Title	On the Power Series Solution of a System of Algebraic Equations
Author(s)	Moritsugu, S.; Furukawa, A.; Kobayashi, H.; Sasaki, T.
Citation	数理解析研究所講究録 (1988), 646: 40-51
Issue Date	1988-02
URL	http://hdl.handle.net/2433/100266
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
第646巻 1988年 40-51

On the Power Series Solution of a System of Algebraic Equations

S.Moritsugu*, A.Furukawa**, H.Kobayashi***, T.Sasaki****

* Dept. of Information Science, Faculty of Science, Univ. of Tokyo

** S.E.G. Corp.

*** Dept. of Math., College of Sci. & Techn., Nihon Univ.

**** The Institute of Physical and Chemical Research

Abstract

This paper discusses the power series solution of a system of algebraic equations which is computed by the multivariate symbolic Newton's method. Applying Newton's method naively, we obtain a power series solution the coefficients of which are large rational function of the initial approximation. An algorithm is given to reduce the solution to the normal form by using Gröbner basis method.

1. Introduction

Newton's method has been introduced into computer algebra by Sieveking(1972), who proposed a fast algorithm for division. A number of useful algorithms based on Newton's method have been proposed since then : to compute power series solution of algebraic equations by Lipson(1976), Kung & Traub(1978) ; as a generalization of Hensel construction in univariate case by Yun(1976a)(1976b), in multivariate case by Zippel(1981).

In this paper, the calculation of power series solution of a system of multivariate algebraic equations is discussed. In preparation, the univariate version of symbolic Newton's method is reviewed. (See Lipson(1976) or Kung & Traub(1978) for mathematical formulation.)

Algorithm 1 [Symbolic Newton iteration : univariate case]

Given an equation $f(x,\varepsilon) = 0$, $f \in \mathbf{Q}[x,\varepsilon]$, with initial approximation $x=x^{(0)}$, s.t. $f(x^{(0)},0)=0$ and $\frac{\partial f}{\partial x}(x^{(0)},0)\neq 0$, calculate the power series expansion of the solution at $\varepsilon=0$,

$$x = \sum_{j=0}^{\infty} a_j \varepsilon^j \ , \ a_0 = x^{(0)} \ . \tag{1.1}$$

method. Apply the iteration formula

$$x^{(k+1)} = x^{(k)} - \frac{f(x^{(k)},\varepsilon)}{\frac{\partial f}{\partial x}(x^{(k)},\varepsilon)}, \qquad k=0,1,\cdots. \tag{1.2}$$

Then,

$$x^{(k)} = \sum_{j=0}^{2^k-1} a_j \varepsilon^j$$

is an $O(\varepsilon^{2^k})$ approximation to the solution (1.1).

□

Algorithm 1 cannot be applied directly to the problem where $\frac{\partial f}{\partial x}(x^{(0)},0)=0$, but Kung & Traub(1978) has shown that such a "general" problem can be reduced to a "regular" problem where $\frac{\partial f}{\partial x}(x^{(0)},0)\neq 0$. Furthermore they proposed purely

symbolic computation using the minimal polynomial of the initial approximation $x^{(0)}$. In this paper, we apply the purely symbolic computation to a system of multivariate equations, restricting ourselves to regular problems, since general problems can be treated similarly to univariate case by using the branching theory(Vainberg & Trenogin(1974)). Our problem is formulated as follows.

Problem

Given a system of n equations with $n+1$ variables,

$$\begin{cases} f_1(x_1,\cdots,x_n,\varepsilon) = 0 \\ \quad\cdots\cdots\cdots\cdots \\ f_n(x_1,\cdots,x_n,\varepsilon) = 0 \end{cases} \tag{1.3}$$

where $f_i(1\leqq i\leqq n) \in \mathbf{Q}[x_1,\cdots,x_n,\varepsilon]$
and a set of initial approximations $x_1^{(0)},\cdots,x_n^{(0)}$ satisfying

$$\begin{cases} f_1(x_1^{(0)},\cdots,x_n^{(0)},0) = 0 \\ \quad\cdots\cdots\cdots\cdots \\ f_n(x_1^{(0)},\cdots,x_n^{(0)},0) = 0 \ , \end{cases} \tag{1.4}$$

solve this system at ε=0 by symbolic Newton's method, and get the power series expansions,

$$\begin{cases} x_1 = \sum_{j=0}^{\infty} a_{1j}\varepsilon^j \ , \quad a_{10} = x_1^{(0)} \\ \quad\cdots\cdots \\ x_n = \sum_{j=0}^{\infty} a_{nj}\varepsilon^j \ , \quad a_{n0} = x_n^{(0)} \end{cases} \tag{1.5}$$

Here, construct the algorithm by which the expansion coefficients a_{ij} are represented in the "simplest" forms.

