is a prefix of the left-hand side of a reduction and the corresponding suffix of the left-hand side of that reduction is the next portion to be scanned. Thus, backtracking may be needed. But when this strategy is implemented with two pushdown stores, the amount of backtracking necessary after a reduction is at most the length of the longest left-hand side of the rules in T. This determines the constant of linearity in the time bound. □

If a Thue system is Church–Rosser, then two strings are congruent modulo this system if and only if they have a common irreducible descendant. This means that any sequence of applications of the rewriting rules can be replaced by one in which first only length-decreasing rules are applied until an irreducible string is obtained, and then only length-increasing rules are applied. But if T is Church–Rosser, then this irreducible string is unique. This yields a strategy for deciding the word problem: given x and y, compute an irreducible descendant $\bar{x}$ of x and an irreducible descendant $\bar{y}$ of y by using the method of Theorem 4.1. Compare $\bar{x}$ and $\bar{y}$ to see if they are identical; if so, x and y are congruent (i.e. $[x]$ and $[y]$ are equal in $\mathbf{M}_T$); if not, x and y are not congruent.

THEOREM 4.2 (Book, 1982). *Let T be a finite Thue system. If T is Church–Rosser, then there is a linear-time algorithm to solve the word problem for T.*

Thue systems that are Church–Rosser have many desirable properties, some of which will be described in this section. The first such property to be discussed relates the notions of irreducible strings and minimal strings.

A string that is minimal with respect to $\overset{*}{\leftrightarrow}_{(T)}$ is also irreducible modulo any Thue system that generates the same congruence. However, for some Thue systems there are irreducible strings that are not minimal, so the cardinality of $\mathbf{M}_T$ is not necessarily the cardinality of $IRR(T)$. Thus, it would be desirable to have an algorithm for determining when a string is minimal, but this cannot be the case.

THEOREM 4.3 (Book & Ó'Dúnlaing, 1981*b*). *The following problem is undecidable:*

INSTANCE: a finite Thue system T on finite alphabet Σ and a string $w \in \Sigma^*$;
QUESTION: is w minimal with respect to $\overset{*}{\leftrightarrow}_{(T)}$?

A proof of Theorem 4.3 can be obtained as a simple reduction from the Correspondence Problem of Post.

For a Thue system T, every congruence class contains at least one minimal element, so that the cardinality of $\mathbf{M}_T$ is at most the cardinality of the set of minimal elements. It is clear that if T is Church–Rosser, then a string is minimal if and only if it is irreducible, so that the cardinality of $\mathbf{M}_T$ is exactly the cardinality of the set of irreducible elements. But as long as T is finite, the set $IRR(T)$ of irreducible elements is a regular set, and a finite-state acceptor recognising $IRR(T)$ can be effectively constructed from T. Hence, if T is finite and Church–Rosser, then one can effectively determine the cardinality of $\mathbf{M}_T$ (Book & Ó'Dúnlaing, 1981*b*); this means that it is decidable whether $\mathbf{M}_T$ is trivial or is finite, properties that are generally undecidable for finitely presented monoids.

As long as the reduction relation is based on decreasing length, the word problem for Church–Rosser Thue systems is equivalent to the common descendant problem (i.e. the problem "given x and y, do x and y have a common descendant?"). However, the common ancestor problem (i.e. the problem "given x and y, do x and y have a common ancestor?") is equivalent to the Correspondence Problem of Post and so is undecidable for finite Thue systems (Book *et al.*, 1982), even if they are Church–Rosser (Narendran, 1983).

The decidability of the word problem for Church–Rosser Thue systems leads to an algorithm for testing the equivalence of finite Church–Rosser systems (Book & Ó'Dúnlaing, 1981*b*), a question that is undecidable for arbitrary finite Thue systems.

There is a very useful notion that has been introduced recently. A Thue system T on alphabet Σ is *reduced* if for every rewriting rule $(u, v) \in T$, $v \in IRR(T)$ and u cannot be reduced using $T - \{(u, v)\}$. Kapur & Narendran (1985*b*) and Narendran (1983) have established the following fact.

THEOREM 4.4. *For any Thue system T_1 that is Church–Rosser, there is a unique reduced Thue system T_2 that is Church–Rosser and equivalent to T_1. Further, if T_1 is finite, then one can effectively construct T_2 from T_1.*

Theorem 4.4 is useful in a variety of settings, particularly in showing that certain questions are undecidable. One example of its usefulness is due to Narendran (1983).

Consider the Thue system $T_1 = \{(aba, ab)\}$ on $\{a, b\}$. It is easy to see that T_1 is not Church–Rosser since *abba* is congruent to *abb* and both of these strings are irreducible. Further, T_1 is not equivalent to any finite Thue system that is Church–Rosser. But the infinite Thue system $T_2 = \{(ab^n a, ab^n) | n \geqslant 1\}$ is equivalent to T_1 and is Church–Rosser. Hence, a given Thue system may not be equivalent to any finite Church–Rosser system while still being equivalent to an infinite Church–Rosser system.

In this example, both T_1 and T_2 are reduced. Pan (1985) considered Thue systems that are finite and reduced, and asked whether two such systems can be equivalent (by Theorem 4.4 it cannot be the case that both are Church–Rosser). Pan showed the existence of such systems and also established the following fact.

THEOREM 4.5. *The following problem is undecidable:*

INSTANCE: a reduced finite Thue system T_1*;*
QUESTION: does there exist a reduced finite Thue system T_2 *such that* T_2 *is both Church–Rosser and equivalent to* T_1*?*

The fact that Thue systems that are Church–Rosser have many useful properties leads us to ask whether one can determine if a given finite Thue system is in fact Church–Rosser. An algorithm to solve this problem was first developed by Book & Ó'Dúnlaing (1981*a*) and a faster algorithm was developed by Kapur *et al.* (1985).

THEOREM 4.6 (Book & Ó'Dúnlaing, 1981*a*). *There is a polynomial-time algorithm to solve the following problem:*

INSTANCE: a finite Thue system T;
QUESTION: is T Church–Rosser?

SKETCH OF THE PROOF. From Theorems 3.1 and 3.2, it is sufficient to note that one can bound the number of critical pairs by a polynomial in the size of T (where the size of T is considered to be the length of a string that encodes all of T's rewriting rules). From Theorem 4.2 we see that one can determine whether any one critical pair resolves in time that is linear in the sum of the lengths of the strings making up that pair. □

Now suppose that a Thue system T_1 is not Church–Rosser. Does there exist a Thue system T_2 such that T_2 is Church–Rosser and $\mathbf{M}_{T_2}$ is isomorphic to $\mathbf{M}_{T_1}$? The answer is always "yes" since one can consider the alphabet $\Delta = \{m | m \in \mathbf{M}_{T_1}\}$ and the Thue system

$$T = \{(m_1 m_2, m_3) | m_1 m_2 = m_3 \text{ in } \mathbf{M}_{T_1}\}.$$

The system T is Church–Rosser since multiplication in any monoid is associative, so that the rules of T only mimic the multiplication table of $\mathbf{M}_{T_1}$, and the monoid $\mathbf{M}_T$ is clearly isomorphic to $\mathbf{M}_{T_1}$. However, this situation is not satisfactory, since T_1 may be taken over a finite alphabet, while if $\mathbf{M}_{T_1}$ is infinite, then T is taken over an infinite alphabet. Thus, we restrict attention to Thue systems that are equivalent to T_1, that is, if Σ is the smallest alphabet such that T_1 can be taken over Σ, then we consider only Thue systems T_2 on Σ such that $\mathbf{M}_{T_2}$ is precisely equal to $\mathbf{M}_{T_1}$. With this restriction the answer to our question is "no", as was shown by Ó'Dúnlaing (1981, 1983*a*).

THEOREM 4.7. *The following problem is undecidable:*

INSTANCE: *a finite Thue system* T_1;
QUESTION: *does there exist a Thue system* T_2 *such that* T_2 *is equivalent to* T_1 *and* T_2 *is Church–Rosser?*

One of the tools used by Ó'Dúnlaing to prove Theorem 4.7 is interesting in its own right.

THEOREM 4.8. *Let* P *be any property of finite Thue systems that satisfies the following conditions:*

(*a*) P *is invariant under equivalence of Thue systems;*
(*b*) *every trivial Thue system has property* P;
(*c*) *every Thue system with property* P *has a decidable word problem.*

Then the following question is undecidable:

INSTANCE: *a finite Thue system* T;
QUESTION: *does* T *have property* P?

Theorem 4.8 is related to a result of Markov regarding finitely presented monoids. But in Theorem 4.8, the property P need only be preserved under equivalence of Thue systems instead of isomorphism of monoids.

5. Specifying Formal Languages

Historically, one motivation for studying Thue systems with the Church–Rosser property is the fact that in some cases it is possible to specify formal languages as congruence classes of Thue systems or as finite unions of congruence classes of Thue systems. Clearly, for any finite Thue system with the Church–Rosser property, every congruence class is a language recognisable by a deterministic linear-bounded automaton; this follows from the fact that there is a deterministic algorithm to solve the word problem in linear time. Nivat and his colleagues initiated research in this area, and their choice of topics was influenced by the interface between algebra and formal language theory with primary emphasis on the class of context-free languages (for example, see Benois, 1969 or Cochet, 1971). Thus, it is reasonable to ask whether every context-free language can be represented as a congruence class or a combination of congruence classes of a finite Thue system that is Church–Rosser.

