Optimal Algorithm for Algebraic Factoring *

Lihong Zhi
Institute of System Science, Academia Sinica
Beijing 100080, P. R. China
lzhi@mmrc.iss.ac.cn

Abstract

This paper presents an optimized method for factoring multivariate polynomials over algebraic extensions fields which defined by an irreducible ascending set. The basic idea is to convert multivariate polynomials to univariate polynomials and algebraic extensions fields to algebraic number fields by suitable integer substitutions, then factorize the univariate polynomials over the algebraic number fields. Finally, construct multivariate factors of the original polynomial by Hensel lemma and TRUEFACTOR test. Some examples with timing are include.

Keywords : Hensel lemma, integer substitution, ascending set, algebraic extensions fields.

I. Introduction

Factoring polynomials over algebraic extensions fields can be traced back to Kronecker[1]. A similar algorithm can also be found in van der Waerden [2] which was adopted and improved by Trager[3]. Along with the development of factoring polynomials over finite fields or integers, Hensel lemma becomes more and more important and it also provides an efficient method for factoring polynomials over algebraic extensions fields. Wang[4], Weinberger, Rothschild[5], Lenstra [6][7] all gave the methods based on Hensel lemma. As we known Wu's characteristic set method is also useful in factoring polynomial over arbitrary fields [8] [9] [10].

The original motivation of considering polynomial factorization over algebraic extensions fields comes from the need of it in decomposing polynomial sets into irreducible ascending sets. It is necessary for Wu's method of geometry proving and

*The present paper is partially supported by the Climbing Project Foundation of China

irreducible decomposition of algebraic varieties. Although some algebra systems such as Maple, Mathematics have implemented the algorithm for factoring polynomials over algebraic extensions fields, yet it is still need to be studied further. The reasons will be given in section 4. This paper aims to consider ways of overcoming the disadvantages of the existed methods and develop more efficient algorithm.

We will introduce some notations in section 2. The algorithm and one example are presented in section 3. At last, we give some remarks and also the timing statistics on 29 examples.

II. Preliminaries and Notations

Let Q denote the field of rational numbers, Z denote the ring of integers and $u_1, \cdots, u_d$ be a set of transcendental elements abbreviated as u. The transcendental extension field obtained from Q by adjoining the $u_i's$ will be denoted by K_0, $K_0 = Q(u_1, \cdots, u_d)$.

Definition 2.1 A non-empty finite polynomial set AS is called *an ascending set* if it can be arranged in the form:

$$A_1(u, y_1), A_2(u, y_1, y_2), \cdots, A_r(u, y_1, \cdots, y_r)$$

with $A_i \in Q[u, y_1, \cdots, y_i]$, $deg_{y_i}(A_i) > 0$ for each i, and $deg_{y_j}(A_i) < deg_{y_j}(A_j)$ for each pair $j < i$. Here, $deg_{y_j}(A_i)$ denotes the highest degree of y_j appears in the polynomial A_i. AS is said to be *contradictory* if $r = 1$, $A_1 \neq 0$ with $deg_{y_1}(A_1) = 0$.

Definition 2.2 The ascending set AS is said to be *irreducible* if A_i as a polynomial in $K_{i-1}[y_i]$ is irreducible, where $K_{i-1} = K_{i-2}(\eta_{i-1})$ with A_{i-1} as the minimal polynomial of η_{i-1} for each $i \geq 2$ and $K_0 = Q(u)$. The field K_r is called *algebraic extension field* of K_0 defined by AS.

Definition 2.3 Suppose the algebraic extension field K_r is defined as above, $K_0 = Q(u_1, \cdots, u_d)$. If $d = 0$, i.e., $K_0 = Q$, then K_r is called *algebraic number field*, otherwise it is called *algebraic function field*.

Let us denote $Q(u) - basis = \{\eta_1^{e_1} \cdots \eta_r^{e_r} : 0 \leq e_i < d_i, 1 \leq i \leq r]$, where d_i is the degree of the minimal polynomial A_i of η_i in y_i. Using some operations in [11], we conclude that it is a $Q(u)$-vector space basis for K_r.

