Multidimensional Systems Theory

Progress, Directions and Open Problems in Multidimensional Systems

Edited by

N. K. Bose

School of Engineering, University of Pittsburgh, U.S.A.

With contributions by
N. K. Bose, J. P. Guiver, E. W. Kamen,
H. M. Valenzuela, and B. Buchberger

D. Reidel Publishing Company

A MEMBER OF THE KLUWER ACADEMIC PUBLISHERS GROUP

Dordrecht / Boston / Lancaster

Mathematics and Its Applications

intervals within which the coefficients of $x(z, w)$ and $y(z, w)$ can vary whilst not destroying the property that $xn + yd$ has no zeros in $\bar{U}^2$. In particular, we perturb the coefficients of $x(z, w)$ and $y(z, w)$ so that those are rational.

This argument will hold in general and proves the existence of $q(z, w) \epsilon Q[z, w]$. Let the perturbed polynomials be,

$$\hat{x}(z, w) = 1$$

$$\hat{y}(z, w) = -(z + \beta)$$

where the parameter β will be determined so that

$$\begin{aligned} &\hat{x}(z, w)n(z, w) + \hat{y}(z, w)d(z, w) \\ &= zw + \beta(w - z) - (1 + 2\beta) \\ &\triangleq \hat{q}(z, w) \end{aligned}$$

has no zeros in $\bar{U}^2$. Invoking the tests for absence of zeros of $\hat{q}(z, w)$ in $\bar{U}^2$, i.e. (i) $\hat{q}(z, w) \neq 0$ in T^2, (ii) $\hat{q}(z, 1) \neq 0$ in $\bar{U}^1$ and (iii) $q(1, w) \neq 0$ in $\bar{U}^1$, it is easy to infer that a suitable choice for β is $\beta = 1$.

The problem posed here, with the polydomain of interest $\bar{U}^2$, could be extended easily to the case of an arbitrary compact polydomain.

PROBLEM # 7

Gröbner Bases, Polynomial Remainder Sequences and Decoding of Multivariate Codes

(B. Buchberger, E. V. Krishnamurthy, and F. Winkler)

Recently Krishnamurthy and Gregory [1], [2] have constructed codes (called Hensel codes) for a finite subset of rationals called the Farey rationals F_N satisfying

$$F_N = \{a/b = Q' : gcd(a, b) = 1 \text{ and } 0 \leq |a| \leq N \text{ and } 0 \leq |b| \leq N\} \text{ where } N > 0 \text{ is an integer.}$$

If $N \leq \sqrt{(p^r - 1)/2}$ then the mapping of the class of rationals F_N to the residue class of integers modulo m ($= p^r$ where p is a prime) then the mapping

$$|\cdot|_m : F_N \rightarrow I_m$$

where

$$I_m = \{|a/b|: a/b \epsilon F_N\}$$

can be made one-to-one and onto.

These codes $a \cdot b^{-1} \bmod p^r$ are called Hensel codes of Farey rationals and are equivalent to their finite segment p-adic expansions. The arithmetic with these codes turn out to be quite simple (similar to p-ary arithmetic) and the forward and inverse mapping from rationals to these codes turn out to be quite easy. Also, recently it has been shown [1] that the inverse mapping of the Hensel code to the corresponding Farey rational can be made using the extended Euclidean algorithm. This permits us to have a practical rational arithmetic system based on the Hensel codes.

Hensel's lemma and the Hensel codes turn out to be very useful for linear algebraic computations giving exact rational results [1], [2].

It is well known that there is a striking similarity between the algebraic structures of integers and the polynomials over a field. In fact these two structures are treated alike under the common algebraic structure – called the Euclidean or gcd domains. In view of this similarity, it is but natural to extend all the above concepts relating to the construction of Hensel codes of rational numbers to the rational polynomials over a finite field. Here, however, we need to deal with the more general class of Farey rationals called Padé rationals which are rational functions over a finite field (the coefficients are from a field) and the numerator and denominator degrees do not respectively exceed $(R - 1)$. Such a Padé rational is denoted by $P(R - 1/R - 1, F_p(x))$ a subset of $F(x)$, the rational polynomial functions over a finite field of characteristic p.
We then code

$$a(x)/b(x) \epsilon P(R - 1/R - 1, F_p(x))$$

as

$$a(x)b^{-1}(x) \bmod x^{2R-1}$$

which is the Hensel code [3].

The Hensel codes for these rational polynomials can then be used in a manner analogous to that for a rational number. This also provides us with a very effective tool for the symbolic manipulation and arithmetic of the rational polynomials over the integers by a suitable choice of p.

If $P(R - 1/R - 1, N, x)$ denotes the class of Padé rationals over

integers where each coefficient is $\leq |N|$, then the choice

$$p > 2RN^2 + 1$$

enables us to construct Hensel codes for the practical problems.

The inverse mapping of these single variable rational polynomials can be obtained using the Euclidean algorithm. Thus a very practical rational polynomial arithmetic system can be devised and the use of Hensel's lemma again helps us to compute the solution for the linear algebraic problems and matrix inversion.