A language L is *congruential* if there is a finite Thue system T such that L is the union of finitely many of T's congruence classes.

Berstel (1977) has shown that the linear context-free language $\{ww^R | w \in \Sigma^*\}$ is not congruential.

Some but not all congruential languages are context-free. To see one example of a congruential language that is not context-free, consider $\Sigma = \{a, b, c\}$ and $T = \{(abc, ab), (bbc, cb)\}$. It is clear that T is Church–Rosser. The string abb is irreducible, but the congruence class of abb is not context-free since

$$[abb] \cap \{a\}^*\{b\}^*(c)^* = \{ab^{f(n)}c^n | n \geqslant 0, f(n) = 2^n + 1\},$$

which is not context-free. Hence, even though a finite Thue system is Church–Rosser, one

cannot conclude that its congruence classes are context-free languages. This leads us to consider certain restrictions.

A Thue system T is *monadic* if $(u, v) \in T$ implies $|u| > |v|$ and $1 \geqslant |v|$, and is *special* if $(u, v) \in T$ implies $v = e$ and $u \neq e$.

Recall that if $x \overset{*}{\to} y$, then x is an ancestor of y and y is a descendant of x. For any string w, let $\Delta^*(w)$ denote the set of descendants of w and let $\langle w \rangle^*$ denote the set of ancestors of w. For any set A of strings, let $\Delta^*(A) = \cup \{\Delta^*(w) | w \in A\}$, let $\langle A \rangle^* = \cup \{\langle w \rangle^* | w \in A\}$, and let $[A] = \cup \{[w] | w \in A\}$.

The first result has been proved in several different situations.

THEOREM 5.1 (Benois, 1969; Berstel, 1979; Book *et al.*, 1982; Book & Otto, 1985). *Let T be a finite monadic Thue system on Σ. For every regular set $R \subseteq \Sigma^*$, the language $\Delta^*(R) = \{y \mid$ for some $x \in R$, $x \overset{*}{\to} y\}$ is again a regular set. Further, from T and a regular expression for R one can construct a regular expression for $\Delta^*(R)$.*

Consider sets of the form $\Delta^*(C)$ where C is a context-free language. Even if T is Church–Rosser sets of this form may not be context-free. This can be seen by applying an often-used technique for proving the undecidability of certain questions about formal languages which involves encoding the set of finite computations of a Turing machine as a combination of languages.

THEOREM 5.2 (Book *et al.*, 1982). *Let Σ be a finite alphabet. For every recursively enumerable set $L \subseteq \Sigma^*$, there is a finite special Thue system T on alphabet Γ and a context-free language $C \subseteq \Gamma^*$ such that T is Church–Rosser and $L = \Delta^*(C) \cap \Sigma^* = \{y \in \Sigma^* \mid$ for some $x \in C$, $x \overset{*}{\to} y\}$. Thus, there exists a finite special Thue system T on Γ and a context-free language C such that $\Delta^*(C)$ is not recursive, let alone context-free.*

Now consider the set of ancestors of a string.

THEOREM 5.3 (Book *et al.*, 1982). *Let T be a finite monadic Thue system on alphabet Σ. For every context-free language $L \subseteq \Sigma^*$, the set of ancestors of strings in L is a context-free language, i.e. $\langle L \rangle^*$ is context-free. Further, from T and a context-free grammar for L one can construct a context-free grammar that generates $\langle L \rangle^*$.*

Nivat (1970) established a special case of this result by considering the situation when L is a singleton set.

Cochet & Nivat (1971) observed that if T is finite, special, and Church–Rosser, then for every string x, the congruence class of x is an unambiguous context-free language. This result can be greatly strengthened.

THEOREM 5.4 (Book, 1982). *Let T be a finite monadic Thue system on alphabet Σ. Suppose that T is Church–Rosser. If $R \subseteq \Sigma^*$ is a regular set, then $[R] = \{y \mid$ for some $x \in R$, x is congruent to $y\}$ is a deterministic context-free language.*

SKETCH OF THE PROOF. Since T is Church–Rosser, $x \overset{*}{\leftrightarrow} y$ if and only if there exists a unique irreducible z such that $x \overset{*}{\to} z$ and $y \overset{*}{\to} z$. Since T is finite, $IRR(T)$ is a regular set, so by Theorem 5.1, if R is regular, then so is $\Delta^*(R)$; hence, $\Delta^*(R) \cap IRR(T) = \{z \in IRR(T) |$ for some $x \in R$, $x \overset{*}{\to} z\}$ is a regular set. We are considering the set $[R] = \{y \mid$ for some

$z \in IRR(T) \cap \Delta^*(R)$, $y \xrightarrow{*} z\}$. Consider a deterministic pushdown store acceptor that when started on input string y implements the algorithm described in the proof of Theorem 4.1. Since T is monadic and the input string is contained on the (one-way, read-only) input tape, only the one pushdown store is needed for memory. Thus, when the computation halts, what remains on the pushdown store is a string z such that the first (leftmost) symbol in z is on the bottom of the store and z is irreducible. Since $IRR(T) \cap \Delta^*(R)$ is a regular set, a deterministic finite-state acceptor to recognise the reversal of that set can be encoded into the finite-state control of the pushdown store acceptor. Hence, when the input has been completely processed, the contents of the pushdown store acceptor can be popped, symbol by symbol, and considered as input to this finite-state acceptor. The pushdown store acceptor accepts its input if and only if the finite-state acceptor accepts the contents of the pushdown store. □

The class of regular subsets of Σ^* forms an infinite Boolean algebra, so Theorem 5.4 shows that a finite monadic Church–Rosser Thue system specifies an infinite Boolean algebra of deterministic context-free languages. Is there a specific type of context-free grammar such that grammars of this type generate precisely these languages? Or, is there a specific type of deterministic pushdown store acceptor that recognises precisely these languages? These are interesting open questions.

As a corollary of Theorem 5.4, Book & Ó'Dúnlaing (1981*b*) used the self-embedding properties of context-free languages to show that it is decidable in polynomial time whether a finite monadic Thue system that is Church–Rosser has at least one congruence class that is infinite. Narendran *et al.* (1985*a*) investigated similar questions about properties of congruence classes for finite Church–Rosser Thue systems that were not required to be monadic. Their results were primarily negative.

THEOREM 5.5. *The following problem is undecidable; in fact, it is* Π_2*-complete.*

INSTANCE: a finite Church–Rosser Thue system T*;*
QUESTION: does there exist w *such that* $[w]$ *is infinite?*

Does a Thue system have any finite congruence class? The answer is "no" if and only if $[e] \neq \{e\}$. Thus, this question is decidable for finite Thue systems (the Church–Rosser property is not required) since it is sufficient to determine whether there exists a rewriting rule of the form (u, e), where $u \neq e$. If such a rule exists, then $[e] \neq \{e\}$ and every congruence class is infinite; if such a rule does not exist, then $[e] = \{e\}$ so that $[e]$ is a congruence class that is finite.

Recall from Theorem 5.3 that for monadic Thue systems, the set of ancestors of a given string is always a context-free language. If the system is also Church–Rosser, then the congruence class of a given string is always a context-free language. Since there are examples of non-monadic Church–Rosser systems where the congruence classes are not context-free languages and there is an example of a special Thue system that is not Church–Rosser where no congruence class is context-free (Theorem 9.5), the following result of Narendran *et al.* (1985*a*) is not surprising.

THEOREM 5.6. *There exists a finite Church–Rosser Thue system over alphabet* Σ *such that the following problem is undecidable:*

INSTANCE: a string w *in* Σ^**;*
QUESTION: is $[w]$ *a context-free language?*

One might consider variations on Theorem 5.6 by asking whether $[w]$ is some restricted type of context-free language, e.g. deterministic context-free, linear context-free, regular, etc. But a general theorem that eliminates the need for a list of theorems has been established.

THEOREM 5.7 (Narendran *et al.*, 1985*a*). *Let Ω be any family of context-free languages that includes all of the finite sets.*

(*a*) *There exists a finite Church–Rosser Thue system over alphabet Σ such that the following problem is Σ_1-hard.*

INSTANCE: a string $w \in \Sigma^*$;
QUESTION: is $[w]$ in Ω?

(*b*) *The following problem is Π_2-hard.*

INSTANCE: a finite Church–Rosser Thue system T;
QUESTION: is every congruence class of T in Ω?

Let us turn to other specifications of formal languages by means of finite Church–Rosser Thue systems.

Motivated by parsing techniques that use a mixed strategy involving simultaneous top-down and bottom-up analysis, and also by several problems about semantics and program transformations that are handled through the theory of program schemes, Boasson & Sénizergues (1985) have studied an interesting subclass of context-free grammars and languages.

