数理解析研究所講究録
1514巻 2006年 22-28

多変数多項式に対する新しい因数分解法

佐々木 建昭 (Tateaki Sasaki) *
筑波大学 数学系
INSTITUTE OF MATHEMATICS, UNIVERSITY OF TSUKUBA

稲葉 大樹 (Daiju Inaba) †
筑波大学 VBL 研究員
VENTURE BUSINESS LABORATORY, UNIVERSITY OF TSUKUBA

Abstract

本稿は数体 K (Q,Z_p,C 等) 上の多変数多項式の新たな因数分解法を提案する。これは Moses-Yun の補間多項式と因子多項式のそれぞれの係数間の双線形関係に基づく算法である。その関係は非常に簡潔かつ一般的で、2変数の場合は K 上の、多変数の場合は従変数に関する多項式環上の線形方程式を与える。なお、対応するヘンゼル因子の主変数に関する次数が1のとき、このアルゴリズムは Kaltofen の方法に帰着する。

1 はじめに

多変数多項式の因数分解のため多くの算法が考案されたが、それらはヘンゼル法と非ヘンゼル法に大別できよう。ヘンゼル法は与えられた多変数多項式をヘンゼル因子に分解し、それらを基に多項式因子を求める。ヘンゼル法は多因子法と1因子法の二つに大別される。多因子法とは複数のヘンゼル因子から多項式因子を求める方法で、1因子法とは1つのヘンゼル因子から多項式因子を求める方法である。

有名な多因子ヘンゼル法として Musser [Mus71] や Wang-Rothschild [WR73] の方法がある。この方法は複数のヘンゼル因子の積を計算し、与多項式を割り切るか否かテストして多項式因子を求める。この方法はヘンゼル因子の個数が大きい場合には組合せ爆発を起こす。これに対し、佐々木らは和零算法を考案した ([SSKS91],[SSH92],[SS93],[Sas01])。これはヘンゼル因子の高次項の和が0になる組合せを見つけ、それにより多項式因子を求める方法である。和零算法は Galligo ら ([GW97],[GR01],[CGKW02] 等) により様々な改良が加えられ、現在最速の方法となっている。

有名な1因子ヘンゼル法として、整係数1変数多項式用の格子算法 [LLL82] が挙げられる。多項式のべき級数根の最小多項式から多項式因子を求める Kaltofen の方法もある [Kal85]。また、Noro-Yokoyama [NY02] はグレブナー基底の基底変換を利用する方法を提案している。

非ヘンゼル法に関して。上述の Kaltofen の算法は非ヘンゼル法にも分類できる。そのほか、既約多項式の根である代数関数を数値的に追跡する Corless らの算法 [CGHKW01]、Ruppert の定理 [Rup99] に基づいて構成された行列の固有ベクトルを計算する Gao の算法 [Gao02] などがある。

本稿では、一般ヘンゼル構成で基本的役割を演じる Moses-Yun の補間多項式 [MY73] を利用する新しい方法を提案する。具体的には、多項式因子と Moses-Yun の補間多項式のそれぞれの係数の間に双線形関係

*sasaki@math.tsukuba.ac.jp
†inaba@math.tsukuba.ac.jp

が成立するので、それを利用する。線形関係は因子多項式の係数に関して、与多項式が2変数ならば $\mathbf{K}$ 上の、3変数以上ならば従変数に関する多項式環上の線形方程式を与える。

本稿で提案する方法は線形方程式を解いて多項式因子を求めるという点で、Kaltofen や Noro-Yokoyama の方法と類似する。実際、ヘンゼル因子をべき級数根に対応させれば、本稿の方法は Kaltofen の方法に帰着する。しかし、Kaltofen の方法には大きな制限が存在する。べき級数根は一般には代数的閉体上でのみ計算できるので、因数分解は代数的閉体上のものとなる。また、べき級数根を求める際に代数的数や浮動小数を用いるため、計算が重くなったり、誤差の問題が発生する。Noro-Yokoyama の方法は上記の制限を気にせず使えるが、与えられた多項式が疎であるとき、その特性を利用しにくい。

