Some Remarks on Directable Automata*

B. Imreh† M. Steinby‡

Abstract

A finite automaton is said to be directable if there exists a word, a directing word, which takes the automaton from every state to the same state. After some general remarks on directable automata and their directing words we present methods for testing the directability of an automaton and for finding the least congruence of an automaton which yields a directable quotient automaton. A well-known conjecture by J. Černý claims that any n-state directable automaton has a directing word of length $\leq (n-1)^2$, but the best known upper bounds are of the order $O(n^3)$. However, for special classes of automata lower bounds can be given. We consider a generalized form of Černý's conjecture proposed by J.-E. Pin for the classes of commutative, definite, reverse definite, generalized definite and nilpotent automata. We also establish the inclusion relationships between these classes within the class of directable automata.

1 Introduction

A finite automaton is *directable* if there is an input word, a *directing word*, which takes the automaton from every state to the same state. (Directable automata and directing words are also called *synchronizable automata* and *synchronizing words*, respectively.) In this paper we discuss a variety of questions concerning directable automata and their directing words. After the preliminaries and general remarks of Sections 2 and 3, we present in Section 4 a method for testing the directability of an automaton. The algorithm is based on the mergeability relation of states, and for computing effectively this relation the inverted transition table of the automaton is used. A congruence of an automaton is *directing* if the corresponding quotient automaton is directable. Such congruences were considered (under a different name) by Ito and Duske [ItD83] who noted that every automaton has a

*This work has been supported by the Finnish Academy of Sciences, the Turku University Foundation and the Hungarian National Foundation for Scientific Research, Grant 2035.

†Department of Informatics, József Attila University, Árpád tér 2, H-6720 Szeged, Hungary

‡Department of Mathematics, University of Turku, SF-20500 Turku, Finland

minimal directing congruence. It gives the largest directable homomorphic image of the automaton. In Section 5 we describe an algorithm for computing the smallest directing congruence.

Černý [Čer64] conjectured that an n-state directable automaton must have a directing word of length $\leq (n-1)^2$. So far, this has been neither proved nor disproved, and the conjecture remains the main problem in the area. The best known upper bounds for the length of the shortest directing word are of the order $O(n^3)$ (cf. [Sta69,ČPR71,Pin78], for example). On the other hand, even better bounds than $(n-1)^2$ can be given for some special classes of automata [Pin79]. Recently, Rystsov [Rys94] proved that for commutative automata the exact bound is $n-1$. In Section 6 we give a short elementary proof of a generalized form of Rystsov's result. The generalization corresponds to an extension of Černý's conjecture proposed by Pin [Pin78]. An automaton is *r- directable*, for some $r \geq 1$, if it has an *r- directing word* which takes the automaton from every state to one of r states which depend on the word only. Pin's conjecture claims that if $1 \leq r \leq n$, then any n-state r-directable automaton has an *r-directing word of length* $\leq (n-r)^2$; for $r = 1$ this is Černý's conjecture. In Section 7 we consider the directability and the directing words of definite, reverse definite, generalized definite and nilpotent automata. In each case we can give exact bounds for the lengths of the minimal r-directing words. We also consider the inclusions and the intersections between these classes when restricted to directable automata. In particular, it is noted that every directable generalized definite automaton is definite.

2 Preliminaries

Although most of our notation is quite standard, some of it will be explained here along with some general notions we shall need. The cardinality of a set A is denoted by $|A|$. If $f : A \to B$ is a mapping, the value $f(a)$ of an element $a \in A$ is often denoted by af. Similarly, we may write Hf for $f(H) = \{af : a \in H\}$ when $H \subseteq A$. The composition of two mappings $f : A \to B$ and $g : B \to C$ is the mapping $fg : A \to C$, $a \mapsto (af)g$, and the product of two relations $\Theta \subseteq A \times B$ and $\rho \subseteq B \times C$ is the relation

$$\Theta\rho = \{(a,c) \in A \times C : (\exists b \in B)\ a\Theta b,\ b\rho c\}$$

from A to C; that $(a,b) \in \Theta$ holds is also expressed by writing $a\Theta b$. The set of equivalence relations on a set A is denoted by $\mathrm{Eq}(A)$. If $\Theta \in \mathrm{Eq}(A)$, the Θ-class of an element a of A is denoted by $a\Theta$, and the set of all such Θ-classes, the quotient set with respect to Θ, is denoted by A/Θ. For any set A, $\mathrm{Eq}(A)$ contains the diagonal relation $\Delta_A = \{(a,a) : a \in A\}$ and the universal relation $\nabla_A = A \times A$. These are the smallest and the greatest element, respectively, of the complete lattice $(\mathrm{Eq}(A), \subseteq)$ (cf. [BuS81], for example).

In this paper X is always a finite nonempty alphabet. The set of all (finite) words over X, also called *X- words*, is denoted by X^* and the empty word by ε.

For the length of a word w we use the notation $\lg(w)$. For any integer $k \geq 0$, X^k denotes the set of all X-words of length k, and also let

$$X^{<k} = \{w \in X^* : \lg(w) < k\},$$

$$X^{\leq k} = \{w \in X^* : \lg(w) \leq k\},$$

$$X^{\geq k} = \{w \in X^* : \lg(w) \geq k\}.$$

The prefix of length k and the suffix of length k of a word w are denoted by $\mathrm{pref}_k(w)$ and $\mathrm{suff}_k(w)$, respectively.

An *automaton*, or an *X-automaton* - to be more specific, is a system $\mathcal{A} = (A, X, \delta)$, where A is the finite nonempty set of *states*, X is the *input alphabet*, and $\delta : A \times X \to A$ is the *transition function*. The transition function is extended to $A \times X^*$ in the usual way. Each word $w \in X^*$ defines then a unary operation $w : A \to A$, $a \mapsto \delta(a, w)$, on the state set, and the state $\delta(a, w)$ into which the input word w takes $\mathcal{A}$ from state a is usually denoted by aw. This notation is extended also to subsets of A : if $H \subseteq A$, then $Hw = \{aw : a \in H\}$.

