JOURNAL OF COMPUTER AND SYSTEM SCIENCES **53**, 487–496 (1996)
ARTICLE NO. 0082

Maximal and Minimal Solutions to Language Equations*

Lila Kari† and Gabriel Thierrin

Department of Mathematics, University of Western Ontario, N6A 5B7 London, Ontario, Canada

Received February 8, 1995; revised August 14, 1995

We consider equations of the type $L \diamond Y = R$, $X \diamond Y = R$, $X^{\diamond n} = R$, $R \diamond X = L \diamond Y$, where $\diamond$ is a binary word (language) operation, L, R are given constant languages and X, Y are the unknowns. We investigate the existence and uniqueness of maximal and minimal solutions, properties of solutions, and the decidability of the existence of solutions.

1. INTRODUCTION

Let Σ be a finite alphabet. A *binary operation* $\diamond$ is a mapping of $\Sigma^* \times \Sigma^*$ into the set of subsets of Σ^*. The operation $\diamond$ is associative if

$$u \diamond (v \diamond w) = (u \diamond v) \diamond w \qquad \forall u, v, w \in \Sigma^*.$$

Given two languages L_1, $L_2 \subseteq \Sigma^*$, we define $L_1 \diamond L_2 = \{u \diamond v \mid u \in L_1, v \in L_2\}$. The well-known operations of catenation, right/left quotient and shuffle product are examples of such operations. Other examples include the insertion and deletion operations. Recall that (see [3, 4]) given words $u, v \in \Sigma^*$, the insertion of v into u is $u \leftarrow v = \{u_1 v u_2 \mid u = u_1 u_2\}$ and the deletion of v from u is defined as $u \rightarrow v = \{w_1 w_2 \mid u = w_1 v w_2\}$. Among other binary operations we mention parallel, permuted, controlled insertion, and deletion [4, 3], k-catenation, and k-quotient ([5]).

In this paper we study equations of the type $L \diamond Y = R$, $X \diamond Y = R$, $X \diamond X = R$, $R \diamond X = L \diamond Y$, where $\diamond$ is a binary word (language) operation, R and L are given nonempty languages and X, Y are unknown languages (the variables). In the following, X, Y, Z and their indexed variants will denote the unknowns, while L, R and their indexed variants will denote the given constant languages.

The case when $\diamond$ denotes catenation and the languages involved are regular has been considered by Conway in [1]. We consider the existence and uniqueness of solutions. While, when exploring maximal solutions, the results refer to the general case of an abstract binary operation $\diamond$, when considering the minimal solutions we deal with the particular cases where the operation $\diamond$ is catenation.

In Section 2 we deal with equations $L \diamond Y = R$. In the general case, we prove that, if the equation has a solution, it has a unique maximal solution. The fact that all solutions to $LY = R$ have the same set of minimal words aids in showing that if a solution exists, the equation also has a minimal solution. A sufficient condition for the minimal solution to be unique is obtained.

The more general equation $X \diamond Y = R$ is considered in Section 3. A solution (X, Y) to the equation is called an X-maximal solution (maximal solution) if any other solution (X, Y') (resp. (X', Y')) with $Y \subseteq Y'$ (resp. $X \subseteq X'$, $Y \subseteq Y'$) has the property $Y' = Y$ (resp. $X' = X$, $Y' = Y$). If a solution to the equation exists, the equation has a unique X-maximal solution. The maximal solution, while it always exists, is not necessarily unique. In the case of catenation, we show that the equation (if it has a solution) always has an X-minimal and a minimal solution. The existence of a nontrivial solution to $XY = R$ proves to be decidable if R is a regular language. It remains an open problem whether the problem is decidable or not in case R is a context-free language. Properties of solutions when the constant languages belong to some important classes of languages, for example various types of codes, are also investigated.

The concept of a minmax solution is introduced and we show that, if the equation has a solution, it also has a minmax solution.

Section 4 deals with equations $X^{\diamond n} = R$. If $n = 2$ and the equation has a solution, it also has a maximal solution. In case of catenation, the existence of solutions also implies the existence of a minimal solution, which is not necessarily unique. If $n = 2$, the problem whether the equation $X^n = R$ has a solution is decidable for given regular languages R (for $n > 2$ the problem remains open). The problem is undecidable for given context-free languages R.

In the end of the section, the notion of a square-root language (a language R which can be written as a square $X^2 = R$) is introduced and its properties are studied.

Finally, in Section 5 we deal with equations $R \diamond X = L \diamond Y$. If a solution to such an equation exists, also an X-maximal solution and a maximal solution exists. In the

* This research was supported by Grant OGP0007877 of the Natural Sciences and Engineering Research Council of Canada.

† E-mail: lkari@julian.uwo.ca.

0022-0000/96 $18.00

case of catenation, the existence of a solution also implies the existence of a minimal solution which is not necessarily unique.

One of the main tools used in proving the existence of minimal or maximal solutions is *Zorn's lemma*. We recall it in the following, together with other notions and notations used throughout the paper.

Let E be a partially ordered set, where $\leqslant$ is the partial order. A subset $C \subseteq E$ is a *chain* if $a, b \in C$ implies $a \leqslant b$ or $b \leqslant a$. The partially ordered set E is said to be *inductive* (respectively *d-inductive*) if every chain $C \subseteq E$ has an upper bound (respectively a lower bound) $x \in E$, that is, for every $c \in C$ we have that $c \leqslant x$ (respectively $x \leqslant c$).

We remark that the term *d-inductive* is not standard. Since we need both forms of inductive sets, the term *d-inductive* (for dual inductive) is used to avoid confusion in the following.

ZORN'S LEMMA. *If a partially ordered set E is inductive (respectively d-inductive), then for every element $u \in E$ there exists a maximal (respectively a minimal) element $u_{\max} \in E$ ($u_{\min} \in E$) such that $u \leqslant u_{\max}$ ($u_{\min} \leqslant u$).*

A nonempty language $L \subseteq \Sigma^+$ is a *prefix* (*suffix*, *outfix*) *code* if $u \in L$, $ux \in L$ ($u \in L$, $xu \in L$ respectively $u_1 u_2 \in L$, $u_1 x u_2 \in L$) implies $x = 1$.

We recall the embedding order $\leqslant_e$: for any $w, v \in \Sigma^+$, $w \leqslant_e v$ if and only if $w = x_1 x_2 \cdots x_n$, $v = y_1 x_1 y_2 x_2 \cdots y_n x_n y_{n+1}$, $n \geqslant 1$, $x_i, y_i \in \Sigma^*$, $1 \leqslant i \leqslant n+1$. A nonempty language $H \subseteq \Sigma^+$ is called a *hypercode* if and only if $x \leqslant_e y$, $x, y \in H$, implies $x = y$.

A language $L \subseteq \Sigma^*$ is said to be *dense* (left dense, right dense) if for every $w \in \Sigma^*$ there exist $u, v \in \Sigma^*$ ($u \in \Sigma^*$, $v \in \Sigma^*$) such that $uwv \in L$ ($uw \in L$, $wv \in L$). A language which is not dense (left dense, right dense) is termed *thin* (*left thin*, *right thin*).

For further unexplained notions in formal language theory and theory of codes the reader is referred to [6, 7].

2. EQUATIONS $L \diamond Y = R$

This section investigates equations of the form $L \diamond Y = R$. After a first result concerning the existence of a maximal solution to such an equation, we focus on the particular case where the operation involved is catenation.

Some properties of solutions to such equations are obtained. Moreover, the existence of minimal solutions is studied and a sufficient condition for a minimal solution to be unique is obtained.

A solution $Y_{\max}$ to the equation $L \diamond Y = R$ is called a *maximal solution* if $L \diamond Y' = R$, $Y_{\max} \subseteq Y'$ implies $Y_{\max} = Y'$. Analogously, a solution $Y_{\min}$ of the equation is called a *minimal solution* if $L \diamond Y' = R$, $Y' \subseteq Y_{\min}$ implies $Y_{\min} = Y'$.

If $\diamond$ is catenation and if the equation $LY = R$ with R regular has a solution $Y \subseteq \Sigma^*$, then it has a unique maximal solution $Y' = (L \backslash R^c)^c$ which is, moreover, a regular language (see [4]). In $(L \backslash R^c)^c$, the symbol $\backslash$ denotes quotient.