□

Through Newton's method, a_{ij} grow into large rational functions of $x_1^{(0)},\cdots,x_n^{(0)}$. Therefore, they must be reduced to as simple forms as possible in

each step of the iteration so that the computation may proceed efficiently.

For the regularity of the problem, we set a restriction.

Assumption 1

Eq.(1.4) has finitely many solutions and $(x_1^{(0)}, \cdots, x_n^{(0)}, 0)$ is a simple zero of it.

□

The solution (1.5) is a local parametric representation of the system (1.3) showing the behavior of the system near $\varepsilon=0$.

In the next section we formulate the multivariate symbolic Newton's method, and we discuss the reduction of a_{ij} by using the relation between $x_1^{(0)}, \cdots, x_n^{(0)}$ in section 3. In section 4 we consider the rationalization of denominator. The whole algorithm is given in section 5, with an example in section 6. Computational efficiency is discussed in section 7.

2. Newton's method for a system of multivariate equations

The iteration formula is analogous to the numerical Newton's method. (See, e.g. Traub(1964).) The proof of convergence is the straightforward extension of the univariate case.

Algorithm 2 [Symbolic Newton's method : multivariate case]

The iteration formula for Eq.(1.3) is

$$\boldsymbol{x}^{(k+1)} = \boldsymbol{x}^{(k)} - \boldsymbol{F}^{-1}(\boldsymbol{x}^{(k)}, \varepsilon)\boldsymbol{f}(\boldsymbol{x}^{(k)}, \varepsilon), \tag{2.1}$$

where,

$$\boldsymbol{x} = \begin{bmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{bmatrix}, \quad \boldsymbol{f} = \begin{bmatrix} f_1 \\ \cdot \\ \cdot \\ \cdot \\ f_n \end{bmatrix}, \quad \boldsymbol{F} = \left[\frac{\partial f_i}{\partial x_j} \right] \text{ (Jacobian matrix) .}$$

Then,

$$x^{(k)} = \sum_{j=0}^{2^k-1} a_j \varepsilon^j \ , \quad a_j = \begin{bmatrix} a_{1j} \\ \cdot \\ \cdot \\ \cdot \\ a_{nj} \end{bmatrix}$$

is an $O(\varepsilon^{2^k})$ approximation to the solution (1.5).

□

Remark

If $F^{-1}(x^{(k)},\varepsilon)$ does not exist, then the iteration cannot be performed. However, Assumption 1 guarantees that $\det F(x^{(0)},0)\neq 0$, which is the constant term of $\det F(x^{(k)},\varepsilon)$ in $\mathbf{Q}(x^{(0)})[\varepsilon]$. Therefore, $\det F(x^{(k)},\varepsilon)\neq 0$ for every k is guaranteed.

□

3. Relation between the initial approximations

In this section, we discuss the relation between $x_1^{(0)},\cdots,x_n^{(0)}$ in (1.4), considering the following zero-dimensional ideal

$$I = (f_1(x_1,\cdots,x_n,0),\cdots,f_n(x_1,\cdots,x_n,0)) \subset \mathbf{Q}[x_1,\cdots,x_n] \qquad (3.1)$$

by using Gröbner basis method. We follow Buchberger(1985) for basic notation and definitions, and we assume that all Gröbner bases which appear in this paper are lexicographic and reduced.

Recently Gianni *et al.*(1986) showed the property of lexicographic Gröbner bases of prime ideals, and proposed an algorithm for the primary decomposition of zero-dimensional ideals.