Subsets of X^* are called *X-languages*, or just *languages*. An *X-recognizer* is a system $\mathbf{A} = (A, X, \delta, a_0, F)$ which consists of an X-automaton (A, X, δ), an *initial state* a_0 $(\in A)$ and a set F $(\subseteq A)$ of *final states*. We say that $\mathbf{A}$ is *based* on the X-automaton (A, X, δ). The *language recognized* by $\mathbf{A}$ is $L(\mathbf{A}) = \{w \in X^* : a_0 w \in F\}$. An X-language is *recognizable*, or *regular*, if it is recognized by an X-automaton. The set of recognizable X-languages is denoted by $\mathrm{Rec}(X)$.

Next we define some basic algebraic notions for automata. These could be taken directly from general algebra by construing automata as unary algebras, but we use the usual definition of an automaton. Nevertheless, for in- depth treatments of these ideas one should consult texts on universal algebra such as [BuS81], for example. An X-automaton (B, X, η) is a *subautomaton* of the X-automaton $\mathcal{A} = (A, X, \delta)$ if $B \subseteq A$ and $\eta(b, x) = \delta(b, x)$ for all $b \in B$ and $x \in X$. An equivalence $\Theta \in \mathrm{Eq}(A)$ is a *congruence* of $\mathcal{A} = (A, X, \delta)$ if for all $a, b \in A$ and $x \in X$, $a\Theta b$ implies $ax\Theta bx$. The set of congruences of $\mathcal{A}$ is denoted by $\mathrm{Con}(\mathcal{A})$. It is well-known that $\mathrm{Con}(\mathcal{A})$ forms a sublattice of the lattice $(\mathrm{Eq}(A), \subseteq)$. Moreover, $\Delta_A, \nabla_A \in \mathrm{Con}(\mathcal{A})$. If $\Theta \in \mathrm{Con}(\mathcal{A})$, the *quotient automaton* $\mathcal{A}/\Theta = (A/\Theta, X, \delta_\Theta)$ is defined so that $\delta_\Theta(a\Theta, x) = \delta(a, x)\Theta$ for all $a\Theta \in A/\Theta$ and $x \in X$. A *morphism* of X-automata from $\mathcal{A} = (A, X, \delta)$ to $\mathcal{B} = (B, X, \eta)$ is a mapping $\varphi : A \to B$ such that for all $a \in A$ and $x \in X$, $\delta(a, x)\varphi = \eta(a\varphi, x)$. We write $\varphi : \mathcal{A} \to \mathcal{B}$ to indicate that $\varphi : A \to B$ is a morphism. An *epimorphism* is a surjective morphism. If there exists an epimorphism $\varphi : \mathcal{A} \to \mathcal{B}$, then $\mathcal{B}$ is an *image* of $\mathcal{A}$. The *direct product* of $\mathcal{A} = (A, X, \delta)$ and $\mathcal{B} = (B, X, \eta)$ is the X-automaton $\mathcal{A} \times \mathcal{B} = (A \times B, X, \gamma)$ in which $\gamma((a, b), x) = (\delta(a, x), \eta(b, x))$ for any $(a, b) \in A \times B$ and $x \in X$.

If $\mathbf{K}$ is a class of automata, then $\mathbf{K}(X)$ denotes the class of X-automata belonging to $\mathbf{K}$. A nonempty class of X-automata is called a *variety of X-automata* if it is closed under the operations of forming subautomata, images and (finite) direct products.

3 Directable automata and directing words

A word $w \in X^*$ is a *directing word* of an X- automaton $\mathcal{A} = (A, X, \delta)$ if it takes $\mathcal{A}$ from every state to the same state, *i.e.* if $|Aw| = 1$, and we call $\mathcal{A}$ *directable* if it has a directing word. The set of directing words of $\mathcal{A}$ is denoted by $\mathrm{DW}(\mathcal{A})$. The class of all directable automata is denoted by **Dir**.

It is obvious that every directing word of an X- automaton $\mathcal{A}$ is a directing word of every subautomaton of $\mathcal{A}$, too. If $\varphi : \mathcal{A} \to \mathcal{B}$ is an epimorphism from $\mathcal{A} = (A, X, \delta)$ onto $\mathcal{B} = (B, X, \eta)$, then $\mathrm{DW}(\mathcal{A}) \subseteq \mathrm{DW}(\mathcal{B})$. Indeed, let w be a directing word of $\mathcal{A}$. If $b, b' \in B$, then $b = a\varphi$ and $b' = a'\varphi$, for some $a, a' \in A$, and therefore

$$\eta(b, w) = \eta(a\varphi, w) = \delta(a, w)\varphi = \delta(a', w)\varphi = \ldots = \eta(b', w).$$

Similarly, $u \in \mathrm{DW}(\mathcal{A})$ and $v \in \mathrm{DW}(\mathcal{B})$ imply that $uv \in \mathrm{DW}(\mathcal{A} \times \mathcal{B})$. These observations lead to the following conclusion.

Remark 3.1. *For any alphabet X, $\mathbf{Dir}(X)$ is a variety of X-automata.*

If w is a directing word of an X-automaton $\mathcal{A}$, then so is uwv for any X-words u and v. This yields the next remark.