The result has been generalized to concern equations $L \diamond Y = R$, where the operation $\diamond$ possesses a right inverse. (The operation $\square$ is said to be the right-inverse of $\diamond$ iff for all words u, v, w we have $w \in (u \diamond v) \Leftrightarrow v \in (u \square w)$). Namely, if a solution to such an equation exists, then the language $(L \square R^c)^c$ is a maximal solution (see [4]). The following proposition further generalizes the result for equations involving arbitrary binary operations, though without constructing the maximal solution.

PROPOSITION 2.1. *Suppose the equation $L \diamond Y = R$ has a solution Y. Then the equation has a unique maximal solution $Y_{\max}$. If the operation $\diamond$ is associative, then $R \diamond x \subseteq R \Leftrightarrow Y_{\max} \diamond x \subseteq Y_{\max}$.*

Proof. Let $u \in \Sigma^*$ such that $L \diamond u \subseteq R$. Then $L \diamond (Y \cup \{u\}) = R$ and hence $Y \cup \{u\}$ is also a solution. Let $Y_{\max} = \{u \in \Sigma^* \mid L \diamond u \subseteq R\}$. The language $Y_{\max}$ is not empty, because $Y \subseteq Y_{\max}$. Since $L \diamond Y = R$, clearly $L \diamond Y_{\max} = R$ and $Y_{\max}$ is a solution of the equation. If Z is another solution, then $L \diamond Z = R$ and hence $Z \subseteq Y_{\max}$. Therefore $Y_{\max}$ is the unique maximal solution of the equation $L \diamond Y = R$.

If $R \diamond x \subseteq R$, then $(L \diamond Y_{\max}) \diamond x = R \diamond x \subseteq R$ and the associativity of $\diamond$ implies $L \diamond (Y_{\max} \diamond x) \subseteq R$. Therefore $Y_{\max} \diamond x \subseteq Y_{\max}$.

Conversely, if $Y_{\max} \diamond x \subseteq Y_{\max}$, then $L \diamond (Y_{\max} \diamond x) \subseteq L \diamond Y_{\max} = R$. Since

$$L \diamond (Y_{\max} \diamond x) = (L \diamond Y_{\max}) \diamond x = R \diamond x,$$

we have that $R \diamond x \subseteq R$. ∎

Note that if Y is a solution of $L \diamond Y = R$ and if $Y_{\max}$ is the maximal solution, then every language T, $Y \subseteq T \subseteq Y_{\max}$ is a solution.

In the remainder of this section we will restrict ourselves to equations where the operation $\diamond$ is catenation.

For a language $T \subseteq X^*$, let $\rho(T) = \{u \in X^* \mid Tu \subseteq T\}$. It is immediate that $1 \in \rho(R)$ and that $\rho(T)$ is a submonoid of X^*. A language R is called *rc-simple* (*lc-simple*), if R is a class of a right (left) congruence. A language R is rc-simple if and only if $Rx \cap R \neq \varnothing$ implies $Rx \subseteq R$. Every rc-simple language R can be decomposed as $R = PQ^*$, where P and Q are prefix codes or 1 (see [8, 2]). If $1 \in R$, then $R = Q^*$. If $1 \notin R$, then P is the set of prefix words of R and $Q^* = \rho(R)$. We have symmetric results for lc-simple languages.

PROPOSITION 2.2. *If the equation $LY = R$ has a solution, R is an rc-simple language and $Y_{\max}$ is the maximal solution*

of the equation, then $Y_{\max}$ is rc-simple. Moreover, $R = P_r Q^*$ and $Y_{\max} = P_y Q^*$, where P_r, P_y, Q are prefix codes or 1.

Proof. As catenation is associative, Proposition 2.1 implies $u \in \rho(R)$ iff $Ru \subseteq R \Leftrightarrow Y_{\max} u \subseteq Y_{\max} \Leftrightarrow u \in \rho(Y_{\max})$. Hence $\rho(R) = \rho(Y_{\max})$.

If $Y_{\max} x \cap Y_{\max} \neq \varnothing$, then $ux = v$ for some $u, v \in Y_{\max}$. If $w \in L$ then $wux = wv$ with $wu, wv \in R$. Therefore $Rx \cap R \neq \varnothing$ and hence $Rx \subseteq R$. Consequently, $LY_{\max} x = Rx \subseteq R$. Since $Y_{\max}$ is maximal with the property $LY_{\max} \subseteq R$, it follows that $Y_{\max} x \subseteq Y_{\max}$. Therefore $Y_{\max}$ is rc-simple.

Consequently, $R = P_r Q_r^*$, $Y_{\max} = P_y Q_y^*$ and $\rho(R) = Q_r^*$, $\rho(Y_{\max}) = Q_y^*$, where Q_r, Q_y are prefix codes or 1. Since $\rho(R) = \rho(Y_{\max})$, it follows that $Q_r = Q_y$. ▮

For a language $L \subseteq \Sigma^*$, $L \neq \varnothing$, $\mu(L) = \{u \in L \mid |u| \leqslant |u'| \ \forall u' \in L\}$ and $m(L) = \{|u| \mid u \in \mu(L)\}$. In other words, $\mu(L)$ contains all words of minimal length of L while $m(L)$ is the length of a minimal word in L.

The following lemma proves that the set of minimal words is common to all solutions of the equation $LY = R$.

LEMMA 2.1. *Let Y, Y' be two solutions of the equation $LY = R$, $R \neq \varnothing$. Then $\mu(Y) = \mu(Y')$.*

Proof. Note first that $m(Y) = m(Y') = m(R) - m(L)$. Let $u \in \mu(Y)$ and $v \in \mu(L)$. The word $w = vu$ belongs to $\mu(R)$. As $R = LY'$, there exists $x \in L$, $y \in Y'$ such that $xy = w$. As $v \in \mu(L)$, we have that $|x| \geqslant |v|$. Assume $|x| > |v|$. Then the word $vy \in LY' = R$ has the property $|vy| < |w| = m(R)$—a contradiction. The only possible remaining situation is $|v| = |x|$, which implies $u = y$, $v = x$. This further implies $u \in Y'$ and, as $|u| = m(Y') = m(Y)$, we conclude that $u \in \mu(Y')$. The other inclusion is similar. ▮

COROLLARY 2.1. *If Y, Y' are two solutions of the equation $LY = R$, $R \neq \varnothing$, then $Y \subseteq \Sigma^* Y'$ and $Y' \subseteq \Sigma^* Y$.*

Proof. Let $u \in Y$ and $s \in \mu(L)$. Then $su \in R$. Since $LY' = R$, $su = tv$ for some $v \in Y'$ and $t \in L$. From $s \in \mu(L)$ follows that $|s| \leqslant |t|$ and $|u| \geqslant |v|$. Therefore $su = tv$ implies $t = ss_1$ and $u = s_1 v$, i.e., $u \in \Sigma^* Y'$, $Y \subseteq \Sigma^* Y'$. Similarly, it can be shown that $Y' \subseteq \Sigma^* Y$. ▮

In the remainder of this section we will investigate the existence and uniqueness of the minimal solution to $LY = R$. Lemma 2.1 will aid in showing that, if the equation has a solution then it also has a minimal solution.

PROPOSITION 2.3. *Suppose that the equation $LY = R$, $L \neq \varnothing$, $R \neq \varnothing$, has a solution Y. Then*:

(i) *The equation has a minimal solution $Y_{\min}$ with $Y_{\min} \subseteq Y$.*

(ii) *If $\mu(L)\, x \cap L \neq \varnothing$ implies $x = 1$ (in particular if L is a prefix code), then the solution is unique.*

Proof. (i) Let $\mathscr{F} = \{Y_i \mid i \in I\}$ be the family of all solutions to the equation $LY = R$ which have the property $Y_i \subseteq Y$. Suppose that $\mathscr{C} = \{Y_j \mid j \in J\}$ is a chain from $\mathscr{F}$, i.e.,

$$\cdots \subseteq Y_j \subseteq \cdots \subseteq Y_k \subseteq \cdots \subseteq Y.$$

Let $\bar{Y} = \bigcap_{j \in J} Y_j$. According to Lemma 2.1, $\bar{Y} \neq \varnothing$, as it contains the set $\mu(Y)$. Let us now show that $\bar{Y}$ is a solution to the equation. As $\bar{Y} \subseteq Y$, we have that $L\bar{Y} \subseteq LY = R$. For the other inclusion, let $u \in R$ and let $P = \{(r, s) \mid r \in L, s \in Y, rs = u\}$. There exists $(x, y) \in P$ such that $y \in Y_j$ for all $j \in J$. Indeed, assume the contrary and let $P = \{(r_1, s_1), (r_2, s_2), \ldots, (r_n, s_n)\}$ be an enumeration of the elements of P. For each $(r_l, s_l) \in P$, there exists $j_l \in J$ such that $s_l \notin Y_{j_l}$. Let $T = \bigcup_{1 \leqslant l \leqslant n} Y_{j_l}$. As the intersection is finite, there is an index k such that $T = Y_k$. Since $LY_k = R$, the equality $x_k y_k = u$ holds for some $y_k \in Y_k \subseteq Y$ and $x_k \in L$. This further implies $(x_k, y_k) \in P$, a contradiction.

