Ideal Regular Languages and Strongly Connected Synchronizing Automata

Rogério Reis, Emanuele Rodaro

Technical Report Series: DCC-2013-03
Version 1.1 October 2013

Departamento de Ciência de Computadores
Faculdade de Ciências da Universidade do Porto
Rua do Campo Alegre, 1021/1055,
4169-007 PORTO,
PORTUGAL
Tel: 220 402 900 Fax: 220 402 950
http://www.dcc.fc.up.pt/Pubs/

Ideal Regular Languages and Strongly Connected Synchronizing Automata

Rogério Reis, Emanuele Rodaro

Centro de Matemática, Universidade do Porto
R. Campo Alegre 687, 4169-007 Porto, Portugal
e-mail: rvr@dcc.fc.up.pt, emanuele.rodaro@fc.up.pt

Abstract. We introduce the notion of reset left regular decomposition of an ideal regular language and we prove that the category formed by these decompositions with certain morphisms is equivalent to the category of strongly connected synchronizing automata. We show that each ideal regular language has at least a reset left regular decomposition. As a consequence, each ideal regular language is the set of synchronizing words of some strongly connected synchronizing automaton. Furthermore, this one-to-one correspondence allows us to introduce the notion of reset decomposition complexity of an ideal. This notion allows the reformulation of Černý's conjecture in pure language theoretic terms.

1 Introduction

Since, in the context of this paper, we do not study automata as languages recognizer, but we are just interest on the action of its transition function δ on the set of states Q, we consider a deterministic finite automaton (DFA) as a tuple $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$, where the initial and final states are deliberately omitted from the definition. These automata are also referred in literature as semiautomata. But, because in some point of this work we also refer to an automaton as a language recognizer, we still call a DFA a tuple $\mathscr{B} = \langle Q', \Sigma', \delta', q_0, F\rangle$, and the language recognized by $\mathscr{B}$ is the set $L[\mathscr{B}] = \{u \in \Sigma^* : \delta'(q_0, u) \in F\}$. A DFA $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ is called synchronizing if there exists a word $w \in \Sigma^*$ "sending" all the states into a single one, i.e. $\delta(q, w) = \delta(q', w)$ for all $q, q' \in Q$. Any such word is said to be synchronizing (or reset) for the DFA $\mathscr{A}$. This notion has been widely studied since the work of Černý in 1964 [11] and his well known conjecture regarding the length of the shortest reset word. This conjecture states that any synchronizing automata $\mathscr{A}$ with n states admits at least a reset word w with $|w| \leq (n-1)^2$. For more information on synchronizing automata we refer the reader to the survey by Volkov [12]. In what follows, when there is no ambiguity on the choice of the action δ of the automaton, we use the notation $q \cdot u$ instead of $\delta(q, u)$. We extend this action to a subset $H \subseteq Q$ in the obvious way $H \cdot u = \{q \cdot u : q \in H\}$ with the convention $\emptyset \cdot u = \emptyset$, and for a language $L \subseteq \Sigma^*$ we use the notation $H \cdot L = \{q \cdot u : q \in H, u \in L\}$. We say that $\mathscr{A}$ is *strongly connected* whenever for any $q, q' \in Q$ there is a word $u \in \Sigma^*$ such that $q \cdot u = q'$. In the realm of synchronizing automata this notion is crucial since it is well known that Černý's conjecture is true if and only if it is true for the class of strongly connected synchronizing automata.

In this paper we study the relationship between ideal regular languages and synchronizing automata. A language $I \subseteq \Sigma^*$ is called a *two-sided ideal* (or simply an ideal) if $\Sigma^* I \Sigma^* \subseteq I$. In this work we will consider only ideal languages which are regular. Denote by $\mathbf{I}_\Sigma$ the class of ideal languages on an alphabet Σ. For a given synchronizing automaton $\mathscr{A}$, $\mathrm{Syn}(\mathscr{A})$ denotes the language of all the words synchronizing $\mathscr{A}$. It is a well known fact that $\mathrm{Syn}(\mathscr{A}) = \Sigma^* \mathrm{Syn}(\mathscr{A})\Sigma^*$ is a regular language which is also an ideal. This ideal is generated by the set of minimal synchronizing words $G = \mathrm{Syn}(\mathscr{A}) \setminus (\Sigma^+ \mathrm{Syn}(\mathscr{A}) \cup \mathrm{Syn}(\mathscr{A})\Sigma^+)$ or equivalently using the bifix or infix operators introduced in [6, 8] we get $G = I^\iota = I^b$. In case the set of generators G is finite, I is called finitely generated ideal and the synchronizing automata whose set of synchronizing words is finitely generated are called finitely generated synchronizing automata (see [5, 7, 9]). It is observed in [3] that the minimal deterministic automaton $\mathscr{A}_I = \langle Q', \Sigma, \delta', q_0, \{s\}\rangle$ recognizing an ideal language I is synchronizing with a unique final state s which is fixed by all the elements of Σ. We will refer to such state as *the sink state* for $\mathscr{A}_I$. Furthermore $\mathrm{Syn}(\mathscr{A}_I) = I$. Thus, each ideal language is endowed with at least

a synchronizing automaton for which I serves as the set of reset words. Therefore, for each ideal I there is a non-empty set $\mathcal{SA}(I)$ of all the synchronizing automata $\mathscr{B}$ with $\mathrm{Syn}(\mathscr{B}) = I$. This simple observation led Maslennikova to introduce in [3] the notion of *reset complexity* of an ideal I as the number of states of the smallest automata in $\mathcal{SA}(I)$. In the same paper it is shown that the reset complexity can be exponentially smaller than the state complexity of the language. In the subsequent paper [1], the authors consider the special case of finitely generated synchronizing automata with the set of the reset words which is a principal ideal $P = \Sigma^* w \Sigma^*$ generated by a word $w \in \Sigma^*$, and it is presented an algorithm to generate a strongly connected synchronizing automaton $\mathscr{B}_w$ with $\mathrm{Syn}(\mathscr{B}_w) = P$ with the same number of states of $\mathscr{A}_P$. In the same paper the author address the question whether or not, for any ideal language I, there is always a strongly connected synchronizing automaton in $\mathcal{SA}(I)$. In Section 3 we answer affirmatively to this question. However, to study and characterize languages which are the reset words of strongly connected synchronizing automata we need to introduce the following provisional class of *strongly connected ideal language*:

Definition 1 *An ideal language I is called strongly connected whenever $I = \mathrm{Syn}(\mathscr{A})$ for some strongly connected synchronizing automaton $\mathscr{A}$.*

The paper is organized as follows. In Section 2 we introduce the notion of a (reset) left regular decomposition of an ideal, and we prove that strongly connected ideal languages are exactly the ideals having a reset left regular decomposition. We also exhibit an equivalence between the category of reset left regular decompositions and the category of the the strongly connected synchronizing automaton on the same alphabet. Using this equivalence we prove in Section 3 that each ideal language is a strongly connected ideal language. Thus, we can introduce the concept of reset regular decomposition complexity of an ideal and give an equivalent formulation of Černý's conjecture using this notion. We give some upper bound to this parameter for a subclass of the ideal languages and finally we state some open problems and direction of future research.

2 Strongly connected ideal languages

In this section we develop a connection between strongly connected synchronizing automata and strongly connected ideal languages. First we need some definitions. A *homomorphism* $\varphi : \mathscr{A} \to \mathscr{B}$ between the two DFA's $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$, $\mathscr{B} = \langle T, \Sigma, \xi \rangle$ is a map $\varphi : Q \to T$ preserving the actions of the two automata, i.e. $\varphi(\delta(q, a)) = \xi(\varphi(q), a)$ for all $a \in \Sigma$. We temporarily denote the class of strongly connected ideals on some finite alphabet Σ by $\mathbf{SCI}_\Sigma$. We denote $\mathbf{SCSA}_\Sigma$ the category of strongly connected synchronizing automata where $\varphi : \mathscr{A} \to \mathscr{B}$ is an arrow if φ is a homomorphism. Note that any homomorphism between strongly connected automata is necessarily surjective. For $L \subseteq \Sigma^*$ and $u \in \Sigma^*$, we put $Lu = \{xu : x \in L\}$, $uL = \{ux : x \in L\}$. We recall that the *reverse* operator $\cdot^R$ is a bijective map on Σ^* such that given a word $u = u_1 u_2 \dots u_k$, $u^R = u_k \dots u_2 u_1$. This operator extends naturaly to languages. To characterize the class $\mathbf{SCI}_\Sigma$ we use the following concept of *reset left regular decomposition.*

Definition 2 *A left regular decomposition is a collection $\{I_i\}_{i \in F}$ of disjoint left ideals I_i of Σ^* for some finite set F such that:*

i) For any $a \in \Sigma$ and $i \in F$, there is a $j \in F$ such that $I_i a \subseteq I_j$

The decomposition $\{I_i\}_{i \in F}$ is called a reset left regular decomposition if it also satisfies the following extra condition:

ii) Let $I = \uplus_{i \in F} I_i$, for any $u \in \Sigma^*$ if there is an $i \in F$ such that $Iu \subseteq I_i$, then $u \in I$.