2 Moses-Yun の補間多項式

2.1 Moses-Yun 行列

本稿では $F(x,u_1,\ldots,u_\ell)$ を数体 $\mathbf{K}$ 上の多変数多項式とし、$F(x,u)$ と略記する。F の x に関する次数を $\deg(F)$ と、F の $u_1,\ldots,u_\ell$ に関する全次数を $\mathrm{tdeg}_u(F)$ と、F の x に関する主係数を $\mathrm{lc}(F)$ と、それぞれ表す。そして、$\deg(F)=n$, $\mathrm{lc}(F)=f_n(u)$ とおく。

$F(x,0)$ が x について無平方かつ $f_n(0)\neq 0$ であると仮定し、$F(x,0)$ を既約分解する。

$$F(x,0)=F_1^{(0)}(x)\cdots F_r^{(0)}(x),\quad \deg(F_i^{(0)})=n_i\ \ (i=1,\cdots,r). \tag{2.1}$$

このとき Moses-Yun 行列 $M\in\mathbf{K}[x]^{r\times n}$ は次式で定義される。

$$\begin{cases} M=\left(W_{i,j}\right),\quad W_{i,j}\in\mathbf{K}[x]\quad (1\le i\le r;\ n-1\ge j\ge 0),\\ W_{1,j}\dfrac{F(x,0)}{F_1^{(0)}(x)}+\cdots+W_{r,j}\dfrac{F(x,0)}{F_r^{(0)}(x)}=x^j\quad (n-1\ge j\ge 0). \end{cases} \tag{2.2}$$

後で用いるため、$W_{i,0},\cdots,W_{i,n-1}$ の計算法を述べる。まず、ユークリッド拡張互除法を用いて次式を満たす多項式 V_i と $W_{i,0}$ を求める。

$$V_i F_i^{(0)}(x)+W_{i,0}F(x,0)/F_i^{(0)}(x)=1,\quad \deg(W_{i,0})<n_i. \tag{2.3}$$

次に、$W_{i,j}$ $(j=1,\ldots,n-1)$ を下記の算式で計算する。

$$W_{i,j}=\mathrm{remainder}(x^jW_{i,0},\ F_i^{(0)})\quad (j=1,\ldots,n-1). \tag{2.4}$$

実際の計算において使用する Moses-Yun の係数行列 $\bar{M}_i\in\mathbf{K}^{n_i\times n}$ を定義する。まず、$(W_{i,n-1},\cdots,W_{i,0})$ を次式のように表現する。

$$(W_{i,n-1},\cdots,W_{i,0})=\textstyle\sum_{l=0}^{n_i-1}(w_{i,n-1}^{(l)},\cdots,w_{i,0}^{(l)})\,x^l,\quad w_{i,j}^{(l)}\in\mathbf{K}\ (l=n_i-1,\ldots,0). \tag{2.5}$$

n_i 個の係数ベクトル $(w_{i,n-1}^{(l)},\ldots,w_{i,0}^{(l)})$, $0\le\ell\le n_i-1$, から成る次の行列が $\bar{M}_i$ である。

$$\bar{M}_i=\begin{pmatrix} w_{i,n-1}^{(n_i-1)} & \cdots & w_{i,0}^{(n_i-1)}\\ \vdots & \cdots & \vdots\\ w_{i,n-1}^{(0)} & \cdots & w_{i,0}^{(0)} \end{pmatrix} \tag{2.6}$$