Definition 2.4 The defect of the $Q(u) - basis$ for K_r is the lowest common multiple of the denominators appearing in the representation of these algebraic functions whose monic minimal polynomials lie in $Z[u]$.

The following propositions and theorems can be generalized from [12][13].

Proposition 2.5 The discriminant of the $Q(u) - basis$ for K_r which is defined by an irreducible ascending set AS is:

$$N_2 N_3 \cdots (discr(A_1)) \quad N_1 N_3 \cdots (discr(A_2)) \cdots,$$

where N_i is the norm map which is the product of the images under the different embeddings from K_i to K_{i-1} and $discr(A_i) = res_{y_i}(A_i, A_i')$ which is the resultant of A_i and A_i' w.r.t.(with respect to) y_i, A_i' is the differential of A_i.

Proposition 2.6 The square of the defect of the $Q(u) - basis$ divides its discriminant.

Lemma 2.7 If F_1 is a monic associate of $F \in K$ then $F_1 \in (1/f)Z[u, \eta_1, \cdots, \eta_r][x]$, where $f = res_{\eta_1}(A_1, \cdots, (res_{\eta_r}(A_r, lc(F)))$.

Theorem 2.8 Let $F \in Z[u, \eta_1, \cdots, \eta_r][x]$. If G is a monic divisor of F over K_r then $G \in 1/(fd)Z[u, \eta_1, \cdots, \eta_r][x]$, where f, d are defined as above.

Extended Hensel Lemma: Let ϕ be the ideal $(x_2 - a_2, x_3 - a_3, \cdots, x_n - a_n)$ and F be a given polynomial in $Z[x, x_2, \cdots, x_n]$, $2 \leq n$, $G_1(x), H_1(x)$ be two relatively prime univariate polynomials in $Z[x]$ such that

$$F(x, x_2, \cdots, x_n) \equiv G_1(x) H_1(x) \mod \phi,$$

then for any integer $k > 1$ there exist multivariate polynomials $G_k(x, x_2, \cdots, x_n)$ and $H_k(x, x_2, \cdots, x_n)$ such that

$$F(x, x_2, \cdots, x_n) \equiv G_k H_k \mod \phi^k$$

and $G_k \equiv G_1 \mod \phi$, $H_k \equiv H_1 \mod \phi$.

III An outline of the factorization algorithm

Now we consider the factorization of multivariate polynomial

$F(u, \eta_1, ..., \eta_r, x, x_2, ..., x_t)$ over algebraic function field K_r which is defined by an irreducible ascending set AS. The standard modular approach to factoring multivariate polynomials over algebraic function fields is divided into five steps:

Step 1 Ensure that the polynomial be square-free.

Step 2 Find lucky integer substitutions to reduce the multivariate polynomial to the univariate polynomial and the algebraic function field to the algebraic number field.

Step 3 Factor the univariate polynomial over the algebraic number field.

Step 4 Lift the univariate factors as well as the ascending set by Hensel lemma.

Step 5 Check true factors.

Step 1 and 4 are handled by the results in [14]. We will explain what conditions the integer substitution should satisfied in the first part of this section. We describe how to find true factors in the second part of this section. At last, a complete algorithm for factoring multivariate polynomials over algebraic function fields is given.

3.1 Substitution Values

The polynomial $F(x_1, x_2, \cdots, x_n)$ is square-free and primitive w.r.t. each variable in field $Q(u_1, \cdots, u_t, \eta_1, \cdots \eta_r)$. Choose a main variable x_i in such a way that makes the leading coefficient of F w.r.t. x_i lie in the field K_r or the degree w.r.t. x_i be low. Without loss of generality, we may assume x_1 to be the main variable and denote it as x. $F = a_m(x_2, \cdots, x_n)x^m + \cdots + a_0(x_2, \cdots, x_n)$, if $a_m \neq 1$, let $F = {a_m}^{m-1}F(x/a_m, x_2, \cdots, x_n)$. In the following text, we always suppose that F is monic. We also presume that every polynomial in AS is monic.

