ISSN 1746-7659, England, UK
Journal of Information and Computing Science
Vol. 12, No. 3, 2017, *pp*.216-219

The Padovan Universal Code

Monojit Das[1]
[1] *Chengail High School, Howrah, W.B., India, Pin-711307*
E-mail: monojitbhu@gmail.com
(Received June 06, 2017, accepted June 30, 2017)

Abstract. In this paper, we consider the series of Padovan numbers. Thereby, we introduce universal coding scheme based on Padovan numbers. This universal coding are used in source coding as well as in cryptography.

Keywords: Zeckendorf 's representation, Padovan numbers, Universal code, Cryptography.

1. Introduction

The universal code maps positive integers which represents the source messages into codewords of different lengths. The codeword elements are a set of digits that are constructed according to specified rule and they may be binary. There are various universal codes including the Elias codes, the Fibonacci universal code, Levenshtein coding and non-universal codes including unary coding, Rice coding, Huffman coding and Golomb coding [9, 8, 1, 6]. If one were to represent numbers as sum of two prime numbers using Goldbach conjecture, inverse sequence may also sequences may also be used to construct a universal code [5].

The simplest of Elias codes is the gamma code in which the binary representation of the source code is preceded by $[log_2 n]$ zeroes indicate codeword for any natural number n. The time requirement for compression and decompression algorithms for cases where decompression time is a critical issue, is advantageous in this coding [3, 4].

Fibonacci universal coding is a universal code which encodes positive integers into binary codewords. These code words end with 11 and have no consecutive 1 before the end. Thus Fibonacci universal code is a uniquely decodable binary code of variable size since it is a prefix code. One disadvantage of this representation is that the size n of the set of integers has to be known in advance since it determines the code size as $1 + \lfloor log_2 n \rfloor$. The property of not having adjacent 1 bits restricts the number of binary patterns available for such codes, so they are longer than the other codes. Although, it is not asymptotically optimal, they perform well compared to the Elias code [3] as long as the number of source message is not too large. The Fibonacci universal code has the additional attribute of robustness, which manifests itself by the local containment of errors.

Fibonacci universal coding has a useful property that sometimes makes it attractive in comparison to other universal coding. It is easier to recover data from a damaged stream. With most other universal codes, if a single bit is altered, none of the data comes after it will be correctly read. On the other hand, with Fibonacci universal coding, a changed bit may cause one token to be read as two, or cause two tokens to be read incorrectly as one, but reading a 0 from the stream will stop the errors from propagating further. Since the only stream that has no 0 in it is a stream of 11 tokens, the total edit distance between a stream damaged by a single bit error and the original stream is at most three.

In this paper we present a variant of Fibonacci universal code based on Padovan sequence with the help of a representation procedure that leads to the Padovan universal code. This universal code may have probable applications in cryptography and have been presented in several studies.

2. Preliminaries

2.1. Fibonacci sequence

Fibonacci number $F(k)$ $(k = 0, \pm 1, \pm 2, \pm 3, \cdots)$ is defined by the second order linear recurrence relation

$$F(k) = F(k-1) + F(k-2) \tag{1}$$

with the initial terms $F(1) = 1, F(2) = 2$.

2.2. Zeckendorf 's Theorem

Zeckendorf's Theorem states "Every positive integer has a unique representation as the sum of non consecutive Fibonacci numbers" [10]. In other word, every positive integer n has unique representation of the form n= ∑_(k=1)^l▒a_k F(k) where a_k ∈{0,1} such that the string a_1 a_2 a_3⋯ does not contain any consecutive 1 and F(k) are Fibonacci numbers. This representation is defined as Zeckendorf's representation [2]. Therefore, when recursive nature of Fibonacci numbers allow some integers to have multiple representations using the above process e.g. 10 can be represented as F(2)+ F(3)+ F(4) or F(2)+ F(5) then in Zeckendorf's representation, is F(2)+ F(5).

3. Padovan Numbers

The Padovan numbers $P(k)$ $(k = 0, \pm1, \pm2, \pm3, \cdots)$ are defined by the recurrence relation:

$$P(k) = P(k-2) + P(k-3) \quad (2)$$

with the initial terms $P(0) = P(1) = P(2) = 1$.

The Padovan sequence is named after Richard Padovan who attributed its discovery to Dutch architect Hans van der Laan in his 1994 essay "Dom. Hans van der Laan: Modern Primitive". The sequence was described by Ian Stewart in his Scientific American column, Mathematical Recreations in June 1996.

Some Padovan numbers are summarized in the Table 1.

Table 1: Padovan Numbers

k	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10
$P(k)$	2	-1	0	1	-1	1	0	0	1	0	1	1	1	2	2	3	4	5	7	9	12

The characteristic equation of (2) is

$$x^3 - x - 1 = 0 \quad (2)$$

This equation has three roots, one real root ρ which is known as the plastic number and the other two roots are complex conjugate. The exact value of ρ is $\frac{\sqrt[3]{108+12\sqrt{69}} + \sqrt[3]{108-12\sqrt{69}}}{6}$. Also $\rho = lim_{k\to\infty} \frac{P(k+1)}{P(k)}$ [7].

4. The Padovan Universal Code

The term "Zeckendorf's representation" is properly used only in reference to the standard Fibonacci sequence, we will use it when discussing similar representations of numbers based on Variant Fibonacci sequences. Daykin proved that only the standard Fibonacci sequence $F(k)$gives all positive integers a unique Zeckendorf's representation [2]. Thus the Variant Fibonacci sequences allow for multiple Zeckendorf's representations of the same integer.

To generate the Padovan universal code as a generalization of Fibonacci universal code, we need to be able to map any given positive integer representing source code into variable length codeword in a manner used earlier by Thomas [9].

For a given positive integer n, construct a vector $A(n)$ such that $A(n)_i = P(i), i = 0, 1, \ldots, d$, where $P(d)$ is the largest number of Padovan series less than or equal to n. A vector $B(n)$ of binary digits with dimension d is constructed such that $A(n)^T B(n) = n$ and $B(n)_d = 1$.

The codeword $PB(n)$ for the positive integer n is defined by a vector with dimension $d + 1$, where $PB(n)_k = B(n)_k$ for $1 \le k \le d$, and $PB(n)_{d+1} = 1$.

If the source code to be represented is a term in Padovan series, the codeword consists of binary set with all zeros followed by two consecutive ones at the termination.

If the source code to be represented is not a term in Padovan series, the codeword consists of binary representation of summation of two or more terms in the series of Padovan numbers such that $A(n)^T B(n) = n$ which includes two consecutive ones at the termination as a part of Zeckendorf's representation. We consider codeword which can be represented by summation of least number of terms in Padovan series.

4.1. Example