Let G be a context-free grammar with terminal alphabet Σ, non-terminal alphabet V, and set P of productions. Let $\stackrel{*}{\Rightarrow}$ denote the binary relation on $(V \cup \Sigma)^*$ determined by the productions, i.e. the derivation relation of the context-free grammar G. Let T be the Thue system on alphabet $\Sigma \cup V$ with P as the set of rewriting rules and let $\stackrel{*}{\leftrightarrow}$ denote the congruence relation of T. For each $A \subseteq V$, define the following languages:

(a) $L(G, A) = \{w \in \Sigma^* | \exists\, a \in A \text{ such that } a \stackrel{*}{\Rightarrow} w\}$;
(b) $\hat{L}(G, A) = \{w \in (V \cup \Sigma)^* | \exists\, a \in A \text{ such that } a \stackrel{*}{\Rightarrow} w\}$;
(c) $LR(G, A) = \{w \in \Sigma^* | \exists\, a \in A \text{ such that } a \stackrel{*}{\leftrightarrow} w\}$;
(d) $\hat{LR}(G, A) = \{w \in (V \cup \Sigma)^* | \exists\, a \in A \text{ such that } a \stackrel{*}{\leftrightarrow} w\}$.

Now $L(G, A)$ is just the union over the set of non-terminal symbols A of the context-free languages obtained by using grammar G and the non-terminal symbols as initial symbols, while $\hat{L}(G, A)$ is the corresponding set of sentential forms. A grammar is *non-terminal separable* (an N.T.S. grammar) if for every $v \in V$, $\hat{LR}(G, v) = \hat{L}(G, v)$. A context-free language L is an *N.T.S. language* if there exists an N.T.S. grammar (Σ, V, P) such that for some $A \subseteq V$, $L = L(G, A)$.

Boasson & Sénizergues have shown that it is decidable whether a context-free grammar is N.T.S. Further, they showed that the class of N.T.S. languages is closed under intersection with regular sets and under reversal but is not closed under homomorphism, union, or quotient. Furthermore, every N.T.S. language is both congruential and deterministic context-free, and the class of N.T.S. languages includes the class of regular sets and the class of parenthesis languages.

One of the most important properties of the class of N.T.S. grammars was established by Sénizergues (1985). He showed that the equivalence problem is decidable but that the

inclusion problem is undecidable. Jantzen (1986) reports that Sénizergues has shown that the context-free group languages (see Muller & Schupp, 1983) are N.T.S.

While N.T.S. grammars generate only deterministic context-free languages, another type of Thue system has been described which specifies languages which are not always context-free. McNaughton, Narendran, and Otto have developed the notion of "Church–Rosser" languages.

A set L is a *Church–Rosser congruential language* if L is the union of finitely many congruence classes of some Church–Rosser Thue system.

A set $L \subseteq \Delta^*$ is a *Church–Rosser language* (*CR*-language) if there exist a finite Church–Rosser Thue system T on alphabet Σ, where $\Delta \subset \Sigma$, strings $t_1, t_2 \in (\Sigma - \Delta)^*$, and $Y \in (\Sigma - \Delta)$ such that for all $w \in \Delta^*$, $t_1 w t_2 \overset{*}{\to} Y$ if and only if w is in L. In this case, T is the *defining CR system* for L.

A set $L \subseteq \Delta^*$ is a *Church–Rosser decidable language* (*CR*-decidable language) if L is a *CR*-language and the defining *CR* system T for L has the property that there exist strings $t_1, t_2 \in (\Sigma - \Delta)^*$, and $N \in (\Sigma - \Delta)$ such that for all $w \in \Delta^*$, $t_1 w t_2 \overset{*}{\to} N$ if and only if w is not in L.

The symbols in $\Sigma - \Delta$ in a defining *CR* system of a *CR*-language or a *CR*-decidable language can be thought of as control characters.

McNaughton *et al.* (1985) observed that both the class of *CR*-languages and the class of *CR*-decidable languages are closed under complementation, and that it is not known whether these two classes of languages are distinct. Notice that nothing has been said about these various types of languages being context-free.

It is known that every regular set and every Church–Rosser congruential language is a *CR*-language, and that every *CR*-language is context-sensitive. McNaughton *et al.* have shown that every deterministic context-free language is *CR*-decidable and that there are context-free languages that are not deterministic context-free but are *CR*-decidable. Further, there are non-context-free languages that are *CR*-decidable.

The closure properties of these classes of languages have been explored in only a limited way, and there is much more to be done. However, one very important property of the various "Church–Rosser languages" defined in this way is that the membership problem is decidable in linear time; this requires specification by a finite Church–Rosser Thue system and the other necessary strings. Thus, it is highly desirable to have precise characterisations of these classes in terms of the languages they specify.

The results on Thue systems and formal languages sketched above are of interest not only due to their importance in formal language theory. Since the theories of regular sets and of context-free languages contain many results about the decidability (and undecidability) of various problems, one can use such results when attempting to determine whether properties of Thue systems or of the monoids presented by Thue systems are decidable or undecidable. This technique is exploited in a strong way by Book (1983), and some of the results will be sketched in section 7.

6. Which Monoids Have Church–Rosser Presentations?

Most of the results in the next four sections are phrased in the algebraic language of monoids. This is done because the language of monoids provides a very convenient mechanism for describing the power of Thue systems that are Church–Rosser. No claim is made that the reader should be interested in monoids or groups.

Suppose that **M** is a monoid with a finite Church–Rosser presentation. What can be said about the algebraic structure of **M** based on this fact? More specifically, how can one characterise those monoids with finite Church–Rosser presentations? There are a few results relating to these questions, and we will review some of them here.

Consider the question of which monoids have Church–Rosser presentations. The first result is a characterisation theorem due to Cochet (1976).

THEOREM 6.1. *Let T be a finite special Church–Rosser Thue system on alphabet Σ. Suppose that $[\Sigma; T]$ is a group* **G**. *Then* **G** *is the free product of finitely many cyclic groups. Conversely, every group that is the free product of finitely many cyclic groups has a presentation of this type.*

Call a Thue system T *two-monadic* if T is monadic and $(u, v) \in T$ implies $|u| = 2$. Avenhaus *et al.* (1986) have characterised those monoids with finite two-monadic presentations that are Church–Rosser.

THEOREM 6.2. *Let T be a finite 2-monadic Thue system on alphabet Σ. Suppose that T is Church–Rosser and $[\Sigma; T]$ is a group. Then the group $[\Sigma; T]$ is a free product of a finitely generated free group and a finite number of finite groups. Conversely, any group that is a free product of a finitely generated free group and a finite number of finite groups has a presentation of this type.*

Gilman (1984) has conjectured that a group **G** is a free product of finitely generated free groups and finite groups if and only if there is a monadic Thue system T on a finite alphabet Σ such that the monoid $[\Sigma; T]$ is the group **G**. It is easy to see that any such group has a presentation of this type, but the converse has not been established.

Now consider commutative monoids that are presented as quotients of free non-commutative monoids. Avenhaus *et al.* (1984) have one result on these monoids.

THEOREM 6.3. *Let T be a finite Church–Rosser Thue system. Suppose that $\mathbf{M}_T$ is both commutative and infinite. If $\mathbf{M}_T$ is cancellative or T is special, then $\mathbf{M}_T$ is either the free cyclic group or the free cyclic monoid.*

Recall that a unit of a monoid is an element that has a two-sided inverse and, further, that the submonoid generated by the set of units is a subgroup of that monoid. Consider a monoid **M** with a finite special Church–Rosser presentation. Squier (1987) has shown that the property of being Church–Rosser is inherited by a presentation of the group of units. This strengthens a result of Adjan (1966) that from a finite special presentation of a monoid one can construct a presentation of its group of units. By using Theorem 6.1, Squier concludes that the group of units of a monoid with a finite special Church–Rosser presentation is a free product of finitely many cyclic groups.

Recall that Dehn's algorithm (in combinatorial group theory) is an algorithm for solving the word problem for fundamental groups of closed, orientable surfaces of genus at least two. Greendlinger (1960) extended Dehn's algorithm and his work gave rise to small cancellation theory (see Lyndon & Schupp, 1977).

Dehn considered presentations of fundamental groups of orientable 2-manifolds. From the standpoint of rewriting systems, Dehn's strategy may be described in the following way. Suppose that a presentation of a group G, consisting of a finite set Σ of generators

and a finite set $R = \{(r_i, e) | 1 \leqslant i \leqslant m_R\}$ of relators, has the following property: every freely reduced non-trivial word w that is equal to the identity e in G has a factorisation xyz where for some i, r_i has a factorisation yt with $|y| > |t|$. Then R can be transformed into a finite set R_1 of relations such that $(u, v) \in R_1$ implies that $|u| > |v|$; moreover, the pair Σ, R_1 is a group presentation of G so that it is sufficient to solve the word problem modulo the presentation $\langle \Sigma, R_1 \rangle$. Thus, given two words w_1 and w_2, one wishes to determine whether w_1 is equal to w_2 in G or, equivalently, whether $w_1 w_2^{-1}$ is equal to 1 in G. (For a description of Dehn's algorithm from the point of view of combinatorial group theory, see Lyndon & Schupp, 1977, or Zieschang *et al.*, 1980.)