Definition 3.1 The evaluation value $\{b_1, \cdots, b_t, a_2, \cdots, a_n\}$ is lucky if it satisfies the following conditions:

1. $F_1 = F(b_1, \cdots, b_t, x, a_2, \cdots, a_n)$ is still square-free and $deg_x F_1 = deg_x F$.
2. $AS_0 = [A_1(b_1, \cdots, b_t, y_1), \cdots, A_r(b_1, \cdots, b_t, y_1, \cdots, y_r)]$ remains to be an irreducible ascending set and $deg_{y_i} A_i^* = deg_{y_i} A_i$, where $A_i^* = A_i(b_1, \cdots, b_t, y_1, \cdots, y_i)$.

We can see that almost all the evaluation values satisfy the first condition. For the second condition, we avoid the case that the irreducible ascending set becomes reducible because it may lead to extraneous factors and dense intermediate results when perform Hensel lifting.

It is fortunate that we have a lot of freedom to choose $b_i's$ which meet the condition. Here we give a description of Hilbert Irreducible Theorem.

Theorem 3.2 Let P be irreducible polynomial in $Z[y_1, \cdots, y_v, x_1, \cdots, x_t]$, by $U(N)$ we denote the number of V-tuples $(b_1, \cdots, b_v) \in Z^v$ such that $|b_i| \leq N$ for $1 \leq i \leq v$ and $P(b_1, \cdots, b_v, x_1, \cdots, x_t)$ is reducible in $Z[x_1, \cdots, x_t]$, then there exist constants a and c (depending on P) such that $U(N) \leq c(2N+1)^{v-a}$ and $0 < a < 1$.

By this theorem and primitive element theory, we can assure that there exist infinitely many specializations of the $u_i's$ which keep the irreducibility of the ascending set. It is hard to check the irreducibility of AS_0, so we need to pay more attention to this problem in the future.

The other problems even after we use lucky integer substitutions are the appearing of extraneous factors and large dense multivariate polynomials. For example : $F = x^2 - u$ is irreducible over extension field $Q(a^2 - 2)$, but if we pick the value of u

as 2 then $F \equiv x^2 - 2 \equiv (x-a)(x+a) \mod (u-2)$ over $Q(a^2-2)$. The extraneous factors will cause more complicate lifting process and combinatorial search. One method to avoid the extraneous factors is to choose two or more sets of integers as the substitution values, select the sets of integers which make the minimal number of factors. It is time-consuming to try different integer substitutions, in general, two or three different integer substitutions are enough to avoid the extraneous factors. In our algorithm, we choose two different substitutions. In order to avoid the expansion of the polynomial after the integer substitutions, we select integers with small in absolute value. Best values are 0,1,-1,etc.

3.2. Early Factor Detection

It is true that the degree of x_i of any factor is less than the degree of x_i in F for any i, but it is not true for the degree of u_i. Degree of u_i in any factors may be larger than the degree of the u_i in the coefficients of the input polynomial or in the coefficients of the minimal polynomials. For example: $F = x^2 - u = (x+u^2y)(x-u^2y)$ over the extension field defined by $AS = [u^3y^2 - 1]$. In [13] Abbott gave a possible upper bound for the degree of u_i, but it is unfortunate that the bound is often too large and Abbott's proof which based on Trager's algorithm is not complete yet.

We also need to worry about the case that $u_i's$ appear in the denominators of the coefficients of factors. For example:

$$F = x^6 - a = (x^2y - a)(x^2a + x^4y + y^2)/y^2.$$

over the extension field defined by $AS = [a^2 - y^3]$.

Because of these two cases, it is necessary to distinguish $x_i's$ from $u_i's$. If the field has no transcendentals, i.e, the field is a algebraic number field, algorithm PFACTORAS will end when the lifting degree δ is bigger than the total degree of x_i in F for $i > 1$, combining factors to find true factors. Otherwise use early detection technique.

In the following algorithm PFACTORAS, after we get

$$\begin{aligned} F \equiv\ & {G_1}^{(\delta)}(u_1, \cdots, u_t, \eta_1, \cdots, \eta_r, x_1, \cdots, x_n) \cdots \\ & {G_m}^{(\delta)}(u_1, \cdots, u_t, \eta_1, \cdots, \eta_r, x_1, \cdots, x_n) \mod (\phi^{\delta+1}, AS), \end{aligned}$$

when $\delta > deg_u(F) + \sum_{i=1}^{r} deg_u(A_i) + \sum_{i=2}^{n} deg_{x_i} F$, we begin TRUEFACTOR test.

