

## Seminar on automata 1996.

S. Eilenberg: Automata, Languages and Machines. Vol A,  
Academic Press, New York 1974.

### 1. PRELIMINARIES

Let us first recall some terminology: A *semiring*  $K$  is equipped with two binary operations which are referred as addition and multiplication. It is required that  $K$  forms an additive commutative monoid and a monoid with respect to multiplication. Neutral elements are denoted by 0 and 1 respectively. Furthermore, it is required that the additive and multiplitive structures obey natural distribution laws.

Let  $X$  be any set, and assume that  $K$  is a semiring.  $K$  is supposed to be commutative unless stated otherwise. A  $K$ -subset  $A$  of  $X$  is then defined to be a function  $A : X \rightarrow K$ . This is an obvious generalisation of the concept of an ordinary subset, which can be defined to be mappings from  $X$  to a binary semiring. If  $x \in X$ , then the image of  $x$ ,  $xA$  in  $K$  is called the *multiplicity with which  $x$  belongs to  $A$* . We denote the set of all  $K$ -subsets of  $X$  by  $K^X$ . The  $K$ -subset  $A$  of  $X$  is said to be *unambiguous*, if  $xA$  can take only values 0 and 1 in  $K$ .

Examples of unambiguous  $K$ -subsets can be given, like

$$\begin{aligned} X : X \rightarrow K, \quad aX = 1 \text{ for all } a \in X, \\ \emptyset : X \rightarrow K, \quad a\emptyset = 0 \text{ for all } a \in X, \\ x : X \rightarrow K, \quad ax = \begin{cases} 1, & \text{if } a = x \\ 0, & \text{if } a \neq x \end{cases}. \end{aligned}$$

The sets in the last example are called *singletons*.

We can now define operations as the *union* of  $K$ -subsets. Let  $\{A_i, i \in I\}$  be an indexed family of  $K$ -subsets of  $X$ . Then we define their union (or *sum*) to be a  $K$ -subset by

$$x \left( \bigcup_{i \in I} A_i \right) = \sum_{i \in I} xA_i.$$

This definition requires some comments, if  $K$  is not a *complete semiring*, i.e a semiring for which the sum above always exists and is well-defind. Then we must require the family  $A_i$  to be *locally finite*, i.e for each  $x \in X$   $xA_i = 0$  holds for all but a finite number of  $i$ :s.

The *intersection*  $A \cap B$  of two  $K$ -subsets  $A$  and  $B$  is defined to be

$$x(A \cap B) = (xA)(xB),$$

and by *multiplication of a  $K$ -subset  $A$*  by an element of  $k \in K$  we mean

$$x(kA) = k(xA).$$

It is now obvious that for each  $K$ -subset  $A$  we have the following *expansion in terms of singletons*:

$$A = \sum_{x \in X} (xA)x.$$

Family  $(xA)x$  is locally finite because

$$y((xA)x) = \begin{cases} xA, & \text{if } y = x \\ 0, & \text{if } y \neq x \end{cases}$$

By a *product* of two  $K$ -subsets  $A$  and  $B$  we understand

$$z(AB) = \sum_{xy=z} (xA)(yB),$$

where sum runs over all decompositions of  $z$ . If there exists only a finite number of them, then the right hand side is well-defined

Let  $\Sigma$  be a finite alphabet and  $K$  a commutative semiring. A  $K - \Sigma$ -automaton  $\mathcal{A} = (Q, I, T)$  is given by finite set  $Q$  of *states* with  $K$ -subsets  $I$  of *initial states* and  $T$  of *terminal states*, and by a  $K$ -subset  $E$  of the cartesian product  $Q \times \Sigma \times Q$ , whose elements are called *transitions*.  $E$  can be extended to be a  $Q \times \Sigma^* \times Q$ -subset by setting  $(p, s, q)E = 0$ , if  $s \notin \Sigma$ . If the image  $k = (p, \sigma, q)E$  is not the zero element, we say that the *edge*

$$p \xrightarrow{k\sigma} q$$

is in  $\mathcal{A}$ . Mapping  $k\sigma$  is called the *label* of the edge. A *path* in  $\mathcal{A}$  is a sequence of consecutive edges, for instance, let a path  $c$  be given by

$$p \xrightarrow{k_1\sigma_1} q_1 \xrightarrow{k_2\sigma_2} \dots \xrightarrow{k_{n-1}\sigma_{n-1}} q_{n-1} \xrightarrow{k_n\sigma_n} q.$$

If we denote  $k = k_1 \dots k_n$  and  $s = \sigma_1 \dots \sigma_n$ , we say that the *label* of the path is  $|c| = ks$  and the *length* of  $c$  is  $\|c\| = n = |s|$ .