Remark 3.2. *For any X-automaton $\mathcal{A}$, $X^*\mathrm{DW}(\mathcal{A})X^* = \mathrm{DW}(\mathcal{A})$.*

With any X-automaton $\mathcal{A} = (A, X, \delta)$ we associate an X-automaton $\mathcal{A}_d = (B, X, \eta)$, where $B = \{Aw : w \in X^*\}$ and $\eta(Aw, x) = Awx$ for all $w \in X^*$ and $x \in X$. This $\mathcal{A}_d$ is the part of the usual subset automaton of $\mathcal{A}$ accessible from state A. For any $w \in X^*$, $\eta(A, w) = Aw$. Hence w is a directing word of $\mathcal{A}$ iff $\eta(A, w)$ is a singleton. This means that $\mathrm{DW}(\mathcal{A})$ is recognized by the X-recognizer (B, X, η, A, F), where $F = \{Aw : w \in X^*, |Aw| = 1\}$, and we can state the following conclusion.

Remark 3.3. *For any X-automaton $\mathcal{A}$,* $\mathrm{DW}(\mathcal{A}) \in \mathrm{Rec}(X)$.

If $\mathcal{A}$ is a directable automaton, let $\mathrm{d}(\mathcal{A}) = \min\{\lg(w) : w \in \mathrm{DW}(\mathcal{A})\}$, and for any $n \geq 1$, we define the number

$$\mathrm{d}(n) = \max\{\mathrm{d}(\mathcal{A}) : \mathcal{A} \in \mathbf{Dir}, |A| = n\}.$$

Černý's conjecture may now be formulated as the claim that $\mathrm{d}(n) = (n-1)^2$ for all $n \geq 1$. In [ČPR71] it was shown that the hypothesis holds for $n \leq 5$. For the general case only upper bounds of the order $\mathcal{O}(n^3)$ are known (cf. [Sta69, ČPR71,Pin78], for example). On the other hand, there are examples showing that $\mathrm{d}(n) \geq (n-1)^2$ for all $n \geq 1$ (cf. [Čer64,Sta69]). We consider some modifications of the problem concerning Černý's conjecture. First of all, the question may be restricted to concern some subclass of **Dir**. If **K** is some class of automata, we set

$$\mathrm{d}_{\mathbf{K}}(n) = \max\{\mathrm{d}(\mathcal{A}) : \mathcal{A} \in \mathbf{K} \cap \mathbf{Dir}, |A| = n\}.$$

Pin [Pin79] has shown that $\mathrm{d}_{\mathbf{K}}(n) = (n-1)^2$ for all prime n when $\mathbf{K}$ is the class of automata in which some input letter defines a circular permutation. As we shall see, there are even classes $\mathbf{K}$ for which $\mathrm{d}_{\mathbf{K}}(n) < (n-1)^2$.

For any $r \geq 1$, we call $w \in X^*$ an *r- directing word* of an X-automaton $\mathcal{A} = (A, X, \delta)$, if $|Aw| \leq r$. Let $\mathrm{DW}(\mathcal{A}, r)$ denote the set of r-directing words of $\mathcal{A}$. If $|A| = n$, then

$$X^* = \mathrm{DW}(\mathcal{A}, n) \supseteq \mathrm{DW}(\mathcal{A}, n-1) \supseteq \ldots \supseteq \mathrm{DW}(\mathcal{A}, 1) = \mathrm{DW}(\mathcal{A}).$$

It is clear that Remarks 3.2 and 3.3 apply also to the languages $\mathrm{DW}(\mathcal{A}, r)$. We say that $\mathcal{A}$ is *r-directable* if $\mathrm{DW}(\mathcal{A}, r) \neq \emptyset$. For each $r \geq 1$, let $\mathbf{Dir}_r$ denote the class of r-directable automata. Clearly, $\mathbf{Dir} = \mathbf{Dir}_1 \subset \mathbf{Dir}_2 \subset \ldots$. Note that for $r \geq 2$ and any X, $\mathbf{Dir}_r(X)$ is not a variety of X-automata; it is not closed under direct products.

For any $r \geq 1$ and $\mathcal{A} \in \mathbf{Dir}_r$, let $\mathrm{d}(\mathcal{A}, r) = \min\{\lg(w) : w \in \mathrm{DW}(\mathcal{A}, r)\}$, and for $1 \leq r \leq n$, let

$$\mathrm{d}(n, r) = \max\{\mathrm{d}(\mathcal{A}, r) : \mathcal{A} \in \mathbf{Dir}_r, |A| = n\}.$$

In [Pin78] Pin put forward the following generalization of Černý's conjecture which we call *Pin's conjecture*: $\mathrm{d}(n, r) = (n-r)^2$ for all $1 \leq r \leq n$. For any class $\mathbf{K}$ of automata, we write

$$\mathrm{d}_{\mathbf{K}}(n, r) = \max\{\mathrm{d}(\mathcal{A}, r) : \mathcal{A} \in \mathbf{K} \cap \mathbf{Dir}_r, |A| = n\},$$

and one can again consider modifications of Pin's conjecture which apply to the numbers $d_{\mathbf{K}}(n, r)$ for various classes $\mathbf{K}$.

4 Testing for directability

Let $\mathcal{A} = (X, A, \delta)$ be an automaton, and suppose $|A| = n$ and $|X| = m$. To find out whether $\mathcal{A}$ is directable or not by constructing the state set $\{Aw : w \in X^*\}$ of $\mathcal{A}_d$ can be quite time-consuming: there may be almost 2^n sets to consider, and for each new set Aw one should form all sets Awx $(x \in X)$ and compare them with the previously found sets. If no essential improvements can be found, the worst case estimate for this method is at least of the order $O(m \cdot 2^n)$. Ito and Duske [ItD83] noted that the directability of $\mathcal{A}$ can be tested by applying an input word t which contains all words over X of length $\mathrm{d}(n)$ as subwords; obviously $\mathcal{A} \in \mathbf{Dir}$ iff $|At| = 1$. They show how one can construct such a word t, but the mere length $m^{\mathrm{d}(n)} + \mathrm{d}(n) - 1$ of the word renders the test unpractical even for small values of n and m. If we assume that Černý's conjecture holds, which is the best we can hope for, the length of the test word will be of the order $O(m^{(n-1)^2})$. We present here a simple $O(m \cdot n^2)$-algorithm for solving the directability problem.