The "reduction" rules in $\langle \Sigma, R_1 \rangle$ are "u reduces to v" for $(u, v) \in R_1$. In addition, the "free reductions" are allowed: "$\sigma\sigma^{-1}$ reduces to e" and "$\sigma^{-1}\sigma$ reduces to e" for $\sigma \in \Sigma$. For the groups that Dehn studied, it is the case that for any w equal to e in G, one can apply the reduction rules in R_1 and the free reductions arbitrarily until no such rule is applicable and *regardless of the order of application of these rules* the final result is e. Thus, to determine whether w_1 is equal to w_2 in G, it is sufficient to determine whether $w_1 w_2^{-1}$ reduces to e by applying *some* finite sequence of the reduction rules. Either $w_1 w_2^{-1}$ reduces to e and w_1 and w_2 are equal in G, or else $w_1 w_2^{-1}$ reduces to something other than e and w_1 and w_2 are not equal in G.

Let T be a Thue system on alphabet Σ. For any $w \in \Sigma^*$, if $[w]$ has exactly one irreducible string, then T is *Church–Rosser on* $[w]$.

It follows from Theorems 4.1 and 4.2 that if T is a finite Thue system that is Church–Rosser on $[w]$ for some string w, then the question of whether a string is congruent to w is decidable in linear time. Furthermore, if the monoid presented by T happens to be a group, then there is a linear-time algorithm to solve the word problem (Book, 1986).

The fact that Dehn's algorithm applies to a finitely presented group G implies that there is a finite Thue system T that presents G and has the property that T is Church–Rosser (with respect to length) on the congruence class of the identity e, so that the word problem for T is decidable in linear time (Domanski & Anshel, 1985). Bücken (1980) showed that the groups that Dehn considered have presentations that could be considered to be Church–Rosser on $[e]$ and, apparently, that the same thing could be said for groups with small cancellation. Thus, it appears that for any finitely presented group with small cancellation the word problem is decidable in linear time.

One would like to develop an abstract theory of groups to which Dehn's algorithm applies, but this appears to be out of reach at this time. Another interesting notion is to develop Dehn's algorithm and small cancellation theory for monoids. A reasonable first step would be to develop characterisations of the class of monoids and the class of groups with Church–Rosser presentations. The interested reader should consult Le Chenadec (1986).

7. Properties of Monoids with Church–Rosser Presentations

We are interested in the decidability or undecidability of various problems about monoids with Church–Rosser presentations. We consider three types of problems.

First, consider properties of a specific monoid **M**. We have the following examples of problems:

the word problem
INSTANCE: two words $u, v \in \Sigma^*$;
QUESTION: are u and v equal in **M**?

the power problem
INSTANCE: two words $u, v \in \Sigma^*$;
QUESTION: does there exist an integer $n \geqslant 0$ such that u and v^n are equal in **M**?

Second, consider properties of a class **C** of monoids. We have the following examples of problems:

the uniform word problem
INSTANCE: a finite presentation of a monoid **M** in **C**;
QUESTION: is the word problem for **M** decidable?

the group problem
INSTANCE: a finite presentation of a monoid **M** in **C**;
QUESTION: is the monoid **M** a group?

the freeness problem
INSTANCE: a finite presentation of a monoid **M** in **C**;
QUESTION: is **M** a free monoid?

Third, consider properties of submonoids of monoids from a given class **C** of monoids where the submonoids are finitely generated. We have the following examples of problems:

the inclusion problem
INSTANCE: a finite presentation of a monoid **M** in **C** and two finite subsets A and B of **M**;
QUESTION: is the submonoid generated by A included in the submonoid generated by B?

the independent set problem
INSTANCE: a finite presentation of a monoid **M** in **C** and a finite subset A of **M**;
QUESTION: does $x \in A$ imply that x is not in the submonoid generated by $A - \{x\}$?

the ideal problem
INSTANCE: a finite presentation of a monoid **M** in **C** and a finite subset A of **M**;
QUESTION: is the submonoid generated by A a right (or left or two-sided) ideal of **M**?

the generalised word problem
INSTANCE: a finite presentation of a monoid **M** in **C**, a finite subset A of **M**, and $x \in \mathbf{M}$;
QUESTION: is x in the submonoid generated by A?

When **C** is the class of free monoids, all of these problems are decidable in polynomial time; often, the techniques of the theory of finite-state acceptors are usable. When **C** is the class of finitely generated free groups, all of these problems are decidable, and Avenhaus & Madlener (1984*a*, *b*) have shown that most of them are solvable in polynomial time and that the problems of the third type are log-space complete for the class **P** of problems that are solvable deterministically in polynomial time. However, in general all of these problems are undecidable.

There are numerous questions that, while undecidable for arbitrary finite Thue systems (or finitely presented monoids), are decidable for Thue systems that are *finite*, *monadic*, *and Church–Rosser*. This was explored by Book (1983), where a decision procedure for

properties expressible by "linear sentences" was developed. A *linear sentence* is a quantified formula in prenex form such that (i) there are constants from Σ^* and both existential and universal variables but every variable is bound by a quantifier, (ii) each variable appears at most once in the formula, and (iii) the quantifiers are existential or universal or both but there is at most one alternation between existential and universal or vice versa. The technique depends heavily on the notion that if T is a finite, monadic, Church–Rosser Thue system on alphabet Σ and R is a regular subset of Σ^*, then the set $\{y \mid \text{for some } x \in R,\ x \overset{*}{\to} y\}$ is again a regular set (Theorem 5.3).

The properties amenable to attack by the method of linear sentences include the following: the power problem, the group problem, the inclusion problem, the independent set problem, the ideal problem, and the generalised word problem. In addition, Green's relations are decidable for monoids presented by finite, monadic, Church–Rosser Thue systems by using the method of linear sentences. In some cases the method applies to regular subsets instead of just finite subsets.

One benefit of the method of linear sentences is that the complexity of its application is amenable to analysis. If the technique is applied to appropriate questions about the congruence generated by a given finite, monadic, Church–Rosser Thue system T, then one can conclude that the questions are decidable deterministically in polynomial time if the sentence is *not* in the form $\forall\exists$; in the $\forall\exists$ case it is decidable in polynomial space, and PSPACE-complete problems can be represented.

There are a number of questions that are not known to be amenable to attack by the decision procedure for linear sentences. In particular, the method does not appear to apply to presentations that are not monadic. Otto (1984*c*) has shown that there is a finite Church–Rosser Thue system (that is not monadic) such that the set of true linear sentences for this Thue system is not recursive. Further, he showed that there are a number of problems that, while being decidable for finite monadic Church–Rosser Thue systems (by the method of linear sentences), are undecidable for certain finite Church–Rosser Thue systems that are not monadic; one example is the independent set problem.

Recently, Otto (1985, 1986*a*, *b*, *c*) has developed some powerful techniques that apply to both monadic and non-monadic Thue systems. His results can be summarised in the following way.

THEOREM 7.1. *Each of the following questions is decidable:*

(*a*) *INSTANCE:* *a finite Church–Rosser Thue system T;*
QUESTION 1: *is $\mathbf{M}_T$ free?*
QUESTION 2: *is $\mathbf{M}_T$ a group?*
(*b*) *INSTANCE:* *a finite monadic Church–Rosser Thue system T;*
QUESTION 3: *is $\mathbf{M}_T$ torsion-free?*
QUESTION 4: *is $\mathbf{M}_T$ a free group?*

Some of the techniques used by Otto suggest a theme that has been investigated only recently. Consider a Thue system T on alphabet Σ and the monoid $\mathbf{M}_T = [\Sigma; T]$. Let $\mathbf{G}_T$ be the group presented by the set Σ of generators and the set T of relations. Which properties of $\mathbf{G}_T$ are inherited by $\mathbf{M}_T$ and vice versa? One example is the following fact due to Perrin & Schupp (1984).

THEOREM 7.2. *Let Σ be a finite alphabet, let $w \in \Sigma^*$, $w \neq e$, and let $T = \{(w, e)\}$. Let $\mathbf{G}_T$ be the group presented by the set Σ of generators and the set T of relators. There exists a string $z \in \Sigma^*$ such that, for $T' = \{(z, e)\}$, the monoid $\mathbf{M}_{T'}$ is isomorphic to the group $\mathbf{G}_T$.*

In Theorem 7.2, the string w is said to have *positive exponents* since only generators from Σ occur in w, that is, none of the inverses of generators occurs in w. Thus, Theorem 7.2 says that if a group $\mathbf{G}$ has a one-relator presentation that has positive exponents, then there is a relator with positive exponents *on the same set of generators* such that the monoid generated by that single relator is in fact the group $\mathbf{G}$. Wrathall (1986) has observed that Theorem 7.2 can be generalised in the following way. Let Σ be a finite alphabet and let T be a Thue system on Σ such that there is at least one rule in T having the form (w, e). Then there exists a Thue system T' on Σ such that the monoid $\mathbf{M}_{T'}$ is isomorphic to the group $\mathbf{G}_T$ presented by the set Σ of generators and the set T of relations.

Another example of properties of $\mathbf{M}_T$ that are inherited by $\mathbf{G}_T$ is due to Wrathall (1987).