Note that if $\{I_i\}_{i \in F}$ is a reset left regular decomposition, then the condition $Iu \subseteq I_i$ implies $u \in I_i$. Since $u \in I$, then $u \in I_j$ for some $j \in F$, hence $Iu \subseteq I_j$. If $j \neq i$ we have both $Iu \subseteq I_i$ and $Iu \subseteq I_j$ and thus $I_i \cap I_j \neq \emptyset$, which is a contradiction. We say that an ideal I has a (reset) left regular decomposition if there is a (reset) left regular decomposition $\{I_i\}_{i \in F}$ such that $I = \uplus_{i \in F} I_i$. The *order* of $\{I_i\}_{i \in F}$ is the cardinality of the family, and we assume that the set F of indices of the family is minimal, and

so the order of $\{I_i\}_{i\in F}$ is also equal to $|F|$. The notion of right regular decomposition is symmetric: exchange left ideals with right ideals and $I_i a, Iu$ with aI_i, uI, respectively. Denote by $\mathbf{RLD}_\Sigma$ ($\mathbf{RRD}_\Sigma$) the category of the reset left regular decompositions, where an arrow $f : \{I_i\}_{i\in F} \to \{J_i\}_{i\in H}$ is any function $f : F \to H$ such that for any $i \in F$, there is an index $f(i) \in H$ with $I_i \subseteq J_{f(i)}$. Note that, given a left regular decomposition (reset left regular decomposition) $\{I_i\}_{i\in F}$, then $\{I_i^R\}_{i\in F}$ is a right regular decomposition (reset right regular decomposition). Thus $\cdot^R$ is a bijection between the objects of $\mathbf{RLD}_\Sigma \to \mathbf{RRD}_\Sigma$. We have the following characterization.

Theorem 3. *An ideal language I is strongly connected if and only if it has a reset left regular decomposition. Moreover $\boldsymbol{RLD}_\Sigma$ and $\boldsymbol{SCSA}_\Sigma$ are equivalent categories via the two functors $\mathcal{A}, \mathcal{I}$ defined by:*

- $\mathcal{A} : \boldsymbol{RLD}_\Sigma \to \boldsymbol{SCSA}_\Sigma$ *which sends*

$$\mathcal{A} : \{I_i\}_{i\in F} \mapsto \mathcal{A}(\{I_i\}_{i\in F}) = \langle \{I_i\}_{i\in F}, \Sigma, \eta\rangle$$

  with $\eta(I_i, a) = I_j$ for $a \in \Sigma$ if and only if $I_i a \subseteq I_j$, and if $f : \{I_i\}_{i\in F} \to \{J_i\}_{i\in H}$ then $\mathcal{A}(f)$ is the homomorphism $\varphi : \mathcal{A}(\{I_i\}_{i\in F}) \to \mathcal{A}(\{J_i\}_{i\in H})$ defined by $\varphi(I_i) = J_m$ where $I_i \subseteq J_m$;
- $\mathcal{I} : \boldsymbol{SCSA}_\Sigma \to \boldsymbol{RLD}_\Sigma$ *sending*

$$\mathcal{I} : \mathscr{A} = \langle Q, \Sigma, \delta\rangle \mapsto \mathcal{I}(\mathscr{A}) = \{\mathcal{I}(\mathscr{A})_q\}_{q\in Q}$$

  where $\mathcal{I}(\mathscr{A})_q = \{u \in \Sigma^* : \delta(Q, u) = q\}$, and if $\varphi : \mathscr{A} \to \mathscr{B}$ is an arrow between $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ and $\mathscr{B} = \langle T, \Sigma, \xi\rangle$, then $\mathcal{I}(\varphi)$ is the arrow defined by $f : Q \to T$ which sends $q \mapsto \varphi(q)$.

Proof. Let us prove the first claim of the theorem. Let $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ be a strongly connected synchronizing automata with $\mathrm{Syn}(\mathscr{A}) = I$. For each $q \in Q$, let:

$$I_q = \{u \in I : Q \cdot u = q\}$$

We claim that $\{I_q\}_{q\in Q}$ is a reset left regular decomposition for I. It is obvious that I_q are left ideals since for any $u \in I_q$ and $v \in \Sigma^*$, we get $Q \cdot vu \subseteq Q \cdot u = \{q\}$, i.e. $Q \cdot vu = \{q\}$. Let $q, q' \in Q$ with $q \neq q'$ and assume $I_q \cap I_{q'} \neq \emptyset$ and let $u \in I_q \cap I_{q'}$. By definition, we have $q = Qu = q'$, which is a contradiction. Hence $I_q \cap I_{q'} = \emptyset$. Clearly $\uplus_{q\in Q} I_q \subseteq I$. Conversely if $u \in I$, since it is a reset word, then $Qu = q'$ for some $q' \in Q$, i.e. $u \in I_{q'}$ and so we have the decomposition $\uplus_{q\in Q} I_q = I$. Moreover for any $a \in \Sigma$, if $u \in I_q$, then $Q \cdot ua = q \cdot a$, thus $I_q a \subseteq I_{q\cdot a}$ and so condition i) of the Definition 2 is fulfilled. Thus it remains to prove that condition ii) is also satisfied. Suppose that $Iw \subseteq I_{\overline{q}}$ for some $\overline{q} \in Q$. Take any $q \in Q$, we claim that $qw = \overline{q}$ and so $w \in \mathrm{Syn}(\mathscr{A}) = I$. Take any $u' \in I$, thus $Q \cdot u' = q'$ for some $q' \in Q$. Since $\mathscr{A}$ is strongly connected, there is $u'' \in \Sigma^*$ such that $q' \cdot u'' = q$. Thus $u = u'u'' \in I$ satisfies $Q \cdot u = q$. Since $Iw \subseteq I_{\overline{q}}$ we get $\overline{q} = Q \cdot (uw) = q \cdot w$, i.e. $q \cdot w = \overline{q}$.

Conversely suppose that I has a reset left regular decomposition $\{I_i\}_{i\in F}$. We associate a DFA $\mathcal{A}(\{I_i\}_{i\in F}) = \langle \{I_i\}_{i\in F}, \Sigma, \eta\rangle$ in the following way. By condition i) of Definition 2 for any I_i and $a \in \Sigma$ there is a $j \in F$ with $I_i \cdot a \subseteq I_j$. Thus we define $\eta(I_i, a) = I_j$. This function is well defined. Let $j, k \in F$ with $j \neq i$, such that $I_i \cdot a \subseteq I_j, I_k$, then $I_i \cdot a \subseteq I_j \cap I_k$, hence $I_j \cap I_k \neq \emptyset$, which is a contradiction. Hence $\mathcal{A}(\{I_i\}_{i\in F})$ is a well defined DFA. It is straightforward to check that $\eta(I_i, u) = I_k$ for $u \in \Sigma^*$ if and only if $I_i u \subseteq I_k$. We prove that $\mathcal{A}(\{I_i\}_{i\in F})$ is strongly connected. Indeed take any $i, j \in F$ and let $w \in I_j$. Since I_j is a left ideal, then $I_i w \subseteq I_j$. Hence $I_i w \subseteq I_j$ implies $\eta(I_i, w) = I_j$ and so $\mathcal{A}(\{I_i\}_{i\in F})$ is strongly connected. We need to prove that $I \subseteq \mathrm{Syn}(\mathcal{A}(\{I_i\}_{i\in F}))$. Let $u \in I$, since $\{I_i\}_{i\in F}$ is a decomposition, $u \in I_j$ for some $j \in F$. Since I_j is a left ideal, we get $I_i u \subseteq I_j$ for any $i \in F$. Hence $\eta(I_i, u) = I_j$ for all $i \in F$, i.e. $u \in \mathrm{Syn}(\mathcal{A}(\{I_i\}_{i\in F}))$. Conversely, let $u \in \mathrm{Syn}(\mathcal{A}(\{I_i\}_{i\in F}))$. By the definition $\eta(I_i, u) = I_j$ for some $j \in F$ and for all $i \in F$. Therefore $I_i u \subseteq I_j$ which implies $Iu \subseteq I_j$ and so by ii) of Definition 2 we get $u \in I$.