The *behaviour* of  $\mathcal{A}$  is the  $K$ -subset of  $\Sigma^*$  defined to be

$$|\mathcal{A}| = \sum_{p, q \in Q} \sum_c (pI) |c| (qT),$$

where  $c$  runs over all paths from  $p$  to  $q$ . For each  $s \in \Sigma^*$  there exists only a finite number of paths from  $p$  to  $q$  labelled as  $ks$ ,  $k \in K$ , and the summation is therefore finite. Now

$$s|\mathcal{A}| = \sum_{p, q \in Q} \sum_{\substack{c: p \rightarrow q \\ |c|=s}} (pI)k(qT).$$

Consider now the  $K$ -subset  $E$ . It is a mapping  $Q \times \Sigma \times Q \rightarrow K$ , and therefore  $E_{pq}$  defined by

$$\sigma E_{pq} = (p, \sigma, q)E$$

is a mapping from  $\Sigma$  to  $K$ , i.e a  $K$ -subset of  $\Sigma$  (or a  $K$ -subset of  $\Sigma^*$  as well, when  $E$  is extended). Hence  $E$  can be understood as a matrix

$$E : Q \times Q \rightarrow K^\Sigma,$$

and it is called *transition matrix*. As well we can understand  $E$  as a matrix with entries

$$E_{pq} : \Sigma^* \rightarrow K,$$

where  $sE_{pq} = 0$  if  $s \notin \Sigma$ .  $K^{\Sigma^*}$  forms now a semiring where addition and product are defined by

$$s(D + E)_{pq} = sD_{pq} + sE_{pq} \quad \text{and} \quad s(DE)_{pq} = s \sum_{r \in Q} (D_{pr})(E_{rq}).$$

The zero element in this semiring is given by  $s\mathbf{0}_{pq} = 0$  always and unit element is given by  $\mathbf{1}_{pq} = 0$  if  $p \neq q$  and

$$s\mathbf{1}_{pp} = \begin{cases} 0, & \text{if } s \neq 1 \\ 1, & \text{if } s = 1 \end{cases}.$$

We can also define  $E^0 = \mathbf{1}$ ,  $E^1 = E$ , and  $E^{n+1} = E^n E$ . We can compute that

$$sE_{pq}^n = \sum_{\substack{c:p \rightarrow q \\ |c|=ks}} k$$

and see that

$$E_{pq}^n = \sum_{\substack{c:p \rightarrow q \\ ||c||=n}} |c|.$$

Further, we can define

$$E_{pq}^* = \sum_{n=0}^{\infty} E_{pq}^n.$$

Then we have  $E_{pq}^* = \sum_{c:p \rightarrow q} |c|$ , and the behaviour of an automaton can be represented as a matrix product

$$|\mathcal{A}| = \sum_{p,q \in Q} (pI)E_{pq}^*(qT) = IE^*T,$$

Where  $I$  is understood as a row vector with entries  $I_{1p} = pI \in K$  and  $T$  as a column vector with  $T_{p1} = pT \in K$ . In general, each  $K$ -subset of  $Q$  can be regarded as a row vector of elements of  $K$ . Furthermore, for each  $s \in \Sigma^*$  the matrix  $sE^*$  is a  $Q \times Q$ -matrix of elements of  $K$ . Let us denote

$$Xs = X(sE^*).$$

Then  $Xs$  is a row vector with  $(Xs)_{1q} = \sum_{p \in Q} X_p(sE^*)_{pq}$ . On the other hand, if we regard  $X$  to be a column vector, we may denote

$$sX = (sE^*)X,$$

and observe that  $(sX)_{p1} = \sum_{q \in Q} (sE^*)_{pq}X_q$ . It is straightforward to verify that the association laws as  $X(st) = (Xs)t$ ,  $(kX)s = k(Xs)$  hold. Especially, for each  $s \in \Sigma^*$  we have

$$s|\mathcal{A}| = s(IE^*T) = I(sE^*)T = (Is)T = I(sT).$$

Let  $\Sigma$  be a finite alphabet. A  $K$ -subset  $A$  of  $\Sigma^*$  is said to be *recognizable*, if there exists a  $K$ - $\Sigma$ -automaton  $\mathcal{A}$  recognizing  $A$ , i.e. an automaton such that  $|\mathcal{A}| = A$ .

