p-Adic Arithmetic Methods for Exact Computations of Rational Numbers

Ankush Vimawala
School of Electrical Engineering and
Computer Science
Oregon State University
Email: vimawala@cs.orst.edu
June 2003

***Abstract*— KrishnaMurthy, Rao and Subramanian described a finite number system in 1975, which enabled exact computations of rational numbers which came to be known as Hensel codes.Hensel codes show promising potential for the future of computer arithmetic of infinite accuracy.This paper gives a brief overview of some of the basic principles of Hensel codes and elucidates various advanced techniques of arithmetic for Hensel codes that have been proposed over the years.**

I. Introduction

Early attempts to implement arithmetic of infinite accuracy were found in the form of multiple modulus residue arithmetic, as in [5],[2].Since an automatic digital computer is a finite machine, it is capable of representing, internally, only a finite set of numbers [2]. Real numnbers have most commonly been represented as floating point numbers, which is nothing but an approximation.p-adic arithmetic makes infinite accuracy arithmetic possible on a finite machine.It appears to combine the best features of residue arithemtic with the best features of fixed-radix arithemetic [2].Introductions to p-Adic numbers are contained in [1],we do not include a full discussion of p-adic numbers in this treatise.

For a given prime number p, every rational number $x = a/b$ can be represented uniquely by an infinite sequence of digits, periodic in nature.[2],[8]. Where a,b are positive integers, gcd(a,b)= 1, and $b \neq 0$.

$$x = a_n p^n + a_{n+1} p^{n+1} + a_{n+2} p^{n+2} + \cdots \quad (1)$$
$$= p^n (c_0 + c_1 p + c_2 p^2 \ldots) \quad (2)$$

$0 \leq a_j < p$ for $j = n, n+1, \ldots$ and $a_n \neq 0$. [6].

The abbreviated notation

$$x = a_n a_{n+1} a_{n+2} \ldots \quad (3)$$

or equivalently

$$x = .c_0 c_1 c_2 \ldots \quad (4)$$

where only the coefficients of the powers of p are exhibited is called the p-adic expansion of x [6]. For example, for $p = 5$, the rational $x = 1/3$ has the 5-adic expansion $1/3 = 0.231313\ldots$. The truncated r-digit expansion of x is termed the Hensel code for x denoted $H(p, r, x)$ [6].

The arithmetic operations on Hensel codes $H(p, r, x)$ are almost similar to the conventional p-ary arithmetic [6]. All the basic operations proceed from left to right. Division of p-adic numbers, unlike that of p-ary numbers is deterministic, with no trial and error.A description of basic arithmetic operations on Hensel codes can be found in [1].

Order N Farey fractions are defined as the set

$F_N = \{\ a/b : gcd(a, b) = 1, 0 \leq a \leq N, 0 < |b| \leq N\}$
[4].If N satisfies the following inequality,

$$N \leq ((p-1)/2)^{1/2} \quad (5)$$

then every order N farey fraction x = a/b with gcd(a,b) = 1 can be represented uniquely by an r-digit ordered sequence. [2],[4],[1].

A. Fast Iterative Division of Hensel Codes

Krishnamurthy, Venu and Murthy propose in [6] a fast iterative scheme for division of Hensel codes based on Newton's method for finding roots of an equation $f(x) = 0$.This section gives a brief overview of their scheme. Newton's method describes an iterative scheme that converges to the root of a function $f(x) = 0$ [10]. More specifically, it consists of computing the sequence of iterates $x_1, x_2, \ldots, x_i \ldots$ using the scheme

$$x_{i+1} = x_i - f(x_i)/f'(x_i) \quad (6)$$

where x_0 is an appropriately chosen initial approximation.

The reciprocal of a given real number a can be found using:

$$f(x) = (1/x - a) \quad (7)$$

so that $f(x) = 0$ is equivalent to $x = 1/a$ when convergence is obtained. hence;

$$x_{i+1} = x_i - (1/x_i - a)/(-1/x_i^2) = (2 - ax_i)xi \quad (8)$$

Quadratic convergence can be obtained using (8)

As shown in [6], (8) can be written for p-adic numbers as:

$$x_{i+1} = [2 - H(p, \infty, x).H(p, r, x^{-1})].H(p, r, x^{-1}) \quad (9)$$

where $H(p, \infty, x)$ denotes the infinite p-adic expansion of x.

This results in:

$$H(p, 2r, x_{i+1}) = x_{i+1} mod p^{2r} = H(p, 2r, x^{-1}) \quad (10)$$

for a proof see [6].

