ICOT Technical Report: TR-194

TR-194

Factorization of uni-variate polynomials over finite fields

by
K. Yokoyama and T. Takeshima
(Fujitsu Ltd.)

July, 1986

ICOT

Mita Kokusai Bldg. 21F
4-28 Mita 1-Chome
Minato-ku Tokyo 108 Japan

(03) 456-3191~5
Telex ICOT J32964

Institute for New Generation Computer Technology

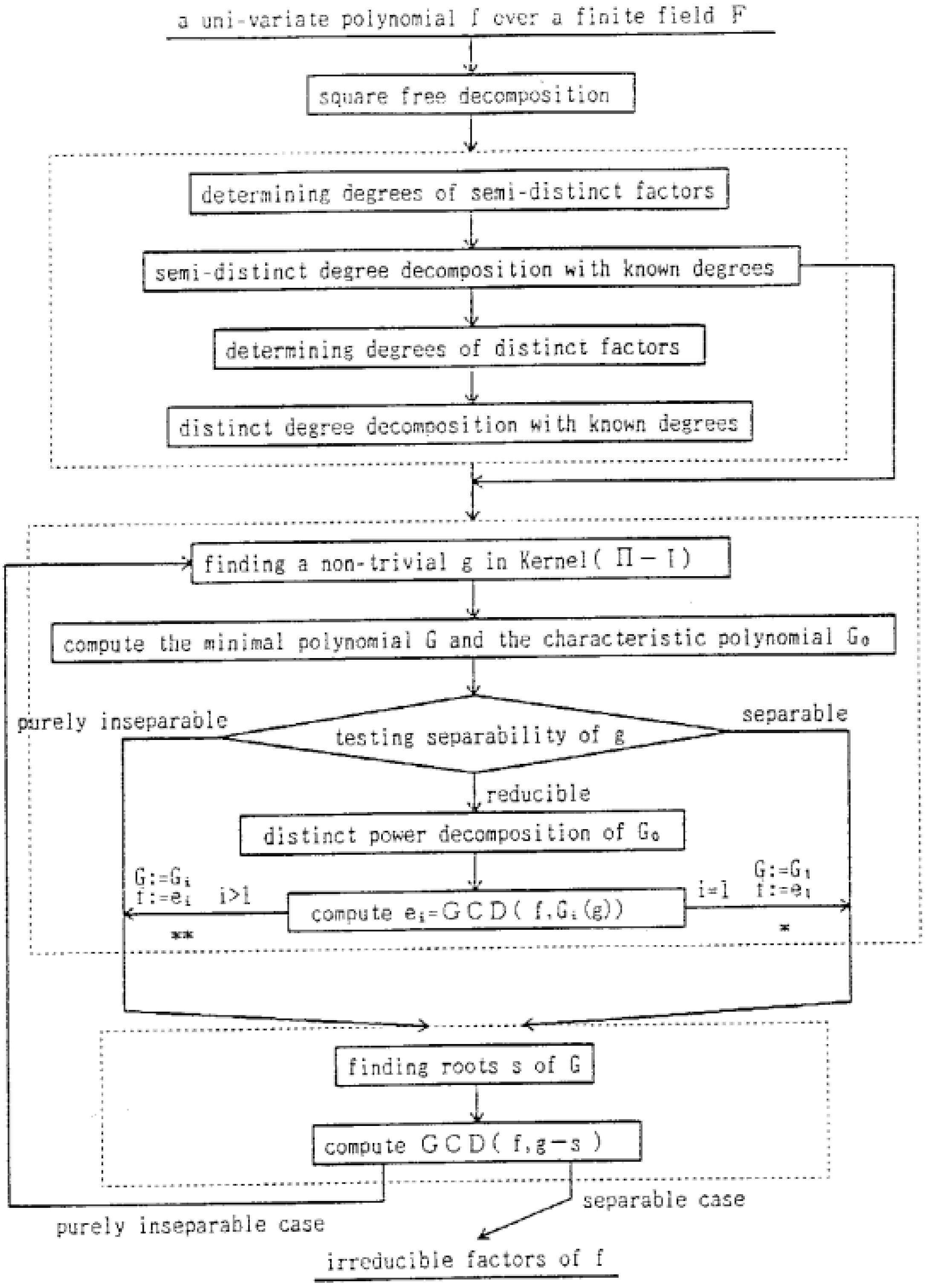
Factorization of uni-variate polynomials over finite fields