Proposition 3.1

Let p be a prime ideal in $\mathbf{Q}[x_1,x_2,\cdots,x_n]$. For almost all linear coordinate transformations, the Gröbner basis of p with respect to the new coordinates $z_1,z_2,\cdots,z_n$ is of the form

$$\{\ z_1 - \varphi_1(z_n)\ ,\ z_2 - \varphi_2(z_n)\ ,\cdots,\ z_{n-1} - \varphi_{n-1}(z_n)\ ,\ \varphi_n(z_n)\ \}\ , \qquad (3.2)$$

for some $\varphi_j(z_n) \in \mathbf{Q}[z_n]$.

□

This is easy to see from Proposition 7.1 of Gianni *et al.*(1986) together with the definition of reduced Gröbner bases.

Algorithm 3.1 [Primary decomposition]

Let $I \subset \mathbf{Q}[x_1, x_2, \cdots, x_n]$ be a zero dimensional ideal. Under almost all coordinate transformations, if $I \cap \mathbf{Q}[z_n] = (g)$ and g is factored to $g_1^{e_1} \cdot g_2^{e_2} \cdot \cdots \cdot g_s^{e_s}$ then

$$I = (I\ ,\ g_1^{e_1}) \cap (I\ ,\ g_2^{e_2}) \cap \cdots \cap (I\ ,\ g_s^{e_s}) \tag{3.3}$$

is the irredundant primary decomposition of I.

□

Considering the primary decomposition of I (3.1) and the multiplicity of $(x_1^{(0)}, \cdots, x_n^{(0)})$, we get the following proposition.

Proposition 3.2

Given $f_1, \cdots, f_n \in \mathbf{Q}[x_1, \cdots, x_n]$ and $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbf{C}^n$ such that

$$f_i(\alpha) = 0, \quad (1 \leqq i \leqq n), \qquad \det F(\alpha) \neq 0,$$

we compute the primary decomposition

$$I = (f_1, \cdots, f_n) = q_1 \cap \cdots \cap q_s\ . \tag{3.4}$$

Then, q_1 is a prime ideal if $\alpha \in V(q_1)$.

□

Proof

Algorithm 3.1 gives a univariate polynomial g such that $(g) = I \cap \mathbf{Q}[x_n]$ which is factored as $g = g_1^{e_1} \cdot \cdots \cdot g_s^{e_s}$. We let $q_1 = (I\ ,\ g_1^{e_1})$, $\alpha \in V(q_1)$. α is of multiplicity 1 from $\det F(\alpha) \neq 0$, and g_1 is irreducible over $\mathbf{Q}$, therefore, every algebraically conjugate element β of α satisfies the condition

$\det F(\beta) \neq 0$. Hence every conjugate of α is of multiplicity 1. Since $\sqrt{q_1} \supset q_1$, we get

$$(\mathbf{Q}[x_1, \cdots, x_n]/q_1)/(\sqrt{q_1}/q_1) \tilde{=} \mathbf{Q}[x_1, \cdots, x_n]/\sqrt{q_1}.$$

We have

$$\dim_{\mathbf{Q}}(\mathbf{Q}[x_1, \cdots, x_n]/\sqrt{q_1}) = \#V(\sqrt{q_1}) \text{ with multiplicity,}$$

$$\dim_{\mathbf{Q}}(\mathbf{Q}[x_1, \cdots, x_n]/q_1) = \#V(q_1) \text{ with multiplicity.}$$

By Proposition 3.1, we see that every element of $V(\sqrt{q_1})$ has the multiplicity 1. Since any two elements of $V(q_1)$ are mutually conjugate, every element of $V(q_1)$ is of multiplicity 1. Hence $\#V(\sqrt{q_1}) = \#V(q_1)$ even if we count multiplicity. Therefore,

$$\dim_{\mathbf{Q}}(\mathbf{Q}[x_1, \cdots, x_n]/\sqrt{q_1}) = \dim_{\mathbf{Q}}(\mathbf{Q}[x_1, \cdots, x_n]/q_1).$$

Consequently, we obtain $\sqrt{q_1} = q_1$.

Q.E.D.

The propositions and the algorithm above show that a simple zero $(x_1^{(0)}, \cdots, x_n^{(0)})$ of q in (3.4) satisfy the relation

$$\{ x_1^{(0)} - \varphi_1(x_n^{(0)}) = 0, \cdots, x_{n-1}^{(0)} - \varphi_2(x_n^{(0)}) = 0, \varphi_n(x_n^{(0)}) = 0 \} \quad (3.5)$$

for some $\varphi_j(x_n^{(0)}) \in \mathbf{Q}[x_n^{(0)}]$. This relation is obtained by computing the Gröbner bases of q.