THEOREM 7.3. *Let T be a Thue system on alphabet Σ. If the monoid $\mathbf{M}_T$ is free, then the group $\mathbf{G}_T$ presented by the set Σ of generators and the set T of relations is also free.*

Another theme in the investigation of the properties of monoids presented by finite (monadic, special) Church–Rosser Thue systems may be described in the following way. Each free monoid has a presentation (the trivial presentation) as a Church–Rosser Thue system. Many questions about strings and about the regular or context-free subsets of finitely generated free monoids are decidable since one can invoke the techniques of the theory of finite-state acceptors and the theory of context-free grammars (or pushdown store acceptors). These same techniques have been used to establish many results regarding the decidability of properties of monoids presented by finite Church–Rosser Thue systems, e.g. (1) the word problem, (2) whether the monoid is trivial or finite or infinite. How far does the (obviously limited) parallel between the theory of finitely generated free monoids and the theory of monoids presented by finite (monadic, special) Church–Rosser Thue systems extend? One problem of which the decidability remains open illustrates the problem.

Let Σ be a finite alphabet. Consider the following problem.

INSTANCE: a finite set $A \subset \Sigma^*$;
QUESTION: is A^* a free submonoid of Σ^* with A as its minimal generating set?

There are many different algorithms for solving this problem, and some can be extended to the case where A is infinite but regular. One loses no generality by assuming that A is the minimal generating set of A^* since in the case of a free monoid one can always effectively construct that unique set from A. If T is a finite monadic Church–Rosser system on Σ, then one can determine whether a given finite set $A \subset \Sigma^*$ is an independent set by using the method of linear sentences mentioned above. It is shown in Book (1983) that if $\mathbf{M}_T$ is cancellative, then one can decide whether the submonoid generated by the finite independent set A is free. But it is not known how to determine whether $\mathbf{M}_T$ is cancellative, and it is not known how to decide the question of freeness when $\mathbf{M}_T$ is not cancellative.

Two additional programs should be investigated. First, one might consider Dehn's problems for finitely presented groups: the word problem, the conjugacy problem, and the isomorphism problem. We have already described results relating to the word problem, but there is more to be done on the other problems if one considers monoids and groups with Church–Rosser presentations. Some recent work on the conjugacy problem for monoids with Church–Rosser presentations is presented in section 8. Second, one might consider the usual strategy employed in the study of universal algebra: consider sub-

objects and the preservation of properties under certain "natural" operations. Again, the subjects are the class of monoids and the class of groups with Church–Rosser presentations.

It is important to note that many of the results reported in this section are quite recent and have not as yet been published. It appears that the general area has great potential for future exploration.

8. The Conjugacy Problem

There are two equivalent definitions of conjugacy in free monoids. The first is that "x is conjugate to y" if there exists a string w such that $xw = wy$. The second is that "x is conjugate to y" if there exist strings u, v such that $x = uv$ and $y = vu$. Of course, these definitions are also equivalent when considering groups. However, the generalisation of these definitions to arbitrary monoids yields concepts that are not necessarily equivalent; in fact, there are situations where the generalisations of neither of these definitions yield an equivalence relation. In group theory the word problem can be reduced to the conjugacy problem, but when arbitrary monoids are considered the two problems are independent of each other. In this section we consider the conjugacy problem with emphasis on monoids with finite Church–Rosser presentations.

Let T be a Thue system on alphabet Σ. For convenience, we denote by $\mathbf{M}$ the monoid $[\Sigma; T]$. Consider the following relations on $\mathbf{M}$:

(a) $u, v \in \Sigma^*$ are *cyclically equal*, $u \approx_{\mathbf{M}} v$ if there exist $x, y \in \Sigma^*$ such that both u and xy are equal in $\mathbf{M}$ and v and yx are equal in $\mathbf{M}$. Let $CE_{\mathbf{M}} = \{(u, v) | u \approx_{\mathbf{M}} v\}$.

(b) $u, v \in \Sigma^*$ are *left-conjugate*, $u \sim_{\mathbf{M}}^{L} v$, if there exist $w \in \Sigma^*$ such that uw and wv are equal in $\mathbf{M}$. Let $CPL_{\mathbf{M}} = \{(u, v) | u \sim_{\mathbf{M}}^{L} v\}$.

Otto (1984*a*) has shown that in general, neither $\approx_{\mathbf{M}}$ nor $\sim_{\mathbf{M}}^{L}$ is an equivalence relation, but if T is special, then $CE_{\mathbf{M}}$ is an equivalence relation.

The following is a continuation of the development above.

(c) $u, v \in \Sigma^*$ are *conjugate*, $u \sim_{\mathbf{M}} v$, if there exist $x, y \in \Sigma^*$ such that both ux and xv are equal in $\mathbf{M}$ and yu and vy are equal in $\mathbf{M}$. Let $CP_{\mathbf{M}} = \{(u, v) | u \sim_{\mathbf{M}} v\}$.

(d) Let $CPLS_{\mathbf{M}} = \{(u, v) | (u, v) \in CPL_{\mathbf{M}} \text{ or } (v, u) \in CPL_{\mathbf{M}}\}$.

(e) Let $CPLS_{\mathbf{M}}^*$ = the transitive closure of $CPLS_{\mathbf{M}}$.

(f) Let $WP_{\mathbf{M}} = \{(u, v) | u \text{ and } v \text{ are equal in } \mathbf{M}\}$.

Now $CPLS_{\mathbf{M}}^*$ is the transitive closure of $CPLS_{\mathbf{M}}$ and is the smallest equivalence relation containing $CPL_{\mathbf{M}}$. On the other hand, $CP_{\mathbf{M}}$ is the largest equivalence class contained in $CPL_{\mathbf{M}}$. In general, $CPLS_{\mathbf{M}}$ is not transitive so that $CPLS_{\mathbf{M}} \neq CPLS_{\mathbf{M}}^*$. Further,

$$WP_{\mathbf{M}} \subseteq CE_{\mathbf{M}} \subseteq CP_{\mathbf{M}} \subseteq CPL_{\mathbf{M}} \subseteq CPLS_{\mathbf{M}} \subseteq CPLS_{\mathbf{M}}^*$$

and there is a monoid $\mathbf{M}$ such that all of the inclusions are proper. Of course, in free monoids, all except the first inclusion are equalities while the first inclusion is proper.

Otto (1984*a*) has established the following results.

THEOREM 8.1. *Let* $\mathbf{M} = [\Sigma; T]$ *where* T *is special. If* T *is Church–Rosser, then*

$$CE_{\mathbf{M}} = CP_{\mathbf{M}} = CPL_{\mathbf{M}} = CPLS_{\mathbf{M}} = CPLS_{\mathbf{M}}^*.$$

This result does not hold for Thue systems that are Church–Rosser and monadic but not simple. Also, one would like to characterise the class of monoids **M** such that the conclusion of Theorem 8.1 holds, but this is an open question.

Call the membership problem for $CP_{\mathbf{M}}$, the *conjugacy problem* for **M**.

THEOREM 8.2.

(*a*) *For finitely presented monoids, the word problem and the conjugacy problem are independent of each other.*

(*b*) *There exists a monoid presented by a finite special Thue system such that the conjugacy problem is undecidable.*

In keeping with the results of section 7, there is the following fact.

THEOREM 8.3. *If T is finite, special, and Church–Rosser, then the conjugacy problem for* **M** *is decidable.*

Consider the complexity of the various forms of the conjugacy problem (when those forms are decidable). This was developed by Narendran & Otto (1985), and the key to their results is the following lemma.

LEMMA 8.4. *Let T be a finite Church–Rosser Thue system on alphabet Σ. For any $u, v \in \Sigma^*$, u and v are left-conjugate if and only if there exists a conjugator w such that $|w| \leqslant 2 \cdot \lambda \cdot \max\{|u|, |v|\}$, where $\lambda = \max\{|x| \mid$ for some y, $(x, y) \in T$ or $(y, x) \in T\}$.*

This allowed Narendran & Otto to obtain the following facts.

THEOREM 8.5. *Let T be a finite Church–Rosser Thue system on alphabet Σ.*

(*a*) *The left-conjugacy problem for* **M** *is solvable non-deterministically in real time.*

(*b*) *The conjugacy problem for* **M** *is solvable non-deterministically in real time.*

(*c*) *Suppose that T is special. Then the conjugacy problem for* **M** *is solvable deterministically in polynomial time.*

The *uniform left-conjugacy problem for finite Church–Rosser Thue systems over alphabet* Σ is the following:

INSTANCE: a finite Church–Rosser Thue system T over Σ, and two strings $u, v \in \Sigma^*$;

QUESTION: is u left-conjugate to v?

We write $ULCP_\Sigma$ for the set of triples (T, u, v) such that the answer is "yes".

The *uniform conjugacy problem for finite Church–Rosser Thue systems over alphabet* Σ is the following:

INSTANCE: a finite Church–Rosser Thue system T over Σ, and two strings $u, v \in \Sigma^*$;

QUESTION: is u conjugate to v?

We write UCP_Σ for the set of triples (T, u, v) such that the answer is "yes".

