Journal of Automata, Languages and Combinatorics **14** (2009) 2, 187–198

AN EFFICIENT DERIVATION METHOD FOR DT0L SYSTEMS AND A MEASURE OF DERIVATION COMPLEXITY

TAISHIN Y. NISHIDA
Faculty of Engineering, Toyama Prefectural University
Kurokawa 5180, Imizu-shi, 939-0398 Toyama, Japan
e-mail: nishida@pu-toyama.ac.jp

ABSTRACT

An efficient derivation method for DT0L systems is proposed. The method, called a lazy derivation, makes two morphisms from a morphism applied at every step. One morphism simulates the original derivation but it is an identity over a set of letters on which every morphism of the system is a bijective coding. The other morphism recovers the original derivation. Generative complexities of a word by normal and lazy derivations are defined. It is shown that, for any integer $k \geq 1$, there is a DT0L system such that the generative complexities per letter of a word w by normal and lazy derivations are $\Theta(|w|^{\frac{1}{k}})$ and $\Theta(1)$, respectively.

Keywords: DT0L systems, efficient derivation, generative complexity

1. Introduction

A language is said to be slender if there exists a positive integer k such that, for every nonnegative integer l, the language has at most k words of length l. M. Andraşiu, et. al. have given the notion of the slender language and pointed out the possibility that slender languages can generate key streams for a cryptosystem [1]. A series of investigations have followed the pioneering work [2, 3, 4, 5, 7, 8]. Among them, T. Nishida has shown that a controlled PDT0L system can generate a cryptographic secure slender language [6]. This is the second and more practical application of L systems to cryptography[1].

The cryptosystem suggested in [6] uses words generated by a PDT0L system as the pseudo-random key stream of the stream cipher. Once a key stream is generated, the stream cipher encrypts or decrypts a message quite rapidly, linearly proportional to the length of the message. Hence it is obvious that encryption and decryption times of the system depend on the time to generate words in a PDT0L language. We note that a key stream must have a length no less than that of the message to be encrypted or decrypted.

[1]The first one is the public-key system using a DT0L system which has been suggested by A. Salomaa [11, pp. 166–174].