2.2 高次の Moses-Yun 行列

$u_1,\ldots,u_\ell$ を生成元とする多項式イデアルを I とする：$I=\langle u_1,\ldots,u_\ell\rangle$. $F_1^{(k)}(x,u),\cdots,F_r^{(k)}(x,u)$ を k 次の Hensel 因子とし、次式を満たすとする。

$$F(x,u)\equiv F_1^{(k)}(x,u)\cdots F_r^{(k)}(x,u)\pmod{I^{k+1}}. \tag{2.7}$$

ただし、$F(x,u)$ の x に関する主係数 $\mathrm{lc}(F)$ は因数分解され、$F_1^{(k)},\cdots,F_r^{(k)}$ に適切に振り分けられているとする。すなわち、全ての $k\geq 1$ に対して、$\mathrm{lc}(F)=\mathrm{lc}(F_1^{(k)})\cdots\mathrm{lc}(F_r^{(k)})$ であるとする (振り分けの詳細については [Wan77] を参照)。k 次の **Moses-Yun 行列** $M^{(k)}$ を次式で定義する。

$$\begin{cases} M^{(k)}=\left(W_{i,j}^{(k)}\right), \quad W_{i,j}^{(k)}\in\mathbf{K}[x,u] \quad (1\leq i\leq r;\ n-1\geq j\geq 0), \\ W_{1,j}^{(k)}\dfrac{F(x,u)}{F_1^{(k)}(x,u)}+\cdots+W_{r,j}^{(k)}\dfrac{F(x,u)}{F_r^{(k)}(x,u)}\equiv x^j \pmod{I^{k+1}}. \end{cases} \tag{2.8}$$

ここで、$F(x,u)/F_1^{(k)}(x,u)$ 等は $u_1,\ldots,u_\ell$ に関するべき級数として計算する。$W_{i,j}^{(k)}$ も $u_1,\ldots,u_\ell$ に関するべき級数として (2.2) の $W_{i,j}$ と同様に計算できる。また、k 次の Moses-Yun 係数行列 $\bar{M}_i^{(k)}$ も前節と同様に定義できる。

$G(x,u)$ を $F(x,u)$ の多項式因子とし、次のように表す。

$$G(x,u)=g_m(u)x^m+g_{m-1}(u)x^{m-1}+\cdots+g_0(u). \tag{2.9}$$

一般性を失わずに次式を仮定する (ただし、$s\in\{1,\ldots,r\}$)。

$$G(x,u)\equiv F_1^{(k)}(x,u)\cdots F_s^{(k)}(x,u)\pmod{I^{k+1}}, \quad k\geq \mathrm{tdeg}_u(G). \tag{2.10}$$

さて、本稿の因数分解アルゴリズムにおける最重要である定理を与える。

定理 1 $i\in\{1,\cdots,s\}$ において、次の関係式が成立する。

$$\begin{cases} g_mW_{i,n-1}^{(k)}+g_{m-1}W_{i,n-2}^{(k)}+\cdots+g_0W_{i,n-m-1}^{(k)}\equiv 0 \pmod{I^{k+1}}, \\ \qquad\vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ g_mW_{i,m}^{(k)}+g_{m-1}W_{i,m-1}^{(k)}+\cdots+g_0W_{i,0}^{(k)}\equiv 0 \pmod{I^{k+1}}. \end{cases} \tag{2.11}$$

証明 $F_i^{(k)}$ $(i=1,\ldots,s)$ は I^{k+1} を法として G を割り切る。なぜなら、(2.4) より

$$g_mW_{i,m}^{(k)}+\cdots+g_0W_{i,0}^{(k)}=\mathrm{remainder}(GW_{i,0}^{(k)},F_i^{(k)})\equiv 0 \pmod{I^{k+1}}.$$

が成り立つからである。上式は (2.11) の最終行に他ならない。最終行に、$x,\ldots,x^{n-m-1}$ を掛けることにより、(2.11) の他の行も示される。 ◇