Narendran *et al.* (1985*b*) were able to make a precise classification of these problems.

THEOREM 8.6. *Both* $ULCP_\Sigma$ *and* UCP_Σ *are NP-complete if* $\|\Sigma\| \geqslant 2$*; both problems are in P if* $\|\Sigma\| = 1$.

9. One-rule Systems

Thue systems with exactly one rewriting rule are a source of interesting problems and examples. Many of the examples are technical but serve to illustrate the difficulties of problems about finite systems and also suggest results that may be true in general. In order to discuss one-rule Thue systems and the monoids they present, it is useful to consider groups presented by a single defining relation, a topic that has been well studied in combinatorial group theory (see Magnus *et al.*, 1966).

Every one-relator group, that is, a group presented by a finite set of generators and a single defining relation, has a solvable word problem; this is a classic result of combinatorial group theory (see Magnus *et al.*, 1966). Adjan (1966) used this fact to show that a monoid with a single defining relator has a decidable word problem. Thus, we know that for every finite alphabet Σ and every $w \in \Sigma^*$, the Thue system $T = \{(w, e)\}$ has a decidable word problem whose complexity is the same as the word problem for the group presented by the relator (w, e). Unfortunately, knowing that these problems are decidable tells us nothing about the inherent complexity of the problems. Avenhaus & Madlener (1978) have shown that the word problem for one-relator groups has complexity that is at worst primitive recursive; this is also true for a few other problems of one-relator groups such as the power problem. However, the work of Avenhaus & Madlener suggests that the word problem for one-relator groups has complexity that is not bounded above by the functions in any one fixed level of the Grzegorczyk hierarchy. In particular, this problem appears not to be subelementary (i.e. not in the Grzegorczyk classes E_n for $n < 3$).

If a finite Thue system is Church–Rosser, then the word problem is decidable in linear time (Theorem 4.2.). Consider the one-rule special Thue systems. In this case the property of being Church–Rosser coincides with an algebraic property that is related to the structure of the string that makes up the relator.

If $w = x^k$ for some $x \in \Sigma^*$ and $k > 1$, then w is *imprimitive*; otherwise, w is *primitive*. In either case, the shortest x such that $w = x^k$ for some $k \geqslant 0$ is the *root* of w, denoted $\rho(w)$. If w is primitive and for some u, v with $0 < |u| < |w|$, $uw = wv$, then w has *overlap*. If w is imprimitive or w has overlap, then there is a proper prefix of w that is also a proper suffix; the longest such common prefix and suffix is the *overlap of* w, denoted $ov(w)$.

Recall that a unit of a monoid is an element that has a two-sided inverse.

THEOREM 9.1. (Book, 1984). *Let* $T = \{(w, e)\}$.

(*a*) *If* w *is primitive and* w *has no overlap, then* $\mathbf{M}_T$ *has no non-trivial units. In this case,* T *is Church–Rosser.*

(*b*) *If* w *is imprimitive and the root of* w *has no overlap, then the group of units of* $\mathbf{M}_T$ *is a finite cyclic group that is non-trivial. In this case,* T *is Church–Rosser.*

(*c*) *If* w *is primitive and* w *has overlap, then the group of units of* $\mathbf{M}_T$ *is infinite. In this case,* T *is not Church–Rosser.*

(*d*) *If* w *is imprimitive and* $\rho(w)$ *has overlap, then the group of units of* $\mathbf{M}_T$ *is infinite but has a finite (but non-trivial) cyclic subgroup. In this case,* T *is not Church–Rosser.*

Thus, we have a situation where one feature of the algebraic structure of the monoid $\mathbf{M}_T$ presented by a Thue system T is closely related to the question of whether T is Church–Rosser.

As noted in Theorem 4.7, it is undecidable for a finite Thue system whether there exists an equivalent finite Thue system that is Church–Rosser. However, this is not true for one-rule special Thue systems. It follows from the proof of Theorem 9.1 that for a one-relator special Thue system T, either T is Church–Rosser or there is no finite Church–Rosser Thue system that is equivalent to T. This fact also applies to "homogeneous" Thue systems, that is, special Thue systems with the property that for some integer $k > 1$ and all rules (w, e) in the Thue system, $|w| = k$.

Consider one-rule systems that are not special. Such a system has the form $T = \{(u, v)\}$ where $|u| \geqslant |v| > 0$. The decidability of the word problem for this class of Thue systems is an open question.

It is clear that if $|u| = |v|$, then the word problem for T is decidable non-deterministically using at most linear space and hence is decidable deterministically in exponential time (in this case, $O(2^{c|uv|})$ for some $c > 0$). Metivier (1985) has shown that if the rewriting is directed so that the rule (u, v) in $T = \{(u, v)\}$ must be applied as replacing u by v but not conversely, then the word problem is decidable non-deterministically in polynomial time. If $|u| > |v|$ and u is primitive and has no overlap, then just as in Theorem 9.1, the Thue system T is Church–Rosser so that there is a linear-time algorithm to solve the word problem. If u is not primitive or u has overlap, then $ov(w)$ is not the empty string. For this case Otto & Wrathall (1985) established the following parallel to Theorem 9.1.

Let $OVL(w) = \{u \mid$ there exist non-empty v_1, v_2 such that $w = uv_1 = v_2u\}$. Let $\pi(w) = |w| - |ov(w)|$; $\pi(w)$ is the *period* of w. Let res (w) be the prefix of w of length equal to the remainder when $|w|$ is divided by $\pi(w)$.

THEOREM 9.2. *Let $T = \{(u, v)\}$ be a Thue system such that $0 \leqslant |v| \leqslant |ov(u)|$. Then T is Church–Rosser if and only if either (a) $|v| \geqslant \pi(u)$ and $v \in OVL(u)$, or (b) $v = res(u)$ and $OVL(u) \cap \{w \mid |res(u)| < |w| < \pi(u)\} = \phi$.*

COROLLARY 9.3. *Let $T = \{(u, v)\}$ be a Thue system such that $0 \leqslant |v| \leqslant |ov(u)|$. Then T is Church–Rosser or there is no Church–Rosser Thue system that is equivalent to T.*

If a finite Thue system is Church–Rosser, then the word problem is decidable in linear time. How many one-rule systems are Church–Rosser? This question can be approached by considering asymptotic density.

A string w is *bordered* if there exist x, y, z such that $w = xz = zy$ and $0 < |x| < |w|$; in this case, z is the *border*. If a string has no border, then it is *unbordered*.

For each positive integer k, fix an alphabet Σ of size k. For each integer $n > 1$, let $u_k(n)$ be the number of strings w in Σ^* of length n such that w is unbordered. Book & Squier (1984) showed that the ratio of $u_k(n)$ to k^n goes to 1 as k and n go to infinity. This fact can be interpreted in the following way.

THEOREM 9.4. *Almost all one-rule Thue systems are Church–Rosser and, hence, have word problems that are decidable in linear time.*

Thus, while the decidability of the word problem for one-rule Thue systems remains an open question, the asymptotic density of systems with decidable word problems suggest that one should attempt to show that all such systems have decidable word problems. For other recent results on the word problem for one-rule Thue systems and the monoids they present, see Howie & Pride (1986).

Another topic of interest for monoids with a single defining relation is the structure of the congruence classes. Consider the Thue system $T = \{(aba, e)\}$. This system is not Church–Rosser, but there is a linear-time algorithm to solve the word problem: ab is congruent to ba so that one can choose $\{a^n, b^n, ab^n | n \geq 0\}$ to be the set of normal forms and then transform each $x \in \{a, b\}^*$ to its unique normal form; two strings are congruent if and only if they have the same normal form. This system is of interest because of an additional fact: for each $x \in \{a, b\}^*$, the congruence class $[x]$ is a deterministic context-free language. Thus, $T = \{(aba, e)\}$ is a Thue system that is not Church–Rosser, that is not equivalent to any Church–Rosser Thue system, and that has the property that every congruence class and every union of congruence classes where the union is taken over any regular subset of $\{a^n, b^n, ab^n | n \geq 0\}$ is a deterministic context-free language.

Is it the case that every one-rule Thue system has the property that every (or some) congruence class is a context-free language? The answer is "no", as can be seen by a very interesting counter-example studied by Jantzen (1981).

THEOREM 9.5. *Let* $\Sigma = \{a, b\}$, *let* $w = abbaab$, *and let* $T = \{(w, e)\}$.

(*a*) *The Thue system* T *is not Church–Rosser and there is no Church–Rosser Thue system that is equivalent to* T.

(*b*) *For each* $x \in \Sigma^*$, *the congruence class of* x *relative to* T *is not a context-free language, that is, no congruence class of the congruence generated by* T *is a context-free language.*

We denote the monoid presented by $[\{a, b\}, (abbaab, e)]$ by $\mathbf{M_J}$ and refer to it as the "Jantzen monoid". (This monoid is, in fact, a group.)