Kazuhiro Yokoyama

Taku Takeshima

Abstract

The Berlekamp's factorization algorithm for uni-variate polynomials over finite fields is enhanced in its sub-algorithm: Distinct degree decomposition and finding non-trivial factors. The key points are: (1) Determination of distinct degree factors in advance by using the concept of p-distinct degree factors; (2) separability test for an arbitrary non-trivial g in Kernel(π-I) where π is the Frobenius map on $GF(q)[x]/(f(x))$; and (3) finding root reduction, that is, reduction of "finding roots of the minimal polynomial $G(x)$ of g" problem to "finding non-trivial factors of $G(x)$" problem. Faster GCD algorithm can be utilized on account that degree of the resulting factor is known in advance. Separability test determines how many irreducible factors are contained in GCD(f,g-s) where s is a root of $G(x)$. In addition, it gives non-trivial factors without "finding roots" procedure, even if GCD(f,g-s) fails to produce an irreducible factor.


a uni-variate polynomial f over a finite field F
square free decomposition
determining degrees of semi-distinct factors
semi-distinct degree decomposition with known degrees
determining degrees of distinct factors
distinct degree decomposition with known degrees
finding a non-trivial g in Kernel(Π − I)
compute the minimal polynomial G and the characteristic polynomial G₀
purely inseparable
separable
testing separability of g
reducible
distinct power decomposition of G₀
G:=Gᵢ
f:=eᵢ
i>1
compute eᵢ=GCD(f,Gᵢ(g))
i=1
G:=G₁
f:=e₁
**
*
finding roots s of G
compute GCD(f,g−s)
separable case
purely inseparable case
irreducible factors of f

*: g is separable w.r.t. e_1 and G_1 is the minimal polynomial of g w.r.t. e_1.

**: g is purely inseparable w.r.t. e_i, G_i is the minimal polynomial of g w.r.t. e_i and i is the multiplicity og G_i.

Fig. 2.

The last contribution is concerned with "finding roots" problem. We can choose the problem to find out non-trivial factors of G instead of the problem to find out roots of G. It is noted that our algorithm assures that every root of G is necessary and sufficient to proceed further steps. The reason for this problem reduction is that GCD(f,B(g)) gives a non-trivial factor of f for every B which is a non-trivial factor of G. We notice that in separable case, the degree of G is the number r of irreducible factors ($r \leq n$), and in many cases $r << n$ is expected.

2. Outline of the Algorithm. In this section we describe the outline of an improved algorithm based on Berlekamp's algorithm. Details of each steps are mentioned in the latter sections. Let F be an arbitrary finite field GF(q) of q-elements and p denote the characteristic of F, i.e q is a power of p.

Algorithm Factoring a Polynomial.

Input: a monic polynomial f in F[x] where F is an arbitrary finite field of q-elements.

Output: irreducible factors of f.

1. Square-free decomposition.

Using derivative of f and finding algorithm of q-th root of F, remove the repeated factors of f. (c.f. Berlekamp (1970))

2. Distinct Degree Decomposition. (New DDD)

We describe some definitions needed in this step.

The distinct degree factor of f with degree m is defined as the product of all irreducible factors of f with degree m.

The p-distinct degree factor of f with degree m is defined as the product of all irreducible factors of f with degree $p^i m$ and $i \geq 0$.

2.1. Determining Degrees of p-Distinct Degree Factors.

2.1.1. Compute the characteristic polynomial Q(x) of π as a linear mapping where π is the Frobenius mapping of an F-algebra F[x]/(f(x)).

1. Introduction. Research of the factorization of uni-variate polynomials over finite fields is originated to the algorithm of Berlekamp (1967). He published an improved one in Berlekamp (1970) after the suggestion from Zassenhaus. (c.f. Zassenhaus (1969)) These two paper have given a basic framework to the research of factoring algorithm. The framework of his algorithm is illustrated in Fig. 1.

Fig. 1.

