数理解析研究所講究録
612巻 1987年 52-66

52

Berlekamp-Massey アルゴリズムの多次元化と Groebner 基底

豊橋技科大　阪田省二郎（ Shojiro Sakata ）

ABSTRACT:

We treat a problem having some close relevance with Groebner basis which plays an important role in Computer Algebra and Symbolic Computation. This is how to find a minimal set of two-dimensional linear recurring relations capable of generating a prescribed finite two-dimensional array over any field, where a linear recurring relation corresponds one-to-one to a bivariate polynomial with coefficients in the field.

Our algorithm for solving the problem is a two-dimensional extension of the Berlekamp-Massey algorithm for synthesizing a shortest linear feedback shift-register capable of generating a given finite sequence. The complexity of computation for an array of size n is $O(n^2)$ under some reasonable assumptioms.

1．まえがき

体 K 上の r 変数多項式環を $R:=K[x_1,\ldots,x_r]$ とする。多項式の組 $F\subseteq R$ を与えられたとき、F によって張られる イデアル $I=I(F)$ の Groebner 基底を求める問題は、B. Buchberger によって一つの構成的解法が与えられている。[1] これを問題 P_0 と呼ぼう。次に、K 上の r 次元配列 $u=(u_n)$, $n\in\Sigma_0$ (:= r 個の非負正数を成分とするあらゆるベクトルの集合) に関する線形再帰関係

$$\sum_{m\in\Gamma_f} f_m u_{m+n} = 0,\quad n\in\Sigma_0$$

を考え、これを多項式 $f=\sum_{m\in\Gamma_f} f_m x^m\in R$ に対応させて、$f[u]=0$ と書く。ただし、$x^m:=x_1{}^{m1}\ldots x_r{}^{mr}$, $\Gamma_f\subset\Sigma$。R の イデアル I に対し、I に属するあらゆる多項式に対応する線形再帰関係を満たす（線形再帰）配列の集合 $G(I):=\{u \mid f[u]=0,\ f\in I\}$ は R 加群である。線形再帰配列の R 加群と Groebner 基底の両方に関連して、互いに逆の関係にある次の二つの基本問題が考えられる。[2] ただし、以下では線形再帰関係と多項式を同義語として用いる。

問題 P_1: 多項式の組 F で張られる イデアル $I=I(F)$ に対し、線形再帰関係の組 F の解空間 $G(F)=G(I)$ を決定せよ。

問題 P_2: 配列の組 U を与えられたとき、U の特性イデアル $I=I(U):=\{f\varepsilon R \mid f[u]=0,\ u\varepsilon U\}$ の Groebner 基底を求めよ。

次も、Groebner 基底に関連する基本問題の一つである。[3)]

問題 P_3: (K 上の) 零点の組 V を与えられて、V の最大定義イデアル $I=I(V):=\{f\varepsilon R \mid f(\alpha)=0,\ \alpha\varepsilon V\}$ の Groebner 基底を求めよ。

問題 P_1 は、問題 P_0 を解いて $I=I(F)$ の Groebner 基底が求められれば解ける。一方、問題 P_3 は、各零点 α に対応して配列 $u_n=\alpha^n$ を導入すれば、問題 P_2 に帰着する。ここでは、問題 P_2 において、2次元 ($r=2$) かつ U が一つの配列 u のみの場合について、効率的に I(U) の Groebner 基底を求める アルゴリズムを示す。これは、有限長の1次元配列に対応する最簡の線形再帰関係を求める Berlekamp-Massey アルゴリズム[4,5)] の2次元版であって、Σ_0 の上で定義された適当な全順序 (ここでは、全次数順序) に従って $n\varepsilon\Sigma_0$ に関し逐次的にその点 n までの部分配列について成立する極小次数多項式の組を構成していくものである。与えられた配列が2重周期配列の有限な部分配列で、その大きさが基本周期平行四辺形の2倍以上あれば、極小次数多項式の組が一意に定められ、それは I(U) の Groebner 基底になっている。次章でアルゴリズムの概要を与える。証明および詳細な解析は JSC へ投稿中の論文[6)] に委ねる。

2．アルゴリズムの概要

まず、いくつかの概念、記号の定義を与える。

K ..... 任意の体.

x ..... 変数の対 (x_1,x_2).

K[x]:=K[x_1,x_2]... 体 K 上の２変数多項式環.

Σ_0 ..... 非負正数対 $m=(m_1,m_2)$ の集合.