Our assumption was false, therefore $(x, y) \in P$ and $y \in Y_j$ for all $j \in J$, which shows that $u \in L\bar{Y}$. This completes the proof of the fact that $\bar{Y}$ is a solution to the equation. We have shown that the partially ordered set $\mathscr{F}$ is d-inductive (every chain has a lower bound belonging to $\mathscr{F}$). According to Zorn's lemma, this implies that there is at least one minimal element $Y_{\min}$ in the family $\mathscr{F}$; that is, there exists $Y_{\min}$, a minimal solution to the equation, with $Y_{\min} \subseteq Y$.

(ii) Suppose now that Y' and Y'' are two solutions of the equation $LY = R$. Let $x \in Y'$. Then $ux \in R$ for any $u \in \mu(L)$. As $ux \in R = LY''$, we have that $ux = vy$ for some $y \in Y''$, $v \in L$. As $u \in \mu(L)$, $|v| \geqslant |u|$. Consequently, $v = ux'$, which implies $\mu(L)\, x' \cap L \neq \varnothing$. According to the hypothesis, this further implies $x' = 1$ and, consequently, $u = v$, $x = y$. We have therefore shown that $x \in Y''$, that is, $Y' \subseteq Y''$. In a similar way we can show that $Y'' \subseteq Y'$, which proves that the solution to the equation is unique. ▮

A special case of minimal solution occurs when R is a left ideal (that is, $\Sigma^* R \subseteq R$) $R \neq \Sigma^*$ and $L = \Sigma^*$. In this case, since every left ideal $R \neq \Sigma^*$ has a unique decomposition of the form $R = \Sigma^* S$, where S is a suffix code, the equation has the unique minimal solution $Y = S$. The solution $Y = \Sigma^* S$ is the unique maximal solution of the equation.

Let $\Sigma = \{a, b\}$, $R = \Sigma^+ \{a, b^2\}$, and $L = \Sigma^+$. Then the unique minimal solution is $Y = \{a, b^2\}$. Since $\mu(L) = \Sigma$ and $aa \in L \cap \mu(L)\, a$, it follows that condition (ii) in the preceding proposition is a sufficient, but not necessary, condition for the uniqueness of the minimal solution.

The equation $LY = R$ *can have more than one minimal solution.* For example, take $\Sigma = \{a\}$, $R = \{a^n \mid n \geqslant 6\}$, and $L = \{a^5, a^6, a^8, a^9\} \cup \{a^{10+n} \mid n \geqslant 0\}$. It is easy to see that $Y_1 = \{a, a^2\}$ and $Y_2 = \{a, a^3\}$ are two distinct minimal solutions of the equation $LY = R$.

PROPOSITION 2.4. *Let Y be a solution of $LY = R$. Then this solution is minimal $\Leftrightarrow A \subseteq Y$, $B \subseteq Y$ and $LA = LB$ implies $A = B$.*

Proof. ($\Rightarrow$) Suppose that $A \neq B$. Without loss of generality, we can assume that $A = A_1 \cup A_2$ with $A_1 \cap B = \varnothing$ and $A_2 \subseteq B$.

If $A_1 = \varnothing$, then $A = A_2 \subset B$. If $C = Y - B$, then $Y' = C \cup A$ is a solution with $Y' \subset Y$—a contradiction with the minimality of Y. If $A_1 \neq \varnothing$, let $C = Y - B - A_1$. Then $Y' = C \cup B$ is a solution with $Y' \subset Y$, contradicting the minimality of Y. Therefore $A = B$.

($\Leftarrow$) Suppose that Y is not minimal. Then there is a solution $Y' \subset Y$ and $LY = R = LY'$. This implies $Y = Y'$, a contradiction. ∎

We conclude this section with some remarks on the decidability of the existence of solutions to the equation $LY = R$. In [4, 3] it has been shown that the problem "Does there exist a solution Y to the equation $LY = R$" is decidable for regular languages L and R. The problem is undecidable for context-free languages L and regular languages R.

3. EQUATIONS $X \diamond Y = R$

Let $R \subseteq \Sigma^*$ be a given language. Every pair (X, Y) satisfying the equality $X \diamond Y = R$ is called a solution of the equation.

In this section we explore the existence and uniqueness of maximal and minimal solutions, with an emphasis on the particular case where the operation $\diamond$ is catenation.

If (X, Y) is a solution of the equation $X \diamond Y = R$ and if $X \diamond u \subseteq R$ ($v \diamond Y \subseteq R$), then $(X, Y \cup \{u\})$ $((X \cup \{v\}, Y))$ is also a solution. If the equation $X \diamond Y = R$ has a solution and $\diamond$ is associative, then, for every language L, the equations $X \diamond Y = R \diamond L$ and $X \diamond Y = L \diamond R$ also have a solution, namely $(X, Y \diamond L)$ and $(L \diamond X, Y)$.

Note that if the operation $\diamond$ is catenation, then the equation $XY = R$ always has two *trivial solutions*, namely $X = \{1\}$, $Y = R$ or $X = R$, $Y = \{1\}$.

A nontrivial solution to the equation is not necessarily unique. For example, if $R = \{a^3, a^4, a^5, a^6\}$ we have the solution (X, Y) with $X = \{a^2, a^3\}$ and $Y = \{a, a^2, a^3\}$, but this solution is not unique, because $X = \{a^2, a^3\}$, $Y = \{a, a^3\}$ is also a solution.

If the language R is rc-simple with $R = PQ^*$ then the equation $XY = R$ has the solution (P, Q^*).

If (X, Y) is a solution of the equation $X \diamond Y = R$, then (X, Y) is called an *X-maximal solution* if $X \diamond Y' = R$ with $Y \subseteq Y'$ implies $Y = Y'$; (X, Y) is called a *Y-maximal solution* if $X' \diamond Y = R$ with $X \subseteq X'$ implies $X = X'$; the solution (X, Y) is called a *maximal solution* if $X' \diamond Y' = R$ with $X \subseteq X'$, $Y \subseteq Y'$ implies $X = X'$, $Y = Y'$.

Note that if (X, Y) is an X-maximal (Y-maximal) solution of $X \diamond Y = R$, then $(X \diamond u) \cap R^c \neq \varnothing$ (respectively $(v \diamond Y) \cap R^c \neq \varnothing$) for every $u \notin Y$ ($v \notin X$). Indeed, if $X \diamond u \cap R^c = \varnothing$, then $X \diamond u \subseteq R$ and $(X, Y \cup \{u\})$ is a solution, a contradiction with the X-maximality of (X, Y).

PROPOSITION 3.1. *Suppose that the equation $X \diamond Y = R$ has the solution (X, Y). The equation has a unique X-maximal solution (Y-maximal solution) and a maximal solution that is not necessarily unique.*

Proof. Let $\mathcal{F} = \{(X, Y_i) \mid i \in I\}$ be the family of all the solutions of the equation $X \diamond Y = R$ with X fixed. Let $Y_{\max} = \bigcup_{i \in I} Y_i$. Then clearly $X \diamond Y_{\max} = R$ and $Y_{\max}$ is a solution containing all the other solutions. Hence $Y_{\max}$ is the unique X-maximal solution.

