LOSSY CHANNEL SYSTEMS (LCS)

Def A Lossy Channel System (LCS) is a tuple $(Q, q_0, C, M, \rightarrow)$ where
1. Q is a finite set of control states
2. $q_0 \in Q$ is the initial control state
3. C is the finite set of channels
4. M is the finite set of messages
5. $\rightarrow \subseteq Q \times OP \times Q$ where $OP := C \times \{\underset{\text{send}}{!}, \underset{\text{receive}}{?}\} \times M$

We write $q \xrightarrow{op} q'$.

Explanation
$c?m$ receive m from c
$c!m$ send m to c

Def A configuration of a LCS is a pair $\gamma = (q, W) \in Q \times \underbrace{(C \rightarrow M^*)}_{(M^*)^C}$.

W assigns to each $c \in C$ a sequence of messages $W(c)$. The initial config. is $\gamma_0 := (q_0, \varepsilon)$ where ε means $W(c) = \varepsilon$ for all $c \in C$.

Lemma: Let $(Q, \leq)$ be a wqo. For $u = u_1 \cdots u_m$, $v = v_1 \cdots v_n \in Q^*$ and $m \leq n$ we write $u \leq^* v$ if there are $1 \leq i_1 < \ldots < i_m \leq n$ with $u_j \leq v_{i_j}$ for all $j = 1, \ldots, m$. Then $(Q^*, \leq^*)$ is a wqo.

(Higman 1952)

Proof: Sheet 06 Ex02.

We call the order of the previous lemma subword-ordering. This gives rise to ordering among configurations of a LCS: We write

$$(q, W) \preccurlyeq (q', W') \iff q = q' \text{ and } W(c) \leq^* W'(c) \text{ for all } c \in C$$

Corrollary $(Q \times (M^*)^C, \preccurlyeq)$ is a wqo.

Notation An upated is $[c := x]$ where $c \in C$ and $x \in M^*$

$$W[c := x](c') = \begin{cases} x & \text{if } c' = c \\ W(c') & \text{otherwise} \end{cases}$$

Def The semantics of a LCS $L = (Q, q_0, C, M, \rightarrow)$ is defined by a transition relation $\rightarrow \subseteq (Q \times M^{*C}) \times (Q \times M^{*C})$ among configurations as follows:

$$(q_1, W[c := m.\sigma]) \longrightarrow (q_2, W[c := \sigma]) \quad \text{if } q_1 \xrightarrow{c?m} q_2$$
$$(q_1, W[c := \sigma]) \longrightarrow (q_2, W[c := \sigma.m]) \quad \text{if } q_1 \xrightarrow{c!m} q_2$$
$$\gamma_1' \longrightarrow \gamma_2' \quad \text{if } \gamma_1' \succcurlyeq \gamma_1 \longrightarrow \gamma_2 \succcurlyeq \gamma_2'$$

for some configuration $\gamma_1, \gamma_2 \in Q \times M^{*C}$.

Remark If we have $(q_1, W[c := \sigma.m.\sigma'])$ and $q_1 \xrightarrow{c?m} q_2$ $(m \notin \sigma)$ then there exists $(q_1, W[c := \sigma.m.\sigma']) \longrightarrow (q_1, W[c := m.\sigma'])$ by the last rule.

Theorem Consider the LCS $(Q, q_0, C, M, \rightarrow)$. The transition system $(Q \times M^{*C}, \rightarrow, \sqsubseteq)$ is a WSTS.

Proof sheet 06 ex 01

To instantiate the Abdulla's backwards search to LCS we need to come up with a suitable minpre function. Let $(Q\, q_0, C, M, \rightarrow)$ be a LCS then we define $\text{minpre}: Q \times M^{*C} \longrightarrow \mathcal{P}_{fin}(Q \times M^{*C})$

$$\text{minpre}(q_2, W_2) := \min(T)$$

where T is the smallest set such that

$(q_1, W_1) \in T$ if $q_1 \xrightarrow{c!m} q_2$ and $W_2 := W_1[c := W_1(c).m]$

$(q_1, W_1) \in T$ if $q_1 \xrightarrow{c!m} q_2$ and the last message in $W_2(c)$ is NOT m or $W_2(c)$ is empty

$(q_1, W_1) \in T$ if $q_1 \xrightarrow{c?m} q_2$ and $W_1 = W_2[c := m.W_2(c)]$

To instantiate the Forward Search to LCS more preparations are necessary: We need to find a way to represent the ideals of LCS and then we have to show that they yield to a post-effective completion.

Theorem (Haines '69) Let $\mathcal{L} \subseteq \Sigma^*$ be any language. $\mathcal{L}\downarrow$ is regular.