Algorithm 3.2 [Computation of the relation of the form (3.5)]

% input : polynomials $\{f_1, \cdots, f_n\}$ in $\mathbf{Q}[x_1, \cdots, x_n, \varepsilon]$ at ε=0 ;

% assumption : $I=(f_1, \cdots, f_n)$ at ε=0 is zero-dimensional. ;

% output : the relation of the form (3.5) ;

(i) $I = q_1 \cap q_2 \cap \cdots \cap q_s$. % primary decomposition by Algorithm 3.1;

(ii) Select a simple zero $(x_1^{(0)}, \cdots, x_n^{(0)})$ and q_i to which the zero belongs.

(iii) Return the Gröbner basis of q_i.

□

Proof

Proposition 3.2 shows that q_i is prime if the zero $(x_1^{(0)}, \cdots, x_n^{(0)})$ is simple. Therefore, the Gröbner basis of q_i takes on the form (3.2) according to Proposition 3.1.

Q.E.D.

Using the relation (3.5), variables $x_1^{(0)}, \cdots, x_{n-1}^{(0)}$ are eliminated from $a_{ij} \in \mathbf{Q}(x_1^{(0)}, \cdots, x_n^{(0)})$ and a_{ij} are represented by only $x_n^{(0)}$, *i.e.* $a_{ij} \in \mathbf{Q}(x_n^{(0)})$.

4. Rationalization of denominator

Here we let $b_{ij} \in \mathbf{Q}[x_n^{(0)}]$ be the denominator of a_{ij}. Considering that $\varphi_n(x_n^{(0)})$ in (3.5) is the minimal polynomial of $x_n^{(0)}$, $1/b_{ij}$ is computed by the extended Euclidean Algorithm (Loos(1982)) as follows.

Since the GCD of b_{ij} and φ_n is 1, there exist polynomials $A, B \in \mathbf{Q}[x_n]$ such that

$$A \cdot b_{ij} + B \cdot \varphi_n = 1.$$

That is, $1/b_{ij} \equiv A \mod \varphi_n$. Hence, $a_{ij} \in \mathbf{Q}(x_n^{(0)})$ is represented as a polynomial of $x_n^{(0)}$ through $\varphi_n(x_n^{(0)})$.

5. The whole algorithm and conclusion

The algorithm for the solution of the Problem is completed as follows.

Algorithm 5 [Solution of the Problem]

(i) Apply Algorithm 3.2 and select the prim ideal to which the initial approximation $x_1^{(0)}, \cdots, x_n^{(0)}$ belongs, and compute the relation (3.5) by using a lexicographic Gröbner basis.

(ii) Iterate the following steps for k=0,1,2,$\cdots$ until the power series solution is obtained to the desired order.

(ii)−(1) Apply the iteration formula (2.1).

(ii)−(2) Reduce the coefficients a_{ij} with the relation (3.5), representing them as polynomials by using the extended Euclidean algorithm.

As the conclusion of the result of Algorithm 5, the following can be shown.

(I) For all the solutions $(x_1^{(0)}, \cdots, x_n^{(0)})$ at $\varepsilon=0$, which are zeros of a certain prim ideal, the common expression is obtained.

(II) Even if the numeric solution $(x_1^{(0)}, \cdots, x_n^{(0)})$ cannot be computed exactly, the symbolic expression of power series expansion is exactly correct.

6. Example

Suppose that the system of equations,

$$\begin{cases} f_1(x_1,x_2,\varepsilon) = x_1^2 + x_2^2 - 2 - \varepsilon = 0 \\ f_2(x_1,x_2,\varepsilon) = -x_1^3 + x_2 - \varepsilon = 0 \end{cases}$$

is given. We apply Algorithm 5 to this system.