$\leqq_T$ ($<_T$) ..... Σ_0 上の全次数順序、即ち $m=(m_1,m_2)\leqq_T n=(n_1,n_2)$ は $(m_1+m_2<n_1+n_2)$ or $((m_1+m_2=n_1+n_2)$ and $(m_1\geqq n_1))$ を意味する.

$\leqq$ ($<$) ..... Σ_0 上の半順序、即ち $m=(m_1,m_2)\leqq n=(n_1,n_2)$ は $(m_1\leqq n_1)$ and $(m_2\leqq n_2)$ を意味する.

$\Sigma_t^p:=\{n\varepsilon\Sigma_0 \mid t\leqq n<_T p\}$;

i, j, k, l ..... 整数.

m, n, p, q, r, s, t .. 非負整数対,即ち Σ_0 の要素.

m_1, m_2 ..... m の第一および第二成分.

n+1:=(n_1-1,n_2+1) ($n_1>0$), (n_2+1,0) ($n_1=0$).

m+n, m-n ..... 通常のベクトル的な和および差（ただし、後者では $m\geqq n$ とする）.

u, v, w ..... ２次元配列、即ち Σ_0 の部分集合 Σ_0^q から体 K の中への写像（$|q|:=|\Sigma_0^q|$ を u の大きさという）.

u_m, v_n, w_r ..... 配列 u, v, w の成分、即ち u_m は写像 u による m の像.（$u=(u_n)$ のように書く.）

u^p:=$(u_n \mid n \varepsilon \Sigma_0{}^p)$ .... $\Sigma_0{}^q$ 上で定義された u の $\Sigma_0{}^p$ 上への制限（ただし、$p \leqq_T q$ とする）.

f, g, h ..... 多項式、即ち K[x] の要素.

f_m, g_n, h_r ..... 多項式 f, g, h の係数.（$f = \sum_{m \varepsilon \Gamma_f} f_m x^m$ のように表す. ここで、Γ_f:=$\{m \mid f_m \neq 0\}$.）

LP(f):= $\max\{m \varepsilon \Gamma_f\}$ .. f の非零項 $f_m x^m$ の中で $\leqq_T$ に関する最大指数対（単に、f の次数と呼ぶ）.

F, G, H ..... K[x] の有限部分集合.

$f^{(i)}$, $g^{(j)}$, $h^{(k)}$ ..... F, G, H の番号付き要素多項式.

$f[u]_n$:= $\sum_{m \varepsilon \Gamma_f} f_m u_{m+n-s}$ （ただし、s=LP(f) とする）.

$f[u]_n=0$ ..... u に対する（n での）線形再帰関係（図1）.
任意の $n \varepsilon \Sigma_s{}^p$ に対して $f[u^p]_n=0$ または $s=LP(f) \geqq_T p$ のとき、$f[u^p]=0$ と書く.

VALPOL(u):=$\{f \varepsilon K[x] \mid f[u]=0\}$.

I(F) ..... F によって生成されるイデアル.

以下で述べるアルゴルズムでは、一つの有限配列 $u = u^q$ を与えられたとして、$n \varepsilon \Sigma_0{}^q$ に関して逐次的に Σ_0 の有限部分集合 $\Delta(u^n)$ および多項式の有限集合 $F=F(u^n)$ を求める。ただし、これらは次のように定義される。

定義： $F=\{f^{(k)} \mid 1\leqq k\leqq l\}$ が次の条件を満たすとき、 F を u^n の（に対して成立する）極小多項式系であるといい、 $F=F(u^n)$ と書く。

(1) $F\subseteq VALPOL(u^n)$;

(2) $S:=\{s^{(k)}=LP(f^{(k)}) \mid 1\leqq k\leqq l\}$ に対し

$$s_1^{(1)}>s_1^{(2)}> \ldots >s_1^{(l)}=0,\ 0=s_2^{(1)}<s_2^{(2)}< \ldots <s_2^{(l)}$$

が成立する（この場合、S によって Σ_0 の有限部分集合 $\Delta(u^n):=\cup_k\Delta_k$ が定まる。ここで、$\Delta_k:=\{m\in\Sigma_0 \mid m\leqq(s_1^{(k)}-1, s_2^{(k+1)}-1)\}$, $1\leqq k\leqq l-1$;