Let us now prove the equivalence of the two categories. Let us prove that if $f : \{I_i\}_{i\in F} \to \{J_i\}_{i\in H}$, then $\mathcal{A}(f) = \varphi$ is a homomorphism between $\mathcal{A}(\{I_i\}_{i\in F}) = \langle Q, \Sigma, \delta\rangle$ and $\mathcal{A}(\{J_i\}_{i\in H}) = \langle T, \Sigma, \eta\rangle$. Indeed, by the definitions for any I_i and $a \in \Sigma$, $\delta(I_i, a) = I_j$ where $I_i a \subseteq I_j$. Since $\varphi(I_i) = J_h$ and $\varphi(I_j) = J_m$ with $I_i \subseteq J_h$ and $I_j \subseteq J_m$, then $I_i a \subseteq J_h a$ and $I_i a \subseteq I_j \subseteq J_m$ which yields $J_h a \subseteq J_m$, hence

$$\varphi(\delta(I_i, a)) = \varphi(I_j) = J_m = \eta(J_h, a) = \eta(\varphi(I_i), a)$$

which shows that $\mathcal{A}(f) = \varphi$ is a homomorphism. Let $g : \{J_i\}_{i\in H} \to \{S_i\}_{i\in T}$ be another arrow, then it is easy to check that $g \circ f$ implies $\mathcal{A}(g \circ f) = \mathcal{A}(g) \circ \mathcal{A}(f)$. Therefore $\mathcal{A} : \mathbf{RLD}_\Sigma \to \mathbf{SCSA}_\Sigma$ is a functor. Let us prove that $\mathcal{I} : \mathbf{SCSA}_\Sigma \to \mathbf{RLD}_\Sigma$ is also a functor. Indeed if $\varphi : \mathscr{A} \to \mathscr{B}$ is a homomorphism of the DFA's $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ and $\mathscr{B} = \langle T, \Sigma, \eta\rangle$, then for any $q \in Q$ and $u \in \Sigma^*$ such that $\delta(Q, u) = \{q\}$, since φ is surjective, we get $\{\varphi(q)\} = \varphi(\delta(Q, u)) = \delta(T, u)$. Thus $\mathcal{I}(\mathscr{A})_q \subseteq \mathcal{I}(\mathscr{B})_{\varphi(q)}$, whence $\mathcal{I}(\varphi) : \mathcal{I}(\mathscr{A}) \to \mathcal{I}(\mathscr{B})$ is the arrow defined by the map $\varphi : Q \to T$. Furthermore, if $\psi : \mathscr{B} \to \mathscr{C}$ is another arrow, using the previous fact it is easy to see that $\mathcal{I}(\psi \circ \varphi) = \mathcal{I}(\psi) \circ \mathcal{I}(\varphi)$, which completes the proof that $\mathcal{I}$ is a functor. By the previous construction it is straightforward to check that $\mathcal{A}(\mathcal{I}(\mathscr{A})) \simeq \mathscr{A}$ and $\mathcal{I}(\mathcal{A}(\{I_i\}_{i\in F})) \simeq \{I_i\}_{i\in F}$. Moreover, it is straightforward to check that $\mathcal{I}\mathcal{A} = id_{\mathbf{RLD}_\Sigma}$ while the function, which associates to each object $\mathscr{A}$ the arrow given by the isomorphism $\mathcal{A}(\mathcal{I}(\mathscr{A})) \simeq \mathscr{A}$, is a natural isomorphism between the functors $id_{\mathbf{SCSA}_\Sigma}$ and $\mathcal{A}\mathcal{I}$, whence $\mathbf{RLD}_\Sigma, \mathbf{SCSA}_\Sigma$ are equivalent categories. □

The following corollary characterizes the case of ideals on a unary alphabet.

Corollary 1. *Let I be an ideal over a unary alphabet $\Sigma = \{a\}$. Then I is strongly connected if and only if $I = \Sigma^*$.*

Proof. Since the alphabet is unary we have $I = a^*a^m a^*$ for some $m \geq 0$. Suppose that I is strongly connected, then by Theorem 3 there is a reset left regular decomposition $\{I_i\}_{i\in F}$ of I. Assume $a^m \in I_j$ for some $j \in F$. We claim $|F| = 1$. Indeed, since I_j is a left ideal we have $a^*a^m \subseteq I_j$, hence $I = a^*a^m a^* = a^*a^m \subseteq I_j$, i.e. $I = I_j$. Therefore, by Theorem 3 the only strongly connected synchronizing automaton having I as set of reset words is the automaton with one state and a loop labelled by a. Hence $I = a^*$. On the other hand, if $I = a^*$ then I is the set of reset words of the synchronizing automaton with one state and a loop labelled by a, which is strongly connected, i.e. I is strongly connected. □

From this Corollary we can assume henceforth that the ideals considered are taken over an alphabet Σ with $|\Sigma| > 1$.

Given a strongly connected ideal language I with $\mathrm{Syn}(\mathscr{B}) = I$ for some strongly connected synchronizing automaton $\mathscr{B} = \langle Q, \Sigma, \delta\rangle$, there is an obvious way to calculate the associated reset left regular decomposition $\mathcal{I}(\mathscr{B})$. It is well known that I is recognized by the power automaton of $\mathscr{B}$ defined by $\mathcal{P}(\mathscr{B}) = \langle 2^Q, \Sigma, \delta, Q, \{\{q\} : q \in Q\}\rangle$, where 2^Q denotes the set of subsets of Q, the initial state is the set Q and the final set of states is formed by all the singletons. Thus, for each $q \in Q$ we can associate the DFA $\mathcal{P}(\mathscr{B})_q = \langle 2^Q, \Sigma, \delta, Q, \{q\}\rangle$ and so we can calculate the associated reset left regular decomposition by $\mathcal{I}(\mathscr{B}) = \{L[\mathcal{P}(\mathscr{B})_q]\}_{q\in Q}$. A first and quite natural issue is to calculate the reset left regular decompositions of the of the reset words of the Černý series $\mathscr{C}_n = \langle\{1, \ldots, n\}, \{a, b\}, \delta_n\rangle$, where a acts like a cyclic permutation $\delta_n(i, a) = i + 1$ for $i = 1, \ldots, n-1$ and $\delta_n(n, a) = 1$, while b fixes all the states except the last one: $\delta_n(i, b) = i$ for $i = 1, \ldots, n-1$ and $\delta_n(n, b) = 1$ (see Fig. 1).

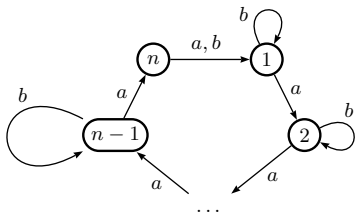

Fig. 1. The Černý automaton $\mathscr{C}_n$.

For example, in the case of $\mathscr{C}_4$ the associated reset left regular decomposition is the one given by

$$\begin{aligned}
L[\mathcal{P}(\mathscr{C})_1] &= (((a^*b)(b+ab+a^4)^*(a^3b+(a^2b(b+a^2)^*ab)))((b+ab^*a^3)+\\
&\quad +((ab^*ab)(b+a^2)^*)ab))^*(ab^*a^2b)(b+((ab^*ab^*)(a(a+b))))^*\\
L[\mathcal{P}(\mathscr{C})_2] &= L[\mathcal{P}(\mathscr{C})_1]ab^*\\
L[\mathcal{P}(\mathscr{C})_3] &= L[\mathcal{P}(\mathscr{C})_1]ab^*ab^*\\
L[\mathcal{P}(\mathscr{C})_4] &= L[\mathcal{P}(\mathscr{C})_1]ab^*ab^*a.
\end{aligned}$$

In general, for $\mathscr{C}_n$ it is not difficult to see that $|\delta_n(\{1,\ldots,n\},ux)|=1$ and $|\delta_n(\{1,\ldots,n\},u)|>1$ for some word $u\in\{a,b\}^*$ and a letter $x\in\{a,b\}$ if and only if $\delta_n(\{1,\ldots,n\},u)=\{n,1\}$ and $x=b$. Thus, if $|\delta_n(Q,w)|=1$, then there is a prefix $w'b$ of w with $\delta_n(Q,w')=\{n,1\}$. Therefore, it is straightforward to check that in this case the decompositions are given by

$$\begin{aligned}
L[\mathcal{P}(\mathscr{C})_1] &= \{w\in\Sigma^* \,:\, \delta_n(\{1,\ldots,n\},w)=\{1\}\}\\
L[\mathcal{P}(\mathscr{C})_\ell] &= L[\mathcal{P}(\mathscr{C})_1](ab^*)^{\ell-1} \quad \text{for } \ell=2,\ldots,n-1\\
L[\mathcal{P}(\mathscr{C})_n] &= L[\mathcal{P}(\mathscr{C})_1](ab^*)^{n-1}a.
\end{aligned}$$

By Theorem 3 if I is strongly connected, we can associate the non-empty set $\mathcal{R}(I)$ of all the reset left regular decompositions of I. We have the following lemma.