(i) The ideal $I = (f_1(x_1,x_2,0),\ f_2(x_1,x_2,0))$ is decomposed as follows.

$$I = (x_1 - 1\ ,\ x_2 - 1) \cap (x_1 + 1\ ,\ x_2 + 1) \cap \left(x_1 - \frac{1}{2}x_2^3 + \frac{3}{2}x_2\ ,\ x_2^4 - 5x_2^2 + 8\right)$$

Here, we select the third prime ideal. Since each basis is already a Gröbner basis, if we let the initial approximations be $x_1^{(0)}, x_2^{(0)}$, the relation between them are

$$x_1^{(0)} - \frac{1}{2}x_2^{(0)3} + \frac{3}{2}x_2^{(0)} = 0\ , \tag{6.1}$$

$$x_2^{(0)4} - 5x_2^{(0)2} + 8 = 0\ . \tag{6.2}$$

Note that (6.2) is the minimal polynomial of $x_2^{(0)}$.

(ii) $k = 0$

(ii)-(1) The iteration formula (2.1) is as follows.

$$\begin{cases} x_1^{(k+1)} = \dfrac{4x_1^{(k)3}x_2^{(k)} + x_1^{(k)2} + x_2^{(k)2} + 2 + (-2x_2^{(k)} + 1)\varepsilon}{6x_1^{(k)2}x_2^{(k)} + 2x_1^{(k)}} \\ \\ x_2^{(k+1)} = \dfrac{-x_1^{(k)3} + 3x_1^{(k)}x_2^{(k)2} + 6x_1^{(k)} + (3x_1^{(k)} + 2)\varepsilon}{6x_1^{(k)}x_2^{(k)} + 2} \end{cases} \tag{6.3}$$

The first iteration gives

$$\begin{cases} x_1^{(1)} = \dfrac{4x_1^{(0)3}x_2^{(0)} + x_1^{(0)2} + x_2^{(0)2} + 2 + (-2x_2^{(0)} + 1)\varepsilon}{6x_1^{(0)2}x_2^{(0)} + 2x_1^{(0)}} \\ \\ x_2^{(1)} = \dfrac{-x_1^{(0)3} + 3x_1^{(0)}x_2^{(0)2} + 6x_1^{(0)} + (3x_1^{(0)} + 2)\varepsilon}{6x_1^{(0)}x_2^{(0)} + 2}. \end{cases} \tag{6.4}$$

(ii)-(2) Using the relations (6.1) and (6.2), and reducing the numerators and denominators of (6.4) respectively, we obtain

$$\begin{cases} x_1^{(1)} = \dfrac{-4x_2^{(0)2} - 4 + (2x_2^{(0)} - 1)\varepsilon}{5x_2^{(0)3} - 9x_2^{(0)}} \\ \\ x_2^{(1)} = \dfrac{12x_2^{(0)3} - 44x_2^{(0)} + (3x_2^{(0)3} - 9x_2^{(0)} + 4)\varepsilon}{12x_2^{(0)2} - 44}. \end{cases} \tag{6.5}$$

Applying the extended Euclidean algorithm to the denominators of (6.5) and (6.2), we obtain

$$\begin{cases} (x_2^{(0)3} - \frac{9}{5}x_2^{(0)})^{-1} \equiv -\frac{5}{28}x_2^{(0)3} + \frac{25}{56}x_2^{(0)} \\ \\ (x_2^{(0)2} - \frac{11}{3}x_2^{(0)})^{-1} \equiv -\frac{9}{28}x_2^{(0)2} + \frac{3}{7} \\ \\ \qquad\qquad \text{mod } x_2^{(0)4} - 5x_2^{(0)2} + 8 \ . \end{cases} \tag{6.6}$$

The reduction of (6.5) with (6.6) and (6.2) gives

$$\begin{cases} x_1^{(1)} = (\frac{1}{2}x_2^{(0)3} - \frac{3}{2}x_2^{(0)}) + (\frac{1}{28}x_2^{(0)3} - \frac{5}{28}x_2^{(0)2} - \frac{5}{56}x_2^{(0)} + \frac{4}{7})\varepsilon \\ \\ x_2^{(1)} = x_2^{(0)} + (-\frac{3}{56}x_2^{(0)3} - \frac{3}{28}x_2^{(0)2} + \frac{9}{28}x_2^{(0)} + \frac{1}{7})\varepsilon \ . \end{cases} \tag{6.7}$$

This is an $O(\varepsilon^2)$ approximation to the solution.