(3) $g\in VALPOL(u^n)$ かつ $LP(g)\in\Delta(u^n)$ を満たす多項式 g は存在しない。

一般に、$\Delta(u^n)$ は u^n に対し一意に決るが、$F(u^n)$ は必ずしも一意ではない。 $F(u^n)$ の集合を $F(u^n)$ と書く。 $F=F(u^n)$ に付随して次の条件を満たす多項式の集合 $G=\{g^{(k)} \mid 1\leqq k\leqq l-1\}$ を導入する。ここで、$|F|=|G|+1=l$ に注意。

(4) $g^{(k)}\in VALPOL(u^{(k)})$ かつ $g^{(k)}[u]_p(k)=d_p(k)\neq 0$

となる $p^{(k)}$ $(<_T n)$, $1\leqq k\leqq l-1$, が存在し、条件 (2) で導入した S と $PG=\{p^{(k)} \mid 1\leqq k\leqq l-1\}$、 $T:=\{t^{(k)}:=LP(g^{(k)}) \mid 1\leqq k\leqq l-1\}$ の間に次の関係が成り立つ。

$$s_1^{(k)}=p_1^{(k)}-t_1^{(k)}+1,\ s_2^{(k+1)}=p_2^{(k)}-t_2^{(k)}+1,\ 1\leqq k\leqq l-1.$$

なお、 $DG:=\{d_p(k)\mid 1\leqq k\leqq l-1\}$ とする。条件 (2) における $\Delta(u^n)$ の定義中の Δ_k は

$$\Delta_k=\{m\in\Sigma_0\mid m\leqq p^{(k)}-t^{(k)}\},\ 1\leqq k\leqq l-1$$

のようにも書けるから、$\Delta(u^n)$ は S によっても T と PG によっても定められる。 $F_N:=\{f\in F\mid f[u]_n\neq 0\}$, $\Delta_{FN}:=\bigcup_{f\in F_N}\{m\in\Sigma_0\mid m\leqq n-LP(f)\}$ とおくと、 $\Delta(u^{n+1})=\Delta(u^n)\cup\Delta_{FN}\supseteq\Delta(u^n)$ である。従って、$\Delta':=\Delta(u^{n+1})$ を定義する S' (F':=F(u^{n+1}) に対応) の要素は、ある $s^{(i)}=(s_1^{(i)},s_2^{(i)})$, $s^{(j)}=(s_1^{(j)},s_2^{(j)})\in S$ に対し、 次のいずれかの型のものに限られる。

(i) $(s_1^{(i)},s_2^{(i)})$;

(ii) $(n_1-s_1^{(i)}+1,n_2-s_2^{(i+1)}+1)$;

(iiia) $(n_1-s_1^{(i)}+1,s_2^{(j)})$;

(iiib) $(s_1^{(i)},n_2-s_2^{(j)}+1)$.

$F_V:=\{f\in F\mid f[u]_n=0\}\subseteq F'$ であり、残りの F'/F の多項式の候補 $h\in$ VALPOL(u^{n+1}) は次のように構成される。

$$h = h(f^{(i)},n,s^{(i)};g^{(j)},p^{(j)},t^{(j)}) := x^{r-s}f - (d_i/d_j)x^{r-n+p-t}g.$$

ここで、$f=f^{(i)}\in F_N$, $f[u]_n=d_i\neq 0$, $s=LP(f)=s^{(i)}\in S$ $(1\leqq i\leqq l)$; $g=g^{(j)}\in G$, $p=p^{(j)}\in PG$, $t=t^{(j)}\in T$, $d_j=d_p(j)\in DG$ $(1\leqq j\leqq l-1)$ であり $r=LP(h)=(r_1,r_2)$ は次で定められる。

$$r_1:=\max\{s_1,\ n_1-s_1^{(j)}+1\},\ r_2:=\max\{s_2,n_2-s_2^{(j+1)}+1\}.$$

上式のようにして多項式 h を構成することを型 <i,j> の Berlekamp 手続きと呼ぶ。

以上の定義に基づき、アルゴリズムは次のようになる。

アルゴリズム：

Step 1: n:=(0,0), F:={1}, G:=ϕ; (明らかに、S={(0,0)}, T=ϕ, PG:=ϕ, DG:=ϕ, Δ=ϕ, l=1) ;

Step 2: F_N:=(fεF | f[u]$_n \neq 0$}; If F=ϕ, then go to Step 3; else begin

F_{NV}:={fεF_N | LP(f)$\leqq$n-s となる sεS が存在する};

