International Journal of Information Technology and Knowledge Management
January-June 2011, Volume 4, No. 1, pp. 81-83

SURVEY OF DOUBLE BASED NUMBER SYSTEM AND THEIR APPLICATION

Rajdeep Chowdhury[1] & Mousumi Basak[2]

In this paper, the Double Based Number System is shown along with its allied applications. We would like to discuss the application of this Number System in the area of digital signal processing. We would like to illustrate and emphasize the discussion with concrete examples of finite impulse response filtering. The application of Double Based Number System is mainly in the area of digital signal processing and finite impulse response filtering, which also allows us for an efficient implementation of the basic arithmetic operations and considerable hardware reductions in look-up table size. Number Systems are primarily chosen to enable a reduction of the complexity of the arithmetic operations as the computational complexity of algorithms crucially depends upon the number of zeros of the input data in the corresponding Number System. Experimentally, it has been observed and shown that the expected number of zeros in the representation of arbitrary integers in the Binary Signed-digit Number System tends to show that, on average for long word.
Keywords: Number System, Numeral System, Double Based Number System, Scalar Multiplication, Koblitz Curves, Greedy Algorithm, Dynamic Programming, Optimal Substructure, Continued Fraction.

1. Introduction

In this paper, the Double Based Number System is shown along with its allied applications. We would like to emphasize the system's application in the practical scenario and the existence of the system in the modern ambience can be basically fragmented into:

Overview

Classical techniques

NAF, JSF, T-NAF

DBNS

Tree Based Approach

Joint DBNS

2. Conceptual Literature Review

Number Systems: In mathematics, a 'Number System' is a set of numbers (in the broadest sense of the word), together with one or more operations, such as addition or multiplication, etc. Examples of number systems include natural numbers, integers, rational numbers, algebraic numbers, real numbers, complex numbers, p-adic numbers, surreal numbers, and hyper-real numbers.

For a comprehensive history of Number Systems, we have to oversee numbers. For a comprehensive history of the symbols used to represent numbers, we have to oversee Numeral System.

Scalar Multiplication: The standard way to compute [n] P is the Double And–Add method. The method relies on the following operations:

1. Addition P + Q, when $P \neq +-Q$;
2. Doubling [2] P.

We are basically interested in techniques that can compute Scalar Multiplication as efficiently and effectively as possible.

The formal definition could be coined as "Given an integer n and a point P on a curve, a Scalar Multiplication consists in computing:

[n] P = P + P + P +.....+ P…….n times.

Signed Digit Representation

The density of NAF is 1/3.

Among all the signed-binary representations, this number is minimal for the NAF. In case, there is some memory available to store more points, we can use non-trivial coefficients. The window ô-adic algorithm of Solinas [Efficient arithmetic on Koblitz Curves, Designs, Codes and Cryptography 19 (2000) 195] is the most powerful method for computing point multiplication for Koblitz Curves. In this way, the existence of a more general window τ-adic form for each element in $Z[\tau]$ is obtained. In particular, this provides a proof for the termination of Solinas algorithm.

[1,2]Department of Computer Application, JIS College of Engineering, Block 'A', Phase III, Kalyani, Nadia-741235, West Bengal, India

Email: [1]dujon18@yahoo.co.in, [2]bultibasak1990@gmail.com

2. IMPLEMENTATION VIA CASE STUDY OF APPLICATIONS

2.1. Koblitz Curves

The parameter set of the five binary Koblitz Curves standardized by NIST are listed below. The curves are of the form y^2 + xy = x^3 + ax^2 + 1, over a binary field.

For the five curves, the following parameters are listed for quick reference:

1. p(t): the reduction polynomial (in explicit and hexadecimal form);
2. a: the curve's a coefficient;
3. G_x, G_y: the x coordinate and y coordinate of the base point G;
4. n: the base point's order;
5. h: the curve's cofactor.

2.2. Greedy Algorithm

A Greedy Algorithm is any algorithm that follows the problem solving concept, meta-heuristic of making the locally optimal choice at each stage with the hope of finding the global optimum.

In general, Greedy Algorithm consists of five pillars:

1. A candidate set, from which a solution is created;
2. A selection function, which chooses the best candidate to be added to the solution;
3. A feasibility function, that is used to determine if a candidate can be used to contribute to a solution;
4. An objective function, which assigns a value to a solution, or a partial solution, and;
5. A solution function, which will indicate when we have discovered a complete solution.