**Proposition 1.1.** *The class of recognizable  $K$ -subsets of  $\Sigma^*$  is closed under finite union, intersection, and reversal.*

By a reversal  $A^\rho$  of a  $K$ -subset  $A$  of  $\Sigma^*$  we understand the composite mapping

$$\Sigma^* \xrightarrow{\rho} \Sigma^* \xrightarrow{A} K.$$

**Proposition 1.2.** *If  $f : \Gamma^* \rightarrow \Sigma^*$  is a fine morphism and  $A$  is a recognizable  $K$ -subset of  $\Sigma^*$ , then there exists a  $K$ - $\Gamma$ -automaton recognizing  $Af^{-1}$ .*

**Proposition 1.3.** *Let  $f : \Gamma^* \rightarrow \Sigma^*$  be a morphism satisfying  $1 = 1f^{-1}$ , and  $A$  a recognizable  $K$ -subset of  $\Gamma^*$ . Then  $Af$  is a recognizable  $K$ -subset of  $\Sigma^*$ .*

All the proof of propositions 1.1-1.3 are analogues of propositions referring to  $\Sigma$ -automata.

**Proposition 1.4.** *Let  $A$  be a recognizable  $K$ -subset of  $\Sigma^*$ . Then  $kA$  is a recognizable  $K$ -subset of  $\Sigma^*$ .*

*Proof.* Let  $\mathcal{A} = (Q, I, T)$  be a  $K$ - $\Sigma$ -automaton recognizing  $A$ . Then  $kA$  is recognized by

$$k\mathcal{A} = (Q, kI, T)$$

with transition matrix unchanged, since

$$|k\mathcal{A}| = (kI)E^*T = k(IE^*T) = k|\mathcal{A}| = kA.$$

A  $K$ - $\Sigma$ -automaton is said to be *normalized*, if  $I = i$  and  $T = t$  are distinct singletons and if there are no edges of forms

$$q \xrightarrow{k\sigma} i, \quad t \xrightarrow{k\sigma} q$$

for non-zero  $k$ . For normalized automaton  $\mathcal{A}$  obviously holds  $|\mathcal{A}| \subset \Sigma^+$ .

**Proposition 1.5.** *Any  $K$ - $\Sigma$ -automaton  $\mathcal{A}$  can be converted into a normalized automaton  $\mathcal{A}'$  which satisfies*

$$|\mathcal{A}'| = |\mathcal{A}| \cap \Sigma^+.$$

*Proof.* Let  $\mathcal{A} = (Q, I, T)$  be a  $K$ - $\Sigma$ -automaton. Define  $Q'$  to be  $Q' = Q \cup i \cup t$ , where  $i \neq t$  are new states. Furthermore, define a transition matrix  $E'$  by

$$\begin{aligned} E'_{pq} &= E_{pq} \\ E'_{iq} &= (IE)_{1q} = \sum_{p \in Q} I_p E_{pq} \\ E'_{pt} &= (ET)_{p1} = \sum_{q \in Q} E_{pq} T_q \\ E'_{it} &= (IET)_{11} = \sum_{p, q \in Q} I_p E_{pq} T_q \\ E'_{tt} &= E'_{ii} = E'_{pi} = E_{ti} = E_{tq} = 0 \end{aligned}$$

It can now be computed that  $E'^*_{it} = IE^+T$ , where  $E^+ = EE^*$ . Now  $\mathcal{A}'$  is normalized, and

$$|\mathcal{A}'| = iE'^*t = E'^*_{it} = IE^+T = IE^*T \cap \Sigma^+ = |\mathcal{A}| \cap \Sigma^+.$$