For any $k \geq 0$, the relation $\mu_{\mathcal{A}}(k)$ of *k-mergeability* on the state set A of $\mathcal{A}$ is defined so that for $a, b \in A$, $(a, b) \in \mu_{\mathcal{A}}(k)$ iff $aw = bw$ for some $w \in X^{\leq k}$. Two states a and b are *mergeable* if they are k- mergeable for some $k \geq 0$. We denote $\mu_{\mathcal{A}} = \bigcup_{k\geq 0} \mu_{\mathcal{A}}(k)$. It is well-known (cf. [Sta69]) that an automaton is directable iff all pairs of its states are mergeable. This and some other obvious facts about the relations $\mu_{\mathcal{A}}(k)$ and $\mu_{\mathcal{A}}$ are stated in the following proposition.

Proposition 4.1. *Let $\mathcal{A} = (A, X, \delta)$ be an n-state automaton.*

(a) *$\mathcal{A}$ is directable iff $\mu_{\mathcal{A}} = \nabla_A$.*

(b) *The relations $\mu_{\mathcal{A}}(k)$ are reflexive and symmetric ($k \geq 0$).*

(c) $\Delta_A = \mu_{\mathcal{A}}(0) \subseteq \mu_{\mathcal{A}}(1) \subseteq \ldots \subseteq \mu_{\mathcal{A}}$.

(d) The relations $\mu_{\mathcal{A}}(k)$ can be computed as follows:

1. $\mu_{\mathcal{A}}(0) = \Delta_A$;
2. $\mu_{\mathcal{A}}(k) = \mu_{\mathcal{A}}(k-1) \cup \{(a,b) : (\exists x \in X)\ (ax, bx) \in \mu_{\mathcal{A}}(k-1)\}$ *for* $k > 0$.

(e) *If $\mu_{\mathcal{A}}(k) = \mu_{\mathcal{A}}(k-1)$ for some $k > 0$, then $\mu_{\mathcal{A}}(k) = \mu_{\mathcal{A}}(k+1) = \ldots = \mu_{\mathcal{A}}$.*

(f) $\Delta_A = \mu_{\mathcal{A}}(0) \subset \mu_{\mathcal{A}}(1) \subset \ldots \subset \mu_{\mathcal{A}}(k) = \mu_{\mathcal{A}}(k+1) = \mu_{\mathcal{A}}$ *for some k, where* $0 \leq k \leq \binom{n}{2}$.

Proposition 4.1 suggests that the directability of $\mathcal{A}$ can be tested by computing successively $\mu_{\mathcal{A}}(0), \mu_{\mathcal{A}}(1), \mu_{\mathcal{A}}(2), \ldots$ until $\mu_{\mathcal{A}}(k) = \mu_{\mathcal{A}}(k-1)$. The most direct way of doing this leads to an $O(m \cdot n^4)$- algorithm, but by organizing the work better, we get an algorithm which operates in time $O(m \cdot n^2)$. A great part of the saving is achieved by using the inverse transition table of $\mathcal{A}$ instead of the transition table itself. Also, we do not form explicitly each $\mu_{\mathcal{A}}(k)$ although they appear in the sequence of relations that are computed.

The algorithm employs two auxiliary data structures, a Boolen $n \times n$-matrix $\mathbf{M}$ and a list *NewPair* of pairs of states. To simplify the notation, we assume that $A = \{1, 2, \ldots, n\}$. Then $\mathbf{M}[i,j] = 1$ means that the pair i, j ($\in A$) is known to be mergeable. Since it suffices to consider just the pairs (i,j), where $1 \leq i < j \leq n$, we actually need just the upper part of $\mathbf{M}$. A pair appears in *NewPair* when i and j have found to be mergeable, but this fact has not yet been used for finding further mergeable pairs. The *inverted transition table*

$$\mathbf{I} = (\mathbf{I}[a,x])_{a\in A, x\in X}$$

is defined so that $\mathbf{I}[a,x] = \{i \in A : ix = a\}$, for any $a \in A, x \in X$. The steps of the algorithm are as follows.

Step 1. (Initialize $\mathbf{M}$ and *NewPair*) $\mathbf{M}[i,j] := 0$ for all $1 \leq i < j \leq n$, and *NewPair* $:= \varepsilon$ (the empty list).

Step 2. Form the inverted transition table $\mathbf{I}$.

Step 3. Find all pairs (a,x) ($\in A \times X$) for which $|\mathbf{I}[a,x]| > 1$. For every such (a,x) consider each pair $i,j \in \mathbf{I}[a,x]$ with $i < j$. If $\mathbf{M}[i,j] = 0$, let $\mathbf{M}[i,j] := 1$ and append (i,j) to *NewPair*.

Step 4. Until $NewPair = \varepsilon$ do the following. Delete the first pair from $NewPair$; suppose it is (a,b). From $\mathbf{I}$ find all pairs (i,j), $i < j$, such that for some $x \in X$, $i \in \mathbf{I}[a,x]$ and $j \in \mathbf{I}[b,x]$, or $i \in \mathbf{I}[b,x]$ and $j \in \mathbf{I}[a,x]$. If $\mathbf{M}[i,j] = 0$, let $\mathbf{M}[i,j] := 1$ and append (i,j) to $NewPair$.

Step 5. If $\mathbf{M}[i,j] = 1$ whenever $1 \leq i < j \leq n$, then $\mathcal{A}$ is directable, otherwise not.