Notable research contributions after Berlekamp such as Moenck (1977), Lazard (1979), Rabin (1980) and Cantor & Zassenhaus (1981) are all devoted to improve the algorithms in concern with "finding roots" sub-algorithm or to apply the methods of "finding roots" to direct factoring algorithms. We investigate algorithm steps mainly before and after "finding roots" step, and added new steps to the current algorithm to improve total efficiency.

Several new steps are introduced, such as determining degrees of p-distinct degree factors (DDPDF), p-distinct degree decomposition with known degrees (PDDD) and determining degrees of distinct factors (DDDF), before DDD step so that the fast GCD algorithm (c.f. von zur Gathen (1984)) should be applicable in DDD step and all steps after DDD.

Another step for improvement is the testing separability (TS & FNTF) before "finding roots" step. In this step we check up the number of irreducible factors contained in GCD(f,g-s) in advance to the actual execution of GCD. Moreover it gives non-trivial factors without executing "finding roots" step, even if GCD(f,g-s) should fail to produce an irreducible factor. In more detail, separability test is applied to an arbitrary non-trivial g in Kernel(Π-I) where Π is the Frobenius map on GF(q)[x]/(f(x)). It screens out three cases; separable case, purely inseparable case and reducible case. In the last case, factoring f is reduced to factoring f's non-trivial factors, which are taken out "finding roots" procedure. In separable case, GCD(f,g-s) gives an irreducible factor for every root s of the minimal polynomial G of g. In purely inseparable case, GCD(f,g-s) gives a product of t irreducible factors, for a known integer t, for every root s of the minimal polynomial G of g.

3.3. If $G=G_0$, then go to step 4. (In this case, g is said to be separable with respect to f.)

Otherwise, decompose G_0 to distinct power parts G_i. (In this case, g is said to be inseparable with respect to f.)

3.4. If there is only one non-trivial power part i.e. $G_0=(G_t)^t$, then go to step 5. (In this case, $G_t=G$. g is said to be purely inseparable with respect to f and t is said to be the multiplicity of G.)

Otherwise compute $e_i=GCD(f,G_i(g))$ for non-trivial power parts G_i. (In this case, g is said to be reducible with respect to f.)

Then g is separable with respect to e_1 and purely inseparable with respect to e_i with i>1. In each cases, G_i is the minimal polynomial of g with respect to e_i. Go to step 4 with (e_i,G_i,g) instead of (f,G,g). (In this step, we can also use GCD-algorithms with a known degree of GCD.)

4. Finding Irreducible Factors of f. (FIF)

4.1. Find all roots c_i's of the minimal polynomial G.

4.2. Compute $H_i=GCD(f,g-c_i)$.

If g is separable, then H_i is an irreducible factor of f.

If g is purely inseparable case, then H_i is a product of t-irreducible factors of f where t is the multiplicity of G. Then go to step 4 replacing f by H_i. (Similarly as in previous steps, we can use GCD-algorithms with a known degree of GCD.)

We may choose the followin step 5 instead of step 4.

5. Finding a Non-Trivial Factor.

5.1. Find a non-trivial factor B of G by some probabilistic algorithm.

5.2. Compute H=GCD(f,B(g)).

If degree b=1, then H is an irreducible factor (separable case) or a product of t irreducible factors (purely inseparable case).

If d=degree b>1, then H is a product of d irreducible factors of f (separable case) or a product of d t irreducible factors of f.

2.1.2. Compute the degrees $d(m)$ of p-distinct degree factors with degree m of f for integers m prime to p by using the fact that $Q(x)=\prod(x^m-1)^{t(m)}$ and $d(m)=mt(m)$.

2.2. p-Distinct Degree Decomposition with known degrees.

Use modified Berlekamp's DDD-algorithm. (c.f. Berlekamp (1970)) But we only have to compute $GCD(f,x^{q^{m'}}-x)$ for integers m prime to p such that $t(m)$ is positive, where $m'=p^t m$ and p^t is the maximal p-power in the condition that $p^t \leqq n$.

Moreover we can use GCD-algorithms with a known degree.

If $t(m)<p$, then the factor obtained in 2.2 is the distinct degree factor of f with degree m. Then go to step 3. Otherwise go to step 2.3.