□

**Theorem 1.6 (Schützenberger).** *A  $K$ -subset  $A$  of  $\Sigma^+$  is recognizable if and only if there is an integer  $n > 1$  and an  $n \times n$ -matrix  $E$  of  $K$ -subsets of  $\Sigma$  such that  $A = E_{1n}^+$ .*

*Proof.* Assume first that  $A$  is recognizable. By proposition 1.5 there exists a normalized  $K$ - $\Sigma$ -automaton  $\mathcal{A} = (Q, i, t)$  with transition matrix  $E$  recognizing  $A$ . By renaming the states we can assume that  $\mathcal{A} = (\{1, \dots, n\}, 1, n)$ . Because  $\mathcal{A}$  is normalized, we have  $n > 1$ , and finally  $A = |\mathcal{A}| = 1E^*n = E_{1n}^* = E_{1n}^+$ .

Assume conversely that  $A = E_{1n}^+$  where  $E$  is an  $n \times n$ -matrix of  $K$ -subsets of  $\Sigma$  and  $n > 1$ . Let  $\mathcal{A} = (\{1, \dots, n\}, 1, n)$  be a  $K$ - $\Sigma$  automaton with transition matrix  $E$ . Then  $|\mathcal{A}| = E_{1n}^+ = A$ .  $\square$

**Corollary 1.7.** *Let  $E$  be an  $n \times n$ -matrix of  $K$ -subsets of  $\Sigma$ . Then for any indices  $i, j \in \{1, \dots, n\}$  the  $K$ -subsets  $E_{ij}^+$  and  $E_{ij}^*$  of  $\Sigma^+$  and  $\Sigma^*$  are recognizable.*

## 2. THE EQUALITY THEOREM

Now we assume that  $K$  is a subsemiring of a field  $F$  which is assumed to be commutative.

**Lemma 2.1.** *Let  $\mathcal{A} = (Q, I, T)$  be a  $K$ - $\Sigma$ -automaton. If  $s|\mathcal{A}| = 0$  for all  $s \in \Sigma^*$  satisfying  $|s| < \text{Card } Q \neq 0$ , then  $s|\mathcal{A}| = 0$  for all  $s \in \Sigma^*$ .*

*Proof.* By assumption  $K$  is a subsemiring of a field  $F$ . Therefore we can regard  $\mathcal{A}$  as an  $F$ - $\Sigma$ -automaton as well; if  $|\mathcal{A}|$  is a zero mapping as a  $F$ -subset, then it is a zero mapping as a  $K$ -subset. Therefore we can assume that  $K$  is a field. Now  $K^Q$ , all the  $K$ -subsets of  $Q$  can be given a structure of a vector space over  $K$ .

The addition in the  $K$ -vector space is given by the sum of  $K$ -subsets and the scalar multiplication is the usual multiplication of a  $K$ -subset by an element of  $K$ . Let us, for example, show how the distribution law is verified. Let  $X_1$  and  $X_2$  be  $K$ -subsets of  $Q$  and  $k$  an element in  $K$ . Then for any  $q \in Q$  we have

$$\begin{aligned} q(k(X_1 + X_2)) &= k(q(X_1 + X_2)) = k(qX_1 + qX_2) = k(qX_1) + k(qX_2) \\ &= q(kX_1) + q(kX_2) = q(kX_1 + kX_2). \end{aligned}$$

Therefore  $k(X_1 + X_2) = kX_1 + kX_2$ . It is obvious that  $K^Q$  is generated by the singleton  $K$ -subsets of  $Q$ . Furthermore, the singleton mappings are linearly independent, since if we have an expression

$$k_1q_1 + k_2q_2 + \dots + k_nq_n = 0,$$

taking the image of  $q_i$  we get

$$\begin{aligned} 0 &= q_i(k_1q_1 + \dots + k_nq_n) = q_i(k_1q_1) + \dots + q_i(k_nq_n) \\ &= k_1(q_iq_1) + \dots + k_n(q_iq_n) = k_i(q_iq_1) = k_i. \end{aligned}$$

Now we obtain that the dimension of  $K^Q$  is  $n = \text{Card } Q$ . The claim becomes now: If  $(Is)T = 0$ , for  $|s|$  satisfying  $|s| < n = \text{Card } Q$ , then  $(Is)T = 0$  for all  $s \in \Sigma^*$ .