Step 1 takes time $\mathcal{O}(n^2)$. If $\mathcal{A}$ is given as a transition table, Step 2 can be carried out in time $\mathcal{O}(m \cdot n)$. In Step 3 one has to consider for each of the m input symbols altogether $n(n-1)/2$ pairs (i,j), therefore the step takes time $\mathcal{O}(m \cdot n^2)$. In Step 4 each pair (i,j) will be considered at most once for each $x \in X$, and this happens when the pair (a,b) for which $\{ix, jx\} = \{a,b\}$ is removed from $NewPair$. Hence, the time bound is $\mathcal{O}(m \cdot n^2)$. Since Step 5 can be carried out in time $\mathcal{O}(n^2)$, the time bound for the whole algorithm is $\mathcal{O}(m \cdot n^2)$.

5 Directing conguences

We call a congruence ρ of an automaton $\mathcal{A} = (A, X, \delta)$ *directing* if the quotient automaton $\mathcal{A}/\rho$ is directable. The set of directing congruences of $\mathcal{A}$ is denoted by $\mathrm{Con}_d(\mathcal{A})$. The following observations are easily verified.

Lemma 5.1. *For any automaton $\mathcal{A}$, $\mathrm{Con}_d(\mathcal{A})$ is a filter of the congruence lattice $\mathrm{Con}(\mathcal{A})$, i.e. (1) $\mathrm{Con}_d(\mathcal{A}) \neq \emptyset$, (2) $\Theta \subseteq \rho$, $\Theta \in \mathrm{Con}_d(\mathcal{A})$ and $\rho \in \mathrm{Con}(\mathcal{A})$ imply $\rho \in \mathrm{Con}_d(\mathcal{A})$, and (3) $\Theta \cap \rho \in \mathrm{Con}_d(\mathcal{A})$ for all $\Theta, \rho \in \mathrm{Con}_d(\mathcal{A})$.*

Corollary 5.2. *Every automaton $\mathcal{A}$ has a unique minimal directing congruence, which we denote by $\rho_{\mathcal{A}}$, $\mathrm{Con}_d(\mathcal{A})$ is the principal filter $[\rho_{\mathcal{A}})$ of $\mathrm{Con}(\mathcal{A})$, and every directable image of $\mathcal{A}$ is an image of $\mathcal{A}/\rho_{\mathcal{A}}$.*

Let $\rho \in \mathrm{Eq}(A)$. We call two states a and b of the automaton $\mathcal{A} = (A, X, \delta)$ ρ-*mergeable* if $(aw, bw) \in \rho$ for some $w \in X^*$. The following obvious lemma shows that our directing congruences are the same as the 'cofinal congruences' of Ito and Duske [ItD83].

Lemma 5.3. *A congruence ρ of $\mathcal{A}$ is directing iff all pairs of states of $\mathcal{A}$ are ρ-mergeable.*

For computing the minimal directing congruence we present a sharper condition for a congruence to be directing. Since any two mergeable states are ρ-mergeable for every congruence ρ, it suffices to consider the nonmergeable pairs of states.

For any automaton $\mathcal{A} = (A, X, \delta)$, let $G_{\mathcal{A}} = (V, E)$ be the directed graph defined as follows. The vertex set $V = \{\{a,b\} : a, b \in A, (a,b) \notin \mu_{\mathcal{A}}\}$ consists of all unordered pairs of nonmergeable states of $\mathcal{A}$. The edge set is $E = \{(\{a,b\}, \{ax, bx\}) : \{a,b\} \in V, x \in X\}$. Note that $\{ax, bx\} \in V$ if $\{a,b\} \in V$ and $x \in X$. It is clear that a congruence which identifies all pairs in V is directing, but it actually suffices to consider a subset of V, the *trap* T of $G_{\mathcal{A}}$ which is the union of (the vertex sets of) all strongly connected components of $G_{\mathcal{A}}$ from which no edges lead outside the component (cf. [DDK85]).

Lemma 5.4. *A congruence ρ of an automaton $\mathcal{A} = (A, X, \delta)$ is directing iff $a\rho b$ for every pair $\{a, b\}$ which belongs to the trap T of $G_{\mathcal{A}}$.*

Proof. For any pair c, d ($\in A$) of nonmergeable states there is a word w ($\in X^*$) such that $\{cw, dw\} \in T$. Hence ρ is directing if it satisfies the condition of the lemma. Suppose now that $\rho \in \mathrm{Con}_d(\mathcal{A})$ and consider any pair $\{a, b\} \in T$. By Lemma 5.3 there is a word w such that $(aw, bw) \in \rho$. Since $\{aw, bw\}$ is in the same strongly connected component as $\{a, b\}, \{awu, bwu\} = \{a, b\}$ for some $u \in X^*$. This shows that also $(a, b) \in \rho$.

For any $a, b \in A$ ($a \neq b$), let $\Theta(a, b)$ be the principal congruence generated by the pair (a, b) (cf. [BuS81]). The last part of the previous proof shows also that $\Theta(a, b) = \Theta(c, d)$ whenever $\{a, b\}$ and $\{c, d\}$ are in the same strongly connected component of $G_{\mathcal{A}}$. Although it will not be used here, we note that Lemma 5.4 yields the following description of the minimal directing congruence.

Corollary 5.5. *For any automaton $\mathcal{A} = (A, X, \delta)$,*

$$\rho_{\mathcal{A}} = \Theta(a_1, b_1) \vee \ldots \vee \Theta(a_k, b_k),$$

for any set $\{\{a_1, b_1\}, \ldots, \{a_k, b_k\}\}$ of representatives of the strongly connected components which form the trap of $G_{\mathcal{A}}$.

Since the reflexive closure $\tau_{\mathcal{A}} = \Delta_{\mathcal{A}} \cup \{(a, b) : \{a, b\} \in T\}$ of the relation corresponding to the trap T of $G_{\mathcal{A}}$ is invariant with respect the state transitions of $\mathcal{A}$, then so is its transitive closure $\tau_{\mathcal{A}}^+$. Since $\tau_{\mathcal{A}}^+$ is the equivalence generated by the pairs in the trap, this means by Lemma 5.4 that $\tau_{\mathcal{A}}^+ = \rho_{\mathcal{A}}$. These observations lead to the following algorithm for finding the minimal directing congruence for a given automaton $\mathcal{A} = (A, X, \delta)$.