If F_{NV}=ϕ, then

begin

G (および S, T, PG, DG, Δ, l) を保持する;

F において F_N に属する多項式だけを 以下の Case A で述べる方法によって変更する;

end;

else begin

S および F_{NV} に属する多項式の次数より S' を定める (この場合、必ず S'$\supset$S となる)。各 s'εS' に対し、s' の型に応じて LP(f')=s' となる f'εF'=F(u^{n+l}) を次のように作る。

Case A (型 (i) の $s'=s^{(i)}=(s_1^{(i)},s_2^{(i)})$ の場合) :
$n-s^{(i)} \leqq p^{(j)}-t^{(j)}$ となる $g^{(j)} \varepsilon G$ $(1 \leqq k \leqq l-1)$ が存在するので、型 <i,j> の Berlekamp 手続きにより h を作り f':=h とおく。

Case B (型 (ii) の $s'=(n_1-s_1^{(i)}+1, n_2-s_2^{(i+1)}+1)$, $1 \leqq i \leqq l-1$, の場合) : $s^{(k)}<(n_1-s_1^{(i)}+1, n_2-s_2^{(i+1)}+1)$ となる $f^{(k)} \varepsilon F_N$ $(1 \leqq k \leqq l)$ が存在するので、型 <k,i> の Berlekamp 手続きにより h を作り、f':=h とおく。

Case C (型 (iiia) の $s'=(n_1-s_1^{(i)}+1, s_2^{(j)})$, $1 \leqq i \leqq l-1$, の場合) : 型 <j,i> の Berlekamp 手続きによって h を作り、 f':=h とおく。

Case D (型 (iiia) の $s'=(n_1+1, s_2^{(j)})$ の場合) :
$f':=x_1^{n_1-s_1^{(j)}+1} f^{(j)}$ とおく。

Case E (型 (iiib) の $s'=(s_1^{(i)}, n_2-s_2^{(j)}+1)$, $2 \leqq j \leqq l$, の場合) : 型 <i,j-1> の Berlekamp 手続きによって h を作り、 f':=h とおく。

Case F (型 (iiib) の $s'=(s_1^{(i)}, n_2+1)$ の場合) :
$f':=x_2^{n_2-s_2^{(i)}+1} f^{(i)}$ とおく。

以上によって F' が定まり、それに付随する G' も G の一部と F_{NV} によって定められる。そこで改めて F:=F', G:=G' とする。それにともなって、S, T, PG, DG, Δ, l も更新される。

end;

Step 3: if n=q, then stop; else n:=n+1; go to Step 2;

計算例： 図２に示された K=GF(2) 上の大きさ１６の２次元配列 u に対し、上記のアルゴリズムによる計算は表１に示すように進行する。例えば、n= (1,0) において f=1 は成立せず、 Case D および Case F に応じて、$\{x_1^2, x_2\} \varepsilon F(u^{(0,1)})$ を得る。 また、 n=(0,1) では、 Case A に対応して $f^{(i)} = x_2$ と $g^{(j)}=1$ より $x_2+x_1 \varepsilon F(u^{(2,0)})$ を得る。 n=(2,1) では、Case D に応じて x_1^3, Case C に応じて $x_1x_2+x_1^2+x_1+1$, CAse F に応じて $x_2^2+x_1x_2+x_2$ をそれぞれ得る。結局、計算結果は次のような多項式系となる。

$$F=\{x_1^3+x_2+x_1+1,\ x_1x_2+x_1+1,\ x_2^2+x_1x_2+x_1^2+x_1+1\} \varepsilon F(u).$$

これは I(F) の Groebner 基底であり、有限配列 u をその一部に含む（無限の大きさをもつ）二重周期配列 v の特性イデアルになっている。

３．むすび

与えられた有限２次元配列が満たす最簡な２次元線形再帰関係の組に対応する極小多項式系を逐次的に求めるアルゴリズムを示した。適当な仮定のもとで、大きさ s の配列に対する計算量は $O(s^2)$ である。

参考文献

1) Buchberger B.(1985). Groebner basis: An algorithmic method in polynomial ideal theory. Bose N.K.(ed.): 'Recent Trends in Multidimensional Systems Theory', D. Reidel Publ. Co., Chapter 6, pp.184-232.

2) Sakata S.(1981). On determining the independent point set for doubly periodic arrays and encoding two-dimensional cyclic codes and their duals, IEEE Trans. Information Theory, vol. IT-27, pp.556-565.