We define  $W$  to be the set of those row vectors  $X_p$  which are orthogonal to  $T$ , namely

$$W = \{X \mid X \in K^Q, XT = 0\}.$$

If  $\dim W = n$  then  $W = K^Q$  and there is nothing left to prove. Therefore we can assume that  $\dim W \leq n - 1$ , and furthermore, we can assume that  $I, T \neq 0$ . Define also  $V_k$  to be a subspace of  $K^Q$  generated by vectors  $Is$  with  $|s| \leq k$

$$V_k = \langle \{Is \mid |s| \leq k\} \rangle$$

Then  $V_0 = \langle I \rangle$  and obviously we have

$$V_0 \subset \dots \subset V_{n-1} \subset W.$$

Counting the dimensions in both sides we obtain that  $V_k = V_{k+1}$  for some  $0 \leq k < n - 1$ . The subspace  $V_{k+2}$  is generated by all the vectors  $Is$ , where  $|s| \leq k + 2$ , that is, by all vectors  $X$  and  $X\sigma$ , where  $X$  is in  $V_{k+1} = V_k$ . Therefore  $V_{k+1} = V_{k+2}$  and by induction,  $V_k = V_{k+p}$  for all positive  $p$ . Thus, for any  $s \in \Sigma^*$  we have  $Is \in W$ , so  $(Is)T = 0$   $\square$

**Lemma 2.2.** *Let  $\mathcal{A} = (Q, I_i, T)$   $i \in \{1, 2\}$  be  $K$ - $\Sigma$ -automata that differ only in their initial subsets. Then  $|\mathcal{A}_1| = |\mathcal{A}_2|$  if and only if*

$$s|\mathcal{A}_1| = s|\mathcal{A}_2|$$

For all those  $s \in \Sigma^*$  satisfying  $|s| < \text{Card } Q$ .

*Proof.* One direction is trivial. Therefore, assume that  $s \in \Sigma^*$  with  $|s| < \text{Card } Q$  satisfy  $s|\mathcal{A}_1| = s|\mathcal{A}_2|$ . Consider the  $K$ - $\Sigma$ -automaton  $\mathcal{A} = (Q, I, T)$  with  $I = I_1 - I_2$ . Because  $K$  can be assumed to be a field, the map  $I_1 - I_2$  can always be defined in an obvious way. It is now straightforward to compute

$$s|\mathcal{A}| = (Is)T = ((I_1 - I_2)s)T = (I_1s)T - (I_2s)T = s|\mathcal{A}_1| - s|\mathcal{A}_2|.$$

The claim follows now directly for the previous lemma.  $\square$

**Theorem 2.3 (The equality theorem).** *Let  $A_1$  and  $A_2$  be recognizable  $K$ -subsets of  $\Sigma^*$  and  $\mathcal{A}_i = (Q_i, I_i, T_i)$   $i \in \{1, 2\}$  two  $K$ -automata recognizing them respectively. Suppose that  $sA_1 = sA_2$  for all  $s \in \Sigma^*$  satisfying  $|s| < \text{Card } Q_1 + \text{Card } Q_2$ . Then  $A_1 = A_2$ .*

*Proof.* Without loss of generality, the sets  $Q_1$  and  $Q_2$  can be assumed to be disjoint. Define a  $K$ - $\Sigma$ -automaton

$$\mathcal{A}_1 \cup \mathcal{A}_2 = (Q_1 \cup Q_2, I_1 \cup I_2, T_1 \cup T_2)$$

with transition matrix

$$E = \begin{pmatrix} E_1 & 0 \\ 0 & E_2 \end{pmatrix}$$

Then modify this automaton to obtain automata

$$\mathcal{B}_i = (Q_1 \cup Q_2, I_i, T_1 \cup T_2), \quad i \in \{1, 2\}$$

with transition matrix unchanged. We see that  $|\mathcal{B}_i| = |\mathcal{A}_i|$  for  $i \in \{1, 2\}$ , for instance,

$$|\mathcal{B}_1| = (I_1 \quad 0) \begin{pmatrix} E_1^* & 0 \\ 0 & E_2^* \end{pmatrix} \begin{pmatrix} T_1 \\ T_2 \end{pmatrix} = I_1 E_1^* T_1 = |\mathcal{A}_1|.$$

The claim follows now from lemma 2.2.  $\square$

Now we can state a decidability result:

**Theorem 2.4.** *Given any two  $K$ - $\Sigma$ -automata  $\mathcal{A}_1$  and  $\mathcal{A}_2$ , it is decidable whether  $|\mathcal{A}_1| = |\mathcal{A}_2|$ .*

It is here silently assumed that the semiring  $K$  is known well enough to carry out all computations for  $|s| < \text{Card } Q_1 + \text{Card } Q_2$ .