For example, Let $p = 5$ and $a = H(5, 4, 3/11) = 0.3403$, to find $x = a^{-1}$ writting a as $a_0a_1a_2a_3$,

$x_0 = a_0^{-1} mod 5 = 3^{-1} mod 5 = 0.2 = H(5, 1, 11/3)$

$ax_0 mod 5^2 = 0.20 * 0.34 = 0.14$
(where * denotes multiplication of Hensel codes, see [1] for basic arithmetic operations on Hensel codes)
$(2 - ax_0) mod 5^2 = 0.20 - 0.14 = 0.11$

$(2 - ax_0)x_0 mod 5^2 = 0.11 * 0.2 = 0.22 = x_1 = H(5, 2, 11/3)$

$ax_1 mod 5^4 = 0.3403 * 0.2200 = 0.1013$

$(2 - ax_1) mod 5^4 = 0.1041$

$(2 - ax_1)x_1 mod 5^4 = 0.2231 = x_2 = H(5, 4, 11/3)$

as can be seen, the above iterative scheme yields quadratic convergence. Higher order convergence can be obtained by extending the Newton's method rewritting (8) as

$$x_{i+1} = x_i(1 + (1 - ax_i)) \quad (11)$$

or

$$x_{i+1} = x_i(1 + y_i) \quad (12)$$

where $y_i = (1 - ax_i)$ pth order convergent iterations can be obtained by using the equation:

$$\underbrace{x_{i+1} = x_i[1 + y_i(1 + y_i(1 + ...)))]}_{(p-1)times}$$

using a pth order convergence iteration,p^i digits of the result are obtained at the ith iteration.

B. Conversion of Hensel Codes to Farey fractions

One of the outstanding problems in the practical utilization of p-adic arithmetic is the conversion of a Hensel code to its equivalent Farey rational [7].This section attempts to gives an overview of a factorisation based scheme, followed by more complex conversion schemes proposed by Krishnamurthy in [7].

1) Background: The r-digit Hensel code of a rational x is denoted

$$H(p, r, x) = (m_x, e_x)$$

where
$x = a/b = (c/d)p^n; gcd(c, d) = gcd(c, p) = gcd(d, p) = 1.$

$m_x = (cd^{-1}) mod p^r$ and $e_x = n.$

The conversion problem is nothing but recovering c and d, given m_x [7].

$$f^{-1} : H(p, r, x) \to F_N$$

The weight w of $H(p, r, x)$ is defined as:

$$w = \sum_{i=0}^{r-1} a_i p^i \quad (13)$$

where

$$0 \le a_i \le p - 1; 0 \le w < p^r$$

The conversion problem ammounts to finding c, d , given a product $c.d^{-1}$ such that

$$cd^{-1} = w + mp^r \quad (14)$$

where

$$0 \le c \le N, 0 \le d \le N$$

It is a complex task, as various values of m which satisfy the range conditions have to be tried, there is no polynomial time algorithm known for this purpose [7].

2) The Factorization Algorithm : This method is based on factoring (14),iteratively for various values of m = 0,1,2 ..., N.

Step 0: Read w; set $w = w + mp^r$ with $m = 0$.
Step 1: Factorize $w = x_iy_i(i = 1, 2, \ldots, k)$
such that $1 \le x_i, y_i < p^r; set\ i = 1.$
Step 2: Set x as specified, according as any of the following conditions hold; else goto Step 3.
i) $x_i \le N$ and $y_i^{-1} \le N; x = x_i/y_i^{-1}$.
ii)$x_i \le N$ and $(p^r - y_i^{-1}) \le N; x = x_i/ - (p^r - y_i^{-1})$.
iii)$(p^r - x_i) \le N$ and $y_i^{-1} \le N; x = -(p^r - x_i)/y_i^{-1}$.
iv)$(p^r - x_i) \le N$ and $(p^r - y_i^{-1}) \le N;$
$x = -(p^r - x_i)/ - (p^r - y_i^{-1})$.
v) $x_i^{-1} \le N$ and $y_i \le N; x = y_i/x_i^{-1}$.
vi) $x_i^{-1} \le N$ and $(p^r - y_i) \le N; x = -(p^r - y_i^{-1})/x_i^{-1}$.
vii)$(p^r - x_i) \le N$ and $y_i \le N; x = y_i/ - (p^r - x_i^{-1})$.
viii)$(p^r - x_i^{-1}) \le N$ and $(p^r - y_i) \le N; x = -(p^r - y_i)/ - (p^r - x_i^{-1})$.
Step 3: If $i \le k - 1$, set $i = i + 1$ and go to Step 2; else go to Step 4.
Step 4: If $m \le p^r - 1$, set $m = m + 1$ and $w = w + mp^r$, and go to Step 1; else stop.

For example: consider
$H(5, 4, x) = 0.2210; w = 37, p^r = 625.$ the solution arises

for $m = 3$ in Step 2 for condition i)
$w = 3.625 + 37 = 1912 = 4.478 = 4.17^{-1} = 4/17$

An alternative scheme for conversion based on the semiweight w_s of a Hensel Code has been proposed in [7]. The semiweight w_s of $H(p, r, x)$ is defined for an even r as:

$$w_s = \sum_{i=0}^{r/2-1} a_i p^i \tag{15}$$

An equivalence class of rationals whose leading r/2 digits are identical is constructed making use of the semiweight, hence the number to be factorised is reduced to the square root of the number to be factorised in the previous algorithm.But the additional computation here is to determine the candidate among the equivalence class of rationals.This is done by converting each of the rationals into thier Hensel codes and comparing with the given Hensel code. For large N, this scheme is also exponential.