In order to establish his results on $\mathbf{M_J}$, Jantzen used certain notions about matrix representations of monoids. This was developed further by Squier & Wrathall (1982), who showed that $\mathbf{M_J}$ is faithfully represented by a specific group of 2×2 matrices of rational numbers. Using the results of Squier & Wrathall, Potts (1984) constructed an infinite, but structurally simple, presentation of $\mathbf{M_J}$ on four generators. Potts' presentation involves a finite number of rule schemata and is locally confluent but not Noetherian; however, every element of $\mathbf{M_J}$ has a unique normal form. Otto (1984*b*) then showed that the presentation of $\mathbf{M_J}$ given by Jantzen (as in Theorem 9.5) does not admit a finite complete rewriting system that is based on a Knuth–Bendix ordering. (Otto did construct a finite complete rewriting system on four generators for $\mathbf{M_J}$, but the underlying ordering for this system is still not a Knuth–Bendix ordering.) Jantzen, Otto, and Potts have extended these results in different ways, sometimes by attacking other examples. However, at this time the appropriate general theory has yet to be developed.

Before leaving the subject of one-rule systems, one point should be made. The Jantzen monoid $\mathbf{M_J}$ has been the subject of a number of papers by different authors. To a very large extent this happened because the system $T = \{(abbaab, e)\}$ that presents $\mathbf{M_J}$ was the first known example of a Thue system with the following properties: (i) T is not Church–Rosser; (ii) there is no Church–Rosser Thue system on $\{a, b\}$ that is equivalent to T; and (iii) no congruence class of T is a context-free language. Clearly, one cannot expect to build a theory based on one example. But all of this work is quite recent, Jantzen's paper having been published only in 1981, and so more can be expected as other examples are extensively investigated. There is reason to hope that eventually a satisfactory general theory can be developed.

10. Other Types of Systems

There are Thue systems that are not Church–Rosser but have some properties that are similar to those of Church–Rosser systems. Two specific types of systems have been studied.

A Thue system on alphabet Σ is *almost-confluent* if for every pair x, y of strings in Σ^*, x and y are congruent if and only if there exist strings z_1, z_2 such that $x \xrightarrow{*} z_1$, $y \xrightarrow{*} z_2$, and z_1 and z_2 can be shown to be congruent by application of only length-preserving rules.

If a Thue system is almost-confluent, then every irreducible string is minimal, but a congruence class may have more than one irreducible element; if the alphabet is finite, there will be only finitely many irreducible elements in any single congruence class. Clearly, the word problem is decidable, but Jantzen & Monien (reported in Book *et al.*, 1981) showed that the word problem for finite almost-confluent systems is PSPACE-complete. In addition, it is decidable whether a finite Thue system is almost-confluent, and Kapur & Narendran (1985*b*) showed that this question is also PSPACE-complete.

Another type of system is called "preperfect".

A Thue system is *preperfect* if for every pair x, y of strings in Σ^*, x and y are congruent if and only if there exists a string z such that both x and y can be shown to be congruent to z by means of application of length-reducing and/or length-preserving rules. The string z may be taken to be minimal.

If a Thue system is preperfect, then an irreducible string need not be minimal, and a congruence class may have more than one irreducible element; if the alphabet is finite, there will be only finitely many irreducible elements in any single congruence class. Clearly, the word problem is decidable, but again it is PSPACE-complete. Narendran & McNaughton (1984) showed that the question of whether a finite Thue system is preperfect is undecidable (this had been conjectured earlier by Berstel, 1977, and others).

Clearly, every Church–Rosser system is almost-confluent and every almost-confluent system is preperfect, but very little is known about the monoids presented by almost-confluent systems or by preperfect systems. The congruence classes of such a system are always context-sensitive languages, but little else is known about the languages that can be specified by such congruence classes.

One topic that has not been discussed here but has been studied is that of infinite Thue systems over finite alphabets. Book *et al.* (1982) studied infinite context-free Thue systems, and Ó'Dúnlaing (1981, 1983*b*) studied infinite regular Thue systems. Narendran (1983) also considered infinite Thue systems. In all of these cases, one has a Thue system such that for some finite number of strings v there exists an infinite set L_v of strings such that $\{(u, v) | u \in L_v\}$ is a subset of the set of rules; thus, such a Thue system has the form

$$\{(u, v(1)) | u \in L_{v(1)}\} \cup \ldots \cup \{(u, v(n)) | u \in L_{v(n)}\}.$$

In a context-free Thue system each $L_{v(i)}$ is a context-free language, and in a regular Thue system each $L_{v(i)}$ is a regular language; thus, while these are infinite systems, they can be considered to be finitely generated. Hence, infinite regular Thue systems and infinite context-free Thue systems serve as examples of systems specified by a finite number of rewriting rule schemata.

Ó'Dúnlaing's results on infinite regular Thue systems show that monadic systems are easier to deal with than non-monadic systems. For example, it is undecidable whether an infinite regular Thue system is Church–Rosser, but the corresponding question for infinite regular monadic Thue systems is decidable.

There is much more to be done regarding infinite Thue systems. For example, one might investigate the types of groups or monoids that are finitely generated but are presented by infinite regular or infinite context-free Church–Rosser Thue systems.

It is a pleasure to thank Maurice Nivat for introducing me to this subject in 1975. As usual, the advice of Celia Wrathall has been more than helpful in the preparation of this paper.

Note Added in Proof

Regarding the discussion in Section 3, C. Squier ("Word problems and a homological finiteness condition for monoids," *Journal of Pure and Applied Algebra*, to appear) has shown that there exists a finitely presented monoid with a decidable word problem that cannot be presented by any finite complete rewriting system. V. Diekert ("Complete semi-Thue systems for Abelian groups," *Theoretical Computer Science* **44** (1986), 199–208) has shown that there are infinitely many such examples. Some of this is discussed by K. Madlener and F. Otto ("Pseudo-natural algorithms for finitely generated presentations of monoids and groups," submitted for publication).

Regarding the discussion in Sections 5 and 6, J.-M. Autebert, L. Boasson, and G. Senizergues ("Groups and NTS languages," submitted for publication) have shown that every context-free group language is NTS. Both V. Diekert (to appear in *Proc., Fourth Symposium on Theoretical Aspects of Computer Science*, Passau, West Germany, February 1987, Lecture Notes in Computer Science, Springer-Verlag) and K. Madlener and F. Otto (personal communication) have shown that any group with a finite Church–Rosser presentation is a context-free group.

References

Adjan, S. (1966). Defining relations and algorithmic problems for groups and semigroups. *Proc. Steklov Inst. Math.* **85.** (English version published by the American Mathematical Society, 1967.)

Avenhaus, J., Book, R., Squier, C. (1984). On expressing commutativity by Church–Rosser presentations: a note on commutative monoids. *R.A.I.R.O.: Informatique Théorique* **18,** 47–52.

Avenhaus, J., Madlener, K. (1978). Algorithmische probleme bei einrelatorgruppen und ihre komplexität. *Arch. Math. Logic* **19,** 3–12.

Avenhaus, J. Madlener, K. (1984*a*). The Nielsen reduction and P-complete problems in free groups. *Theor. Comp. Sci.* **32,** 61–76.

Avenhaus, J., Madlener, K. (1984*b*). On the complexity of intersection and conjugacy problems in free groups. *Theor. Comp. Sci.* **32,** 279–295.

Avenhaus, J., Madlener, K., Otto, F. (1986). Groups presented by finite two-monadic Church–Rosser Thue systems. *Trans. Amer. Math. Soc.* **297,** 427–443.

Bauer, G. (1984). *Zur Darstellung von Monoiden durch Regelsysteme.* Doctoral dissertation, Universität Kaiserslautern.

Bauer, G. (1985). N-level rewriting systems. *Theor. Comp. Sci.* **40,** 85–99.

Bauer, G., Otto, F. (1984). Finite complete rewriting systems and the complexity of the word problem. *Acta Inf.* **21,** 521–540.

Benois, M. (1969). Parties rationelle du group libre. *C.R. Acad. Sci. Paris,* Sér. A-B **269,** A1188–A1190.

Berstel, J. (1977). *Congruences plus que parfaites et langages algébriques.* Séminaire d'Informatique Théorique, Institut de Programmation, 1976–77, 123–147.

Berstel, J. (1979). *Transductions and Context-free Languages.* Stuttgart: Teubner.

Boasson, L., Sénizergues, G. (1985). N.T.S. languages are deterministic and congruential. *J. Comp. Syst. Sci.* **31,** 332–342.

Book, R. (1982). Confluent and other types of Thue systems. *J. Assoc. Comp. Mach.* **29,** 171–183.

Book, R. (1983). Decidable questions of Church–Rosser congruences. *Theor. Comp. Sci.* **24,** 301–312.

Book, R. (1984). Homogeneous Thue systems and the Church–Rosser property. *Discr. Math.* **48,** 137–145.

Book, R. (1986). Dehn's algorithm and the complexity of word problems. (Submitted).

Book, R., Jantzen, M., Monien, B., Ó'Dúnlaing, C., Wrathall, C. (1981). On the complexity of word problems in certain Thue systems. Math. Found. Comp. Sci., *Springer Lec. Notes Comp. Sci.* **118,** 216–223.