Lemma 1. *Let $\{I_i\}_{i\in F}$ be a reset left regular decompositions of I and let $\{J_k\}_{k\in H}$ be a left regular decomposition of an ideal J. If $I\subseteq J$, then the non-empty elements of $\{I_i\cap J_k\}_{i\in F,k\in H}$ form a reset left regular decomposition of I.*

Proof. Let $T\subseteq F\times H$ be the set of pair of indices (i,j) for which $I_i\cap J_j\neq\emptyset$ and rename the set $\{I_i\cap J_k\}_{(i,k)\in T}$ by $\{S_j\}_{j\in T}$. It is clear each S_j is a left ideal and $S_j\cap S_t=\emptyset$ for $j\neq t$. Furthermore $\uplus_{j\in T}S_j=I$. Condition i) is also verified. Take any S_j and suppose that $S_j=I_i\cap J_k$ for some $(i,k)\in T$, and let $a\in\Sigma$. Then $I_ia\subseteq I_s$, $J_ka\subseteq J_t$ for some $s\in F,t\in H$. Hence $(I_i\cap J_k)a=I_ia\cap J_ka\subseteq I_s\cap J_t=S_h$ for some $h\in T$, i.e. $S_ja\subseteq S_h$. Let us prove that reset condition ii) is also fulfilled. Assume $Iu\subseteq S_t$ for some $t\in T$ and $u\in\Sigma^*$. Thus $S_t=I_i\cap J_k$, for some $i\in F,k\in H$, hence $S_t\subseteq I_i$ which implies $Iu\subseteq I_i$. Hence $u\in I$ since $\{I_i\}_{i\in F}$ is a reset left regular decompositions of I. □

Given $\mathcal{I},\mathcal{J}\in\mathcal{R}(I)$ with $\mathcal{I}=\{I_i\}_{i\in F}$ and $\mathcal{J}=\{J_k\}_{k\in H}$ by Lemma 1 the family $\mathcal{I}\wedge\mathcal{J}=\{I_i\cap J_k\}_{i\in F,k\in H}$ is still a reset left regular decomposition. Thus we have the following immediate result.

Corollary 2. *The family of the reset left regular decompositions of a strongly connected ideal I is a $\wedge$-semilattice.*

Let $\|I\|=\min\{|u|:u\in I\}$. It is a well known fact that Černý conjecture holds if and only if it holds for strongly connected synchronizing automata. The following proposition reformulates Černý conjecture in a purely language theoretic context.

Proposition 4 *Černý's conjecture is true for strongly connected synchronizing automata if and only if for any strongly connected ideal I and any reset left regular decomposition $\{I_i\}_{i\in F}$ of I we have:*

$$|F|\geq\sqrt{\|I\|}+1$$

Proof. Suppose that Černý's conjecture is true for strongly connected synchronizing automata. Let I be a strongly connected ideal and let $\{I_i\}_{i\in F}$ be a reset left regular decomposition of I. Let $\mathcal{A}(\{I_i\}_{i\in F})$ be the standard synchronizing automata associated to this decomposition as in Theorem 3. This automaton has $|F|$ states, hence there is a synchronizing word $u\in\mathrm{Syn}(\mathcal{A}(\{\mathscr{I}\}_{\in\mathscr{F}}))=I$ with $|u|\leq(|F|-1)^2$. Thus $|F|\geq\sqrt{|u|}+1\geq\sqrt{\|I\|}+1$.

Conversely, take any strongly connected synchronizing automata $\mathscr{A}$ with n states and let $\mathcal{I}(\mathscr{A})$ be the associated reset left regular decomposition of $I=\mathrm{Syn}(\mathscr{A})$ as in Theorem 3. Since the order of this decomposition is n, then $n\geq\sqrt{\|I\|}+1$. Thus we have that there is a $u\in\mathrm{Syn}(\mathscr{A})$ with $|u|\leq(n-1)^2$ and so Černý's conjecture holds for $\mathscr{A}$. □

3 Ideal languages are strongly connected ideal languages

The notion of strongly connected ideal languages ($\mathbf{SCI}_\Sigma$) has been temporarily introduced in Section 2 to study the relationship between strongly connected synchronizing automata and ideal languages. In this section we actually show that $\mathbf{SCI}_\Sigma = \mathbf{I}_\Sigma$. This is done by indirectly showing, through Theorem 3 and the concept of reset left regular decomposition, that each ideal language I has at least a strongly connected synchronizing automata with set of reset words I. However the number of states of such automaton is in general a double exponential. Therefore, a quite natural issue is finding results that show the existence of smaller automata even for proper classes on $\mathbf{I}_\Sigma$. Before we prove the main result of this section we introduce some notions which are crucial for the sequel.

Let $\mathscr{C} = \langle Q, \Sigma, \delta\rangle$ be an automaton with n states and a sink state s. Note that for such an automaton $|Q \cdot u| = 1$ if and only if $Q \cdot u = \{s\}$. Fix a word $u \in \Sigma^*$ and a subset $H \subseteq Q$. Assume $u = u_1 \dots u_r$ for $u_1, \dots, u_r \in \Sigma$ and $r = |u|$. For $0 \leq i < j \leq r$ we use the standard notation $u[i, j]$ to indicate the factor $u_i u_{i+1} \dots u_j$ if $i > 0$, otherwise $u[0, j] = u_1 \dots u_j$ with the convention that $u[0, 0] = \epsilon$ and $u[i, i] = u_i$ if $i > 0$. There is a unique tuple $0 \leq i_1 < i_2 < \ldots < i_k = r$ of indices such that:

$$|H| = |H \cdot u[0, i_1]| > |H \cdot u[0, i_2]| > \ldots > |H \cdot u[0, i_k]|$$

and for any $i_s < j \leq i_{s+1}$ with $1 \leq s \leq k-1$, we have $|H \cdot u[0, j]| = |H \cdot u[0, i_{s+1}]|$. In other words this indices show the longest prefixes $u[0, j]$ such that $|H \cdot u[0, j]| > |H \cdot u[0, j+1]|$. We call such tuple the *ladder decomposition* of the pair (H, u). The *ladder map* with respect to the word u is the function $\lambda_u : 2^Q \to 2^{2^Q}$ defined by

$$\lambda_u(H) = \{H \cdot u[0, i_1], H \cdot u[0, i_2], \dots, H \cdot u[0, i_k]\}$$

where $i_1 < i_2 < \ldots < i_k$ is the ladder decomposition of (H, u). Note that the range λ_u is contained in the set $\mathcal{L}(Q)$ formed by families $\{H_1, \dots, H_s\}$ with $|H_1| > |H_2| > \ldots > |H_s|$. Note that we have the following upper bounds

$$|\mathcal{L}(Q)| \leq \prod_{i=1}^{|Q|} \binom{|Q|}{i} \leq 2^{n^2} \tag{1}$$

We now introduce a partial internal operation $\star$ on $\mathcal{L}$. Let $\mathcal{V}_1 = \{T_1, \dots, T_m\}$ and $\mathcal{V}_2 = \{H_1, \dots, H_s\}$ with $|T_1| > |T_2| > \ldots > |T_m| \geq |H_1| > |H_2| > \ldots > |H_s|$, then:

$$\mathcal{V}_1 \star \mathcal{V}_2 = \begin{cases} \{T_1, \dots, T_{m-1}, H_1, \dots, H_s\} \text{ if } |T_m| = |H_1| \\ \{T_1, \dots, T_m, H_1, \dots, H_s\} \quad \text{otherwise} \end{cases}$$

We have the following lemma.