Let $(X, Y_{\max})$ be the unique X-maximal solution of $X \diamond Y = R$ and let $\mathcal{G} = \{(X_j, Y_{\max}) \mid j \in J\}$ be the family of all the solutions of $X \diamond Y_{\max} = R$ with $Y_{\max}$ fixed. Let $X_{\max} = \bigcup_{j \in J} X_j$. Then clearly $X_{\max} \diamond Y_{\max} = R$ and $X_{\max}$ is a solution containing all the other solutions in relation with $Y_{\max}$. Suppose that (X', Y') is a solution with $X_{\max} \subseteq X'$ and $Y_{\max} \subseteq Y'$. Since $X \subseteq X_{\max}$, we have that $X \diamond Y' = R$ and hence $Y' = Y_{\max}$ because $Y_{\max}$ is the X-maximal solution. Therefore $X' \diamond Y_{\max} = R$ and $(X', Y_{\max}) \in \mathcal{G}$. Since $X_{\max} = \bigcup_{j \in J} X_j$ and $X_{\max} \subseteq X'$, it follows that $X_{\max} = X'$. Hence $(X_{\max}, Y_{\max})$ is a maximal solution of the equation $X \diamond Y = R$.

The maximal solution is not necessarily unique. Indeed, suppose that the operation $\diamond$ is catenation. The equation $X \diamond Y = \Sigma^4 = \{u \in \Sigma^* \mid |u| = 4\}$ has the maximal solution $X = \Sigma$ and $Y = \Sigma^3$ and the maximal solution $X = \Sigma^2 = Y$. ∎

In the remainder of this section we will consider only the particular case where the operation involved is catenation. In this case and if R is regular, the existence of a solution to the equation is decidable, as shown by the following result.

PROPOSITION 3.2. *The problem whether or not the equation $XY = R$ has a nontrivial solution is decidable for regular languages R.*

Proof. According to [4], there exists a finite number n of distinct regular languages R_i, $1 \leqslant i \leqslant n$, such that, for each $L \subseteq \Sigma^*$, the following statements are equivalent:

(i) there exists a solution Y to the equation $LY = R$.

(ii) there exists an i, $1 \leqslant i \leqslant n$, such that $LR_i = R$ and $Y \subseteq R_i$.

The regular languages R_i can be effectively constructed.

In a similar way, one can obtain a list of distinct regular languages $L_1, ..., L_m$ with the following property. For any language L', the equation $XL' = R$ has a solution X iff it has a solution among the languages L_j, $1 \leqslant j \leqslant m$, and $X \subseteq L_j$.

Moreover, one can remove from the above lists languages R_i (resp. L_j) for which the equation $LR_i = R$ (resp. $L_j L' = R$) does not hold for any language L (resp. L').

Note that the equation has a solution iff it also has a regular solution (L_j, R_i), $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$. The algorithm for deciding our problem will consist in constructing these lists. Then we consider all the products $L_j R_i$, $1 \leqslant j \leqslant m$ and $1 \leqslant i \leqslant n$. If we find one pair different from $(1, R)$, $(R, 1)$, for which the product equals R, a nontrivial solution to the equation exists. Otherwise, the equation has no nontrivial solutions. ▮

A solution $(X, Y_{\min})$ to the equation $XY = R$ is called an X-minimal solution if $XY' = R$ with $Y' \subseteq Y_{\min}$ implies $Y_{\min} = Y'$. A Y-minimal solution is defined symmetrically. A solution $(X_{\min}, Y_{\min})$ is called a *minimal solution* if $X'Y' = R$ with $X' \subseteq X_{\min}$, $Y' \subseteq Y_{\min}$ implies $X_{\min} = X'$ and $Y_{\min} = Y'$.

PROPOSITION 3.3. *Let (X, Y) be a solution of $XY = R$. Then*:

(i) *There exists an X-minimal (Y-minimal) solution $(X, Y_{\min})$ (respectively $(X_{\min}, Y)$) with $Y_{\min} \subseteq Y$ (respectively $X_{\min} \subseteq X$).*

(ii) *There exists a minimal solution $(X_{\min}, Y_{\min})$ with $X_{\min} \subseteq X$ and $Y_{\min} \subseteq Y$.*

Proof. (i) Since X is fixed, we can consider the equation $LY = R$, where $L = X$. By Proposition 2.3, this equation has a minimal solution $Y_{\min} \subseteq Y$. This implies that $(X, Y_{\min})$ is an X-minimal solution.

(ii) Let $(X_{\min}, Y)$ be a Y-minimal solution. By (i), there exists a $X_{\min}$-minimal solution, say $(X_{\min}, Y_{\min})$, with $Y_{\min} \subseteq Y$. Let (X', Y') be a solution such that $X' \subseteq X_{\min}$, $Y' \subseteq Y_{\min}$. If $X' \subset X_{\min}$, then $X'Y' = R$ implies $X'Y = R$ and $X_{\min}$ is no more a Y-minimal solution, a contradiction. Hence $X' = X_{\min}$. If $Y' \subset Y_{\min}$, then $X_{\min} Y' = X'Y' = R$ implies that $(X_{\min}, Y_{\min})$ is no more a $X_{\min}$-minimal solution, a contradiction. Hence $Y' = Y_{\min}$ and $(X_{\min}, Y_{\min})$ is a minimal solution. ▮

For example, the equation $XY = \Sigma^+$ has the minimal solution (Σ, Σ^*).

PROPOSITION 3.4. *Let (X, Y) be a solution of $XY = R$. Then this solution is X-minimal $\Leftrightarrow A \subseteq Y$, $B \subseteq Y$ and $XA = XB$ implies $A = B$.*

Proof. Similar to the one of Proposition 2.4 by considering the equation $LY = R$ with $L = X$. ▮

A special case of Y-minimal solution occurs when R is a right ideal, $R \neq \Sigma^*$. In this case, there is a Y-minimal solution $(X = P, Y = \Sigma^*)$, where P is a prefix code. This follows from the fact that every right ideal $R \neq \Sigma^*$ can be written as $P\Sigma^*$, where P is a prefix code.

We give below some properties of solutions to the equation $XY = R$ when the language R belongs to some special classes of languages, for example different types of codes and commutative languages. Recall that a language L is called commutative if $w \in L$ implies that all the words obtained from w by arbitrarily permuting its letters belong to L. A language L is commutative iff $uxyv \in L$ implies $uyxv \in L$.

PROPOSITION 3.5. *Let (X_1, Y_1) be a solution of the equation $XY = R$ and let $X' = X_1 - \{1\}$, $Y' = Y_1 - \{1\}$.*

(i) *If $T = (X_1 \backslash R^c)^c$, then (X_1, T) is a solution of the equation $XY = R$ and, for any solution of the form (X_1, Z), we have $Z \subseteq T$.*

(iia) *If R is a prefix (suffix) code, then Y' (X'), if not empty, is a prefix (suffix) code.*

(iib) *If R is an outfix code (respectively a hypercode), then X' and Y', if not empty, are outfix codes (respectively hypercodes).*

(iiia) *If R is commutative and if (X_1, Y_1) is an X_1-maximal (Y_1-maximal) solution, then Y_1 is commutative (X_1 is commutative).*

(iiib) *If X_1 is a prefix (Y_1 is a suffix) code and if R is commutative, then Y_1 is commutative (X_1 is commutative).*

(iva) *If R is left thin (right thin), then Y_1 is left thin (X_1 is right thin).*

(ivb) *If R is thin, then both X_1 and Y_1 are thin.*

Proof. (i) We show first that $X_1 T \subseteq R$. If not, there exist words $u \in X_1$, $v \in T$ such that $uv \in R^c$. This implies that $v = (u \backslash uv) \subseteq (X_1 \backslash R^c)$, a contradiction because $v \in T$.

Let Y' be a language such that $X_1 Y' \subseteq R$. Then $Y' \subseteq T$. Indeed, otherwise $Y' - T \neq \varnothing$. Let $v \in Y' - T$. Since $v \in X_1 \backslash R^c$, there exist $w \in R^c$, $u \in X_1$ such that $uv = w$. Hence $w \in X_1 Y' \subseteq R$, a contradiction because $w \in R^c$.

From the above considerations it follows that $R = X_1 Y_1 \subseteq X_1 T \subseteq R$, which implies that (X_1, T) is a solution to the equation.

Since (X_1, Z) is a solution, we have $Z \subseteq T$.

(iia) Let $u, ur \in Y'$ with $r \in X^*$. For all $v \in X'$, $vu, vur \in R$. Since R is a prefix code, $r = 1$ and this implies Y' is a prefix code.

(iib) Suppose first that R is an outfix code. Let $u = u_1 u_2$, $u_1 x u_2 \in Y'$. Then, for every $w \in X'$, $wu_1 u_2, wu_1 x u_2 \in R$. Since R is outfix, $x = 1$ and hence Y' is an outfix code. Similarly, it can be shown that X' is an outfix code.