Proof: Recall that the complement of a dwcl set is upcl. (sheet 07 ex01). Since $\leq$ is a wqo, upcl. sets can be represented as the upcl. of the finite set of the minimal elements.

$$\overline{\mathcal{L}\downarrow} = \underbrace{\min(\overline{\mathcal{L}\downarrow})}_{\{\omega_1, \dots, \omega_n\}}\uparrow = \bigcup_{w \in \min(\overline{\mathcal{L}\downarrow})} \{\omega\}\uparrow$$

We know that

$$\underbrace{\{\omega\}\uparrow}_{\text{say } \omega = a_1 \dots a_k,\ a_i \in \Sigma} = \Sigma^* a_1 \Sigma^* a_2 \Sigma^* \dots \Sigma^* a_k \Sigma^*$$

is regular. By closure of Reg_Σ under finite unions and complement we have:

$$\mathcal{L}\downarrow = \overline{\overline{\mathcal{L}\downarrow}} = \overline{\bigcup_{w \in \min(\overline{\mathcal{L}\downarrow})} \{\omega\}\uparrow}$$

Def Simple Regular Expressions

$e ::= (a + \varepsilon) \mid (a_1 + \ldots + a_m)^*$ ATOMIC ELEMENTS

$p ::= \varepsilon \mid e \cdot p$ PRODUCTS (~ Ideals!

$r ::= \emptyset \mid p + r$ SRE

Remark: The halting problem of a TM can be reformulated in the following way:

$$TM \text{ halts} \Leftrightarrow \mathcal{L}(TM) = \emptyset \Leftrightarrow \varepsilon \in \underbrace{\mathcal{L}(TM)\downarrow}_{\text{regular after theorem}}$$

Now, the question whether the halting problem must then be decidable comes up. This is not the case: While we can say there must one dwd. set which contains ε, we can not compute which one it actually is. So the halting problem is still undecidable and everything fits together.

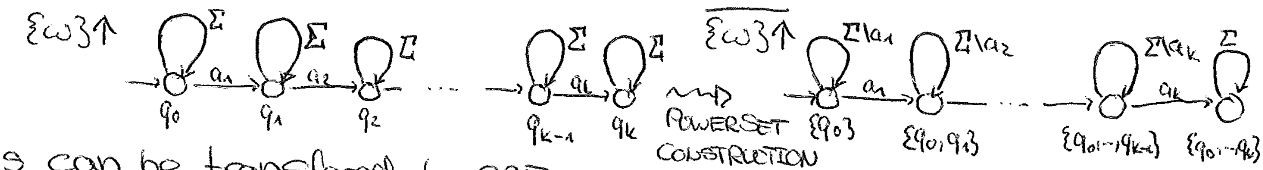
Theorem (Bouajjani '98) $\mathcal{L} \subseteq \Sigma^*$ is dwd. if and only if it is simple regular.

Proof ($\Leftarrow$) $\mathcal{L}(r)$ is dwd. for every $r \in SRE$ (sheet 08 ex 03)

($\Rightarrow$) Let $\mathcal{L} \subseteq \Sigma^*$ be dwd.

$$\mathcal{L} = \overline{\overline{\mathcal{L}}} = \overline{\bigcup_{w \in \min\{\overline{\mathcal{L}}\}} \{w\}\uparrow} = \bigcap_{w \in \min(\overline{\mathcal{L}})} \overline{\{w\}\uparrow}$$

So we have to represent only $\overline{\{w\}\uparrow}$ as SRE. Wlog $w = a_1 \ldots a_k$. From the perspective of AUTOMATA we have:



This can be transfered to SRE:

$$(\Sigma \setminus a_1)^* (a_1 + \varepsilon)(\Sigma \setminus a_2)^* (a_2 + \varepsilon) \ldots (\Sigma \setminus a_k)^* (a_k + \varepsilon)(\Sigma)^*$$

See Meyer's Lecture Notes for more details

Now, we will use the previous theorem to establish a post-effective completion for LCS.

Recall that we have to show the three following properties:

① Ideals(S) are recursive enumerable.

② $I \subseteq J$ is decidable for $I, J \in \text{Ideals}(S)$

③ $\widehat{post}(I) := \{J_i \mid post(I)\downarrow = \underbrace{J_1 \cup \ldots \cup J_k}_{\text{canonical decomposition of maximal ideals}}\}$ is decidable

The set of configurations is

$$S = Q \times \underbrace{\mathcal{M}^* \times \dots \times \mathcal{M}^*}_{|C|} \qquad \text{with } Q, \mathcal{M} \text{ finite}$$

<u>Lemma</u>: $\text{Ideals}(S_1 \times S_2) = \text{Ideals}(S_1) \times \text{Ideals}(S_2)$

① $\text{Ideals}(S) = \text{Ideals}(Q) \times \text{Ideals}(\mathcal{M}^*)^{|C|}$
$\qquad\qquad = Q \times SRE(\mathcal{M})^{|C|}$

Since Q and $\mathcal{M}$ is finite and since we represent $\text{Ideals}(\mathcal{M}^*)$ as SRE we can enumerate the $\text{Ideals}(S)$ recursively.