系 2 定理 1 における G は、$F(x,u)$ の多項式因子の倍数であってもよい。 ◇

3 多項式の因数分解

3.1 因数分解アルゴリズム

(2.11) では $n-m$ 個の関係式があるが、その中の 1 つのみ (以下では、最終行) を利用する。その理由は次の命題が成立するからである。

命題 3　(2.11) の中の 1 つの関係式から他の $n-m-1$ 個の関係式を導き出すことができる (証明略)。 ◇

我々の因数分解アルゴリズムは、簡単に言えば次の三つのステップから成る。

ステップ 1：$F(x,0)$ を因数分解した後、(2.1) の $F_1^{(0)}$ を $F_1^{(0)} := \mathrm{const} \times F_1^{(0)}$ (ただし、$\mathrm{const} = [f_n/\mathrm{lc}(F_1^{(0)})]_{u=0}$) と置き換え、$F_1^{(0)}(x)$ と $\tilde{F}^{(0)}(x) = f_n(0)F(x,0)/F_1^{(0)}(x)$ を初期因子として、$f_n(u)F(x,u)$ をヘンゼル構成する。

$$\begin{cases} f_n(u)F(x,u) \equiv F_1^{(k)}(x,u)\tilde{F}^{(k)}(x,u) \pmod{I^{k+1}}, \\ \mathrm{lc}(F_1^{(k)}) = \mathrm{lc}(\tilde{F}^{(k)}) \equiv f_n(u) \pmod{I^{k+1}}. \end{cases} \tag{3.12}$$

ステップ 2：因子多項式 $G(x,u)$ として、ヘンゼル因子 $F_1^{(k)}$ を含むものを探す。まず、$F_1^{(k)}$ に対応する k 次 Moses-Yun 多項式を

$$(W_{1,m}^{(k)}, \cdots, W_{1,0}^{(k)}) = \textstyle\sum_{l=0}^{n_1-1} (\tilde{w}_{l,m}, \cdots, \tilde{w}_{l,0})\, x^l, \quad \tilde{w}_{l,j} \in \mathbf{K}[u]. \tag{3.13}$$

として、Moses-Yun の係数行列 $\bar{M}_1^{(k)}$ を構成する。

$$\bar{M}_1^{(k)} = \begin{pmatrix} \tilde{w}_{n_1-1,m} & \cdots & \tilde{w}_{n_1-1,0} \\ \vdots & \cdots & \vdots \\ \tilde{w}_{0,m} & \cdots & \tilde{w}_{0,0} \end{pmatrix}. \tag{3.14}$$

ステップ 3：(2.9) の形で表現された $G(x,u)$ に対し、$g_m(u) = f_n(u)$ とおき、$g_{m-1}(u), \ldots, g_0(u)$ を未知多項式として、次の線形方程式を解いて $g_{m-1}, \ldots, g_0$ を決定する。

$$\bar{M}_1^{(k)} g \equiv 0 \pmod{I^{k+1}}, \quad g = (g_m, \cdots, g_0)^T. \tag{3.15}$$

$\mathrm{tdeg}_u(G) = e$ とおき、因数分解に必要なヘンゼル構成の次数 k を考える。各 $j \in \{0, \cdots, m\}$ に対し、

$$\begin{cases} g_j(u) = \hat{g}_j^{(0)} + \hat{g}_j^{(1)}(u) + \cdots + \hat{g}_j^{(e)}(u), \\ \hat{g}_j^{(l)} \ : \text{全次数が } l \text{ である項の和.} \end{cases} \tag{3.16}$$

とおく。$\tilde{w}_{i,j}$ $(0 \le i \le n_1-1;\ 0 \le j \le n-1)$ は次式のように表すことができる。

$$\begin{cases} \tilde{w}_{i,j}(u) = \hat{w}_{i,j}^{(0)} + \hat{w}_{i,j}^{(1)}(u) + \cdots + \hat{w}_{i,j}^{(k)}(u), \\ \hat{w}_{i,j}^{(l)} \ : \text{全次数が } l \text{ である項の和.} \end{cases} \tag{3.17}$$