Lemma 2. *With the above notation for any $u, v \in \Sigma^*$ we have:*

$$\lambda_{vu}(T) = \lambda_v(T) \star \lambda_u(T \cdot v)$$

Proof. It follows from the definitions. □

The *gap function* of $u \in \Sigma^*$ is the map defined by $\gamma_u(H) = |\lambda_u(H)|$. Using Lemma 2 and the definition of $\star$ it is straightforward to check that the following equality holds:

$$\gamma_{vu}(H) = \gamma_v(H) + \gamma_u(H \cdot v) - 1, \quad \forall u, v \in \Sigma^* \tag{2}$$

We introduce a function which is fundamental in the sequel. Let $m = \frac{n^2+n}{2} + 1$ and let $\mathbb{Z}_m$ be the ring of the integers modulo m. For an integer $t \geq 1$, $[2^Q]_t$ denotes the set of subsets of Q of cardinality t. Let $\mathbb{T}_t = \mathbb{Z}_m([2^Q]_t \uplus \Sigma)$ be the free $\mathbb{Z}_m$-module on $[2^Q]_t \uplus \Sigma$. Let $H \in [2^Q]_t$, $a \in \Sigma$ and $p \in \mathbb{Z}_m([2^Q]_t \uplus \Sigma)$. We denote by $p(H)$, $p(a)$ the coefficients in $\mathbb{Z}_m$ of p with terms H, a, respectively. Note that p can be decomposed as the sum of the two following terms

$$p\langle Q\rangle = \sum_{H \subseteq Q} p(H), \quad p\langle \Sigma\rangle = \sum_{a \in \Sigma} p(a)$$

Fix an element $u \in \Sigma^*$ and $H \subseteq Q$ with $|H| > 1$. The *last set* of (H, u) is the smallest set $S \in \lambda_u(H)$ different from $\{s\}$. There is a maximal factor $u[i, j]$ such that $|S| = |H \cdot u[0, k]|$ for all $i \leq k \leq j$. The *tail* of (H, u) is the element of $\mathbb{Z}_m([2^Q]_t \uplus \Sigma)$ with $t = |S| \geq 2$ defined by

$$\mathcal{T}(H, u) = \begin{cases} \sum_{k=i}^{j-1} (H \cdot u[0, k] + u[k + 1, k + 1]), \text{ if } u[0, j] = u \\ \sum_{k=i}^{j} (H \cdot u[0, k] + u[k + 1, k + 1]), \text{ otherwise.} \end{cases}$$

Consider the set $\mathbb{T} = \uplus_{t=2}^{n} \mathbb{T}_t$ and for an element $\mathcal{T} \in \mathbb{T}_t$ the integer $t \geq 2$ is called *the index* of $\mathcal{T}$ and it is denoted by $\mathrm{Ind}(\mathcal{T})$. We give to $\mathbb{T}$ a structure of semigroup by introducing an internal binary operation $\diamond$ defined in the following way. Let $\mathcal{T}_1 \in \mathbb{T}_i, \mathcal{T}_2 \in \mathbb{T}_j$, then

$$\mathcal{T}_1 \diamond \mathcal{T}_2 = \begin{cases} \mathcal{T}_{\min\{i,j\}} \text{ if } i \neq j \\ \mathcal{T}_1 + \mathcal{T}_2 \quad \text{otherwise} \end{cases}$$

Note that $(\mathbb{T}, \diamond)$ has a graded structure with respect to the semilattice $([2, n], \min)$, i.e. $\mathbb{T}_i \diamond \mathbb{T}_j \subseteq \mathbb{T}_{\min\{i,j\}}$. Let $u \in \Sigma^*$, the *tail map* is the function $\tau_u : 2^Q \to \mathbb{T}$ defined by

$$\tau_u(H) = \begin{cases} \mathcal{T}(H, u) \text{ if } |H| > 1 \\ 0_n \qquad \text{otherwise} \end{cases}$$

where 0_n is the zero of $\mathbb{T}_n$. We have the following lemma.

Lemma 3. *With the above notation for any $u, v \in \Sigma^*$ we have:*

$$\tau_{vu}(T) = \tau_v(T) \diamond \tau_u(T \cdot v)$$

Proof. It follows from the definitions. □

We denote by $\mathrm{Hom}(A, B)$ the set of the maps $f : A \to B$. The following lemma shows a nice property shared by these functions introduced.

Lemma 4. *Consider the following maps*

1. $\mu : \Sigma^* \to \mathrm{Hom}(2^Q, \mathbb{T})$ *defined by* $\mu(u) = \tau_u$,
2. $\xi : \Sigma^* \to \mathrm{Hom}(2^Q, [1, |Q|])$ *defined by* $\xi(u) = \gamma_u$,
3. $\psi : \Sigma^* \to \mathrm{Hom}(2^Q, \mathcal{L}(Q))$ *defined by* $\psi(u) = \lambda_u$.

Then $\mathrm{Ker}(\mu), \mathrm{Ker}(\xi), \mathrm{Ker}(\psi)$ *are left congruences on* Σ^*.

Proof. We prove that $\mathrm{Ker}(\mu)$ is a left congruence. Let $a \in \Sigma$ and $u, v \in \Sigma^*$ with $\mu(u) = \mu(v)$. Hence $\tau_u = \tau_v$ and so by Lemma 3 we have

$$\tau_{au}(T) = \tau_a(T) \diamond \tau_u(T \cdot a) = \tau_a(T) \diamond \tau_v(T \cdot a) = \tau_{av}(T)$$

for any $T \subseteq Q$, whence $\tau_{au} = \tau_{av}$, i.e. $\mu(au) = \mu(av)$. Similarly the other cases follows from Lemma 2 and Equation (2). □

We are now ready to prove the main theorem of this section.

Theorem 5. *Let $I \subseteq \Sigma^*$ be an ideal language, then I is a strongly connected ideal language.*

Proof. Put $J = I^R$. Let $\mathscr{A}_J = \langle Q, \Sigma, \delta, q_0, \{s\} \rangle$ be the minimal DFA recognizing J and let μ be the map of Lemma 4 defined with respect to $\mathscr{A}_J$. We claim that the equivalence classes of the relation $\sim = (J \times J) \cap \mathrm{Ker}(\mu)$ form a reset right regular decomposition of J. From Lemma 4, $\mathrm{Ker}(\mu)$ has finite index, thus $\sim$ has also finite index. Since $J = \mathrm{Syn}(\mathscr{A}_J)$, for any $H \subseteq Q$ and $u \in J$ we have $H \cdot u = \{s\}$. Hence it is straightforward to check that $\tau_u = \tau_{uv}$ for any $v \in \Sigma^*$. Therefore the $\sim$-classes are right ideals and form a finite partition $\{J_i\}_{i \in F}$ of J. Furthermore, by Lemma 4, $\mathrm{Ker}(\mu)$ is a left congruences of Σ^*, and so, since J is an ideal, it is also a congruence on J, hence for any J_i and $a \in \Sigma$, we get $aJ_i \subseteq J_j$ for some $j \in F$. Thus condition i) of Definition 2 is satisfied and so $\{J_i\}_{i \in F}$ is a right regular

decomposition. We claim that also condition ii) is satisfied. Assume, contrary to our claim, that there are $i \in F$ and $v \in \Sigma^* \setminus J$ such that $vJ \subseteq J_i$. Write $H = Q \cdot v$. Since $\mathrm{Syn}(\mathscr{A}_J) = J$ we get $|H| > 1$. Thus let $t = \min\{|H \cdot r| : r \in \Sigma^* \text{ and } H \cdot r \neq \{s\}\}$ and let $S \in \{H \cdot r : r \in \Sigma^* \text{ and } |H \cdot r| = t\}$. Let $x \in \Sigma^*$ such that $H \cdot x = S$ and let $u = vx$. Note that $u \in \Sigma^* \setminus J$, $uJ \subseteq J_i$ and $Q \cdot u = S$ with $|S| = t$. Since $\mathrm{Syn}(\mathscr{A}_J) = J$ and $\mathscr{A}_J$ is a synchronizing automaton with zero, then there is a synchronizing word $w \in J$ with $|w| < \frac{n^2+n}{2} + 1$ where $n = |Q|$ (see [10]). Let T' be the last set of (S, w) and let w' be the maximal prefix of w such that $S \cdot w' = T'$. Thus, there is a letter $a \in \Sigma$ such that $w'a$ is a prefix of w and $|T'a| = 1$. We consider two mutually exclusive cases.

i) Suppose $|T' \cdot b| = 1$ for any $b \in \Sigma$. It is not difficult to check that $\mathcal{T}(Q, uw) = \mathcal{T}(Q, uw'a)$. Since $|\Sigma| > 1$ consider a letter $b \in \Sigma$ with $b \neq a$. Since $Q \cdot uw' = T'$ and $|T' \cdot b| = 1$, we also have $\mathcal{T}(Q, uw'bw) = \mathcal{T}(Q, uw'b)$. Since $uJ \subseteq J_i$ we have $uw, uw'bw \in J_i$ (being $w'bw \in J$). Hence we get
$$\mathcal{T}(Q, uw'a) = \mathcal{T}(Q, uw) = \mathcal{T}(Q, uw'bw) = \mathcal{T}(Q, uw'b)$$
In particular we get $\mathcal{T}(Q, uw'a)\langle\Sigma\rangle = \mathcal{T}(Q, uw'b)\langle\Sigma\rangle$, from which it follows $a = b$, a contradiction.