② We define

$$\mathcal{L}(q, r_1, \dots, r_k) := \{(q, w_1, \dots, w_k) \mid w_i \in \mathcal{L}(r_i)\ \forall i \in \{1, \dots, k\}\}$$

So we have the following equivalence

$$\mathcal{L}(q, r_1, \dots, r_k) \subseteq \mathcal{L}(q', r_1', \dots, r_k') \Leftrightarrow q = q' \wedge \forall i \in \{1, \dots, k\}\ \mathcal{L}(r_i) \subseteq \mathcal{L}(r_i')$$

Hence we only need a decision procedure for $\mathcal{L}(p) \subseteq \mathcal{L}(p')$; but first note that

$\mathcal{L}(\varepsilon) \subseteq \mathcal{L}(p)$ is always true
$\mathcal{L}(p) \not\subseteq \mathcal{L}(\varepsilon)$ if $p \neq \varepsilon$

<u>Remark</u>:
- $\mathcal{L}(r) \subseteq \mathcal{L}(r')$ is decidable because $SRE_\Sigma \subseteq REG_\Sigma$
- The algorithm on the left side shows that for SRE_Σ the check is more efficient: poly time instead of PSPACE

For atomic expressions:

$\mathcal{L}(a + \varepsilon) \subseteq \mathcal{L}(A^*)$ <u>iff</u> $a \in A$
$\mathcal{L}(A^*) \subseteq \mathcal{L}(B^*)$ <u>iff</u> $A \subseteq B$
$\mathcal{L}(A^*) \not\subseteq \mathcal{L}(a + \varepsilon)$

Now for two products:

$$\mathcal{L}(e_1 \cdot p_1) \subseteq \mathcal{L}(e_2 \cdot p_2) \text{ \underline{iff} } \begin{cases} \mathcal{L}(e_1 \cdot p_1) \subseteq \mathcal{L}(p_2) & \text{if } \mathcal{L}(e_1) \not\subseteq \mathcal{L}(e_2) \\ \mathcal{L}(p_1) \subseteq \mathcal{L}(p_2) & \text{if } \mathcal{L}(e_1) = \mathcal{L}(e_2) = \mathcal{L}(a + \varepsilon) \\ \mathcal{L}(p_1) \subseteq \mathcal{L}(e_2 \cdot p_2) & \text{if } \mathcal{L}(e_1) \subseteq \mathcal{L}(e_2) = \mathcal{L}(A^*) \end{cases}$$

③ $\widehat{post}$ is decidable for LCS

We are given an ideal $\mathcal{L}((q, p_1, \dots, p_k))$. So we need to define $p \oplus op$ for $op \in \{?a, !a\}_{a \in \mathcal{M}}$

$$(e \cdot p) \oplus ?a = \begin{cases} ep & \text{if } e = A^* \text{ and } a \in A \\ p & \text{if } e = (a + \varepsilon) \\ p \oplus ?a & \text{otherwise} \end{cases}$$

$$\varepsilon \oplus ?a = \emptyset$$

$$p \oplus !a = p(a + \varepsilon)$$

Question: Given a wqo $(X, \leq)$ with an effective completion. can we describe Ideals(X^*) in terms of Ideals(X)?

First recall: X^* is wqo by $\leq_*$ defined as $w \leq_* w'$ iff $\exists w''$ subword of w' such that $\forall i$: $w(i) \leq w''(i)$ and $|w| = |w''|$

So yes it is possible by the following definition:

Def The simple regular expressions over X SRE(X) can also defined as

$e ::= (a + \epsilon) \mid A^*$ $\quad a \in$ Ideals(X) and $A \subseteq$ Ideals(X) finite

$p ::= \epsilon \mid e \cdot p$ $\quad$ products

$r ::= \emptyset \mid p + r$

Moreover, one can prove a correspondence between the ideals of X and the products of SRE(X)

Theorem: Let $(X, \leq)$ be wqo. Then we have

$$\text{Ideals}(X^*) = \{\mathcal{L}(p) \mid p \text{ product of SRE}(X)\}$$

and

$$\text{DwdSets}(X^*) = \{\mathcal{L}(r) \mid r \in \text{SRE}(X)\}$$

Proof sheet 08 ex 03.

Theorem: Let $(\hat{X}, \xrightarrow{\wedge}, \subseteq)$ be an effective completion of $(X, \rightarrow, \leq)$. Then $\mathcal{L}(p) \subseteq \mathcal{L}(p')$ is decidable for products p, p' in SRE(X).