Book, R., Jantzen, M., Wrathall, C. (1982). Monadic Thue systems. *Theor. Comp. Sci.* **19,** 231–251.
Book, R., Ó'Dúnlaing, C. (1981*a*). Testing for the Church–Rosser property. *Theor. Comp. Sci.* **16,** 223–229.
Book, R., Ó'Dúnlaing, C. (1981*b*). Thue congruences and the Church–Rosser property. *Semigroup Forum* **22,** 325–331.
Book, R., Otto, F. (1985). Cancellation rules and extended word problems. *Inf. Proc. Lett.* **20,** 5–11.
Book, R., Squier, C. (1984). Almost all one-rule Thue systems have decidable word problems. *Discr. Math.* **49,** 237–240.
Buchberger, B. (1985). Basic features and development of the critical/pair completion procedure. In: (J.-P. Jouannaud, ed.) Rewriting Techniques and Applications, *Springer Lec. Notes Comp. Sci.* **202,** 1–45.
Bücken, H. (1980). Reduction-systems and small cancellation theory. *Proc. Fourth Conf. Automated Deduction,* 53–59.
Cochet, Y. (1971). *Sur l'algébricité des classes de certaines congruences définés sur le monoide libre.* Thèse 3eme cycles, Rennes.
Cochet, Y. (1976). Church–Rosser congruences on free semigroups. *Colloq. Math. Soc. Janos Bolyai: Algebraic Theory of Semigroups* **20,** 51–60.
Cochet, Y., Nivat, M. (1971). Une généralization des ensembles de Dyck. *Israel J. Math.* **9,** 389–395.
Domanski, B., Anshel, M. (1985). The complexity of the word problem for groups of Dehn's algorithm. *J. Algor.* **6,** 543–549.
Gilman, R. (1984). Computations with rational subsets of confluent groups. In: (Fitch, J., ed.) EUROSAM 1984, *Springer Lec. Notes Comp. Sci.* **174,** 207–212.
Greedlinger, M. (1960). Dehn's algorithm for the word problem. *Comm. Pure Appl. Math.* **13,** 67–83.
Howie, J., Pride, S. (1986). The word problem for one-relator semigroups. *Math. Proc. of the Cambridge Phil. Soc.* **99,** 33–44.
Huet, G. (1980). Confluent reductions: abstract properties and applications to term-rewriting systems. *J. Assoc. Comp. Mach.* **27,** 797–821.
Huet, G., Oppen, D. (1980). Equations and rewrite rules. In: (Book, R., ed.) *Formal Language Theory: Perspectives and Open Problems,* pp. 349–405. New York: Academic Press.
Jantzen, M. (1981). On a special monoid with a single defining relation. *Theor. Comp. Sci.* **16,** 61–73.
Jantzen, M. (1984). Thue systems and the Church–Rosser property. In: (Chytil, M. and Koubet, V., eds), Math. Found. Comp. Sci., *Springer Lec. Notes Comp. Sci.* **176,** 80–95.
Jantzen, M. (1986). Confluent string rewriting and congruences. *Bull. EATCS* **28,** 52–72.
Jouannaud, J.-P. (ed.) (1985). Rewriting techniques and applications. *Springer Lec. Notes Comp. Sci.* **202.**
Kapur, D., Krishnamoorthy, M., McNaughton, R., Narendran, P. (1985). An $O(|T^3|)$ algorithm for testing the Church–Rosser property of Thue systems. *Theor. Comp. Sci.* **35,** 109–114.
Kapur, D., Narendran, P. (1985*a*). A finite Thue system with decidable word problem and without equivalent finite canonical system. *Theor. Comp. Sci.* **35,** 337–344.
Kapur, D., Narendran, P. (1985*b*). The Knuth–Bendix completion procedure and Thue systems. *SIAM J. Comp.* **14,** 1052–1072.
Knuth, D., Bendix, P. (1970). Simple word problems in universal algebras. In: (Leech, J., ed.) *Computational Problems in Abstract Algebra,* pp. 263–297. Oxford: Pergamon Press.
Le Chenadec, P. (1986). Canonical forms in finitely presented algebras. *Research Notes in Theoretical Computer Science.* London/New York: Pitman/Wiley.
Lyndon, R., Schupp, P. (1977). *Combinatorial Group Theory.* Berlin: Springer-Verlag.
McNaughton, R., Narendran, P., Otto, F. (1985). Church–Rosser Thue systems and formal languages. (Manuscript.)
Madlener, K., Otto, F. (1985). Pseudo-natural algorithms for decision problems in certain types of string-rewriting systems. *J. Symbolic Computation* **1,** 383–418.
Magnus, W., Karrass, A., Solitar, D. (1966). *Combinatorial Group Theory.* New York: Wiley-Interscience.
Metivier, Y. (1985). Calcul de longueurs de chaînes de réécriture dans le monoïde libre. *Theor. Comp. Sci.* **35,** 71–88.
Muller, D., Schupp, P. (1983). Groups, the theory of ends, and context-free languages. *J. Comp. Syst. Sci.* **26,** 295–310.
Narendran, P. (1983). *Church–Rosser and Related Thue Systems.* Ph.D. dissertation, Rennsselaer Polytechnic Institute. Also appears as Report No. 84CRD176, General Electric Corporate Research and Development Center, Schenectady, N.Y.
Narendran, P., McNaughton, R. (1984). The undecidability of the preperfectness of Thue systems. *Theor. Comp. Sci.* **31,** 165–174.
Narendran, P., Ó'Dúnlaing, C., Rolletschek, H. (1985*a*). Complexity of certain decision problems about congruential languages. *J. Comp. Syst. Sci.* **30,** 343–358.
Narendran, P., Otto, F. (1985). Complexity results on the conjugacy problem for monoids. *Theor. Comp. Sci.* **35,** 227–243.
Narendran, P., Otto, F., Winklmann, K. (1985*b*). The uniform conjugacy problem for finite Church–Rosser Thue systems is NP-complete. *Inf. Control* **63,** 58–66.
Newman, M. H. A. (1942). On theories with a combinatorial definition of "equivalence". *Ann. Math.* **43,** 223–243.

Nivat. M. (1970). On some families of languages related to the Dyck systems. *Proc. 2nd ACM Sym. Theory Comp.* 221–225.

Nivat, M., Benois, M. (1972). *Congruences parfaites.* Seminaire Dubriel, 25e Année, 1971–72, 7–01–09.

Ó'Dúnlaing, C. (1981). *Finite and Infinite Regular Thue Systems.* Ph.D. dissertation, University of California, Santa Barbara.

Ó'Dúnlaing, C. (1983*a*). Undecidable questions of Thue systems. *Theor. Comp. Sci.* **23,** 339–345.

Ó'Dúnlaing, C. (1983*b*). Infinite regular Thue systems. *Theor. Comp. Sci.* **25,** 339–345.

Otto, F. (1984*a*). Conjugacy in monoids with a special Church–Rosser presentation is decidable. *Semigroup Forum* **29,** 223–240.

Otto, F. (1984*b*). Finite complete rewriting systems for the Jantzen monoid and the Greenlinger group. *Theor. Comp. Sci.* **32,** 249–260.

Otto, F. (1984*c*). Some undecidability results for non-monadic Church–Rosser Thue systems. *Theor. Comp. Sci.* **33,** 261–278.

Otto, F. (1985). Elements of finite order for finite monadic Church–Rosser Thue systems. *Trans. Am. Math. Soc.* **291,** 629–637.

Otto, F. (1986*a*). *Decision Problems and their Complexity for Monadic Church–Rosser Thue Systems.* Habilitationsschrift, Universität Kaiserslautern.

Otto, F. (1986*b*). On deciding whether a monoid is a free monoid or is a group. *Acta Informatica* **23,** 99–110.

Otto, F. (1986*c*). Church–Rosser Thue systems that present free monoids. *SIAM J. Comp.* **15,** 786–792.

Otto, F., Wrathall, C. (1985). A note on Thue systems with a single defining relation. *Math. Syst. Theor.* **18,** 135–143.

Pan, L. (1985). On reduced Thue systems. *Math. Syst. Theor.* **18,** 145–151.

Perrin, D., Schupp, P. (1984). Sur les monoids à une relateur qui sont des groupes. *Theor. Comp. Sci.* **33,** 331–334.

Potts, D. (1984). Remarks on an example of Jantzen. *Theor. Comp. Sci.* **29,** 277–284.

Sénizergues, G. (1985). The equivalence and inclusion problems for N.T.S. languages. *J. Comp. Syst. Sci.* **31,** 303–331.

Squier, C. (1987). Units of special Church–Rosser monoids. *Theor. Comp. Sci.* (to appear).

Squier, C., Wrathall, C. (1982). A note on representations of a certain monoid. *Theor. Comp. Sci.* **17,** 229–231.

Thue, A. (1914). Probleme über Veranderungen von Zeichenreihen nach gegeben Regeln. *Skr. Vid. Kristianaia. I. Mat. Naturv. Klasse,* **10/34.**

Wrathall, C. (1987). On monoids and groups. (In preparation.)

Zieschang, H., Vogt, E., Coldewey, H.-D. (1980). Surfaces and planar discontinuous groups. *Springer Lec. Notes Math.* **835.**