### 3. THE UNDECIDABILITY OF INCLUSION

Since now we assume that our semiring is  $\mathbb{N}_0$ , the set of all nonnegative integers equipped with the natural multiplication and addition. By notation  $\mathbf{k}$  we understand the set  $\{0, \dots, k-1\}$ . The source of the result to be stated is well-known

**Post correspondence problem.** *A finite alphabet  $\Sigma$  and two morphisms  $g, h : \Sigma^* \rightarrow \mathbf{k}^*$  are given. Decide whether there exist  $s \in \Sigma^+$  such that  $sg = sh$ .*

We denote  $\Sigma = \{\sigma_1, \dots, \sigma_n\}$ , and  $x_i = \sigma_i g, y_i = \sigma_i h$ , where  $x_i, y_i \in \mathbf{k}^*$ . If  $s \in \Sigma^+$  is given by  $s = \sigma_{i_1} \dots \sigma_{i_k}$ , then  $sg = sh$  if and only if

$$x_{i_1} \dots x_{i_k} = y_{i_1} \dots y_{i_k}.$$

The problem can then be introduced as follows: given a finite set  $\{X_1, \dots, X_n\}$  of  $2 \times 1$  column vectors of binary sequences,

$$X_i = \begin{pmatrix} x_i \\ y_i \end{pmatrix}.$$

Decide whether there exists a sequence of indices  $i_1, \dots, i_k$  such that the upper entry equals to lower one, when the matrices are catenated componentwise.

**Proposition 3.1.** *Post correspondence problem is undecidable.*

Let  $A$  and  $B$  be  $\mathbb{N}_0$ -subsets. If  $sB \leq sA$  for all  $s \in \Sigma^*$ , we write  $B \leq A$ . If  $B \leq A$ , we define the *difference*  $A - B$  to be a  $\mathbb{N}_0$ -subset to be

$$s(A - B) = sA - sB.$$

More generally, we define  $A \dot{-} B$  to be a  $\mathbb{N}_0$ -subset by

$$s(A \dot{-} B) = \begin{cases} sA - sB, & \text{if } sA \leq sB \\ 0 & \text{otherwise.} \end{cases}$$

**Lemma 3.2.** *Let  $\lambda$  be a mapping from  $\mathbf{k}^*$  to  $\mathbb{N}_0^{2 \times 2}$  defined by*

$$s\lambda = \begin{pmatrix} k^{|s_1|} & 0 \\ \langle s_1 \rangle & 1 \end{pmatrix},$$

where  $\langle s \rangle = \sigma_0 k^n + \sigma_1 k^{n-1} + \dots + \sigma_n$  is the  $k$ -adic representation of  $s = s_0 s_1 \dots s_n$ . Then  $\lambda$  is an injective morphism.

*Proof.* It is obvious that  $\lambda$  is injective, since the  $k$ -adic representation is unique. To prove that  $\lambda$  is a morphism, we observe that  $\langle s_1 s_2 \rangle = k^{|s_2|} \langle s_1 \rangle + \langle s_2 \rangle$ . Then it is straightforward to compute

$$\begin{pmatrix} k^{|s_1|} & 0 \\ \langle s_1 \rangle & 1 \end{pmatrix} \begin{pmatrix} k^{|s_2|} & 0 \\ \langle s_2 \rangle & 1 \end{pmatrix} = \begin{pmatrix} k^{|s_1|+|s_2|} & k^{|s_1|} \\ k^{|s_2|} \langle s_1 \rangle + \langle s_2 \rangle & 1 \end{pmatrix} = \begin{pmatrix} k^{|s_1 s_2|} & k^{|s_1|} \\ \langle s_1 s_2 \rangle & 1 \end{pmatrix}.$$

□



**Theorem 3.3.** *Assume that  $B$  and  $C$  are recognizable  $\mathbb{N}_0$ -subsets such that  $B \leq C$ . It is undecidable whether or not there exists  $s \in \Sigma^*$  satisfying  $sB = sC$ .*

*Proof.* We will show that a decision procedure for the existence of such an element  $s \in \Sigma^*$  mentioned above leads to a decision procedure for the Post correspondence problem, which is known to be undecidable. Then we can conclude that the problem 3.3. is undecidable.