2.3. Determining Degrees of Distinct Degree Factors.

Use modified Gunji and Arnon's Method. (c.f. Gunji & Arnon (1981))

2.4. Distinct Degree Decomposition with known degrees.

Similarly as in step 2.2, use modified Berlekamp's DDD-algorithm.

By step 2, we can assume that f is a product of r irreducible factors h_i, $1 \leqq i \leqq r$, with the same degree m.

3. Testing Separability and Finding Non-Trivial Factors. (TS & FNTF)

We describe some definitions needed in this step.

Let g be a non-trivial element of Kernel(π-I). Then there are c_i's in F such that $g=c_i$ mod h_i for $1 \leqq i \leqq r$.

<u>The characteristic polynomial</u> G_0 of g in Kernel(π-I) with respect to f is defined by $G_0=\prod_{i=1}^{r}(x-c_i)$ where $g=c_i$ mod h_i and $c_i \in F$.

<u>The minimal polynomial</u> G of f with respect to f is defined as the monic polynomial of minimal degree such that $G(g)=0$ mod f.

3.1 Find a non-trivial element g of Kernel(π-I).

3.2. Compute the minimal polynomial G and the characteristic polynomial G_0 of g with respect to f.

3. A New Distinct Degree Decomposition. Let $f(x)$ be a square-free and monic polynomial of degree n. Moreover assume that $f(x)$ is a product of r distinct irreducible factors h_i, $1 \le i \le r$, with degree $h_i = n_i$ over **F**, i.e. $f(x) = \prod_{i=1}^{r} h_i$ and $\sum_{i=1}^{r} n_i = n$. Consider the ring $R = F[x]/(f(x))$ and $R_i = F[x]/(h_i(x))$, $1 \le i \le r$. By the Chinese Remainder Theorem we have an isomorphism of F-algebras $R = R_1 \oplus R_2 \oplus \ldots \oplus R_r$. Let π denote the Frobenius mapping on R, i.e. $\pi(g) = g^q \bmod f$ for every g in R, and I denote the identity on R. Moreover let π_i denote the Frobenius mapping on R_i and I_i denote the identity on R_i for $1 \le i \le r$. Then we can identify π with $\pi_1 \oplus \pi_2 \oplus \ldots \oplus \pi_r$ by $\pi(g) = \pi_1(g_1) \oplus \pi_2(g_2) \oplus \ldots \oplus \pi_r(g_r)$ for every g in R such that $g = g_1 \oplus g_2 \oplus \ldots \oplus g_r$ where $g_i \in R_i$ for $1 \le i \le r$.

Now we consider the characteristic polynomial $Q(x)$ of π and $Q_i(x)$ of π_i for $1 \le i \le r$ as linear mappings over vector spaces. Let **Q** be a matrix associated with π with respect to the basis $\{1, x, x^2, \ldots, x^{n-1}\}$, i.e. **Q** is the matrix defined by Berlekamp (1967). Then it follows that $Q(x) = \det(x\mathbf{I} - \mathbf{Q})$ where **I** is the identity matrix. First we show the following theorem.

<u>Theorem 3.1.</u> $Q(x) = \prod_{i=1}^{r} (x^{n_i} - 1)$.

Proof. First we show that $Q_i(x) = x^{n_i} - 1$ for $1 \le i \le r$. Let $Q'_i(x)$ be the monic minimal polynomial of π_i. Then $Q'_1 | Q_i$. We notice that R_i is an algebraic extension field of **F** of degree n_i. From this and Fermat's Theorem, it follows that $g^{q^{n_i}} - g = 0$ for any g in R_i. This implies that $(\pi_i)^{n_i} - I_i = 0$. So $Q'_1(x) | x^{n_i} - 1$. Assume that degree d of $Q'_i(x)$ is less than n_i, i.e. $Q'_i(x) \neq x^{n_i} - 1$. Let $Q'_i(x) = \sum_{j=0}^{d} q_j\, x^j$. Then $\sum_{j=0}^{d} q_j\, (\pi_i)^j = 0$. So for any g in R_i, $\sum_{j=0}^{d} q_j\, (\pi_i)^j(g) = \sum_{j=0}^{d} q_j\, g^{q^j} = 0$. Let $Q''_i(x) = \sum_{j=0}^{d} q_j\, x^{q^j}$. Then $Q''_i(g) = 0$ for any g in R_i. By Fermat's theorem $(x^{q^{n_i}} - x) | Q''_i(x)$. This contradicts the assumption. Therefore degree $Q'_i(x) = n_i$ and $Q'_i(x) = x^{n_i} - 1$. But degree $Q_i(x) = n_i$ and $Q'_i(x) | Q_i(x)$. Since both $Q_i(x)$ and $Q'_i(x)$ are monic, we conclude that $Q'_i(x) = Q_i(x) = x^{n_i} - 1$.