(3.16), (3.17) より線形方程式 (3.15) を書き換え、全次数が同じ項どうしで係数比較することにより、次の線形方程式が得られる。

$$\begin{pmatrix} \vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \vdots \\ \vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \vdots \\ \ddots & \hat{w}_{i,j}^{(0)} & & & \hat{w}_{i,j-1}^{(0)} & & & \ddots \\ \ddots & \hat{w}_{i,j}^{(1)} & \hat{w}_{i,j}^{(0)} & & \hat{w}_{i,j-1}^{(1)} & \hat{w}_{i,j-1}^{(0)} & & \ddots \\ \ddots & \vdots & \hat{w}_{i,j}^{(1)} & \ddots & \vdots & \hat{w}_{i,j-1}^{(1)} & \ddots & \ddots \\ \ddots & \hat{w}_{i,j}^{(k)} & \vdots & \ddots & \hat{w}_{i,j-1}^{(k)} & \vdots & \ddots & \ddots \\ \vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \vdots \\ \vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \vdots \end{pmatrix} \times \begin{pmatrix} \vdots \\ \hat{g}_j^{(0)} \\ \vdots \\ \hat{g}_j^{(e)} \\ \hat{g}_{j-1}^{(0)} \\ \vdots \\ \hat{g}_{j-1}^{(e)} \\ \vdots \end{pmatrix} \equiv 0. \tag{3.18}$$

上記の係数行列の大きさは $[n_1 \cdot (k+1)] \times [(m+1) \cdot (e+1)]$ であり、右側のベクトルは $(m+1)(e+1)$ 次元である。このうち、$\hat{g}_m^{(0)}, \ldots, \hat{g}_m^{(e)}$ は $f_n(u)$ で定まるので、未知多項式の個数は $m(e+1)$ である。したがって、この線形方程式が解を持つためには、k は次の不等式を満たすことが必要である。

$$n_1 \times (k+1) \ \geq \ m \times (e+1). \tag{3.19}$$

線形方程式 (3.18) の解法の方針は、係数行列の左側の $e+1$ 列を除く $m \times (e+1)$ 列の対角化である。$F(x,u)$ が2変数多項式ならば $\hat{w}_{i,j}^{(l)} \in \mathbf{K}$ であり、対角化は容易である。与多項式が3変数以上の場合、(3.18) は多項式環 $K[u]$ 上の線型方程式となるが、この対角化は全次数のより小さい成分を基に他の成分の消去を行うことでできる。ここで、線形方程式 (3.18) は常に解を持つとは限らないことを注意しておく。もしも m と e の値が小さければ、たとえ $F(x,u)$ が2変数多項式であっても解は存在しない。また、3変数以上の場合、上述のように消去法を進めれば有理式が現れる場合があるが、その時点で解は存在しないことになる。

例 4　次の2変数多項式の因数分解を行う。

$$F(x,u) = x^4 + (u-2)\,x^3 - (u-1)\,x^2 + (u^2-2)\,x + u \tag{3.20}$$

$F(x,0)$ を因数分解する。

$$F(x,0) = x(x+1)(x-1)(x-2) \tag{3.21}$$

$F_1^{(0)} = x+1$, $\tilde{F}^{(0)} = x(x-1)(x-2) = x^3 - 3x^2 + 2x$ を初期因子として F をヘンゼル構成する：

$$F(x,u) \ \equiv \ F_1^{(3)} \tilde{F}^{(3)} \pmod{u^4} \tag{3.22}$$

$$F_1^{(3)} \ = \ x + 1 + u/2 + u^2/8 \tag{3.23}$$

$F_1^{(3)}$ に対応する3次の Moses-Yun 多項式を計算する。

$$\begin{aligned}
W_{1,3}^{(3)} &= \ \ 1/6 \ + \ 1/12u \ + \ 1/24u^2 \ - \ \ 5/288u^3 \\
W_{1,2}^{(3)} &= -1/6 \ \ \ \ \ \ \ \ - \ 1/48u^2 \ + \ \ 1/36u^3 \\
W_{1,1}^{(3)} &= \ \ 1/6 \ - \ 1/12u \ + \ 1/24u^2 \ - \ 11/288u^3 \\
W_{1,0}^{(3)} &= -1/6 \ + \ \ 1/6u \ - \ 5/48u^2 \ + \ \ 5/72u^3
\end{aligned}$$