Suppose now that R is a hypercode. If $u, v \in Y'$ with $u \leqslant_e v$ (where $\leqslant_e$ is the embedding order), then, since the embedding order is compatible, for every $w \in X'$, $wu \leqslant_e wv$ with $wu, wv \in R$. Since R is a hypercode, $wu = wv$, $u = v$, and Y' is a hypercode. Similarly, it can be proved that X' is a hypercode.

(iiia) Since $X_1 Y_1 = R$ and since Y_1 is X_1-maximal, $X_1 y \subseteq R$ implies $y \in Y_1$. If $w \in X_1$ and $uxyv \in Y_1$, then $wuxyv \in X_1 Y_1 = R$. Hence $wuyxv \in R$ for all $w \in X_1$. Therefore $uyxv \in Y_1$; that is, Y_1 is commutative.

(iiib) If $uxyv \in Y_1$ and $w \in X_1$, then $wuxyv \in X_1 Y_1 = R$ and $wuyxv \in X_1 Y_1 = R$. Hence $wuyxv = x_1 y_1$ with $x_1 \in X_1$. Since X_1 is a prefix code and $w \in X_1$, this implies $w = x_1$. Therefore $uyxv \in Y_1$ and Y_1 is commutative.

(iva) Since R is left thin, there exists $u \in \Sigma^*$ such that $vu \notin R$ for any $v \in \Sigma^*$. Suppose that Y_1 is not left thin and hence left dense. Then, for $u \in \Sigma^*$ above, there exists $x \in \Sigma^*$ such that $xu \in Y_1$. As (X_1, Y_1) is a solution of $XY = R$, there exists $w \in X_1$ such that $wxu \in R$. This contradicts the fact that R was left thin. Therefore Y_1 is left thin.

(ivb) If R is thin, there exists $u \in \Sigma^*$ such that $xuy \notin R$ for any $x, y \in \Sigma^*$. Suppose Y_1 is not thin; that is, Y_1 is dense. Then, for u above, there exist $x', y' \in \Sigma^*$ such that $x'uy' \in Y_1$. This implies $vx'uy' \in R$ for some $v \in X_1$—a contradiction. ∎

Note that, if R is (right, left) dense, then X or Y are not necessarily (right, left) dense. For example, take $R = \Sigma^* a$, $a \in \Sigma$. Then R is right dense and $X = \Sigma^*$, $Y = a$ is a solution, but Y is not right dense. If $R = \Sigma^+$, then R is dense. $X = \Sigma$ and $Y = \Sigma^*$ is a solution with Σ not dense.

EXAMPLES. (1) Let R be the prefix code $R = \Sigma^k$, where $k \geqslant 2$. Then the equation $XY = R$ has the solutions $X = \Sigma^m$, $Y = \Sigma^n$ where $m, n \geqslant 1$ and $m + n = k$.

(2) Let $\Sigma = \{a, b\}$ and let R be the prefix code $R = \{ba, aba\}$. The equation $XY = R$ has a nontrivial solution $X = \{b, ab\}$, $Y = \{a\}$.

(3) In all the nontrivial solutions (X, Y) given for the preceding examples, both X and Y were prefix codes. However, this is not the case in general for the left side of the solution. Take, for example, the equation $XY = R = b^* a$. Then R is a prefix code and $X = b^*$, $Y = a$ is a solution, where X is not a prefix code. Note that X and Y are commutative even though R is not.

Note that, if (X, Y) is a solution of $XY = R$ with R a prefix code and if X is a prefix code, then either $X = R$ or $X \cap R = \varnothing$. Indeed, let $U = X \cap R$. If $u \in U$, then $uY \subseteq R$ with $u \in R$. Since R is a prefix code, this implies that $Y = \{1\}$ and hence $X = R$.

A solution $(X_{\min}, Y_{\max})$ of the equation $XY = R$ is said to be a *minmax solution* if there is no other solution (X', Y') with $X' \subseteq X_{\min}$ and $Y_{\max} \subseteq Y'$. For example the trivial solution $(1, R)$ is a minmax solution. If $R = \Sigma^+$, then $(1, \Sigma^+)$ and (Σ, Σ^*) are both minmax solutions. This also shows that a minmax solution is not, in general, unique.

PROPOSITION 3.6. *If the equation $XY = R$ has a solution (X, Y), then it has a minmax solution $(X_{\min}, Y_{\max})$ such that $X_{\min} \subseteq X$ and $Y \subseteq Y_{\max}$.*

Proof. Let $\mathscr{P}(\Sigma)$ be the family of pairs (X, Y) of subsets X and Y of Σ^*. Define the relation $\subseteq$ on $\mathscr{P}(\Sigma)$ by

$$(X, Y) \subseteq (X', Y') \Leftrightarrow X' \subseteq X,\ Y \subseteq Y'.$$

The relation $\subseteq$ is a partial order on $\mathscr{P}(\Sigma)$.

Let $\mathscr{F} = \{(X_i, Y_i) \mid i \in I\}$ be the family of all the solutions of the equation $XY = R$ with $X_i \subseteq X$ and $Y \subseteq Y_i$. The family $\mathscr{F}$ is partially ordered with the partial order $\subseteq$ defined on $\mathscr{P}(\Sigma)$.

Let $\mathscr{C} = \{(X_j, Y_j) \mid j \in J \subseteq I\}$ be a chain of pairs (X_j, Y_j) from the family $\mathscr{F}$,

$$\cdots \subseteq (X_j, Y_j) \subseteq \cdots \subseteq (X_k, Y_k) \subseteq \cdots,$$

where $(X_j, Y_j) \subseteq (X_k, Y_k)$; i.e., $X_k \subseteq X_j$ and $Y_j \subseteq Y_k$.

Let $X_m = \bigcup_{j \in J} X_j$ and $Y_m = \bigcup_{j \in J} Y_j$. We will show that (X_m, Y_m) is a solution of the equation $XY = R$. If the chain is finite, this is immediate.

Suppose now that the chain is infinite. Notice first that $X_m \neq \varnothing$.

Indeed, as $X_j Y_j = R$ for all $j \in J$ and $Y_m = \bigcup_{j \in J} Y_j$ we have that $R = X_j Y_j \subseteq X_j Y_m = R$. According to Lemma 2.1 this implies $\mu(X_j) = \mu(X_k)$ for all $j, k \in J$, which further means that $X_m \neq \varnothing$.

Since $X_m \subseteq X_j$, $X_m Y_m \subseteq X_j Y_m = R$. For the other inclusion, let $u \in R$. For all $j \in J$, there exist $x_j \in X_j$ and $y_j \in Y_j$ such that $x_j y_j = u$. There is a pair (x, y) in the finite set $P = \{(r, s) \mid r \in X, s \in Y_m, rs = u\}$ such that $x \in X_j$ for all $j \in J$.

Assume the contrary, and let $P = \{(r_1, s_1), (r_2, s_2), \ldots, (r_n, s_n)\}$ be an enumeration of the words in P. For each l, $1 \leqslant l \leqslant n$, there exists j_l such that $r_l \notin X_{j_l}$. Take $T = \bigcap_{1 \leqslant l \leqslant n} X_{j_l}$. As the intersection is finite and its elements belong to the chain, there exists a k such that $T = X_k$. As $X_k Y_k = R$, there are words $x_k \in X_k \subseteq X$ and $y_k \in Y_k \subseteq Y_m$ such that $x_k y_k = u$. This implies $(x_k, y_k) \in P$, a contradiction. Consequently, there exists $(x, y) \in P$ such that $x \in X_m$. This implies $u = xy \in X_m Y_m$ and the second inclusion is proved.

We have therefore shown that (X_m, Y_m) is a solution to the equation.

From the above considerations, it follows that $\mathscr{F}$ is inductive and that we can apply Zorn's lemma to the family $\mathscr{F}$ of the solutions of the equation $XY = R$. Therefore there is at least a maximal element $(X_{\min}, Y_{\max})$; that is, $X_{\min} Y_{\max} = R$ and this solution is a minmax solution. ∎

By inverting the roles of X and Y, we have a symmetric definition and similar results concerning maxmin solutions $(X_{\max}, Y_{\min})$ of $XY = R$.