The above concept can further be generalized to multivariable rational polynomials [3] over a field and integers and the arithmetic can be performed in a similar way. This is useful for inversion of matrices whose entries are multivariate rational polynomials. However, the inverse mapping of the Hensel code to its equivalent rational polynomial cannot be realized by the Conventional Extended Euclidean algorithm since the multivariable polynomials are not Euclidean domains. The decoding has to be then based on the solution of a large matrix equation involving a Toeplitz matrix [4]. However, fortunately, it has been found recently that Gröbner bases [5] can be a very effective tool to decode the multivariable Hensel code. Naturally the algorithm for decoding the multivariable Hensel code will have several other applications – in multivariable Padé approximation [4], in the construction and decoding of multivariable Goppa Codes [6], and in the construction of matrix Padé approximants [4].

The examples below indicate the decoding of the Hensel code of a Farey rational, Padé rational and multivariable Padé rational. The proof of the algorithm for the Farey rational and single variable Padé rational is available in [1]. The proof of the multivariable decoding algorithm based on Gröbner bases has not been worked out in all the details so far.

Examples

1. Rationals

Let $p = 5$, $r = 4$; Hensel code of $\frac{10}{13} = 10 \cdot 13^{-1} \bmod 625 = 145 = .0401$.

The extended Euclidean algorithm:

i	q_i	625	0
		145	1

1	4	45	−4
2	3	10	13
3	4	5	−56
4	2	0	125

Decoding of Hensel code gives 10/13.

2. Rational Polynomials over GF(p)

Let $p = 17$, $2R - 1 = 3$, $R - 1 = 1$; Hensel code of $(x + 1)/(2x + 1) \stackrel{L}{=} 1 + 16x + 2x^2$.

i	q_i	x^3 / $1 + 16x + 2x^2$	0 / 1	
1	$9x + 13$	$4x + 4$	$8x + 4$	Decoding of
2	$9x + 12$	4	$13x^2 = 4x + 4$	Hensel code gives
3	$x + 1$	0	$4x^3$	$\frac{4x + 4}{8x + 4} = \frac{x + 1}{2x + 1}$

3. Multivariable Hensel Code

Let $p = 7, 2 \cdot 2 \cdot (R - 1) = 4$; Hensel code of

$$\frac{5y + 3}{5x + 5y + 1} = 3x^3 + x^2y + 2y^3 + \\ + 5x^2 + 6xy + y^2 + 6x + 4y + 3.$$

The algorithm [5] for constructing the Gröbner base:

i	p_i	t_i
1	x^4	0
2	x^3y	0
3	x^2y^2	0
4	xy^3	0
5	y^4	0
6	$3x^3 + x^2y + 2y^3 + 5x^2 + + 6xy + y^2 + 6x + 4y + 3$	1
7	$4x^2y + 2xy^2 + 5y^3 + + 2xy + 6y^2 + 3y + 4$	$2x + 6$
8	$2y + 4$	$2x + 2y + 6$
9	$5x + 4$	$4x^2y + 2xy^2 + 5y^3 + 6x^2 + + 3xy + 4y^2 + 6x + 6y + 6$
10	5	$5xy^2 + y^3 + 4xy + 5y^2 + + 6x + 4y + 4$

The column for the q_i's was omitted here, because there is no single quotient which can be associated with one step in the algorithm.

Decoding of Hensel code gives

$$\frac{2y + 4}{2x + 2y + 6} = \frac{5y + 3}{5x + 5y + 1}.$$

REFERENCES

[1] E. V. Krishnamurthy and R. T. Gregory. *Methods and Applications of Error-free Computation*, Springer-Verlag, New York, 1984.

[2] E. V. Krishnamurthy, 'Hensel's Methods in Linear Algebraic Computing – I', *Techn. Report CAMP* Nr. 83–27.0, Institut für Mathematik, Johannes Kepler Universität, Linz, Austria.

[3] E. V. Krishnamurthy, 'Hensel's Methods in Linear Algebraic Computing – II', *Techn. Report CAMP* Nr. 83–28.0, Institut für Mathematik, Johannes Kepler Universität, Linz, Austria.

[4] G. A. Baker and P. Graves-Morris, 'Padé Approximants', Parts I and II, Vols. 13, 14, *Encylopaedia of Mathematics and its Applications*, Addison-Wesley, Reading, Mass., 1981.

[5] B. Buchberger, 'Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory', Chapter 6, (this volume).

[6] R. J. McEliece, 'The Theory of Information and Coding', Vol. 3, *Encyclopaedia of Mathematics and its Application*, Addison-Wesley, Reading, Mass., 1977.

PROBLEM # 8

Invariance of Stability Property under Coefficient Perturbation

In system design, it is often necessary to preserve one or more characteristics of the system when system element values fluctuate about their respective nominal values. Investigations into the conditions for invariance of the multivariate polynomial positivity property under coefficient perturbation were undertaken in [1]. An interesting recent result of potential significance in the design of stable robust systems is due to Kharitonov [2]. Let

$$f(s) = \sum_{k=0}^{n} a_k s^{n-k} \qquad a_0 \neq 0$$

be a polynomial with real coefficients. (Kharitonov restricted $f(s)$ to be monic, i.e. $a_0 = 1$; however, his basic result is adaptable for non-monic polynomials and also generalizable to polynomials with complex coeffi-