次に、因子候補となる $G(x,u)$ を次のようにおいてみる。

$$G(x,u) = x^2 + (g_{10} + g_{11}u)x + (g_{00} + g_{01}u) \tag{3.24}$$

(2.11) より次式が成り立つ。

$$W_{1,3}^{(3)} \cdot 1 + W_{1,2}^{(3)}(g_{10} + g_{11}u) + W_{1,1}^{(3)}(g_{00} + g_{01}u) \equiv 0 \pmod{u^4} \tag{3.25}$$

u に関して係数比較を行うことで、次の線形方程式が得られる (係数行列は第1行から順に u^0, u^1, u^2, u^3 に対応する)。

$$\begin{pmatrix} 1/6 & -1/6 & 0 & 1/6 & 0 \\ 1/12 & 0 & -1/6 & -1/12 & 1/6 \\ 1/24 & -1/48 & 0 & 1/24 & -1/12 \\ -5/288 & 1/36 & -1/48 & -11/288 & 1/24 \end{pmatrix} \begin{pmatrix} 1 \\ g_{10} \\ g_{11} \\ g_{00} \\ g_{01} \end{pmatrix} = 0 \tag{3.26}$$

これを解くと次の解が得られる。

$$g_{10}=0, \quad g_{11}=1, \quad g_{00}=-1, \quad g_{01}=0 \tag{3.27}$$

以上より、$G(x,u)=x^2+ux-1$ が得られる。(3.21) の他の因子に対しても同様に行う。すると $F(x,u)$ は次の通りに因数分解される。

$$F(x,u)=(x^2+ux-1)(x^2-2x+u) \tag{3.28}$$

3.2 3変数以上の多項式の因数分解について

近年、多変数多項式の因数分解法として、因子多項式の係数を未知とし、未知係数に関する線形方程式に帰着する算法がいくつか提案されている。これらのいくつかは、因子多項式を単項式の和として表わし、単項式の未定係数を決定する方法である。最近注目を集めている Gao の算法がそうである。これらの方法では、全次数が e 以下のすべての単項式を扱うので、3変数以上の場合は行列サイズが非常に大きくなる。これに対して、本稿のアルゴリズムは係数多項式を全次数ごとにまとめて扱うので、与多項式が疎な場合、疎な性質を利用しながら、線型方程式を解くことが可能である。しかしながら、3変数以上の場合、線形方程式は解くのは実際上は多大な時間を必要とする。

よく知られている3変数以上の多項式の因数分解法として、与えられた多項式 $F(x,u_1,u_2,\ldots,u_\ell)$ に対し、2変数多項式 $\tilde{F}(x,u_1)=F(x,u_1,0,\ldots,0)$ を

$$\tilde{F}(x,u_1)=\tilde{G}_1(x,u_1)\cdots\tilde{G}_r(x,u_1) \tag{3.29}$$

と因数分解した後、$\tilde{G}_1(x,0),\ldots,\tilde{G}_r(x,0)$ を初期因子として F をヘンゼル構成し、ヘンゼル因子の組合せで多項式因子を求める方法がある。このように、2変数多項式に帰着すれば、数体 K 上で線形方程式を解くことになるので、大幅な効率化が望める。しかし、この場合でも因子組合せ問題が発生することに変わりない (因子数は大幅に少なくなるが)。

4 おわりに

本稿で提案した方法を計算機に実装して従来のヘンゼル法に基づく因数分解法と比較したが、効率に関して現段階では良い結果を得ていない。この原因の一つは、多項式因子となり得る G の次数 m が未定なので、ある程度小さい値から一つづつ増やしつつ、試行錯誤で決めざるを得ないことである。これは、この種の算法としては致し方ない。第二の原因は G の全次数 e が未定なことである。多因子法では $e\leq \mathrm{tdeg}(F)/2$ と設定できたが、1因子法では理論的には $e<\mathrm{tdeg}(F)$ とせざるを得ず、高次までヘンゼル構成するのに多大な時間がかかるのである。この場合も、たとえば $e=\mathrm{tdeg}(F)/2$ と設定して試し計算をすることで、多くの場合は計算できるが、駄目な場合もある。そのときは他の因子を使って $e=\mathrm{tdeg}(F)/2$ として計算すればよいのだが、いずれにしてもいくつかの試行が必要である。