Step 1. Compute $\mu_{\mathcal{A}}$ using the method described in Section 4.

Step 2. Form the graph $G_{\mathcal{A}} = (V, E)$; the vertex set is obtained from $\mu_{\mathcal{A}}$.

Step 3. Compute the strongly connected components forming the trap T of $G_{\mathcal{A}}$ using the algorithm of [DDK85].

Step 4. Form the relation $\tau_{\mathcal{A}}$ and compute the transitive closure; $\tau_{\mathcal{A}}^+ = \rho_{\mathcal{A}}$.

We know that the computation of $\mu_{\mathcal{A}}$ takes time $O(m \cdot n^2)$. The vertex set V is then obtained in time $O(n^2)$, and computing the set E of edges can be done in time $O(m \cdot n^2)$. In [DDK85] Tarjan's algorithm [Tar72] for computing the strongly connected components of a directed graph is modified to yield the trap. The algorithm works in time $O(\nu + e)$, where ν is the number of vertices and e is the number of edges. In the present case $\nu \leq n(n-1)/2$ and $e \leq m \cdot n(n-1)/2$, for $n = |A|$ and $m = |X|$. Hence, also Step 3 can be carried out in time $O(m \cdot n^2)$. Step 4 takes time $O(n^3)$ if we use Warshall's algorithm (cf. [AHU83], for example) for computing the transitive closure. The total time used by algorithm is therefore bounded by $O(m \cdot n^2 + n^3)$.

6 Directable commutative automata

An automaton $\mathcal{A} = (A, X, \delta)$ is called *commutative* if $axy = ayx$ for all $a \in A$ and $x, y \in X$. Let **Com** denote the class of commutative automata. Rystsov [Rys94] has shown that $d_{\mathbf{Com}}(n) = n - 1$ for every $n \geq 1$. We give a simple proof for a generalization of this fact. The generalization corresponds to Pin's conjecture.

Proposition 6.1. $d_{\mathbf{Com}}(n, r) = n - r$ *whenever* $1 \leq r \leq n$.

Proof. Suppose $\mathcal{A} = (A, X, \delta)$ is commutative and r-directable, where $1 \leq r \leq n = |A|$. Let $w = x_1 \ldots x_m$ $(x_i \in X)$ be an r-directing word of $\mathcal{A}$ of minimal length. The commutativity of $\mathcal{A}$ implies that $Auv = (Av)u \subseteq Au$ for all $u, v \in X^*$. Hence $A \supseteq Ax_1 \supseteq Ax_1x_2 \supseteq \ldots \supseteq Aw$. All of these inclusions must be proper as $Ax_1 \ldots x_{i-1} = Ax_1 \ldots x_{i-1}x_i$, for some $1 \leq i \leq m$, would imply that $Ax_1 \ldots x_{i-1}x_{i+1} \ldots x_m = Aw$, contradicting the assumption that w is of minimal length. Therefore

$$n = |A| > |Ax_1| > \ldots > |Ax_1 \ldots x_{m-1}| > r,$$

and this implies that $m \leq n - r$. To see that equality is possible in all cases, it suffices to consider the automata $\mathcal{A}(n, X) = (\{1, \ldots, n\}, X, \delta)$, where $n \geq 1$, X is any alphabet and $\delta(i, x) = \min\{i + 1, n\}$ for all $i \in \{1, \ldots, n\}$ and $x \in X$.

7 Definiteness, nilpotency and directability

Let $k \geq 0$. An automaton $\mathcal{A} = (A, X, \delta)$ is *weakly k-definite* if $aw = bw$ for all $w \in X^k$ and all $a, b \in A$, and it is *definite* if it is weakly k-definite for some k. If $\mathcal{A}$ is definite and k is the smallest number for which it is weakly k-definite, then $\mathcal{A}$ is *k-definite* [Kle56,PRS63]. Let **Def** denote the class of all definite automata.

It is clear that every definite automaton is directable. Moreover, if an X-automaton $\mathcal{A}$ is weakly *k-definite*, then $\mathrm{DW}(\mathcal{A}) = P \cup X^{\geq k}$ for some $P \subseteq X^{<k}$. In [PRS63] it was shown that an n-state definite automaton is k- definite for some $k \leq n - 1$. This shows that $d_{\mathbf{Def}}(n) \leq n - 1$ for every $n \geq 1$. That actually $d_{\mathbf{Def}}(n) = n - 1$, is again witnessed by the automata $\mathcal{A}(n, X)$. This observation can be generalized to read as follows.

Proposition 7.1. $d_{\mathbf{Def}}(n, r) = n - r$ *whenever* $1 \leq r \leq n$.

Proof. Let $\mathcal{A} = (A, X, \delta)$ be a given automaton. For every $i \geq 0$, we define on A a relation ρ_i so that for any $a, b \in A$,

$$a \rho_i b \text{ iff } (\forall w \in X^i) \; aw = bw.$$

It is easy to see (*cf.* [Ste69]) that these relations are congruences of $\mathcal{A}$, and that $\mathcal{A}$ is k-definite $(k \geq 0)$ iff

1. $\Delta_A = \rho_0 \subset \rho_1 \subset \ldots \subset \rho_{k-1} \subset \rho_k = \nabla_A$.

Suppose now that $\mathcal{A}$ has n states and is k- definite. It is clear that if $0 \le i \le k$ and $w \in X^i$, then $aw\rho_{k-i}bw$ for all $a, b \in A$. On the other hand, by (1) the number of ρ_{k-i}-classes is at least $i+1$. Hence $|Aw| \le n-i$ for every $w \in X^i$. Moreover, $|Aw| = 1$ whenever $\lg(w) \ge k$. This means that if $1 \le r \le n$ and $w \in X^{n-r}$, then $|Aw| \le r$. Hence $d_{\mathbf{Def}}(n,r) \le n-r$. That the bound is exact, can be seen by considering again the automata $\mathcal{A}(n, X)$.