Now we consider $Q(x)$. We take another basis as follows; $\{0 \oplus \ldots \oplus 0 \oplus b_{i,j} \oplus \ldots \oplus 0; 1 \le i \le r \text{ and } 1 \le j \le n_i\}$ where $\{b_{i,j}; 1 \le j \le n_i\}$ is a basis of R_i.

Replace f by H and go to step 3.

Repeating 5.1 to get B of degree 1 lead us to finding a root of C. But for the inseparable case, to get a root is not indispensable. For we have to re-select g in step 3.

The out line of algorithm is illustrated in Fig. 2.

Fig. 2.

So $(x^s-1)|(x^u-1)$ and this is a contradiction. Therefore $(x^s-1)|(x^m-1)$ implies that $s|m$. Conversely assume $s|m$. Then it follows that $(x^s-1)|(x^m-1)$. By separability of (x^m-1), (x^m-1) has at most one (x^s-1) as a factor.

Then for a positive integer s prime to p, the multiplicity $q(s)$ of (x^s-1) in Q is uniquely determined and $q(s)=\sum_{s|m} t(m)$. So let $\underline{t}={}^t(t(1),\ldots)$, $\underline{t}'={}^t(t'(1),\ldots)$ and $\underline{q}={}^t(q(1),\ldots)$. Then $A\underline{t}=A\underline{t}'=\underline{q}$ where A is a matrix defined by $A=(a_{i,j})$ such that $a_{i,j}=1$ for $i|j$ or 0 for otherwise where i and j are taken over all positive integers prime to p. Then A is an upper triangular matrix and det $A=1$. So the solution of $A\underline{t}=\underline{q}$ for $\underline{t}$ is uniquely determined. Hence the decomposition is uniquely determined. #

We present an algorithm determining p-decomposition numbers $t(m)$. Let $N=\{N_1,\ldots,N_u\}$ be a subset in $\{1,2,\ldots,n\}$ which consists of all elements prime to p and $N_1>N_2>\ldots>N_u$.

```
Algorithm Determining p-Decomposition Numbers of f.
Input: the characteristic polynomial $Q(x)$ of ii and the set $N$.
Output: non-trivial p-decomposition numbers $t(N_i)$.
Initialize: $Q_1=Q$.
Recursion: Compute $t(N_i)$ as the multiplicity of $(x^{N_i}-1)^{t(N_i)}$ in $Q_i$.
           $Q_{i+1}=Q_i/(x^{N_i}-1)$.
```

Two processes of determing the characteristic polynoinial $Q(x)$ of ii and determining p-decomposition number are called collectively the process of determining degree of p-distinct factors (DDPDD).

Now we consider the relation between $t(m)$ and $s(i)$ where $s(i)$ is the number of irreducible factors of f with degree i. Then the following relation exists.

Lemma 3.5. $t(m)=\sum_{j\geq 0} p^j s(p^j m)$ for any positive integers m prime to p.