多変数多項式の因数分解では、和零算法という極めて効率的な因子組合せ法があるので、それに勝る算法を開発するのは容易ではない。本稿では1因子法を提案したが、Moses-Yun 補間式に基づく多因子法が開発できて初めて和零算法と比肩し得る算法になるであろう。しかし、多因子法について研究を続けているが、今だ線形演算で因子が計算できる方法を見つけていない。

参 考 文 献

[CGHKW01] R. M. Corless, M. W. Giesbrecht, M. van Hoeij, I. S. Kotsireas, S. M. Watt: Towards factoring bivariate approximate polynomials. *Proc. ISSAC 2001 (International Symposium on Symbolic and Algebraic Computation)*, ACM, 85-92 (2001).

[CGKW02] R. M. Corless, A. Galligo, I. S. Kotsireas, S. M. Watt: A geometric-numeric algorithm for absolute factorization of multivariate polynomials. *Proc. ISSAC 2002 (International Symposium on Symbolic and Algebraic Computation)*, ACM, 37-45 (2002).

[Gao02] S. Gao: Factoring multivariate polynomials via partial differental equations. Math. Comp. **72**, 801-822 (2002).

[GR01] A. Galligo, D. Rupprecht: Irreducible decomposition of curves. J. Symb. Comp. **33**, 661-677 (2002).

[GW97] A. Galligo, S. Watt: A numerical absolute primality test for bivariate polynomials. *Proc. ISSAC 1997 (International Symposium on Symbolic and Algebraic Computation)*, ACM, 217-224 (1997).

[Kal85] E. Kaltofen: Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization. SIAM J. Comput. **14**, 469-489 (1985).

[LLL82] A. K. Lenstra, H. W. Lenstra, L. Lovasz: Factoring polynomials with rational coefficients. Math. Ann. **261**, 515-534 (1982).

[Mus71] D. R. Musser: Algorithms for polynomial factorizations. Ph. D. Thesis, University of Wisconsin, 1971.

[MY73] J. Moses and D. Y. Y. Yun: The EZGCD algorithm. *Proc. 1973 ACM National Conference*, ACM, 159-166 (1973).

[NY02] M. Noro, K. Yokoyama: Yet another practical implementation of polynomial factorization over finite fields. *Proc. ISSAC 2002 (International Symposium on Symbolic and Algebraic Computation)*, ACM, 200-206 (2002).

[Rup99] W. M. Ruppert: Reducibility of polynomials $f(x, y)$ modulo p. J. Num. Theory. **77**, 62-70 (1999).

[Sas01] T. Sasaki: Approximate multivariate polynomial factorization based on zero-sum relations. *Proc. ISSAC 2001 (International Symposium on Symbolic and Algebraic Computation)*, ACM, 284-291 (2001).

[SS93] T. Sasaki and M. Sasaki: A unified method for multivariate polynomial factorizations. Japan J. Indus. Appl. Math. **10**, 21-39 (1993).

[SSKS91] T. Sasaki, M. Suzuki, K. Miroslav, M. Sasaki: Approximate factorization of multivariate polynomials and absolute irreducibility testing. Japan J. Indus. Appl. Math. **8**, 357-375 (1991).

[SST92] T. Sasaki, T. Saito, T. Hilano: Analysis of approximate factorization algorithm. Japan J. Indus. Appl. Math. **9**, 351-368 (1992).

[vanH01] M. van Hoeij: Factoring polynomials and 0-1 vectors. Lecture Notes in Comput. Sci. No.1 2146, Splinger Berlin, 45-50 (2001).

[Wan77] P. S. Wang: Preserving sparseness in multivariate polynomial factorization. *Proc. 1977 MACSYMA Users Conference*, MIT, 55-61 (1977).

[WR75] P. S. Wang and L. P. Rothschild: Factoring multivariate polynomials over the integers. Math. Comp. **29**, 935-950 (1975).