Let $F_i^* \equiv DF_i \mod (\phi^{\delta+1}, AS)$, $G_i = F_i^*/D$ over $Q(u_1, \cdots, u_t, \eta_1, \cdots, \eta_r)$, where F_i is either some ${G_i}^{(\delta)}$ or the product of two or more ${G_i}^{(\delta)} \mod (\phi^{\delta+1}, AS)$ and D is the largest factor whose square can divide the discriminant of K_r. True factors of F over K_r can be obtained from those $G_i's$.

Algorithm PFACTORAS

Input: A square-free polynomial
$F \in Q(u_1, \cdots, u_t, \eta_1, \cdots, \eta_r)[x_1, \cdots, x_n]$,
an irreducible ascending set
$AS = [A_1(u_1, \cdots, u_t, y_1), \cdots, A_r(u_1, \cdots, u_t, y_1, \cdots, y_r)]$.
Output: A list of irreducible factors over $Q(u_1, \cdots, u_t, \eta_1, \cdots, \eta_r)$.

Step 1 Choose a set of lucky evaluation value $b_1, \cdots, b_t, a_2, \cdots, a_n$ such that

$$F_0 = F(b_1, \cdots, b_t, \eta_1, \cdots, \eta_r, x_1, a_2, \cdots, a_n),$$

$$AS^{(0)} = [A_1(b_1, \cdots, b_t, y_1), \cdots, A_r(b_1, \cdots, b_t, y_1, \cdots, y_r)].$$

Step 2

$$\begin{aligned} PUFACTORAS(F_0) \;\equiv\; & {G_1}^{(0)}(\eta_1, \cdots, \eta_r, x_1) \cdots \\ & {G_m}^{(0)}(\eta_1, \cdots, \eta_r, x_1) \;\; mod \;\; (\phi, AS), \end{aligned}$$

where $\phi = (u_1 - b_1, \cdots, u_t - b_t, x_2 - a_2, \cdots, x_n - a_t)$;
Step 3 Hensel lift for factors ${G_i}^{(0)}$ and $AS^{(0)}$ such that

$$\begin{aligned} F \;\equiv\; & {G_1}^{(\delta)}(u, \eta_1, \cdots, \eta_r, x_1, \cdots, x_n) \cdots \\ & {G_m}^{(\delta)}(u, \eta_1, \cdots, \eta_r, x_1, \cdots, x_n) \;\; mod \;\; (\phi^{\delta+1}, AS). \\ AS \;\equiv\; & AS^{(\delta)} \;\; mod \;\; (\phi^{\delta+1}) \end{aligned}$$

Step 4 By TRUEFACTOR test, we obtain

$$F = G_1(u, \eta_1, \cdots, \eta_r, x_1, \cdots, x_n) \cdots G_s(u, \eta_1, \cdots, \eta_r, x_1, \cdots, x_n) \;\; over \;\; K$$

Algorithm PUFACTORAS
Input: A square-free polynomial $F \in Q(\eta_1, \cdots, \eta_r)[x]$,
an irreducible ascending set $AS = [A_1(y_1), \cdots, A_r(y_1, \cdots, y_r)]$.
Output: a list of irreducible factors over $Q(\eta_1, \cdots, \eta_r)$.

Step 1 Choose a set of integers c_i, computing
$CS = CHARSET(\{AS \cup \{w - c_1 y_1 - \cdots - c_r y_r\}\})$,
according to the order:$w \prec y_1 \prec \cdots \prec y_r$.
Step 2 If CS is not quasi-linear then go to Step 1 and try other c_i.
Step 3 $CS = \{C_0(w), y_1 - C_1(w), \cdots, y_r - C_r(w)\}$.
Step 4 $F^* = F(C_1(w), \cdots, C_r(w), x)$.
$UFACTOR(F^*) = F_1(w, x) \cdots F_s(w, x)$ over $Q(C_0(w))$.