4. EQUATION $X \diamond X = R$

If the operation $\diamond$ is associative, then the nth power of a language L is well defined as

$$L^{\diamond n} = \underbrace{L \diamond L \diamond \cdots \diamond L}_{n \text{ times}}.$$

(If the operation is not associative, then $L \diamond (L \diamond L)$ can be different from $(L \diamond L) \diamond L$.)

We now consider equations of the form $X \diamond X = R$ and $X^n = R$, where R is a given language. Clearly such equations do not always have a solution. For example, if $\diamond$ is catenation and $R = \{a\}$, $a \in \Sigma$, then the equation has no solution for $n \geqslant 2$.

A solution X of the equation $X \diamond X = R$ or the equation $X^n = R$ is called a *maximal solution* if, given any solution X' with $X \subseteq X'$, we have $X = X'$.

PROPOSITION 4.1. (i) *If the equation $X \diamond X = R$ has a solution X, then it has a maximal solution $X_{\max}$ with $X \subseteq X_{\max}$.*

(ii) *If the operation $\diamond$ is associative and if the equation $X^{\diamond n} = R$ has a solution X, then it has a maximal solution $X_{\max}$ with $X \subseteq X_{\max}$.*

Proof. (i) Let $\mathscr{F} = \{X_i \mid i \in I\}$ be the family of all the solutions of the equation $X \diamond X = R$ with $X \subseteq X_i$. If $\{X_k \mid k \in K\}$ is a chain (relatively to inclusion) of solutions, then the language $\bar{X} = \bigcup_{k \in K} X_k$ is also a solution of the equation. Therefore we can apply the Zorn lemma and hence this equation has a maximal solution $X_{\max}$ and $X \subseteq X_{\max}$.

(ii) The proof is similar to the proof given in (i). ∎

The following result gives a sufficient condition under which the solution to the equation $X^n = R$ is unique.

PROPOSITION 4.2. *If the equation $X^n = R$ with R a prefix (suffix) code has a solution X, then this solution is unique and X is a prefix (suffix) code.*

Proof. If $n = 1$, this is trivial.

Let $n \geqslant 2$. If $u, ux \in X$, then $u^n, u^n x \in R$ and $x = 1$. Therefore $X = P$ is a prefix code. If Q is another solution, then Q is a prefix code and $P^n = Q^n = R$. Let $P_r(\Sigma)$ be the set of all the prefix codes over Σ. The set $P_r(\Sigma)$ is a free semigroup with the operation of catenation of languages. Let P_Σ be the set of generators of $P_r(\Sigma)$. Then P and Q have unique decompositions of the form:

$$P = P_1 P_2 \cdots P_k, \quad Q = Q_1 Q_2 \cdots Q_r, \quad P_i, Q_j \in P_\Sigma.$$

From $P^n = Q^n$ it follows then that

$$(P_1 P_2 \cdots P_k) \cdots (P_1 P_2 \cdots P_k) = R = (Q_1 Q_2 \cdots Q_r) \cdots (Q_1 Q_2 \cdots Q_r).$$

This further implies $k = r$ and $P_i = Q_i$, $1 \leqslant i \leqslant r$; that is, $P = Q$. ∎

The following two results deal with the decidability of the problem whether or not the equation $X^n = R$ has a solution. If $n = 2$ and R is regular, the problem is decidable, as shown by the proposition below.

PROPOSITION 4.3. *The problem whether there exists a solution X to the equation $X^2 = R$ is decidable for regular languages R. Moreover, in case of an affirmative answer, the maximal solution is regular and can be effectively constructed.*

Proof. Let R be a regular language and let R_i, $1 \leqslant i \leqslant n$, L_j, $1 \leqslant j \leqslant m$, be the lists of regular languages constructed in Proposition 3.2.

Claim. If the equation $X^2 = R$ has a solution X, it also has a regular solution.

As X is a solution to the equation, we can state that X is a solution to the equation $XY = R$, where Y is the only variable. This implies that there exists an index $1 \leqslant i \leqslant n$ such that $XR_i = R$ and $X \subseteq R_i$. If we now fix the language R_i, then X is a solution to the equation $XR_i = R$. Consequently, there exists an index $1 \leqslant j \leqslant m$ such that $L_j R_i = R$ and $X \subseteq L_j$.

Take now $X_0 = L_j \cap R_i$. We have that $R = XX \subseteq X_0 X_0 \subseteq R$; therefore X_0 is a solution.

The algorithm for deciding our problem will consist in constructing the lists R_i, $1 \leqslant i \leqslant n$ and L_j, $1 \leqslant j \leqslant m$, and all the possible intersections $X_0 = R_i \cap L_j$. It continues by verifying, for each such X_0, whether or not the equality $X_0 X_0 = R$ holds. The answer is YES if at least one such X_0 is found, and NO otherwise. A maximal such language gives a maximal solution. Note that all the intersections $R_i \cap L_j$ are regular, as intersections of regular languages, and that they can be effectively constructed. ∎

PROPOSITION 4.4. *The problem whether or not the equation $X^n = R$, $n \geqslant 2$, has a solution is undecidable for context-free languages R.*

Proof. Let R be a context-free language over Σ and let $\#$ be a symbol not belonging to Σ.

Consider the language $R_\# = (\Sigma^* \#)^{n-1} R \#$.

Claim. The equation $X^n = (\Sigma^* \#)^{n-1} R \#$ has a solution iff $X = \Sigma^* \#$ and $R = \Sigma^*$.

The implication $\Leftarrow$ is immediate.

For the other implication notice that the language $R_{\#}$ is a prefix code. According to Proposition 4.2, this implies that the equation $X^n = R_{\#}$ has a unique solution, which is also a prefix code.

It is therefore enough to prove that $X = \Sigma^*\#$ is a solution to the equation. Let $x \in X$. As $x^n \in R_{\#}$, the word x has to end in $\#$, that is, $x = w\#$, $w \in (\Sigma \cup \{\#\})^*$. As any word in $R_{\#}$ contains exactly n markers, we deduce that, in fact, $w \in \Sigma^*$; that is, $X \subseteq \Sigma^*\#$.

For the other inclusion, consider a word $w\#$ in $\Sigma^*\#$. The word $(w\#)^{n-1}\alpha\#$ belongs to $R_{\#} = X^n$ for some $\alpha \in R$.

Therefore we have $(w\#)^{n-1}\alpha\# = u_1\#u_2\#\cdots u_n\#$, for some $u_1\#, ..., u_n\# \in X$. From the forms of the words and the fact that they both contain exactly n markers, we conclude that $u_1 = w$, which implies $w\# \in X$; that is, we have $\Sigma^*\# \subseteq X$.

The fact that $X = \Sigma^*\#$ further implies $R = \Sigma^*$, and the proof of the claim is complete.

From the claim it follows that, if we could decide the existence of a solution to an equation $X^n = R$, R context-free, we could in particular decide the existence of a solution to the equation $X^n = R_{\#}$. This, in turn, would imply that we can decide whether or not $R = \Sigma^*$ for context-free languages R—a contradiction. ▮

We now turn our attention to the existence of minimal solutions to equations $X^2 = R$. The following lemma aids in showing that, if the equation has a solution, then it also has a minimal one.

LEMMA 4.1. *If X and X' are two solutions of $X^2 = R$, then $\mu(X) = \mu(X')$ and $m(X) = m(R)/2$.*

Proof. Similar to the corresponding proof of Lemma 2.1. ▮

PROPOSITION 4.5. *If X is a solution of the equation $X^2 = R$, then there is a minimal solution $X_{\min}$ such that $X_{\min} \subseteq X$.*

Proof. Let $\mathscr{F} = \{X_i \mid i \in I\}$ be the family of all the solutions X_i of $X^2 = R$ with $X_i \subseteq X$. Suppose that $\mathscr{C} = \{X_j \mid j \in J \subseteq I\}$ is a chain from $\mathscr{F}$, i.e.,

$$\cdots \subseteq X_k \subseteq \cdots \subseteq X_j \subseteq \cdots \subseteq X.$$

Let $\bar{X} = \bigcap_{j \in J} X_j$. Since, by Lemma 4.1, the languages $\{\mu(X_i) \mid i \in I\}$ are all equal, it follows that $\bar{X} \neq \varnothing$, because $\mu(X_i) \subseteq \bar{X}$.