First we will define a morphism  $\gamma : \mathbf{2}^* \rightarrow \mathbb{N}_0^{2 \times 2}$  by

$$0\gamma = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \quad 1\gamma = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}.$$

From lemma 3.2. it follows that  $\gamma$  is injective. In fact, the choice of  $\gamma$  is unessential, all we need to know is that  $\gamma$  is injective. Suppose now that we are given two morphisms  $g, h : \Sigma^* \rightarrow \mathbf{2}^*$ . Consider now the compositions  $g\gamma, h\gamma : \Sigma^* \rightarrow \mathbb{N}_0^{2 \times 2}$ , and denote

$$g\gamma = \begin{pmatrix} G_{00} & G_{01} \\ G_{10} & G_{11} \end{pmatrix}, \quad h\gamma = \begin{pmatrix} H_{00} & H_{01} \\ H_{10} & H_{11} \end{pmatrix}$$

Here  $G_{ij}$  and  $H_{ij}$  are functions  $\Sigma^* \rightarrow \mathbb{N}_0$ , which are entirely determined when  $g, h$ , and  $\gamma$  are given. But a function  $\Sigma^* \rightarrow \mathbb{N}_0$  is a  $\mathbb{N}_0$ -subset of  $\Sigma^*$ . These subsets are recognizable by corollary 1.7. Define then  $\mathbb{N}_0$ -subsets  $A, B$ , and  $C$  to be

$$\begin{aligned} A &= \sum_{i,j=1,2} (G_{ij} - H_{ij})^2 \\ B &= 2 \sum_{i,j=1,2} G_{ij}H_{ij} \\ C &= \sum_{i,j=1,2} G_{ij}^2 + H_{ij}^2. \end{aligned}$$

Here sum and multiplication is understood in the natural way, to be union and intersection. Then we have  $A + B = C$  and  $B \leq C$ . Furthermore,  $B$  and  $C$  are recognizable, since they are obtained from recognizable  $\mathbb{N}_0$ -subsets by union and intersection.

Choose now  $s \in \Sigma^*$ . We have

$$\begin{aligned} & sB = sC \\ \iff & sA = 0 \\ \iff & s(G_{ij} - H_{ij})^2 = 0 \\ \iff & sG_{ij} = sH_{ij} \\ \iff & sg\gamma = sh\gamma \\ \iff & sg = sh, \end{aligned}$$

since  $\gamma$  is injective. Now we see that a decision procedure finding such an  $s$  leads to a decision procedure for the Post correspondence problem.  $\square$

**Theorem 3.4.** *Let  $B$  and  $C$  be recognizable  $\mathbb{N}_0$ -subsets of  $\Sigma^*$ . It is undecidable whether or not  $B \leq C$ .*

*Proof.* We take an arbitrary instance of problem in theorem 3.3, and show that if there is a decision procedure for 3.4, then there is a decision procedure for 3.3, too.

Take any two recognizable  $\mathbb{N}_0$ -subsets  $B'$  and  $C'$  such that  $B' \leq C'$ . Define  $B = B' + \Sigma^+$  and  $C = C'$ . Then  $B$  and  $C$  are recognizable  $\mathbb{N}_0$ -subsets. Now the inequality  $B \leq C$  holds if and only if  $sB' < sC'$  for all  $s \in \Sigma^+$ , since  $sB = sB' + s\Sigma^+$  and  $sC = sC'$ . If there is a decision procedure to decide whether  $B \leq C$ , it would lead to a procedure to decide whether  $sB' < sC'$  for all  $s \in \Sigma^+$ . Because  $B' \leq C'$ , we can conclude from this whether there exists  $s \in \Sigma^+$  such that  $sB' = sC'$ . This is however undecidable by theorem 3.3.  $\square$