ii) Thus, we can assume that there is a letter $b \in \Sigma$, such that $|T' \cdot b| > 1$. Since $uw, uw'bw \in J_i$ (being $w, w'bw \in J$), we have $\mathcal{T}(Q, uw'bw) = \mathcal{T}(Q, uw)$. Hence, by Lemma 3 we have
$$\mathcal{T}(Q, uw) = \mathcal{T}(Q, uw'bw) = \mathcal{T}(Q, uw'b) \diamond \mathcal{T}(T, w)$$
with $T = T' \cdot b$. Since $|T'| = t$ is minimal and $|T| > 1$ we have $|T| = |T'| = t$, hence $\mathrm{Ind}(\mathcal{T}(Q, uw'b)) = \mathrm{Ind}(\mathcal{T}(T, w)) = t$. Therefore, by the previous equality and the definition of $\diamond$ we get
$$\mathcal{T}(Q, uw) = \mathcal{T}(Q, uw'bw) = \mathcal{T}(Q, uw'b) + \mathcal{T}(T, w)$$
In particular we have
$$\mathcal{T}(Q, uw)\langle Q\rangle = \mathcal{T}(Q, uw'bw)\langle Q\rangle = \mathcal{T}(Q, uw'b)\langle Q\rangle + \mathcal{T}(T, w)\langle Q\rangle \tag{3}$$
Furthermore, T' is the last set of $(Q, uw'a)$ and uw' is the maximal prefix of $uw'a$ such that $T' = Q \cdot uw'$, since $|T'| = |T|$ we have that T is the last set of $(Q, uw'b)$ and $uw'b$ is the maximal prefix of $uw'b$ with $T = Q \cdot uw'b$. Thus, by the definition of tail we have $\mathcal{T}(Q, uw'a)\langle Q\rangle = \mathcal{T}(Q, uw'b)\langle Q\rangle$. We have already observed that $\mathcal{T}(Q, uw) = \mathcal{T}(Q, uw'a)$, hence by (3)
$$\mathcal{T}(T, w)\langle Q\rangle = 0 \tag{4}$$
Let $0 = i_1 < i_2 < \ldots < i_\ell \leq |w|$ be the maximal set of indices such that $T = T \cdot w[0, i_j]$ for all $1 \leq j \leq \ell$. Therefore, by the definition of tail and (4) we have in particular
$$0 = \mathcal{T}(T, w)(T) = \ell \mod \frac{n^2+n}{2} + 1$$
Since $\ell \geq 1$ we have that ℓ is a multiple of $\frac{n^2+n}{2} + 1$. However $\ell \leq |w| < \frac{n^2+n}{2} + 1$, which is a contradiction.

Therefore $v \in J$ and this concludes the proof of the fact that $\{J_i\}_{i \in F}$ is a reset right regular decomposition. Hence $\{J_i^R\}_{i \in F}$ is a reset left regular decomposition and so by Theorem 3 I is a strongly connected ideal language. □

Corollary 3. *Let I be an ideal language such that I^R has state complexity n. Then there is a strongly connected synchronizing automata $\mathscr{B}$ with N states and $\mathrm{Syn}(\mathscr{B}) = I$ such that:*
$$N \leq m^{k2^n} \left(\sum_{t=2}^{n} m^{\binom{n}{t}} \right)^{2^n}$$
where $k = |\Sigma|$ and $m = \left(\frac{n^2+n}{2} + 1\right)$.

Proof. By Theorem 5 I has a reset left regular decomposition $\{I_i\}_{i\in F}$ with $|F| \leq |\operatorname{Hom}(2^Q, \mathbb{T})|$ where

$$\mathbb{T} = \biguplus_{t=2}^{n} \mathbb{Z}_m([2^Q]_t \uplus \Sigma)$$

Hence we get the bound

$$|F| \leq \left(\sum_{t=2}^{n} m^{\binom{n}{t}+k}\right)^{2^n} \leq m^{k2^n} \left(\sum_{t=2}^{n} m^{\binom{n}{t}}\right)^{2^n}$$

Take $\mathscr{B} = \mathcal{A}(\{I_i\}_{i\in F})$ where $\mathcal{A}(\cdot)$ is the correspondence in Theorem **??**. Then $\mathscr{B}$ has $|F|$ states and $\operatorname{Syn}(\mathscr{B}) = I$. □

This Corollary shows a double exponential upper bound for the number of states of the associated strongly connected automaton with respect to the state complexity of the reverse of the ideal language. This bound seems far from been tight, indeed at the cost of a slight complication to the proof it is possible to prove that it is enough to consider $m = \frac{k}{2} + \frac{n^2+n}{4} + 1$. This is a better bound that the one presented in Corollary 3 for $k \leq \frac{n^2+n}{2}$. We outline this strategy in the following remark.

Remark 1 *In the proof of Theorem 5 we take as $w = a_1 \dots a_k w'$, where w' is a synchronizing word of lenght less or equal to $\frac{n^2+n}{2}$ and $\Sigma = \{a_1, \dots, a_k\}$. Thanks to the prefix $a_1 \dots a_k$ of w, in point ii) it is easy to see that in $\mathcal{T}(T, w)\langle Q\rangle$ it appears at least onother element $T' \neq T$. Therefore at least one between $\mathcal{T}(T, w)(T), \mathcal{T}(T, w)(T')$, say the first one, satisfies*

$$1 \leq \mathcal{T}(T, w)(T) \leq \frac{|w|}{2} < \frac{k}{2} + \frac{n^2+n}{4} + 1$$

Since $\mathcal{T}(T, w)(T) = 0 \mod m$ we obtain again a contradiction.

Therefore it is quite natural to look for better general constructions than the one given in Theorem 5 or to to consider the same task in particular classes of ideal languages. For instance in [1] it is shown an algorithm that given a principal ideal $I = \Sigma^* w \Sigma^*$ with $|w| = n$ in inputs, it returns a strongly connected synchronizing automaton with $n+1$ states. Therefore in this case the bound is linear with respect to the state complexity of I^R although it is not known whether or not it is tight. Even more recently in [2] the authors prove that in the case I is finitely generated, there is always a strongly connected synchronizing automaton with at most $2^{\|I\|}$ states and this bound is tight for ideals of the form $\Sigma^{\geq n} = \{u \in \Sigma^* : |u| \geq n\}$ for any $n > 0$.

Similarly to [3], where the author has introduced the notion of reset complexity of an ideal I ($\operatorname{rc}(I)$) as the number of states of the smallest synchronizing automaton $\mathscr{A}$ with $\operatorname{Syn}(\mathscr{A}) = I$, we can also give a similar notion in the realm of strongly connected synchronizing automata/reset left regular decomposition. By Theorem 5 for any ideal languages I, the set $\mathcal{R}(I)$ of all the reset left regular decomposition of I is non-empty. Thus we can define the *reset regular decomposition complexity of I* as the integer

$$\operatorname{rdc}(I) = \min\{|F| : \{I_i\}_{i\in F} \in \mathcal{R}(I)\}$$

By the correspondence introduced in Theorem 3, $\operatorname{rdc}(I)$ is also the number of states of the smallest strongly connected synchronizing automaton with the set of reset words equal to I. Furthermore we have $\operatorname{rc}(I) \leq \operatorname{rdc}(I)$. In the context of left regular decompositions we can give an analogous notion. However, since for a given ideal I the minimal left (right) regular decomposition is always the trivial one $\{I\}$, in this case we define the *regular decomposition complexity of I* as

$$\operatorname{dc}(I) = \min\{|F| > 1 : \{I_i\}_{i\in F} \text{ is a left regular decomposition of } I\}$$

Note that $\operatorname{dc}(I) \leq \operatorname{rdc}(I)$ holds. The importance of the index $\operatorname{rdc}(I)$ can be also understood by the following theorem where we present a purely language theoretic restatement of Černý's conjecture.

Theorem 6. *Černý's conjecture holds if and only if for any ideal language I we have:*

$$\mathrm{rdc}(I) \geq \sqrt{\|I\|} + 1$$

where $\|I\| = \min\{|w| : w \in I\}$.

Proof. This a consequence of the fact that Černý's conjecture holds if and only if it holds for strongly connected automata and Proposition 4. □

Note that using the well known upper bound $(n^3 - n)/6$ (see [4]) for the shortest reset word of a synchronizing automaton, we have the lower bound $\mathrm{rdc}(I) \geq \sqrt[3]{6\|I\|}$. In general, a natural issue would be to study bounds for $\mathrm{rdc}(I)$, $\mathrm{dc}(I)$ depending on the state complexity of I or I^R. In particular the study of both upper and lower bounds of $\mathrm{rdc}(I)$ can be an interesting topic that can (maybe) shed some light on the Černý's conjecture. For instance, even a lower bound $\mathrm{rdc}(I) \geq \sqrt{\|I\|}/c$ for some constant $c > 0$ would be a major breakthrough for this conjecture and all the theory of synchronizing automata.

