IRP ∩ LSI IS NOT RECURSIVELY ENUMERABLE

TETSUYA ISHIU

Throughout this paper, let Σ be a fixed finite set of alphabets.

Definition 0.1. For a language L over Σ and $n \geq 0$, let $N(L, n) = \mathrm{card}\{w \in L \mid |w| = n\}$. We say that L is *slender* if and only if there exists a k such that $N(L, n) \leq k$ for every $n \in \mathbb{N}$.

Theorem 0.2 (M. Andraşiu, J. Dassow, Gh. Păun, A. Salomaa [1])**.** *For every regular language L, the slenderness of L is decidable.*

It is easy to see that the union of two slender languages is slender.

Theorem 0.3. *Moreover, if $\mathcal{G}$ is a set of recursive functions from Σ^* into Σ^*,*

IRP ∩ LSI is not recursively enumerable.

Proof. Let $\mathcal{R}$ be the set of all regular languages. Let $\langle L_n : n \in \mathbb{N}\rangle$ be a recursive enumeration of all regular languages. Suppose that $\langle g_n : n \in \mathbb{N}\rangle$ is a recursive enumeration of IRP.

We shall build a function $f \in \mathrm{IRP}$ so that $f \neq g_n$ for every $n \in \mathbb{N}$. This will be a contradiction.

Inductively, we shall define an increasing sequence $\langle f_n : n \in \mathbb{N}\rangle$ of partial functions from Σ^* into Σ^*, and an increasing sequence $\langle M_n : n \in \mathbb{N}\rangle$ of regular languages such that for every $n \in \mathbb{N}$,

(i) f_n is a bijection from M_n onto M_n,
(ii) $f_{n+1} \neq g_n \restriction M_{n+1}$,
(iii) either $L_n \subseteq M_{n+1}$ or $(\Sigma^* \setminus L_n) \subseteq M_{n+1}$,
(iv) M_{n+1} is not co-slender.
(v) for all but finitely many $x \in M_n$, $f(x) = x$, and
(vi) for every $x \in M_n$, $|f(x)| = |x|$.

First let $f_0 = M_0 = \varnothing$. Suppose that we have defined f_n and M_n. Since M_n is not co-slender, there exist two distinct element x_n and x'_n of $\Sigma^* \setminus M_n$ that have the same length. Consider $M_n \cup L_n$. If it is not co-slender, then let $M_{n+1} = M_n \cup L_n \cup \{x_n, x'_n\}$. Suppose not, i.e. $M_n \cup L_n$ is co-slender. It means that $\Sigma^* \setminus (M_n \cup L_n)$ is slender. Note that $\Sigma^* \setminus (M_n \cup L_n) = (\Sigma^* \setminus M_n) \cap (\Sigma^* \setminus L_n)$. Since M_n is not co-slender, $\Sigma^* \setminus M_n$ is not slender. We have

$$\Sigma^* \setminus M_n = ((\Sigma^* \setminus M_n) \cap L_n) \cup ((\Sigma^* \setminus M_n) \cap (\Sigma^* \setminus L_n))$$

Date: May 13, 2012.

This material is based upon work supported by the National Science Foundation under Grant No. 0700983.

Since $\Sigma^*\setminus M_n$ is not slender and $(\Sigma^*\setminus M_n)\cap(\Sigma^*\setminus L_n)$ is slender, $(\Sigma^*\setminus M_n)\cap L_n$ is not slender. Note

$$\begin{aligned}\Sigma^* \setminus ((\Sigma^* \setminus M_n) \cap L_n) &= (\Sigma^* \setminus (\Sigma^* \setminus M_n)) \cup (\Sigma^* \setminus L_n)\\ &= M_n \cup (\Sigma^* \setminus L_n)\end{aligned}$$

So, $M_n \cup (\Sigma^* \setminus L_n)$ is not co-slender. let $M_{n+1} = M_n \cup (\Sigma^* \setminus L_n) \cup \{x_n, x'_n\}$.