(ii) $k = 1$

Only the result of the second iteration is shown here.

$$\begin{cases} x_1^{(1)} = (\frac{1}{2}x_2^{(0)3} - \frac{3}{2}x_2^{(0)}) + (\frac{1}{28}x_2^{(0)3} - \frac{5}{28}x_2^{(0)2} - \frac{5}{56}x_2^{(0)} + \frac{4}{7})\varepsilon \\ \qquad + (-\frac{27}{784}x_2^{(0)3} + \frac{51}{1568}x_2^{(0)2} + \frac{291}{3136}x_2^{(0)} - \frac{19}{196})\varepsilon^2 \\ \qquad + (\frac{4941}{351232}x_2^{(0)3} - \frac{5035}{175616}x_2^{(0)2} - \frac{3215}{87808}x_2^{(0)} + \frac{1895}{21952})\varepsilon^3 \\ x_2^{(1)} = x_2^{(0)} + (-\frac{3}{56}x_2^{(0)3} - \frac{3}{28}x_2^{(0)2} + \frac{9}{28}x_2^{(0)} + \frac{1}{7})\varepsilon \\ \qquad + (-\frac{3}{1568}x_2^{(0)3} + \frac{39}{1568}x_2^{(0)2} - \frac{45}{1568}x_2^{(0)} - \frac{3}{196})\varepsilon^2 \\ \qquad + (\frac{1349}{351232}x_2^{(0)3} - \frac{2531}{175616}x_2^{(0)2} + \frac{13}{2744}x_2^{(0)} + \frac{255}{21952})\varepsilon^3 . \end{cases} \tag{6.8}$$

This is an $O(\varepsilon^4)$ approximation to the solution. At this iteration step, the rational expression of ε is transformed into the truncated power series of ε, by calculating the expansion of the reciprocal of the denominator polynomial.

7. Note on the computational efficiency

When we apply the iteration formula (2.1), the convergence is second order, but the computation of $F^{-1}(x^{(k)},\varepsilon)$ in each iteration step is time consuming. If we use $F^{-1}(x^{(0)},0)$ in place of $F^{-1}(x^{(k)},\varepsilon)$, which is the constant term of the latter for every k, the convergence is first order, that is, $x^{(k)}$ is an $O(\varepsilon^{(k)})$ approximation. However, the computational complexity in each step becomes small. When the desired order of the power series solution is not high, this modified method may be more efficient.

Acknowledgements

We would like to express our sincere gratitude to the editor and the referees for valuable and helpful comments.

References

Buchberger,B. (1970). Ein algorithmishes Kriterium für die Lösbarkeit eines

algebraichen Gleichungssystems. *Aequationes Mathematicae*. 4/3, 374-383.

Buchberger,B. (1985). Gröbner bases : An algorithmic method in polynomial ideal theory. N.K.Bose. (ed.) *Recent Trends in Multidimensional Systems Theory*. D.Reidel Publ.Comp. Chapter 6.

Gianni,P., Trager,B., Zacharias,C. (1986). Gröbner bases and primary decomposition of polynomial ideals. *Preprint*.

Kung,H.T., Traub,J.F. (1978) All Algebraic Functions Can Be Computed Fast. *J. ACM*. 25/2, 245-260.

Lipson,J.,D. (1976). Newton's Method : A Great Algebraic Algorithm. *Proc. SYMSAC '76*. ACM. 260-270.

Loos,R. (1982). Computing in Algebraic Extensions. B.Buchberger *et al.* (ed.) *Computer Algebra*. Springer-Verlag. 173-187.

Sieveking,M. (1972). An Algorithm for Division of Powerseries. *Computing*. 10, 153-156.

Traub,J.F. (1964). Iterative Methods for the Solutions of Equations. Prentice-Hall.

Yun,D.Y.Y. (1976a). Hensel Meets Newton - Algebraic Constructions in Analytic Setting. J.F.Traub. (ed.) *Analytic Computational Complexity*. Academic Press. 205-216.

Yun,D.Y.Y. (1976b). Algebraic Algorithms using p-adic Constructions. *Proc. SYMSAC '76*. ACM. 248-259.

Vainberg,M.M., Trenogin,V.A. (1974). Theory of Branching of Solutions of Non-linear Equations. Noordhoff International Publishing.

Zippel,R. (1981). Newton's Iteration and the Sparse Hensel Algorithm. *Proc. SYMSAC '81*. ACM. 68-72.