Greedy Algorithm produces good and optimum solutions on some mathematical problems, but not on others. Most problems for which they work will comprehensively have two properties:

2.3. Greedy Choice Property

We can make whatever choice seems best at the moment and then essentially solve the sub-problems that arise later. The choice made by a Greedy Algorithm may depend on choices made so far but not on the future choices or all the solutions to the sub-problems. It iteratively makes Greedy choices, one after another, thereby reducing each given problem into a smaller one. In other words, a Greedy Algorithm never reconsiders its choices.

This is the main difference from Dynamic Programming, which is exhaustive and is guaranteed to find the solution. After every stage, Dynamic Programming makes exclusive decisions based on all the decisions made in the previous stage, thereby reconsidering the previous stage's algorithmic path to the solution.

2.4. Optimal Substructure

"A problem exhibits Optimal Substructure, if an optimal solution to a problem contains optimal solutions to its sub-problems." Said distinctively, a problem has Optimal Substructure if the best next move always leads to the optimal solution. An example of 'Non-Optimal Substructure' would be a situation where capturing a queen in the game of chess (good next move) might eventually lead to the loss of the game (bad overall move).

2.5. Continued Fractions and Ostrowski's Number System

A simple Continued Fraction is an expression of the form:

_ = a0 +
|
a1 +
|
a2 +
|
a3 + · · ·, where the partial quotients ai are integers _ 1

A Continued Fraction is represented by the sequence (an)n2N, which can either be finite or infinite.

An important result is that every irrational real number _ can be expressed uniquely as an infinite simple Continued Fraction, written is a compact abbreviated notation as _ = [a0, a1, a2, a3, . . .]. Similarly, every rational number can be expressed uniquely as a finite simple Continued Fraction.

For example, the infinite Continued Fraction expansions of the irrationals _ and e are:

_ = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, . . .]

e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, . . .]

3. CONCLUSION

This paper is an earnest attempt on the part of the authors to bring some theory at the surface of some previously unproved experimental statements about the Double Based Number System (DBNS).

We use results from Diophantine Approximation to address the problem of converting integers into DBNS.

Although the material presented in this paper is mainly theoretical, these algorithms can be used to solve various problems and for representing large numbers.

The feasibility study will be put to use in pursuing for the answer to some more difficult and complex questions related to the Double Based Number System and its generalization, the multi-dimensional logarithmic number system.

At the end of the survey, it can be concluded that the paper titled "Survey of Double Based Number System and Their Application" can be furnished as a ready reference for Double Based Number System's effective implementation in practical scenario and usage world. The paper is a preface to the Number System and its feasible applications.

REFERENCES

[1] S.Singha, A.Sinha, "Survey of Various Number Systems and Their Applications", International Journal of Computer Science & Communication, 1, Number-1, (2010), pp 73-76.

[2] V.Dimitrov, G.A.Jullien, W.C.Miller, "Theory and Applications for a Double- Base Number System," Proceedings of 13th IEEE Symposium on Computer Arithmetic (ARITH '97), 1997, pp 44-53.

[3] V.Dimitrov, G.A.Jullien, W.C.Miller, "Theory and Applications of the Double-Base Number System," IEEE Transaction on Computers, 48, No. 10, 1999, pp 1098-1107.

[4] G.H.Hardy, E.M.Wright, "An Introduction to the Theory of Numbers", 5th edition Oxford, England: Clarendon Press, 1979, pp 14, 15 and 19.

[5] C.Chiang, L.Johnson, "Residue Arithmetic and VLSI," Technical Report, California Institute of Technology, Pasadena, CA. 91125.

[6] H.Garner, "The Residue Number System," IRE Transaction on Electronic Computers, 1959.

[7] T.Aoki, H.Amada, T.Higuchi, "Real/Complex Reconfigurable Arithmetic Using Redundant Complex Number Systems," Proceedings of 13 th IEEE Symposium on Computer Arithmetic (ARITH '97), 1997, pp 200-207.

[8] J.Duprat, Y.Herreros, S.Kla, "New Redundant Representations of Complex Numbers and Vectors," IEEE Transaction on Computers, 42, No.7, 1993, pp 817-824.