Step 5 Substitute $w = \sum_{i=1}^{r} c_i y_i$ for w in F_i.

Step 6 Return $F = F_1(y_1, \cdots, y_r, x) \cdots F_s(y_1, \cdots, y_r, x)$.

Algorithm UFACTOR

Input: $F(x, \alpha)$ a square-free polynomial over $Q(\alpha)$,
$m(x)$ the monic minimal polynomial of α.

Output: A list of irreducible factors over $Q(\alpha)$.

Step 1 Choose a positive integer s:
$G(x, \alpha) = F(x - s\alpha, \alpha)$,
$R(x) = res_y(G(x, y), m(y))$.

Step 2 If $R(x)$ is not square-free then factor
$R(x)/(GCD(R(x), R'(x))) = F_1(x) \cdots F_s(x)$.
If $s = 1$ go to Step1;
For each factor F_i, compute
$G_i = GCD(F(x + s\alpha, F_i(x + s\alpha))$,
$F^* = F(x + s\alpha)/(G_1 \cdots G_s)$.
Return $F = UFACTOR(F^*) \prod_{i=1}^{s} UFACTOR(G_i)$.

Step 3 Factor $R(x) = H_1(x) \cdots H_t(x)$ over Q.

Step 4 If $t = 1$ then return(F).

Step 5 For each H_i do
$H_i(x, \alpha) = GCD(H_i(x, \alpha), G(x, \alpha))$ *over* $Q(\alpha)$,
$G(x, \alpha) = G(x, \alpha)/H_i(x, \alpha)$ *over* $Q(\alpha)$,
$H_i(x, \alpha) = H_i(x + s\alpha, \alpha)$.

Step 6 Return $F(x, \alpha) = H_1(x, \alpha) \cdots H_t(x, \alpha)$.

Example 1. To factor
$F = x^4 - ax^2r - yabr + ar^2x^2 - ar^2yb - y^2ab + y^2r - r^4$ over $Q(r, a, b)$
where a, b are defined by $AS = [a^2 - r, b^2 - ab + r]$.

Step 1 Picking the substitution value 2 for r and 1 for y, F is mapped to $F_0 = x^4 + 2ax^2 - 7ab - 14$, AS is mapped to $AS^{(0)} = [a^2 - 2, b^2 - ab + 2]$ which is still an irreducible ascending set.

Step 2 Computing a characteristic set of $\{AS^{(0)} \cup \{w - b\}\}$ according to the order $w \prec a \prec b$, we get $\{w^4 + 2w^2 + 4, 2a + w^3, b - w\}$.
Substituting $\{a = -w^3/2, b = w\}$ in F_0,
factoring $F_0 = (x^2 + w - 2w^3)(x^2 + w^3 - w)$ *over* $Q(w)$,
we have $F_0 = (x^2 + b + 4a)(x^2 - b - 2a)$ over $Q(a, b)$.

Step 3 Hensel lift $AS^{(0)}$ and the two factors of f:

$$\begin{aligned} F &\equiv (x^2+yb+4ar-4a)(x^2-yb-ar) \ \ mod \ \ ((r-2,y-1)^2, AS); \\ AS &\equiv [a^2-r, b^2-ab+r] \ \ mod \ \ (r-2,y-1)^2; \\ F &\equiv (x^2+yb+ar^2)(x^2-yb-ar) \ \ mod \ \ ((r-2,y-1)^3, AS); \\ AS &\equiv [a^2-r, b^2-ab+r] \ \ mod \ \ (r-2,y-1)^3. \end{aligned}$$

Step 4 We can check that
$F = (x^2+yb+ar^2)(x^2-yb-ar)$ over $Q(r,a,b)$.

IV. Experiments

We have implemented the algorithms in MAPLE 5.2. Below we give the timing statistics on a set of 29 examples. The experiments were all made in MAPLE 5.2 on SPARC 2. The timings are given in CPU seconds. The meaning of the headings of the table is explained as follows: Ex–the example number; Cfactor–time for D.M.Wang's algorithm which included in his CharSet package; Factor1–time for the MAPLE 5.2 built-in factorization function using the method of Trager; Factor2–time for the MAPLE 5.2 built-in factorization function using the method of Lenstra; Zfactor–time for our implementation for factorization. We use the long dash — to indicate that there are no result after 5 hours.