Definite automata correspond to *definite languages* [Kle56,PRS63]. Next we consider automata that correspond to *reverse definite languages* [Brz63,Gin66]. An automaton $\mathcal{A} = (A, X, \delta)$ is *weakly reverse k-definite* ($k \ge 0$) if $awx = aw$ for all $a \in A, w \in X^k$ and $x \in X$. *Reverse definite* and *reverse k-definite* automata are now defined in the natural way. Let **RDef** be the class of reverse definite automata. If $\mathcal{A} = (A, X, \delta)$ is weakly reverse k-definite, then for all $a \in A$ and $w \in X^{\ge k}$, aw is a 'dead state', *i.e.* $awx = aw$ for every $x \in X$. This means that $\mathcal{A}$ is directable exactly in case it has just one such dead state. Recall that an automaton $\mathcal{A} = (A, X, \delta)$ is *nilpotent* (cf. [GéP72]) if there is a state $a_0 \in A$, called the *absorbing state*, and a bound $k \ge 0$ such that $aw = a_0$ whenever $a \in A$ and $\lg(w) \ge k$. Let **Nil** denote the class of nilpotent automata.

Proposition 7.2. $\mathbf{RDef} \cap \mathbf{Dir} = \mathbf{Nil}$, *and* $d_{\mathbf{RDef}}(n,r) = d_{\mathbf{Nil}}(n,r) = n-r$ *for all* $1 \le r \le n$.

Proof. Any nilpotent automaton is clearly both reverse definite and directable, and the converse we noted already above. Hence $\mathbf{RDef} \cap \mathbf{Dir} = \mathbf{Nil}$ holds. Since $\mathbf{Nil} \subseteq \mathbf{Def}$, we get $d_{\mathbf{Nil}}(n,r) \le d_{\mathbf{Def}}(n,r) = n-r$ for all $1 \le r \le n$. Once more, equality is seen to hold by considering the automata $\mathcal{A}(n, X)$ which are also nilpotent.

An X-language L is *generalized definite* [Gin66] if it has a representation

$$L = P \cup Q_1 X^* R_1 \cup \ldots \cup Q_m X^* R_m,$$

where $m \ge 0$ and the sets P, Q_i and R_i are finite. Let us call an automaton $\mathcal{A} = (A, X, \delta)$ *generalized definite* if there are integers $h, k \ge 0$ such that $asut = asvt$, for all $a \in A$, $s \in X^h$, $t \in X^k$ and $u, v \in X^*$. This definition is justified by the following facts.

Proposition 7.3. *Let* $\mathbf{A} = (A, X, \delta, a_0, F)$ *be an* X*-recognizer based on a given* X*-automaton* $\mathcal{A} = (A, X, \delta)$.

(a) *If* $L(\mathbf{A})$ *is a generalized definite language and* $\mathbf{A}$ *is its minimal recognizer, then the automaton* $\mathcal{A}$ *is generalized definite.*

(b) *If the automaton* $\mathcal{A}$ *is generalized definite, then the language* $L(\mathbf{A})$ *is also generalized definite.*

Proof. Suppose first that $L(\mathbf{A}) = P \cup Q_1 X^* R_1 \cup \ldots \cup Q_m X^* R_m$, where $m \ge 0$ and all of the sets P, Q_i and R_i are finite, and that $\mathbf{A}$ is a minimal recognizer of $L(\mathbf{A})$. We may then assume that $P \subseteq X^{<h+k}$, $Q_1, \ldots, Q_m \subseteq X^h$ and $R_1, \ldots, R_m \subseteq X^k$,

for some $h, k \geq 0$. Consider any $a \in A$, $s \in X^h$, $t \in X^k$ and $u, v \in X^*$. Since **A** is minimal, there is a word $r \in X^*$ such that $a = a_0 r$. For any $w \in X^*$,

$$\lg(rsutw), \lg(rsvtw) \geq h + k \text{ and}$$

$$\mathrm{pref}_h(rsutw) = \mathrm{pref}_h(rsvtw), \quad \mathrm{suff}_k(rsutw) = \mathrm{suff}_k(rsvtw),$$

and hence $rsutw \in L(\mathbf{A})$ iff $rsvtw \in L(\mathbf{A})$. This shows that $a_0 rsut = asut$ and $a_0 rsvt = asvt$ are equivalent states, and since **A** is minimal, $asut = asvt$ must hold. Hence $\mathcal{A}$ is generalized definite.

Assume now that $\mathcal{A}$ is generalized definite and let $h, k \geq 0$ be such that $asut = asvt$ whenever $a \in A$, $s \in X^h$, $r \in X^k$ and $u, v \in X^*$. Consider any words $u, v \in X^*$ such that $\lg(u)$, $\lg(v) \geq h + k$, $\mathrm{pref}_h(u) = \mathrm{pref}_h(v)$ and $\mathrm{suff}_k(u) = \mathrm{suff}_k(v)$. We may then write $u = su't$ and $v = sv't$, where $s \in X^h$ and $t \in X^k$. Now

$$u \in L(\mathbf{A}) \Leftrightarrow a_0 su'v \in F \Leftrightarrow a_0 sv't \in F \Leftrightarrow v \in L(\mathbf{A}),$$

which shows that $L(\mathbf{A})$ is generalized definite.

Let **GDef** denote the class of generalized definite automata. Clearly, **Def** $\subset$ **GDef** and **RDef** $\subset$ **GDef**, but it turns out that all directable generalized definite automata are definite.