As we have already observed, Corollary 3 gives an upper bound to $\mathrm{rdc}(I)$ with respect to the state complexity of I^R . In case we consider $\mathrm{dc}(I)$ we obtain a better bound as it is shown in the following theorem.

Theorem 7. *Let I be an ideal language such that I^R has state complexity n. Then I has a left regular decomposition $\{I_i\}_{i\in F}$ with $|F| \leq n^{2^n}$. In particular, there is a strongly connected automata $\mathscr{B}$ with $I \subseteq \mathrm{Syn}(\mathscr{B})$ and with a number of states $\leq n^{2^n}$.*

Proof. Consider the above definitions with respect to the minimal DFA $\mathscr{A}_J = \langle Q, \Sigma, \delta, q_0, \{s\}\rangle$ recognizing $J = I^R$. With the notation of Lemma 4 let $\xi_J : J \to \mathrm{Hom}(2^Q, [1, |Q|])$ be the restriction of ξ to the ideal J. Since J is an ideal and by Lemma 4 we have that $\mathrm{Ker}(\xi_J)$ is a left congruence on J. Moreover, since $J = \mathrm{Syn}(\mathscr{A}_I)$ it is straightforward checking that $\gamma_u = \gamma_{uv}$ for any $v \in \Sigma^*$. Therefore the $\mathrm{Ker}(\xi_J)$-classes form a finite partition (being $\mathrm{Hom}(2^Q, [1, |Q|])$ finite) of right ideals. More precisely we have $J = \uplus_{i\in F} J_i$ where $F = \xi_J(J)$ and $J_i = \{u \in J : \xi_J(u) = i\}$ for $i \in F$ is a right ideal of Σ^*. Furthermore, since $\mathrm{Ker}(\xi_J)$ is a left congruence, for any J_i we have $aJ_i \subseteq J_j$ for some $j \in F$. Hence condition i) of Definition 2 is satisfied and so $\{J_i\}_{i\in F}$ is a right regular decomposition. Therefore $\{J_i^R\}_{i\in F}$ is a left regular decomposition of I with:

$$|F| \leq |\,\mathrm{Hom}(2^Q, [1, |Q|])| = n^{2^n}$$

since $|Q| = n$. The last statement is a consequence of Theorem 3. □

We now show that for a subclass of the class of ideal languages we can improve the bound of Corollary 3. First we need some definitions. Given a DFA $\mathscr{B} = \langle Q', \Sigma, \delta'\rangle$ with a sink state s, we say that $\mathscr{B}$ has a *funnel* $\overline{q} \in Q' \setminus \{s\}$ if $\delta'(q, a) = s$ for some $q \neq \overline{q}, s$ and $a \in \Sigma$ implies $q = \overline{q}$. In other words, every path going to the sink state passes from the state $\overline{q}$. We say that $\mathscr{D}$ is *free from funnels* whenever for any DFA $\mathscr{B}$ which is a sub-automaton[1] of $\mathscr{D}$, $\mathscr{B}$ has no funnel. We have the following theorem.

Theorem 8. *Let $I \subseteq \Sigma^*$ be an ideal language such that the minimal DFA $\mathscr{A}_{I^R} = \langle Q, \Sigma, \delta, q_0, \{s\}\rangle$ recognizing I^R is free from funnels. Let $|Q| = n$ be the state complexity of I^R, then I has a reset left regular decomposition $\{I_i\}_{i\in F}$ with $|F| \leq 2^{n^2 2^n}$. In particular, there is a strongly connected synchronizing automaton $\mathscr{B}$ with $I = \mathrm{Syn}(\mathscr{B})$ and with a number of states $\leq 2^{n^2 2^n}$.*

Proof. Consider the above definitions with respect to the minimal DFA $\mathscr{A}_J = \langle Q, \Sigma, \delta, q_0, \{s\}\rangle$ recognizing $J = I^R$. With the notation of Lemma 4 let $\psi_J : J \to \mathrm{Hom}(2^Q, \mathcal{L}(Q))$ be the restriction of ψ to the ideal $J = I^R$. Similarly to the proof of Theorem 7 it is possible to prove that the $\mathrm{Ker}(\psi_J)$-classes $J_i = \{u \in J : \psi_J(u) = i\}$ for $i \in F$ are right ideals and form a finite partition of J (since $\mathrm{Hom}(2^Q, \mathcal{L}(Q))$ is finite). Furthermore, since $\mathrm{Ker}(\psi_J)$ is a left congruence, also condition i) of

[1] A DFA sub-automaton.

Definition 2 is satisfied and so $\{J_i\}_{i\in F}$ is a right regular decomposition. We claim that also condition ii) is satisfied. Assume, by absurd, that there are $i \in F$ and $u \in \Sigma^* \setminus J$ such that $uJ \subseteq J_i$. From Lemma 2 we have $\lambda_{uv}(Q) = \lambda_u(Q) \star \lambda_v(Q \cdot u),\ \ \forall v \in J$ and with $|Q \cdot u| > 1$. Write $H = Q \cdot u$. Since $\psi(uJ) = \psi(J_i) = i$, it is easy to see that

$$\lambda_v(H) = \lambda_{v'}(H),\ \ \forall v, v' \in J \tag{5}$$

Fix a $v \in J$, note that $\{s\} \in \lambda_v(H)$ and let $S \in \lambda_v(H)$ be the last set of (H, v). Let x be a prefix of v such that $H \cdot x = S$. We claim that $|S| = 2$. Suppose, by absurd, that $|S| > 2$. Since $s \in S$, there are at least two different elements $q, q' \in S$ different from s. We show that the right languages of q and q' with respect to $\mathscr{A}_J$ coincide. Suppose that there is a $w \in \Sigma^*$ such that $q \cdot w = s$ but $q' \cdot w \neq s$. Thus by definition of λ, $\lambda_{xwv}(H)$ contains an element S' with $1 < |S'| < |S|$. Hence $\lambda_{xwv}(H) \neq \lambda_v(H)$ which contradicts (5) ($xwv \in J$ since J is an ideal). Therefore q, q' are equal in the minimal DFA $\mathscr{A}_J$, which is a contradiction. Hence $S = \{q, s\}$. Consider the sub-automaton $\mathscr{B} = \langle Q', \Sigma, \delta\rangle$ of $\mathscr{A}_J$ induced by S, i.e. $Q' = S \cdot \Sigma^*$. It is obvious that $\mathscr{B}$ is a DFA, we claim that $q \in S$ is a funnel for $\mathscr{B}$. Indeed, suppose that there is a $q' \neq q, s$ and $a \in \Sigma$ such that $q' \cdot a = s$. By definition of $\mathscr{B}$ there is a word $r \in \Sigma^*$ such that $q \cdot r = q'$. Consider the word $v' = xrav$ (recall $H \cdot x = S$). Clearly $v' \in J$. It is not difficult to check that $\lambda_{v'}(H)$ contains the set $\{q', s\} \neq S$. However this contradicts (5). Thus $q' = q$, and so q is a funnel of $\mathscr{B}$, contradicting the statement of the theorem. Hence $u \in J$ and so $\{J_i^R\}_{i\in F}$ is a reset right regular decomposition for I. By the upper bound (1) we obtain $|F| \leq |\operatorname{Hom}(2^Q, \mathcal{L}(Q))| = 2^{n^2 2^n}$. The last statement is a consequence of Theorem 3. □

We now characterize the ideals such that the minimal DFA recognizing them are free from funnels. We say that $J \subseteq \Sigma^*$ is a *free funnel ideal* whenever there is no word $u \in \Sigma^*$ with $u \notin J$ and a maximal subset $\Sigma' \subseteq \Sigma$ such that $u\Sigma' \subseteq J$ and the following closure property holds:

$$\text{if } uv \notin J \text{ and } uv\Sigma'' \subseteq J, \text{ then } \Sigma'' = \Sigma' \tag{6}$$

Theorem 9. *$J \subseteq \Sigma^*$ is a free funnel ideal if and only if $\mathscr{A}_J$ is free from funnels.*

Proof. Assume J is not a free funnel ideal, hence there is a regular language L and $\Sigma' \subseteq \Sigma$ such that $L\Sigma' \subseteq J$ and condition (6) holds. We prove that the minimal DFA $\mathscr{A}_J = \langle Q, \Sigma, \delta, q_0, \{s\}\rangle$ recognizing J is not free from funnels. Let $u \in L$ and consider the sub-automaton $\mathscr{D} = \langle q_0 \cdot u\Sigma^*, \Sigma, \delta\rangle$ of $\mathscr{A}_J$. We claim $\overline{q} = q_0 \cdot u$ is a funnel for $\mathscr{D}$. Let $q \in q_0 \cdot u\Sigma^*$ with $q \neq \overline{q}, s$ such that $q \cdot a = s$ for some $a \in \Sigma$, and let $v \in \Sigma^*$ such that $q = q_0 \cdot uv$. By the maximality of Σ' we have $\overline{q} \cdot \Sigma'' = \{s\}$ if and only if $\Sigma'' = \Sigma'$, we claim that the same holds for q. Since $\mathscr{A}_J$ recognizes J, we get $uv \notin J$, and $q \cdot \Sigma'' = \{s\}$ if and only if $uv\Sigma'' \subseteq J$, hence, by condition (6), we have $\Sigma'' = \Sigma'$. Therefore, $\overline{q}, q$ have the same right language with respect to $\mathscr{A}_J$. Hence, by the minimality of $\mathscr{A}_J$, we get $\overline{q} = q$, i.e. $\overline{q}$ is a funnel for $\mathscr{D}$.