Proof. For any u, $(x^u-1)=(x^{o(u)}-1)^{e(u)}$. So by theorem 3.1 and lemma 3.2, $t(m)=\sum_{j\geq 0} e(p^j m)s(p^j m)=\sum_{j\geq 0} p^j s(p^j m)$. #

Then the associated matrix Q' is as follows;

$$Q' = \left| \begin{array}{lllll} Q_1, & 0, & 0, & \ldots, & 0 \\ 0, & Q_2, & 0, & \ldots, & 0 \\ 0, & 0, & Q_3, & \ldots, & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0, & 0, & 0, & \ldots, & Q_r \end{array} \right| .$$

where Q_i denotes the associated matrix of Π_i with respect to the basis $\{b_{i,j}; 1 \leqq j \leqq n_i\}$. Hence by the previous argument and $\det(xI-Q)=\det(xI-Q')$, it follows that $Q(x)=\det(xI-Q')=\prod_{i=1}^{r} \det(xI_i-Q_i)=\prod_{i=1}^{r}(x^{n_i}-1)$ where I_i is the identity matrix associated with I_i. #

Next we consider $(x^{n_i}-1)$. We use the following;

Definition 3.2. $e(m)$ and $o(m)$ are defined for a positive integer m by $m=e(m)o(m)$ where $e(m)$ and $o(m)$ are positive integers, $(p,o(m))=1$ and $e(m)$ is a power of p. $e(m)$ is said to be the p-part of m and $o(m)$ is said to be the p'-part of m.

Then $x^m-1=(x^{o(m)}-1)^{e(m)}$ for a positive integer m. So by theorem 3.1, it follows that $Q(x)=\prod_{i=1}^{r}(x^{o(n_i)}-1)^{e(n_i)}$.

Definition 3.3. Let $t(m)$ denote the sum of $e(n_i)$ such that p'-part of n_i is m. Then $Q(x)=\prod (x^m-1)^{t(m)}$ where the product is taken over all positive integer m prime to p. We say this decomposition the p-decomposition of Q(x) and $t(m)$ the p-decomposition number of m of Q(x).

We show the uniqueness of this decomposition.

Lemma 3.4. $t(m)$ is uniquely determined for any positive integer m prime to p.

Proof. Assume that $Q(x)=\prod (x^s-1)^{t(s)}$. First we show that $(x^s-1)|(x^m-1)$ iff $s|m$ for integers s and m which are prime to p. Moreover we show that the multiplicity of (x^s-1) in (x^m-1) is one for the case $s|m$. Assume that $(x^s-1)|(x^m-1)$ and $s\nmid m$. Let $m=ts+u$ and $0<u<s$. Since $p\nmid s$, then (x^s-1) is separable. For any root c of (x^s-1) in the algebraic closure of F, it follows that $c^m-1=c^{ts+u}-1=c^u-1=0$.

By lemma 3.8 we only consider the case $t(m) \geq p$. To obtain $f_{p^i m}$, we need to compute $s(p^i m)$. We modify the method of Gunji & Arnon (1981) to this case. Instead of Π, we need to consider the Frobenius map π' of $F[x]/(\tilde{f}_m)$.

<u>Algorithm Determining Degrees of Distinct Factors.</u>

```
Input: $\tilde{f}_m$ and $m$ where $t(m) \geq p$.
Output: $s(p^i m)$ of irreducible factors of $f$ with degree $p^i m$.
1. For $j=0$ to $t$ where $p^t m \leq n$ and $p^{t+1} m > n$,
     compute $v_j = \dim \mathrm{Kernel}( \pi'^{p^j m} - 1 )$.
2. For $j=t$ to $1$,
     compute $s(p^j m) = (v_j - v_{j-1} - \sum_{k=j+1}^{t} s(p^k m))/p^{j-1}(p-1)$.
3. For $j=0$,
     compute $s(m) = v_0 - \sum_{k=1}^{t} s(p^k m)$.
```

We show the correctness of this algorithm in the following. (c.f. Gunji & Arnon (1981))

<u>Proposition 3.9.</u> Let $\underline{v} = {}^t(v_0, v_1, \ldots, v_t)$ and $\underline{s} = {}^t(s(m), s(pm), \ldots, s(p^t m))$. Then $\underline{v}$ and $\underline{s}$ satisfy the following equation;

$A\underline{s} = \underline{v}$ where the matrix $A = (a_{i,j})_{0 \leq i,j \leq t}$ is defined by $a_{i,j} = p^{\min\{i,j\}}$.