Timing Statistics in MAPLE 5.2

Ex	Cfactor	Factor1	Factor2	Zfactor
1	0.25	1.63	2.45	0.48
2	1.45	1.18	1.70	1.13
3	1.23	3.20	4.53	1.90
4	0.18	1.38	2.18	1.43
5	1.18	1.08	1.53	0.91
6	0.90	2.51	3.28	1.93
7	1.33	2.21	4.15	2.25
8	4.25	4.78	5.51	3.30
9	2.00	9.00	8.38	6.65
10	—	1277	897	25.00
11	—	—	—	59.00
12	0.61	2.18	0.21	0.46
13	3.95	6.45	22.83	4.86
14	5.26	4.20	3.23	3.96
15	2.73	3.68	2.76	1.91
16	1.78	2.00	4.33	1.15
17	16.3	3.76	4.51	15.81
18	403.6	3444	422.58	65.53
19	0.76	1.66	1.16	1.55
20	6.70	6.68	11.56	6.25
21	1.85	2.66	3.28	0.81
22	11.46	10.96	6.01	2.91
23	290.70	—	—	23.15
24	2.51	6.83	10.95	3.95
25	11.91	9.63	14.60	11.78
26	—	4.61	10.08	1.50
27	2091	16.38	17.05	14.00
28	—	67.60	61.33	58.51
29	—	—	—	10088

V. Conclusions The experiments show that our algorithm is efficient for factoring polynomials over algebraic extension fields defined by an irreducible ascending set, especially for the cases involving the transcendental elements. We can also see that Maple's built-in factorization function is not sufficient for using. Factor1 and Factor2 have difficult in factoring the example 11 and 23, 29. For example 10 they also take longer time. Cfactor has made great improvement but it may also be inefficient for factoring polynomial involving transcendental elements, see examples

10, 11, 28 and 29.

Acknowledgments The present paper is part of the author's Ph.D-thesis written under the supervision of Prof.Wu Wentsun at Institute of System Science, Academia Sinica. I would like to thank Prof.Wu for initiating and supervising my research. I am also grateful to Prof. Liu Zhuojun for his suggestions and checking the style of the manuscript.

Reference

1. Kronecker L.: Grundzuge einer arithmetischen Theorie der algebraischen Groben. J.f.d.reine u.angew.Math.92, 1882, pp.1-22.

2. van der Waerden. B.L.: Modern algebra. vol.1 New York 1953.

3. Trager B.M.: Algebraic Factoring and Rational Function Integration. SYMSAC 1976, pp.219-226.

4. Wang P.S.: Factoring Multivariate Polynomials over Algebraic Number Fields. Math Comp, 1976, 30: 324-336.

5. Weinberger P.J. Rothschild, L.P.: Factoring Polynomials over Algebraic Number Fields. ACM Trans.Math.Software, 1976, 2: 335-350.

6. Lenstra A.K.: Lattices and Factorization of Polynomials over algebraic Number Fields. Proc.EUROCAM'82, 32-39.

7. Lenstra A.K.: Factoring Multivariate Polynomials over Algebraic Number Fields. SIAM J.Comp, 1987, 16: 591-598.

8. Hu S., Wang D.M.: Fast Factorization of Polynomials over Rational Number Field or its Extension Fields. Kexue Tongbao, 1986, 31: 150-156.

9. Wang D.M.: A Method for Factorizing Multivariate Polynomials over Successive algebraic extension Fields. Preprint.RISC-LINZ Johannes Kepler University,Austria 1992.

10. Wu W.T.: Some Remarks on Factorization and GCD of Multivariate Polynomials. MM Research PrePrints No 11 1993, pp.1-15.

11. Wu W. T.: Basic Principles of Mechanical Theorem Proving in Elementary Geometries.J. Syst. Sci. Math. Sci. **4**,207–235(1984).