It is clear that $\bar{X}^2 \subseteq R$. To prove that $R \subseteq \bar{X}^2$, let $u \in R$. Then, using a similar method as in the proof of Proposition 3.6, it can be shown that there exist x, $y \in \bar{X}$ such that $u = xy$. Hence $\bar{X}^2 = R$ and, consequently, $\bar{X} \in \mathscr{F}$.

It follows that, since every chain $\mathscr{C}$ of $\mathscr{F}$ has a lower bound in $\mathscr{F}$, the family $\mathscr{F}$ is d-inductive and we can then apply the Zorn's lemma. Therefore there is a minimal solution $X_{\min}$ of the equation $X^2 = R$ with $X_{\min} \subseteq X$. ▮

Note that, if the equation $X^2 = R$ has a solution, the minimal solution is not necessarily unique. For example, let $\Sigma = \{a\}$ and $R = \{a^{2n} \mid n \geqslant 1\}$. The equation $X^2 = R$ has the following two solutions:

$$X_1 = \{a^1, a^3, a^7\} \cup \{a^{2k+1} \mid k \geqslant 5\}$$
$$X_2 = \{a^1, a^3, a^5\} \cup \{a^{2k+1} \mid k \geqslant 5\}.$$

Let X_1' and X_2' be two minimal solutions contained respectively in X_1 and X_2. It is easy to see that $\{a^1, a^3, a^7\} \subseteq X_1'$ and $\{a^1, a^3, a^5\} \subseteq X_2'$ and, hence, these solutions are distinct. (Assuming that the Goldbach's conjecture is true, the equation $X^2 = R$ also has the solution $X = \{a\} \cup \{a^p \mid p$ odd prime number$\}$.)

Obviously, the equation $X^2 = R$ does not always have a solution. We consider in the remainder of this section languages that have the property that they can be written as the catenation XX for a language $X \subseteq \Sigma^*$.

A nonempty language L is called a *sr-language* (*square root language*) if the equation $X^2 = L$ has a solution.

EXAMPLES. (1) $\Sigma^{2n} = \Sigma^n\Sigma^n$;

(2) $L = \{u^2\}$;

(3) $L = \Sigma_{n>5} = \{u \in \Sigma^* \mid |u| > 5\}$; $L = \Sigma_{n>2}\Sigma_{n>2}$.

It is immediate that a language L contains a sr-language iff it contains a word w of the form $w = u^2$.

Given a language $L \subseteq \Sigma^*$, we consider the following two conditions:

$$u^2 \in L,\ v^2 \in L \Rightarrow uv,\ vu \in L \qquad (\alpha)$$

$$x \in L \Rightarrow \exists u^2 \in L,\ v^2 \in L \quad \text{with} \quad x = uv. \qquad (\beta)$$

Note that the intersection of languages satisfying (α) is also a language satisfying (α).

An sr-language L satisfying the condition (α) is called a *complete sr-language*.

In general, a sr-language is not complete. For example, the language $L = \{a^2, a^4, a^6\}$ over $\Sigma = \{a, b\}$ is a sr-language because $L = X^2$ with $X = \{a, a^3\}$. We have $(a^2)^2 \in L$, $a^2 \in L$, but $a^2a = a^3 \notin L$; i.e., condition (α) is not satisfied.

PROPOSITION 4.6. *A language L is a complete sr-language $\Leftrightarrow$ L satisfies both conditions (α) and (β).*

Proof. ($\Rightarrow$) Let $x \in L$. As L is an sr-language, $L = X^2$ for some language X. Consequently there exist r, $s \in X$ such that $x = rs$. Clearly, r^2 and s^2 are in $X^2 = L$, therefore condition (β) is satisfied.

($\Leftarrow$) Let $X=\{u\,|u^2\in L\}$. Then, by (α), we have $X^2\subseteq L$ and, by (β), we have $L\subseteq X^2$. Hence $L=X^2$. ▮

PROPOSITION 4.7. *Let $L\subseteq\Sigma^*$ be a nonempty language. Then there exists a language $T\subseteq\Sigma^*$:*

(i) *$L\subseteq T$ and T is a complete sr-language*;

(ii) *if $L\subseteq L'\subseteq T$, where L' is a complete sr-language, then $L'=T$.*

Proof. Let $F(L)=\{L_i\,|\,i\in I\}$ be the family of complete sr-languages containing L. Since $\Sigma^*\in F(L)$, this family is not empty.

Let $D=\{L_j\,|\,j\in J\}$ be a descending chain of languages $L_j\in F(L)$,

$$\cdots\supseteq L_r\supseteq\cdots\supseteq L_s\supseteq\cdots\supseteq L,$$

and let $K=\bigcap_{j\in J}L_j$. Clearly $L\subseteq K$ and K satisfies condition (α). To show that K satisfies condition (β), we have to show that $x\in K$ implies the existence of $u^2, v^2\in K$ such that $x=uv$.

For every $i\in J$, there exist $u_i^2, v_i^2\in L_i$ such that $x=u_iv_i$. If $P=\{(u_i, v_i)\,|\,x=u_iv_i, i\in J\}$, then this set is finite. Let $P=\{(u_1, v_1), (u_2, v_2), ..., (u_n, v_n)\}$ be an enumeration of the words in P. There is a pair $(u, v)\in P$ such that for every $i\in J$, $u^2, v^2\in L_i$ and $x=uv$. Assume the contrary. For each r, $1\leqslant r\leqslant n$, there exists i_r such that $u_r^2\notin L_{i_r}$ or $v_r^2\notin L_{i_r}$. Let $S=\bigcap_{1\leqslant r\leqslant n}L_{i_r}$. Then clearly $S\in D$ and $S=L_k$ for some $k\in J$. Hence $x=u_kv_k$ with $u_k^2, v_k^2\in L_k$ and $(u_k, v_k)\in P$. Since $L_k\subseteq L_{i_r}$, $1\leqslant r\leqslant n$, we have a contradiction. Hence K satisfies condition (β).

The above considerations show that $F(L)$ is a d-inductive family and that we can use the Zorn's lemma for $F(L)$. Therefore the family $F(L)$ has at least a minimal element T having the properties (i) and (ii). ▮

5. EQUATIONS $R\diamond X=L\diamond Y$

Consider the equation $R\diamond X=L\diamond Y$, where R, L are given languages and X, Y are unknown languages. If $R=L$, this equation has infinitely many solutions $X=Y=T$, where T is any given language. If the equation $R\diamond X=L$ ($R=L\diamond Y$) has a solution X (Y), then the equation $R\diamond X=L\diamond Y$ has the solution $(X, \{1\})$ ($(\{1\}, Y)$), provided that $L\diamond\{1\}=L(R\diamond\{1\}=R)$.

Note that if the operation $\diamond$ is associative and if (X, Y) is a solution, then $(X\diamond T, Y\diamond T)$ is also a solution for any nonempty language T.

If X, Y are solutions of the equation $R\diamond X=L\diamond Y$, then:

(i) (X, Y) is called an *X-maximal* (X-minimal) solution if $R\diamond X=L\diamond Y'$ with $Y\subseteq Y'$ ($Y'\subseteq Y$) implies $Y=Y'$.

(ii) (X, Y) is called a *Y-maximal* (Y-minimal) solution if $R\diamond X'=L\diamond Y$ with $X\subseteq X'$ ($X'\subseteq X$) implies $X=X'$.

(iii) the solution (X, Y) is called a *maximal* (minimal) solution if $R\diamond X'=L\diamond Y'$ with $X\subseteq X'$, $Y\subseteq Y'$ ($X'\subseteq X$, $Y'\subseteq Y$) imply $X=X'$, $Y=Y'$.

PROPOSITION 5.1. *Suppose that the equation $R\diamond X=L\diamond Y$ has the solution (X, Y). Then*:

(i) *The equation has a unique X-maximal solution (Y-maximal solution).*

(ii) *The equation has a unique maximal solution containing all the other solutions.*

(iii) *Let $(X_{\max}, Y_{\max})$ be the maximal solution of the equation and let $T=R\diamond X_{\max}=L\diamond Y_{\max}$. Then $X_{\max}$ and $Y_{\max}$ are respectively maximal solutions of the equations $T=R\diamond X$, respectively $T=L\diamond Y$.*

Proof. (i) Let $\mathscr{F}=\{(X, Y_i)\,|\,i\in I\}$ be the family of all the solutions of the equation $R\diamond X=L\diamond Y$ with X fixed. Let $Y_{\max}=\bigcup_{i\in I}Y_i$. Then clearly $R\diamond X=L\diamond Y_{\max}$ and $Y_{\max}$ is a solution containing all the other solutions. Hence $Y_{\max}$ is the unique X-maximal solution.

