Chapter 7
The Fifth and the Sixth Order Gopala Hemachandra Representations and the Use of These Representations in Symmetric Cryptography

Çağla Çelemoğlu
Ondokuz Mayis University, Turkey

Ayşe Nalli
https://orcid.org/0000-0002-0489-3649
Karabük University, Turkey

ABSTRACT

We all know that every positive integer has a unique Fibonacci representation, but some positive integers have multiple Gopala Hemachandra (GH) representations, or some positive integers haven't any GH representation. Here, the authors found the first k-positive integer k=(3 2^((m-1))-1) for which there is no Zeckendorf's representation for Gopala Hemachandra sequence whose order m. Thus, the authors formulated the first positive integer whose Zeckendorf's representation can't be found in terms of its order. The authors also described the fourth, the fifth, and the sixth order GH representation of positive integers and obtained the fifth and the sixth order GH representations of the first 26 positive integers uniformly according to a certain rule with a table. Finally, the authors used these GH representations in symmetric cryptography, and the authors made some applications with a method which they construct similar to Nalli and Ozyilmaz.

DOI: 10.4018/978-1-6684-3991-3.ch007

INTRODUCTION

The Fibonacci sequence, $\{F_k\}_0^\infty$, is a sequence of numbers, beginning with the integer couple 0 and 1, in which the value of any element is computed by taking the summation of the two antecedent numbers. If so, for $k \geq 2$, $F_k = F_{k-1} + F_{k-2}$ (Koshy, 2001). There have been many studies in the literature dealing with the quadratic number sequences. One of the studied areas of the Fibonacci sequence is the representations and codes of this sequence.

A universal code transforms positive integers representing source messages into code words of different lengths. There are various universal codes such as the Elias codes, the Fibonacci universal code, Narayana code and non-universal codes such as Rice coding, Huffman coding and Golomb coding (Thomas, 2007), (Platos et., 2007), (Buschmann and Bystrykh, 2013),(Kirthi and Kak, 2016). The best known of them is the Fibonacci code and the Fibonacci code is more useful in comparison with other universal codes. Because Fibonacci universal code is a prefix code of variable size, it is uniquely decodable binary code. Also, this code easily fixs data from damaged parts of code words (Kirthi and Kak, 2016). Fibonacci and Gopala Hemachandra universal codes encode positive integers with binary representations and these code words are obtained based on Zeckendorf representation. Each positive integer has one and only one representation as the summation of non-sequential Fibonacci numbers by Zeckendorf's theorem (Zeckendorf, 1972). Fibonacci sequences and codes can also be defined from higher orders.

Definition 1. The *m*th order Fibonacci numbers, that are represented by $F_k^{(m)}$, are described with iteration relation as follows:

$$F_k^{(m)} = F_{k-1}^{(m)} + F_{k-2}^{(m)} + \dots + F_{k-m}^{(m)}$$

for $k>0$ and the boundary conditions $F_0^{(m)} = 1$ and $F_k^{(m)} = 0$ ($-m<k<0$) (Klein and Ben-Nissan, 2010).

One representation can be obtained for each positive integer *A* with a binary string of length *t*, $l_1 l_2 \dots l_{t-1} l_t$, such that $A = \sum_{i=1}^{t} l_i F_i^{(m)}$. The representation is one and only if one uses algorithm to find it as follows: When it is given the integer *A*, it is detected the largest Fibonacci number $F_t^{(2)}$ equivalent or smaller to *A*; after that it is continued repeating with $A - F_t^{(2)}$ (Klein and Ben-Nissan, 2010). For instance 17=1+3+13, hence its Fibonacci representation is 101001.

According to above algorithm, Fibonacci numbers aren't used consecutively in any of these summations, that is, in the binary representation, there are no contiguous 1 bits. When generalizing this procedure to higher orders, the same operations are realized as above. Additionally, it is appended (m–1) 1 bits to the *m*th order variant of Fibonacci representation of *k* to build the *m*th order variant of Fibonacci code of any positive integer *k*. But, unlike the Fibonacci representation, there are no adjacent of *m* 1 bits in the statement (Klein and Ben-Nissan, 2010).

In this study, the authors found that the first *k* positive integer $k = (3.2^{(m-1)} - 1)$ for which there is no Zeckendorf's representation for Gopala Hemachandra sequence whose order *m*. Thus, the authors formulated the first *k* positive integer whose Zeckendorf's representation can't be found in terms of its order. The authors also described the fourth, the fifth and the sixth order GH representation of positive