Now, define $f_{n+1} : M_{n+1} \to M_{n+1}$ as follows. If $g_n(x_n) \neq x_n$, then

$$f_{n+1}(x) = \begin{cases} f_n(x) & \text{if } x \in M_n \\ x & \text{if } x \notin M_n \end{cases}$$

If $g_n(x_n) = x_n$, then

$$f_{n+1}(x) = \begin{cases} f_n(x) & \text{if } x \in M_n \\ x & \text{if } x \notin M_n \\ x'_n & \text{if } x = x_n \\ x_n & \text{if } x = x'_n \end{cases}$$

That is, for every $x \in M_{n+1} \setminus M_n$, set $f_{n+1}(x) = x$ except $x = x_n, x'_n$. If $g_n(x_n) \neq x_n$, then let $f_{n+1}(x_n) = x_n$ and $f_{n+1}(x'_n) = x'_n$. It makes $f_{n+1} \neq g_n \restriction M_{n+1}$. If $g_n(x_n) = x_n$, then we make $f_{n+1}(x_n)$ and $g_n(x_n)$ different by letting $f_{n+1}(x_n) = x'_n$ and $f_{n+1}(x'_n) = x_n$.

Let $f = \bigcup_{n\in\mathbb{N}} f_{n+1}$.

Claim 1. For every regular language L, there exists an $n \in \mathbb{N}$ such that either $L \subseteq M_n$ or $\Sigma^* \setminus L \subseteq M_n$.

$\vdash$ There exists an $n \in \mathbb{N}$ such that $L_n = L$. Then, by (iii), either $L \subseteq M_{n+1}$ or $\Sigma^* \setminus L \subseteq M_{n+1}$. $\dashv$ (Claim 1)

Claim 2. The domain of f is Σ^*.

$\vdash$ Let $x \in \Sigma^*$. We shall show that $x \in M_n$ for some $n \in \mathbb{N}$. Consider the language $L = \{x\}$. By Claim 1, there exists an $n \in \mathbb{N}$ such that either $L \subseteq M_n$ or $\Sigma^* \setminus L \subseteq M_n$. If $L \subseteq M_n$, it clearly implies $x \in M_n$. If $\Sigma^* \setminus L \subseteq M_n$, then trivially M_n is co-slender. This is a contradiction. $\dashv$ (Claim 2)

Claim 3. For every $n \in \mathbb{N}$, $f \neq g_n$.

$\vdash$ Since $f(x_n) \neq g_n(x_n)$. $\dashv$ (Claim 3)

Claim 4. f is IRP.

$\vdash$ Let L be a regular language. By Claim 1, there exists an $n \in \mathbb{N}$ such that either $L \subseteq M_n$ or $\Sigma^* \setminus L \subseteq M_n$.

First suppose that $L \subseteq M_n$. Recall that $f \upharpoonright M_n = f_n$ is identity at all but finitely many points. Then, $f^{-1}(L)$ and L differ only at finitely many strings. Hence, $f^{-1}(L)$ is regular.

Conversely, suppose that $\Sigma^* \setminus L \subseteq M_n$. By the same argument, $f^{-1}(\Sigma^* \setminus L)$ is regular. Since f is a bijection, $f^{-1}(\Sigma^* \setminus L) = \Sigma^* \setminus (f^{-1}L)$. Since $f^{-1}(L)$ is the complement of a regular language, $f^{-1}(L)$ is regular. $\dashv$ (Claim 4)

$\square$(Theorem 0.3)

Corollary 0.4. *$MTT^* \subsetneq IRP$.*

References

1. Mircea Andraşiu, Gheorghe Păun, Jürgen Dassow, and Arto Salomaa, *Language-theoretic problems arising from Richelieu cryptosystems*, Theoret. Comput. Sci. **116** (1993), no. 2, 339–357. MR MR1231949 (94i:68149)