12. Encarnacion, M. K.: On a Modular Algorithm for Computing GCDs of Polynomials over Algebraic Number Fields. ISSAC'94 58-65.

13. Abbott J.A.: On the Factorization of Polynomials over Algebraic Fields. PH.D thesis.school of Math.Scis.University of Bath England, 1989.

14. Zhi L.H.: Polynomial Factorization over Algebraic Fields and its Applications . PH.D thesis. Institute of Systems Science, 1996.

1. $F = x^4 - 1$; $AS_1 = [a^2 + 1]$; $a \prec x$;
2. $F = x^4 + ax^3 + 2x^3 + 2ax^2 + 5x^2 + 2ax + 6x + 6$; $AS_1 = [a^2 + 1]$; $a \prec x$;
3. $F = 2ax^4 + 3x^4 + 3ax^3 - 2x^3 - 2ax^2 - 2x^2 + ax - 1$; $AS_1 = [a^2 + 1]$; $a \prec x$;
4. $F = y^2 + x^2$; $AS_1 = [a^2 + 1]$; $a \prec x \prec y$;
5. $F = x^2 + x - 1$; $AS_1 = [a^2 - 5]$; $a \prec x$;
6. $F = x^4 + 3x^2 + 4$; $AS_1 = [a^2 + a + 2]$; $a \prec x$;
7. $F = 64x^6 - 4$; $AS_1 = [a^3 + 2]$;$a \prec x$;
8. $F = 16x^4 + 8x^3 + 4x^2 + 2x + 1$; $AS_1 = [a^4 + a^3 + a^2 + a + 1]$; $a \prec x$;
9. $F = x^4 + y^4$; $AS_1 = [a^4 + 1]$; $a \prec x \prec y$;
10. $F = x^8 + 2x^7 + (-y - z^2 - 8)x^6 + (-4y + 6z^2 - 40)x^5 + (y^2 + (2z^2 - 48)y + z^4 + 32z^2 + 256)x^4 + (-4y^2 + (2z^2 + 32)y - 4z^4 + 32z^2 + 960)x^3 + (-y^3 + (-3z^2 + 28)y^2 + (2z^4 - 4z^2 + 384)y - z^6 - 32z^4 + 144z^2 - 1152)x^2 + (2y^3 + (-4z^2 + 72)y^2 + (6z^4 + 24z^2 - 576)y + 2z^6 - 48z^4 - 576z^2 + 3456)x + y^4 + (-z^2 - 12)y^3 + (z^4 + 24z^2 + 144)y^2 + (-z^6 + 24z^4 - 432z^2 - 1728)y + z^8 - 12z^6 + 144z^4 - 1728z^2 + 20736$; $AS_1 = [a^4 + a^3 + a^2 + a + 1]$; $a \prec y \prec x \prec z$;
11. $F = x^5 - 5vyx^3 - 5uzx^3 + 5uy^2x^2 + 5z^2yx^2 + 5v^2zx^2 + 5vu^2x^2 - 5zy^3x + 5v^2y^2x - 5vuzyx - 5u^3yx - 5vz^3x + 5u^2z^2x - 5v^3ux + y^5 - 5vuy^3 + 5vz^2y^2 + 5u^2zy^2 - 5uz^3y - 5v^3zy + 5v^2u^2y + z^5 + 5v^2uz^2 - 5vu^3z + u^5 + v^5$; $AS_1 = [a^4 + a^3 + a^2 + a + 1]$. $u \prec v \prec x \prec y$.
12. $F = x^2 + ax + 1$; $AS_1 = [a^2 + 1]$; $a \prec x$;
13. $F = x^3 - 3$; $AS_1 = [a^6 + 3a^5 + 6a^4 + a^3 - 3a^2 + 12a + 16]$; $a \prec x$;
14. $F = x^{14} - 2x^8 - 2x^7 - 2x^4 - 4x^3 - x^2 + 2x + 1$; $AS_1 = [a^2 - 2a - 1]$; $a \prec x$;
15. $F = (47x^6 + 21x^5 + 598x^4 + 1561x^3 + 1198x^2 + 261x + 47)/47$; $AS_1 = [a^2 - a + 3]$; $a \prec x$;
16. $F = (16x^6 - 1)/16$; $AS_1 = [a^3 + 2]$; $a \prec x$;

