

A Product-Based Binary Number System

Jeffrey Uhlmann

Department of Electrical Engineering and Computer Science, University of Missouri, Columbia, USA

Email address:

uhlmannj@missouri.edu

To cite this article:

Jeffrey Uhlmann. A Product-Based Binary Number System. *Applied and Computational Mathematics*. Vol. 7, No. 5, 2018, pp. 217-218.

doi: 10.11648/j.acm.20180705.11

Received: December 10, 2018; **Accepted:** January 2, 2018; **Published:** January 28, 2019

Abstract: The fundamental theorem of arithmetic says that every natural number greater than 1 is either a prime itself or can be factorized as a product of a unique multiset of primes. Every such integer can also be uniquely decomposed as a sum of powers of 2. In this note we point out that these facts can be combined to develop a binary number system which uniquely represents each integer as the product of a subset of a special set of prime powers which we refer to as *P-primes*.

Keywords: Binary Numbers, Number Systems, Mathematics Education, Number Theory, Prime Factorization, Prime Numbers

1. Introduction

The fundamental theorem of arithmetic says that every natural number greater than 1 is either a prime itself or can be factorized as a product of a unique multiset of primes. This means that each integer n can be expressed as a product of powers of primes:

$$n = \prod_{i=0}^{\infty} p_i^{a_i} \quad (1)$$

where p_i is the i th prime and a_i is an integer representing its multiplicity [2]. Each integer n can of course also be expressed as a sum of powers of 2:

$$n = \sum_{i=0}^{\infty} w_i 2^i \quad (2)$$

where $w_i \in \{0, 1\}$ is a binary inclusion/exclusion variable for each power of 2. This sum provides a unique binary representation for each integer and is the basis for encoding integers on computers.

What is interesting to note is that these product and sum expressions for integers can be combined to define a product-based binary number system. Specifically, Eq. (2) says that the integer exponent of each term $p_i^{a_i}$ from Eq. (1) can be uniquely expressed as a sum of powers of 2. For example, if $p_i = 7$ and $a_i = 21$ then 7^{21} can be decomposed into a unique set

of multiplicands with power-of-2 exponents as

$$7^{21} = 7^{(2^0+2^2+2^4)} = 7^1 \cdot 7^4 \cdot 7^{16} \quad (3)$$

Thus, the factorization of an integer n as the product of a multiset of primes can be replaced with an alternative factorization in the form of the product of a subset of the set $\{p_j^{2^i}; i \geq 0, j \geq 1\}$, where p_j is the j th prime. We will call this the set of *power primes*, or *P-primes*.

2. The P-Prime Number System

The relationship between P-primes and ordinary primes can be illuminated by the following definition:

Definition: A number $q > 1$ is a P-prime if and only if it cannot be formed as the product of a subset of smaller P-primes.

This definition is distinguished from the definition of ordinary primes by the use of the word *subset*, and its equivalence to the set $\{p_j^{2^i}; i \geq 0, j \geq 1\}$ can be deduced directly from the representation of Eq. (2). The fact that every integer can be represented uniquely as the product of a *set* of P-primes immediately implies a binary number representation for each integer n with the i th bit designating the inclusion/exclusion of the i th P-prime from its product set¹.

As an example, the number 1800, which has prime factors $2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5$, can be expressed as a product of P-primes,

¹ The definition of P-primes (under the name u-primes) and their use to define a product-based binary number system was first explored by the author as part of his masters work on subset recognizing automata in 1985-86 and was subsequently

documented as an appendix in his 1995 doctoral dissertation [5].

$1800 = 2^1 \cdot 2^2 \cdot 3^2 \cdot 5^2$, and represented in binary form as

2	3	4	5	7	9	11	13	16	17	19	23	25	...
1	0	1	0	0	1	0	0	0	0	0	0	1	...0...

Thus far we have only considered the representation of integers greater than zero, but the general representation of all positive and negative integers can be obtained by augmenting the set of P-primes to include, e.g., -1 . It can be verified that P-primes can be multiplied efficiently on a digit-by-digit basis: If the digits in position i of both multiplicands are zero then the digit in position i of their product zero. If the digits differ then the digit in position i is 1. If the digits in position i of both multiplicands are 1 then the digit in position i is zero and the digit in position j corresponding to the square of the P-prime associated with position i is 1. If the digits in position j of the multiplicands differ then the digit in position j is reset to zero and the position corresponding to the square of the P-prime associated with position j is 1. This general (and familiar) quadratic-carry rule is straightforward to determine for all other cases. It is also similarly straightforward to perform division by carrying in the direction of the square root of P-primes.

Unfortunately, there does not appear to be an efficient algorithm for addition and subtraction unless there exists an efficient algorithm for prime factorization. In this respect, the P-prime representation suffers limitations similar to other nonstandard numeral representations [3], such as the Quote system [1, 4], in that it may have elegant theoretical properties but is not necessarily practical for general computational applications.

3. Conclusion

The P-Prime representation is primarily of theoretical and pedagogical interest as a product-based alternative to the conventional sum-based powers-of-two binary representation of integers. Unlike other numeral systems it combines the conventional prime-number and binary representations of positive integers in a way that can offer different perspectives on various results from number theory, e.g., based on the fact that the P-prime representation defines a one-to-one mapping of binary strings to the positive integers in a manner that relates to the distribution of primes.

References

- [1] E. C. R. Hehner and R. N. S. Horspool, "A new representation of the rational numbers for fast easy arithmetic," *SIAM Journal of Computing*. 8:2, pp. 124-134, 1979.
- [2] Herstein, I. N., *Abstract Algebra*, Macmillan Publishing, p. 30, 1986.
- [3] Donald Knuth, *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, 3rd Edition, Addison-Wesley, 1997.
- [4] C. Serpa and J. Buesca, "Piecewise Expanding Maps: Combinatorics, Dynamics and Representation of Rational Numbers," *ESAIM: Proceedings and Surveys*, Vol. 46, pp. 213-216, 2014.
- [5] Uhlmann, J. K., (1995). *Dynamic Map Building and Localization: New Theoretical Foundations*, A16, pp. 243-24, Doctoral Dissertation, University of Oxford.