3) Moeller H.M., Buchberger B.(1982). The construction of multivariate polynomials with preassigned zeros, in Buchberger B.(ed.): Proc. EUROCAL '82, pp.24-31.

4) Berlekamp E.R.(1968). Nonbinary BCH decoding, 'Algebraic Coding Theory', Chapters 7 and 10, pp.176-199, 218-240.

5) Massey J.L.(1969). Shift-register synthesis and BCH decoding, IEEE Trans. Information Theory, vol. IT-15, pp.122-127.

6) Sakata S., Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array. (Submitted for publication in J. of Symbolic Computation.)

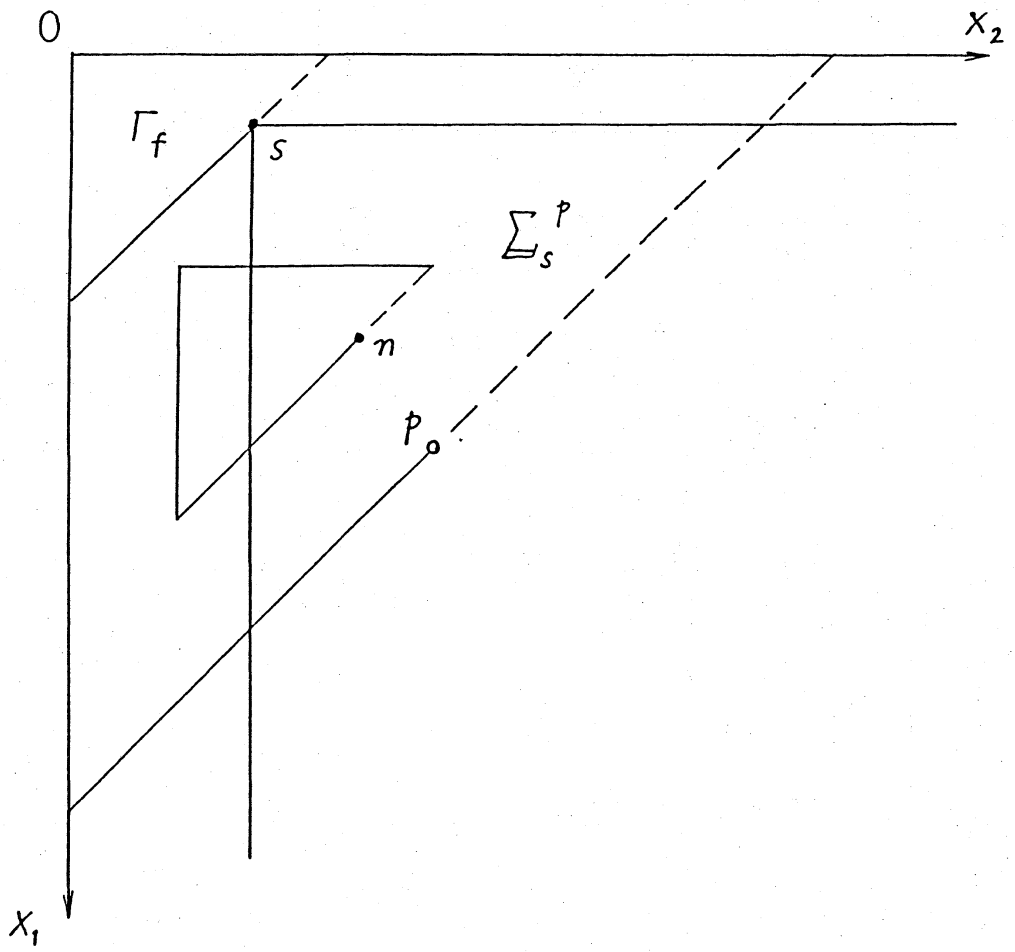


Fig. 1. LR relation

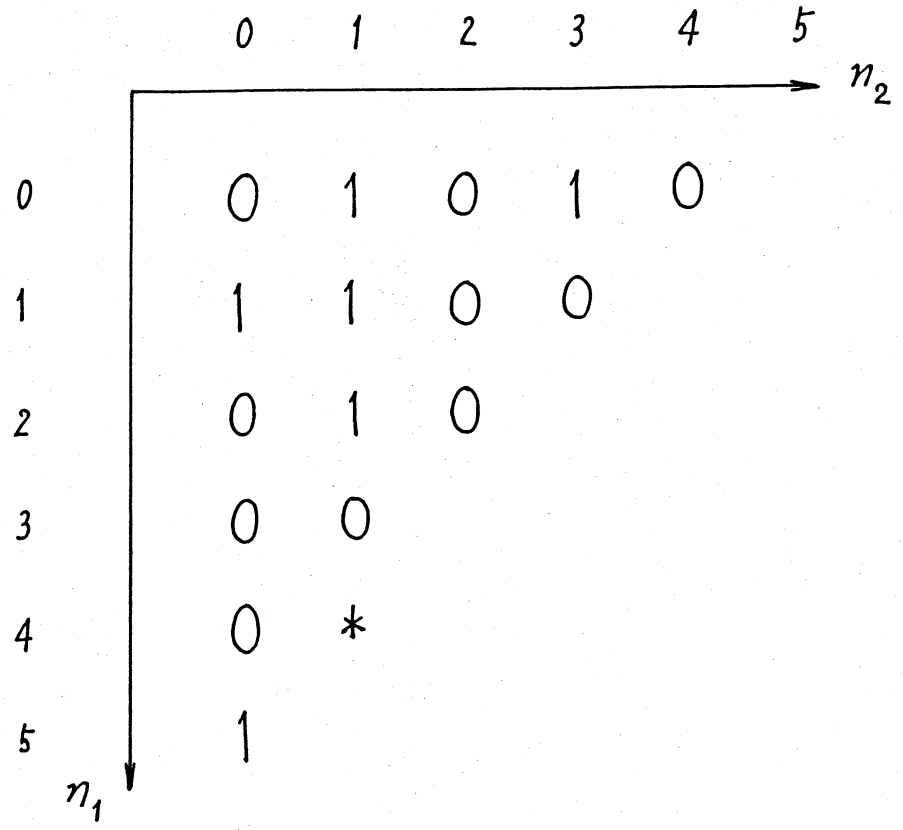
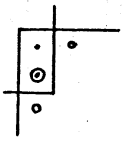
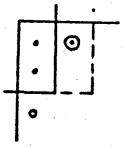
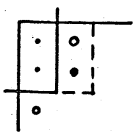
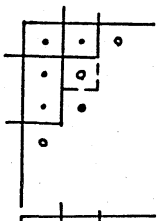
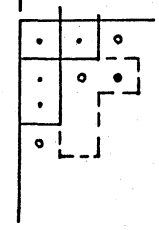


Fig. 2 A finite 2D array

Table 1. An example of computation