3) Primitive Root Based Algorithm: Krishnamurthy in [7] describes a deterministic, trial and error free algorithm based on generating isobaric sets of Farey rationals.

Let g be a primitive root of an odd prime p and let w be the weight of H(p,r,x) ,then the set of rationals

$$S = \left\{ \frac{w_s.g^i mod\ p^r}{g^i mod\ p^r} : o \leq i \leq \phi(p^r) - 1 \right\} \tag{16}$$

where $\phi(m)$ is the Euler's Totient Function of m, constiutes an equaivalent class of reduced Farey rationals of order $(p^r - 1)$.whose weights are all equal to w.This set S is called the set of isobaric rationals of weight w, since all rationals of S have weight w.

If the isobaric set S' defined by

$$S' = \left\{ \frac{w_s.g^i mod\ p^{r/2}}{g^i mod\ p^{r/2}} : o \leq i \leq \phi(p^{r/2}) - 1 \right\} \tag{17}$$

with w_s as the semiweight of $H(p, r, x)$ is generated, then S' contains all reduced Farey rationals of order N', where $N' = (p^{r/2} - 1)$. By (5), the order N Farey rationals which constitute our $H(p, r, x)$ are contained in S'. We can therefore select from this set S' the required rational x [7].

The algorithm proceeds as follows:

Step 1: Generate the isobaric set S' from w_s, the semiweight of $H(p, r, x)$.

Step 2: convert Farey rational a/b of order N, also the rational $-(p^{r/2} - a)/b$ into Hensel code and compare with the given H(p,r,x). If for some a/b, $H(p, r, a/b)$ agrees with $H(p, r, x)$ then $x = a/b$;if on the other hand, $H(p, r, -(p^{r/2} - a)/b)$ agrees with $H(p, r, x)$ then $x = -(p^{r/2} - a)/b$.

The cardinality of the isobaric set S equals $\phi(p^{r/2})$ [7], and hence grows exponentially with r.

For example:
Let $H(5, 4, x) = 0.1214p^2 = 5^2 = 25$,
$w_s = 0.12 = 11, g = 2$

$$S' = \left\{ \frac{w_s.g^k mod\ 25}{g^k mod\ 25} : o \leq k \leq 19 \right\}$$

$S' = \{ 11/1, 22/2, 19/4, 13/8, 1/16, 2/7, 4/14, 8/3, 16/6, 7/12, 14/24, 3/23, 6/21, 12/17, 24/9, 23/18, 21/11, 17/22, 9/19, 18/3 \}$ all the rationals in S' have thier leading two digits equal to 0.12 and have semiweights 11. To convert $H(5, 4, x) = 0.1214$, using the algorithm, results in $x = a/b = 2/7$.

Krishnamurthy, in [7] also proposes an extension to the above algorithm.By using two simultaneous p-adic systems with different values of p for each. The semiweights of the Hensel codes are then used to generate two different isobaric sets. Since each order N Farey rational has a unique code in each system, the intersection of these two isobaric sets uniquely identifies the rational x [7] .

II. Conclusion

This paper serves to give an overview of an advanced algorithm for division of Hensel codes, and looks at the conversion problem concluding with an explanation of the advanced optimised algorithms that have been proposed to address this issue, the optmised method can be seen juxtaposed against the conventional factorization method.

p-Adic arithmetic may hold the answer to many yet-unanswered questions.The applications may not only be limited to the area of cryptography or computer arithmetic.Only the future can proove to us the value of this unique arithmetic.

References

[1] C. K. Koc, *A Tutorial on P-Adic Arithmetic*, Technical Report,Oregon State University 2002.

[2] Robert Todd Gregory, *The use of Finite Segment P-adic Arithmetic for Exact Computation*, BIT 18(3):282-300,1978.

[3] R.T. Gregory *Error Free Computation with Rational Numbers*, BIT 21(2):194-202 1981.

[4] Peter Kornerup, R. T. Gregory,*Mapping Integers and Hensel Codes onto Farey Fractions*, BIT 23(1):9-20,1983.

[5] M. Tienari,V. Suokonautio,*A Set of Procedures Making Real Arithmetic of Unlimited Accuracy in ALGOL* , BIT 6(4):332-338,1966.

[6] E. V. Krishnamurthy, Venu K. Murthy,*Fast Iterative Division of p-adic Numbers*, IEEE transactions on computers 32(4):396-398,April 1983.

[7] E. V. Krishnamurthy,*On the Conversion of Hensel Codes to Farey Rationals*, IEEE transactions on computers 32(4):331-337,April 1983.

[8] Antoine Froment,*Error Free Computation: A Direct Method to Convert Finite-Segment p-Adic Numbers into Rational Numbers*, IEEE transactions on computers 32(4):337-343,April 1983.

[9] C.J. Zarowski, H.C. Card,*On Addition and Multiplication with Hensel Codes*, IEEE transactions on computers 39(12):1417-1423,December 1990.

[10] Department of Mathematics,University of Minnesota,*DELTA-M Mathematics On-Line* , http://www.math.umn.edu/itcep/delta-m/tse/index.shtml, chapter 7, section 6