Proof. By Gunji & Arnon (1981) Cor. 3.4, $v_i = \sum_{j=0}^{t} (p^i m, p^j m) s(p^j m)$ $= \sum_{j=0}^{t} p^{\min\{i,j\}} s(p^j m)$. So by the above matrix A, $A\underline{s} = \underline{v}$. Hence the solution of $A\underline{s} = \underline{v}$ for $\underline{s}$ is obtained by the above algorithm. #

Now we can determine the distinct degree factor $f_{p^i m}$ by the following way. Let U be the set which consists of all non-negative integer u such that $s(p^u m)$ is positive and $U = \{u_1, u_2, \ldots, u_{t'}\}$ where $u_1 < u_2 < \ldots < u_{t'}$. Then we use the same method as in the algorithm of p-distinct degree decomposition.

<u>Algorithm Distinct Degree Decomposition with known degrees.</u>

Input: the p-distinct degree factor $\tilde{f}_m$ of f with degree m and

Definition 3.6. Let $\tilde{f}_m=\prod h_i$ where the product is taken over all i such that p'-part of n_i is equal to m. $\tilde{f}_m$ is said to be the p-distinct degree factor of f with degree m and decomposition of f to p-distinct degree factors is said to be p-distinct degree decomposition. Then $d(m)=\text{degree } \tilde{f}_m=mt(m)$ is the degree of p-distinct degree factor of f with degree m.

We present an algorithm of p-distinct degree decomposition with known degrees based on Berlekamp's DDD-algorithm. Let $D=\{d_1,d_2,\ldots,d_v\}$ be the set which consists of all positive integers d such that t(d) is positive and $d_1<d_2<\ldots<d_v$. Moreover let p^t be the maximal p-power such that $p^t\leq n$. (c.f. Berlekamp (1970), Algorithm 3.02)

```
Algorithm p-Distinct Degree Decomposition with known degrees.
Input: $f \in F$ and $D=\{d_1,d_2,\ldots,d_v\}$.
Output: $\tilde{f}_{d_i}$ for $1\leq i\leq v$.
Initialize: $F^{(0)}=f(x)$, $R^{(0)}=x$ and $d_0=0$.
Recursion: $R^{(i)}=(R^{(i-1)})^{q^{k_i}} \bmod F^{(i-1)}$ where $k_i=p^t(d_i-d_{i-1})$.
           $\tilde{f}_{d_i}=GCD(F^{(i-1)},R^{(i)}-x)$.
           $F^{(i)}=F^{(i-1)}/\tilde{f}_{d_i}$.
```

In the above algorithm we can use a GCD-algorithm with a known degree of GCD. Because we know degree $\tilde{f}_m=d(m)=mt(m)$ for a positive integer m prime to p. We describe GCD-algorithms with a known degree of GCD in the latter.

Definition 3.7. Let f_m be the product of all irreducible factors of f with degree m. f_m is said to be the distinct degree factor of f with degree m. Then the following holds.

Lemma 3.8. If $t(m)<p$ then $s(m)=t(m)$ and $s(p^i m)=0$ for $i\geq 1$. So in this case, $f_m=\tilde{f}_m$.

4. Testing Separability and Finding Non-Trivial Factors. In this section, we consider properties of roots of the Zassenhaus's polynomial.(c.f. Zassenhaus (1969)) Assume that f(x) is square-free and has r distinct irreducible factors $h_i(x)$ with the same degree m. First consider Kernel(π-I). Find a non trivial polynomial g(x) in Kernel(π-I), i.e. $g(x)\notin F$, and fix it. Then there are c_i's, $1\leqq i\leqq r$, in F such that $g\equiv c_i$ mod h_i. Again "separability" of g is defined in the following.

Definition 4.1. The characteristic polynomial $G_0(x)$ of g with respect to f is defined by $G_0=\prod_{i=1}^{r}(x-c_i)$.

Definition 4.2. g is said to be separable with respect to f if G_0 has no multiple root, i.e. G_0 is separable polynomial over F. Otherwise g is said to be inseparable with respect to f.