Conversely, assume $\mathscr{A}_J = \langle Q, \Sigma, \delta, q_0, \{s\}\rangle$ is not free from funnels, and let $\mathscr{D} = \langle Q', \Sigma, \delta, \{s\}\rangle$ be a sub-automaton of $\mathscr{A}_J$ with a funnel $\overline{q}$. Since $\mathscr{A}_J$ is minimal, there is a $v \in \Sigma^*$ with $q_0 \cdot v = \overline{q}$. Thus the set

$$\mathcal{S} = \min\{Q \cdot vw : q_0 \cdot vw \neq s, w \in \Sigma^*\}$$

is non-empty, and let $v' \in \Sigma^*$ such that $S = Q \cdot vv' \in \mathcal{S}$ with $|S|$ minimal. We claim $|S| = 2$. Indeed, suppose that there are two different states $q, q' \in S \setminus \{s\}$ with $q = q_0vv'$. We prove that the right languages of q, q' with respect to $\mathscr{A}_J$ are equal. Assume that there is a word w such that $q' \cdot w = s$, but $q \cdot w \neq s$. Then $1 < |S \cdot w| < |S|$ and $q_0 \cdot vv'w \neq s$, which contradicts the choice of S. Conversely, suppose that there is a word w such that $q \cdot w = s$, but $q' \cdot w \neq s$. Thus, $q_0 \cdot vv'w = s$, hence we have

$$vv'w \in L[\mathscr{A}_J] = J = \operatorname{Syn}(\mathscr{A}_J)$$

Thus $q' \cdot w \in S \cdot w = Q \cdot vv'w = \{s\}$, a contradiction. Therefore, by the minimality of $\mathscr{A}_J$, we get $q' = q$. Hence $|S| = 2$ and so $S = \{q, s\}$ where $q = q_0vv'$. Since $q \in Q'$ and $\overline{q}$ is a funnel for $\mathscr{D}$, it is easy to see that there is a word w such that $\overline{q} = q_0vv'w$. Write $u = vv'w$, and let

$$\Sigma' = \{a \in \Sigma : \overline{q} \cdot a = s\}$$

Clearly $u \notin J$ and it is straightforward to check then $u\Sigma' \subseteq J$ and Σ' is maximal with respect to the property $u\Sigma'' \subseteq J$. We prove that condition (6) holds for u. Assume $ur \notin J$, $ur\Sigma'' \subseteq J$ for some $r \in \Sigma^*$. Since $\overline{q}$ is a funnel we have $q_0 \cdot ur = \overline{q}$, moreover $ura \in J$ if and only if $\overline{q} \cdot a = s$ if and only if $a \in \Sigma'$, i.e. $\Sigma'' = \Sigma'$. Therefore, condition (6) holds and so J is not a free funnel ideal. □

Open Problems

We list some open problems originated by the previous results, I stands for an ideal language.

1. Give a tight upper bound of $\mathrm{rdc}(I)$ ($\mathrm{dc}(I)$) with respect to the state complexity of I^R or I.
2. In case I is finitely generated is true that $\mathrm{rdc}(I) \geq \|I\| + 1$? The same problem in case I is a principal ideal language has been raised in [1]. This would give a better bound for the shortest synchronizing word for the class of finitely generated synchronizing automata with respect to the bound obtained in [9].
3. The proof of Theorem 5 uses the minimal DFA recognizing I^R. Is there a proof using another automaton associated to I?
4. Recall that $\mathcal{R}(I)$ is the set of all the reset left regular decompositions of I and the order of a decomposition $\mathcal{I} \in \mathcal{R}(I)$ is just the cardinality $|\mathcal{I}|$. We denote by $\mathcal{R}_k(I)$ the set of reset left regular decompositions of I of order $k \geq 1$.
   A quite natural question is whether $\sup\{k \geq 1 : \mathcal{R}_k(I) \neq \emptyset\} = \infty$ or not? In particular, what is the case if we consider I in the class of finitely generated ideals or in the even smaller class of principal ideals? This would answer to the question whether or not, given a principal ideal P, there are arbitrary big strongly connected synchronizing automata having a P as set of reset words.
5. By Theorem 3, a naive way to calculate $\mathcal{R}_k(I)$ can be accomplished by building all the strongly connected synchronizing automata with k states and checking if their set of reset words coincides with I. Thus, it is natural to ask whether there is a more "efficient" way to perform this task without passing from the construction of all the automata with k states.

Acknowledgments

The authors thank E. Pribavkina for pointing out the unary case alphabet in Corollary 1. We also acknowledge M. Berlinkov for the useful comments and suggesting the strategy outlined in Remark 1 which improves the bound of Corollary 3 for ideals I on alphabets Σ with $|\Sigma| \leq \frac{n^2+n}{2}$, where n is the state complexity of I^R.

References

1. Gusev, V., Maslennikova, M., Pribavkina, E.: Principal ideal languages and synchronizing automata. in V. Halava, J. Karhumaki, Y. Matiyasevich (eds.) RuFiDimII, TUCS Lecture Notes 17 (2012)
2. Gusev, V., Maslennikova, M., Pribavkina, E.: Finitely generated ideal languages and synchronizing automata. In: J. Karhumäki, L. Zamboni (eds.) Proc. WORDS 2013, Lecture Notes in Computer Science, vol. 8079. Springer Berlin / Heidelberg (2013)
3. Maslennikova, M.: Reset complexity of ideal languages. In: M. Bieliková, G. Friedrich, G. Gottlob, S. Katzenbeisser, R. Špánek, G. Turán (eds.) Int. Conf. SOFSEM 2012, Proc. Volume II, Institute of Computer Science Academy of Sci- ences of the Czech Republic. pp. 33–44 (2012)
4. Pin, J.E.: On two combinatorial problems arising from automata theory. Ann Discrete Math. 17, 535–548 (1983)
5. Pribavkina, E., Rodaro, E.: Finitely generated synchronizing automata. In: Language and Automata Theory and Applications, Lecture Notes in Computer Science, vol. 5457, pp. 672–683. Springer Berlin / Heidelberg (2009)
6. Pribavkina, E., Rodaro, E.: State complexity of prefix, suffix, bifix and infix operators on regular languages. In: Gao, Y., Lu, H., Seki, S., Yu, S. (eds.) Developments in Language Theory, Lecture Notes in Computer Science, vol. 6224, pp. 376–386. Springer Berlin / Heidelberg (2010)

7. Pribavkina, E., Rodaro, E.: Recognizing synchronizing automata with finitely many minimal synchronizing words is pspace-complete. In: Models of Computation in Context, Lecture Notes in Computer Science, vol. 6735, pp. 230–238. Springer Berlin / Heidelberg (2011)
8. Pribavkina, E.V., Rodaro, E.: State complexity of code operators. International Journal of Foundations of Computer Science 22(07), 1669–1681 (2011)
9. Pribavkina, E.V., Rodaro, E.: Synchronizing automata with finitely many minimal synchronizing words. Information and Computation 209(3), 568 – 579 (2011), http://www.sciencedirect.com/science/article/pii/S0890540110002063
10. Rystsov, I.: Reset words for commutative and solvable automata. Theoretical Computer Science 172(1–2), 273 – 279 (1997), http://www.sciencedirect.com/science/article/pii/S0304397596001363
11. Černý, J.: Poznámka k homogénnym eksperimentom s konečnými automatami [in slovak]. Mat.-Fyz. Čas. Slovensk. Akad. Vied. 14, 208–216 (1964)
12. Volkov, M.V.: Synchronizing automata and the Černý conjecture. In C. Martín-Vide, F. Otto, H. Fernau (eds.), Languages and Automata: Theory and Applications. LATA 2008, Lect. Notes Comp. Sci, Berlin, Springer 5196, 11–27 (2008)