17. $F = x^8 - x^7 - x^6 + x^4 - x^2 + x + 1$; $AS_1 = [a^4 - a + 1]$; $a \prec x$;

18. $F = x^9 + 9x^8 + 36x^7 + 69x^6 + 36x^5 - 99x^4 - 303x^3 - 450x^2 - 342x - 226$; $AS_1 = [a^9 - 15a^6 - 87a^3 - 125]$; $a \prec x$;

19. $F = x^2 + x + 1$; $AS_1 = [a^2 + 3]$; $a \prec x$;

20. $F = 745092b - 252156 + 540900c + 21032664c^2b^2 + 2010720b^2 + 7117713c^2b - 132367c^2 + 3076830c^3 - 7843500c^3b^2 + 2792322c^3b - 3779244bc - 10724400b^2c + 21225240bc^5 + 26306208b^2c^5 + 8257464c^5 - 436536c^4 + 6094008b^2c^4 + 594432bc^4$; $AS_1 = [-1 + b + 6b^2 + 12b^3]$; $b \prec c$;

21. $F = 22540009426896317848166025972903447015109 2xy^2 -$

    $1320363182624852672643752736926987173041 08xy +$

    $1933627112800367802354514382818148222856 2x -$

    $1593819351377205448494726228826851114990 38y^2 +$

    $9336377600647791121728498603633575284698 4y -$

    $1367280843761763879254867459499319709746 5$; $AS_1 = [2x^2 - 1]$; $x \prec y$;

22. $F = x^6 - 3x^4 + 3x^2 - xa^3 - x^5a^3 + 2x^4a^3 - x^2a^2 + x^3a^3 - 1 - xa^2 - x^5a + x^4a^2 - x^5a^2 - xa + 2x^3a^2 - 2x^2a^3 + 2x^3a$; $AS_1 = [a^4 - a + 1]$; $a \prec x$;

23. $F = 10x^3 + 4x^2z^2 + 4x^2y^3 - 5xy - 2yz^2 - 5zx - 2y^3z + 2y^2z^2 - 8y^2 - 4z^2 + 2 - 6z$; $AS_1 = [-1 + z^3 - z^2 + r^2, -y^4 - y^2z^2 + y^2r^2 + z^2 - 2 - z + r^2z + r^2]$; $z \prec y \prec x$;

24. $F = -370x^2y - 10x^3 + 60x^2z + 4xy - 24zy + 74rzy + 2rzx + 37rz - 37y + 12r^3 - 24r$; $AS_1 = [2 + z^2, -2z + y + 4y^2]$; $z \prec y \prec x$;

25. $F = x^4 + 2x^3 + x^2 - 1$; $AS_1 = [a^2 + 1, b^2 - 3, c^2 + 5]$; $a \prec b \prec c \prec x$;

26. $F = (2xy + 1)z^2 + 1$; $AS_1 = [3x^2 + x + 2, xy^2 + 2]$; $x \prec y \prec z$;

27. $F = 10x^3 + 4x^2z^2 + 4x^2y^3 - 5xy - 2yz^2 - 5zx - 2y^3z + 2y^2z^2 - 8y^2 - 4z^2 + 2 - 6z$; $AS_1 = [8 + z^3 - z^2, -y^4 - y^2z^2 + y^29 + z^2 + 8z + 7]$; $z \prec y \prec x$;

28. $F = 10x^3 + 4x^2z^2 + 4x^2y^3 - 5xy - 2yz^2 - 5zx - 2y^3z + 2y^2z^2 - 8y^2 - 4z^2 + 2 - 6z$; $AS_1 = [-1 + z^3 - z^2 + r^2, -y^4 - y^2 * z^2 + y^2 * r^2 + z^2 - 2 - z + r^2 * z + r^2]$; $r \prec z \prec y \prec x$;

29. $F = x^{11} - (2 + z^3)^3$; $AS_1 = [(z + a)^{11} - 2 - z^3]$; $a \prec z \prec x$.