Proposition 7.4. $\mathbf{GDef} \cap \mathbf{Dir} = \mathbf{Def}$, *and hence* $\mathrm{d}_{\mathbf{GDef}}(n, r) = n - r$ *for all* $1 \leq r \leq n$.

Proof. Let $\mathcal{A} = (A, X, \delta)$ be a directable generalized definite automaton, and let $h, k \geq 0$ be such that $asut = asvt$ whenever $a \in A$, $s \in X^h$, $t \in X^k$ and $u, v \in X^*$. Let u be a directing word of $\mathcal{A}$. If $w \in X^{h+k}$, we may write $w = st$ with $s \in X^h$ and $t \in X^k$. Then for any $a, b \in A$,

$$aw = ast = as\varepsilon t = asut = bsut = \ldots = bw.$$

Hence $\mathcal{A}$ is definite. The converse inclusion is obvious.

If we add to Propositions 7.2 and 7.4 the obvious fact $\mathbf{Def} \cap \mathbf{RDef} = \mathbf{Nil}$, we get the following complete description of the inclusion relationships between and the intersections of the classes **Def**, **RDef**, **GDef** and **Nil**.

Proposition 7.5.

1. $\mathbf{Nil} \subset \mathbf{Def} \subset \mathbf{Dir}, \mathbf{Def} \subset \mathbf{GDef}, \mathbf{Nil} \subset \mathbf{RDef} \subset \mathbf{GDef}$,
2. $\mathbf{GDef} \cap \mathbf{Dir} = \mathbf{Def}$, *and*
3. $\mathbf{Dir} \cap \mathbf{RDef} = \mathbf{Def} \cap \mathbf{RDef} = \mathbf{Nil}$.

The relations of Proposition 7.5 are summarized by the inclusion diagram of Figure 1.

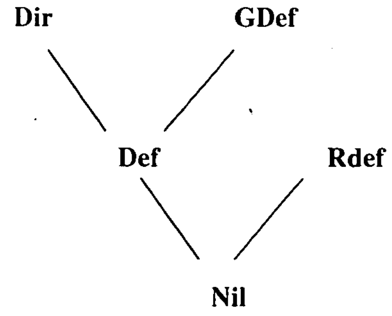

Figure 1

Finally, we note that within the intersection **Dir** $\cap$ **Com** all of the classes **Def**, **RDef**, **GDef** and **Nil** are equal. This follows from the next observation.

Remark 7.6. **Dir** $\cap$ **Com** $\cap$ **GDef** = **Com** $\cap$ **Nil**.

Proof. If $\mathcal{A} = (A, X, \delta) \in$ **Dir** $\cap$ **Com** $\cap$ **GDef**, then $\mathcal{A}$ is k-definite for some $k \geq 0$. Then for any $a, b \in A$ and $u, v \in X^{\geq k}$, $au = bvu = buv = bv$, which shows that $\mathcal{A}$ is nilpotent. The converse inclusion follows from Proposition 7.5.

References

[AHU83] A.V. Aho, J.E. Hopcroft & J.D. Ullman: *Data structures and algorithms.* - Addison-Wesley, Reading, Mass. 1983.

[Brz62] J.A. Brzozowski: Canonical regular expressions and minimal state graphs for definite events.- *Proc. Symp. Math. Theory of Automata*, Microwave Research Inst. Symp. Ser. **12** (Brooklyn 1963), Brooklyn, New York 1963, 529-561.

[BuS81] S. Burris & H.P. Sankappanavar: *A course in universal algebra.* - Springer-Verlag, New York 1981.

[Čer64] J. Černý: Poznámka k homogénym experimentom s konecinými automatami. - *Mat.-fyz. cas. SAV* **14** (1964), 208-215.

[ČPR71] J. Černý, A. Piricka & B. Rosenauerová: On directable automata - *Kybernetika (Praha)* **7** (1971), 289-297.

[DDK85] J. Demel, M. Demlova & V. Koubek: Fast algorithms constructing minimal subalgebras, congruences, and ideals in a finite algebra. - *Theoret. Comput. Sci.* **36** (1985), 203-216.

[GéP72] F. Gécseg & I. Peák: *Algebraic theory of automata.* - Akadémiai Kiadó, Budapest 1972.

[Gin66] A. Ginzburg: About some properties of definite, reverse-definite and related automata. *IEEE Trans. Electronic Computers* **EC-15** (1966), 806-810.

[ItD83] M. Ito & J. Duske: On cofinal and definite automata. - *Acta Cybern.* **6** (1983), 181-189.

[Kle56] S.C. Kleene: Representation of events in nerve nets and finite automata. - *Automata Sutides*, Princeton University Press, Princeton N.J. 1956, 3-41.

[PRS63] M. Perles, M.O. Rabin & E. Shamir: The theory of definite automata. - *IEEE Trans. Electronic Computers* **EC-12** (1963), 233-243.

[Pin78] J.-E. Pin: Sur les mots synchronisants dans un automata fini. - *Elekron. Inform.- Verarb. u. Kybernetik, EIK* **14** (1978), 297-303.

[Pin79] J.-E. Pin: Sur un cas particulier de la conjecture de Cerny. - *Automata, languages and programming,* ICALP'79 (Proc. Coll., Udine 1979), LNCS 62, Springer-Verlag, Berlin 1979, 345-352.

[Rys94] I. Rystsov: Exact linear bound for the length of reset words in commutative automata (to appear).

[Sta69] P.H. Starke: *Abstrakte Automaten.* - VEB Deutscher Verlag der Wissenschaften, Berlin 1969.

[Ste69] M. Steinby: On definite automata and related systems. - *Ann. Acad. Sci. Fenn.*, Ser. A, I Math. **444**, Helsinki 1969.

[Tar72] R. Tarjan: Depth first search and linear graph algorithms.- *SIAM J. Computing* **1** (1972), 146-160.

Received March 20, 1995