(ii) Let $\mathscr{F}=\{(X_i, Y_i)\,|\,i\in I\}$ be the family of all the solutions of the equation $R\diamond X=L\diamond Y$ and define a partial order $\subseteq$ on $\mathscr{F}$ by

$$(X_i, Y_i)\subseteq(X_j, Y_j)\Leftrightarrow X_i\subseteq X_j,\ Y_i\subseteq Y_j.$$

Let Γ be a chain of elements of $\mathscr{F}$:

$$\cdots\subseteq(X_i, Y_i)\subseteq\cdots\subseteq(X_j, Y_j)\subseteq\cdots,\ i, j\in K\subseteq I.$$

Let $(X_\gamma=\bigcup_{i\in K}X_i,\ Y_\gamma=\bigcup_{i\in K}Y_i)$. Then (X_γ, Y_γ) is a solution of the equation $R\diamond X=L\diamond Y$. Indeed, let $r\in R$ and $x\in X_\gamma$. Then $x\in X_i$ for some $i\in K$. Since $R\diamond X_i=L\diamond Y_i$, we have $r\diamond x\subseteq L\diamond Y_i\subseteq L\diamond Y_\gamma$ and hence $R\diamond X_\gamma\subseteq L\diamond Y_\gamma$. We have the symmetric inclusion $L\diamond Y_\gamma\subseteq R\diamond X_\gamma$ and therefore $R\diamond X_\gamma=L\diamond Y_\gamma$.

It follows from the above considerations that $\mathscr{F}$ is inductive. By applying Zorn's lemma we deduce that $\mathscr{F}=\{(X_i, Y_i)\,|\,i\in I\}$ has at least a maximal element, say $(X_{\max}, Y_{\max})$, that is, a maximal solution of the equation $R\diamond X=L\diamond Y$.

Suppose that $(X_{\max}, Y_{\max})$ and (X', Y') are two different maximal solutions, $R\diamond X_{\max}=L\diamond Y_{\max}$ and $R\diamond X'=L\diamond Y'$. We have that $(R\diamond X_{\max})\cup(R\diamond X')=(L\diamond Y_{\max})\cup(L\diamond Y')$, which implies $R\diamond(X_{\max}\cup X')=L\diamond(Y_{\max}\cup Y')$. As the solutions we have considered are maximal, we deduce that $X_{\max}\cup X'=X_{\max}$ and $Y_{\max}\cup Y'=Y_{\max}$; that is, $X_{\max}=X'$ and $Y_{\max}=Y'$.

If $(\bar X, \bar Y)$ is a solution of the equation, then $(X_{\max}\cup\bar X, Y_{\max}\cup\bar Y)$ is also a solution. Hence $X_{\max}\cup\bar X=X_{\max}$, $Y_{\max}\cup\bar Y=Y_{\max}$; therefore $\bar X\subseteq X_{\max}$ and $\bar Y\subseteq Y_{\max}$.

(iii) Suppose that $R\diamond X'=T$ with $X_{\max}\subset X'$. Then $R\diamond X'=T=L\diamond Y_{\max}$. Therefore $(X', Y_{\max})$ is a solution of $R\diamond X=L\diamond Y$ and the solution $(X_{\max}, Y_{\max})$ is not maximal, a contradiction. The proof is the same for the equation $R\diamond X'=T$. ▮

COROLLARY 5.1. *If* $(X_{\max}, Y_{\max})$ *is the maximal solution of the equation* $RX = LY$, *then* $X_{\max} = P_m\Sigma^*$ *and* $Y_{\max} = Q_m\Sigma^*$, *where* P_m *is either* 1 *or a prefix code and* Q_m *is either* 1 *or a prefix code.*

Proof. From $RX_{\max} = LY_{\max}$ follows $RX_{\max}\Sigma^* = LY_{\max}\Sigma^*$ and, therefore, $(X_{\max}\Sigma^*, Y_{\max}\Sigma^*)$ is a solution. Since $(X_{\max}, Y_{\max})$ is the unique maximal solution containing all solutions, $X_{\max}\Sigma^* \subseteq X_{\max}$ and $Y_{\max}\Sigma^* \subseteq Y_{\max}$ and, hence, $X_{\max}\Sigma^* = X_{\max}$, $Y_{\max}\Sigma^* = Y_{\max}$; that is, $X_{\max}$ and $Y_{\max}$ are right ideals of Σ^*. The corollary then follows from the fact that every right ideal of Σ^* can be written as $P\Sigma^*$, where P is either 1 or a prefix code. ∎

For example, the equation $RX = LY$ with $R = \Sigma$ and $L = \Sigma^2$ has the maximal solution $X = \Sigma\Sigma^*$ and $Y = \Sigma^*$.

PROPOSITION 5.2. *If the equation* $RX = L$ $(LY = R)$ *has a solution, then the equation* $RX = LY$ *has the solution* $((R\backslash L^c)^c, \{1\})$ $(((L\backslash R^c)^c, \{1\}))$. *If R and L are regular, then these solutions are also regular.*

Proof. It follows from [4, 3]. ∎

PROPOSITION 5.3. *If the equation* $RX = LY$ *has a solution* (X, Y), *then it has an X-minimal and a Y-minimal solution.*

Proof. Let $S = RX$, where X is the first component of the given solution. By Proposition 2.3, the equation $S = LY$ has a minimal solution $Y_{\min}$ which is also an X-minimal solution. ∎

The equation $RX = LY$ can have more than one X-minimal or Y-minimal solution. For example, take $\Sigma = \{a\}$, $R = \{a^n \mid n \geqslant 7\}$ and $L = \{a^5, a^6, a^8, a^9\} \cup \{a^{10+n} \mid n \geqslant 0\}$. It is easy to see that $X_1 = \{a\}$, $Y_1 = \{a^3, a^4\}$ and $X_2 = \{a\}$, $Y_2 = \{a^3, a^5\}$ are two distinct X_1-minimal solutions of the equation $RX = LY$. Note that these two solutions are also minimal solutions of the equation $RX = LY$.

The following example shows that the family $\mathscr{F}$ of solutions $\{(X_i, Y_i) \mid i \in I\}$ of the equation $RX = LY$ is not necessarily d-inductive with respect to the order $\subseteq$, where $(X_i, Y_i) \subseteq (X_j, Y_j)$ iff $X_i \subseteq X_j$, $Y_i \subseteq Y_j$. This means that it is not possible to use Zorn's lemma to show the existence of minimal solutions.

Let $\Sigma = \{a\}$, $R = \{a\}$ and $L = \{a^2\}$. Then the equation $RX = LY$ has the following solutions (X_n, Y_n), where $Y_n = \{a^k \mid k \geqslant n\}$ and $X_n = \{a^{k+1} \mid k \geqslant n\}$. The chain $\{(X_n, Y_n) \mid n \geqslant 1\}$ has no lower bound, because $\bigcap_{n \geqslant 1} X_n = \bigcap_{n \geqslant 1} Y_n = \varnothing$, and hence $\mathscr{F}$ is not d-inductive. However, this equation has a minimal solution $X = \{a^2\}$, $Y = \{a\}$.

REFERENCES

1. J. H. Conway, "Regular Algebra and Finite Machines," Chapman & Hall, London, 1971.
2. M. Ito and G. Thierrin, Congruences, infix and cohesive prefix codes, *Theoret. Comput. Sci.* **136** (1994), 471–485.
3. L. Kari, "On Insertion and Deletion in Formal Languages," Ph.D. thesis, University of Turku, Finland, 1991.
4. L. Kari, On language equations with invertible operations, *Theoret. Comput. Sci.* **132** (1994), 129–150.
5. L. Kari and G. Thierrin, *K*-catenation and applications: *k*-prefix codes, *J. Inform. Optim. Sci.* **16**, No. 2 (1995), 263–276.
6. A. Salomaa, "Formal Languages," Academic Press, London, 1973.
7. H. J. Shyr, "Free Monoids and Languages," Institute of Applied Mathematics, National Chung-Hsing University, Taichung, Taiwan, 1991.
8. G. Thierrin, Décompositions des langages réguliers, *Rev. Inform. Recherche Opér.* **2–3** (1969), 45–50.