$\|n\|$	n	u_n	F	S	G	T	PG	Δ
0	0, 0	0	1	0, 0	ϕ			
1	1, 0	1	as above					
2	0, 1	1	X_1^2	2, 0	1	0, 0	1, 0	
			X_2	0, 1				
3	2, 0	0	X_1^2	2, 0	1	0, 0	1, 0	
			X_2+X_1	0, 1				
4	1, 1	1	as above					
5	0, 2	0	X_1^2	2, 0	1	0, 0	1, 0	
			X_2+X_1+1	0, 1				
6	3, 0	0	as above					
7	2, 1	1	as above					
8	1, 2	0	X_1^3	3, 0	X_2+X_1+1	0, 1	2, 1	
			$X_1X_2+X_1^2+X_1+1$	1, 1	X_1^2	2, 0	2, 1	
			$X_2^2+X_1X_2+X_2$	0, 2				

9	0,3	1	X_1^3	3, 0	X_2+X_1+1	0, 1	2, 1
			$X_1X_2+X_1+1$	1, 1	X_1^2	2, 0	2, 1
			$X_2^2+X_1X_2+X_2$	0, 2			
10	4,0	0	X_1^3	3, 0	as above		
			$X_1X_2+X_1+1$	1, 1			
			$X_2^2+X_1X_2+X_1^2+X_2$	0, 2			
11	3,1	0	as above				
12	2,2	0	as above				
13	1,3	0	X_1^3	3, 0	as above		
			$X_1X_2+X_1+1$	1, 1			
			$X_2^2+X_1X_2+X_1^2+X_1+1$	0, 2			
14	0,4	0	as above				
15	5,0	1	as above				
16	4,1	*	$X_1^3+X_2+X_1+1$	3, 0	as above		
			$X_1X_2+X_1+1$	1, 1			
			$X_2^2+X_1X_2+X_1^2+X_1+1$	0, 2