Definition 4.3. (c.f. Zassenhaus (1969) and Berlekamp (1970)) The minimal polynomial, i.e. Zassenhaus's polynomial, G(x) of g is defined as follows; Since g belongs to Kernel(π-I), $1,g,g^2,\ldots,g^{r-1}$ and g^r belong to Kernel(π-I). So by the fact that dim Kernel(π-I)=r, there are non trivial linear relations between $1,g,\ldots,g^r$. In these relations, replacing g by x non trivial polynomials are obtained. Then there exists a polynomial G(x) uniquely such that degree of G(x) is minimal and G(x) is monic. This G(x) is said to be the minimal polynomial of g with respect to f.

Now we show some lemmas.

Lemma 4.4. $G(c_i)=0$ for c_i such that $g(x)\equiv c_i$ mod $h_i(x)$, $1\leqq i\leqq r$. Moreover set $\{c'_1,\ldots,c'_{r'}\}$ be the set of all distinct elements of $\{c_1,\ldots,c_r\}$.
Then $G(x)=\prod_{i=1}^{r'}(x-c'_i)$.

Proof. Set $H(x)=\prod_{i=1}^{r'}(x-c'_i)$. Since $G(g)\equiv 0$ mod f(x), $G(c_i)\equiv 0$ mod $h_i(x)$ and $G(c_i)=0$. So $H(x)|G(x)$. Conversely $H(g)\equiv H(c_i)\equiv 0$ mod $h_i(x)$ for $1\leqq i\leqq r$. This implies that $H(g)\equiv 0$ mod f(x) and $G(x)|H(x)$. Hence $G(x)=H(x)$. #

Lemma 4.5.

(1) g is separable iff $G_0(x)=G(x)$.

(2) g is separable iff degree G(x)=r=dim Kernel(π-I).

$\{s(p^{u_1}m),\ldots,s(p^{u_{t'}}m)\}$.

Output: non-trivial distinct degree factors $f_{p^{u_i}m}$.

Initialize: $F^{(0)}=\bar{f}_m$ and $R^{(0)}=x$.

Recursion: $R^{(i)}=(R^{(i-1)})^{q^{k_i}} \bmod F^{(i-1)}$ where $k_i=p^{u_i}m-p^{u_{i-1}}m$.

$$f_{p^{u_i}m}=GCD(F^{(i-1)},R^{(i)}-x).$$
$$F^{(i)}=F^{(i-1)}/f_{p^{u_i}m}.$$

Similarly as in the algorithm of p-distinct degree decomposition, we use a GCD-algorithm with a known degree.

Finally in this section we present a modified Bordin-von zur Gathen-Hopcroft's GCD-algorithm with a known degree. (c.f. von zur Gathen (1984))

Algorithm Modified Bordin-von zur Gathen-Hopcroft's GCD with a known degree.

Input: $g, h \in F[x]$ with degree $g=u<v=$degree h and $w=$degree $GCD(g,h)$.

Output: $GCD(g,h)$.

1. Construct the w-th principal subresultant matrix P_w of (g,h).

2. Compute $y_0,\ldots,y_{u-w-1},z_0,\ldots,z_{v-w-1}$ such that
$P_w{}^t(y_{u-w-1},\ldots,y_0,z_{v-w-1},\ldots,z_0)={}^t(0,\ldots,0,1)$.
Set $y=y_{u-w-1}x^{u-w-1}+\ldots+y_0$ and $z=z_{v-w-1}x^{v-w-1}+\ldots+z_0$.

3. Compute $a=gy+hz$ and $a'=a/$leading coefficient of a.

Return a' as the $GCD(g,h)$.

The w-th principal subresultant matrix is as follows;

$$P_w=\left|\begin{array}{cccccc} g_u & & & h_v & & \\ g_{u-1} & g_u & & h_{v-1} & h_v & \\ : & : & & : & & \\ g_{u-v+w+1} & \cdots & g_u & h_{v-m+w+1} & \cdots & h_v \\ : & & : & : & & : \\ g_{2w-v+1} & \cdots & g_w & h_{2w-u+1} & \cdots & h_w \end{array}\right|.$$

The correctness of the above algorithm follows from von zur Gathen (1982), Th 2.3.

By the above theorem, we present an algorithm determining the minimal polynomial G and the characteristic polynomial G_0 of g with respect to f.

Algorithm Determining the Minimal and Characteristic Polynomials.

Input: $g(x) \in \mathrm{Kernel}(\Pi - I)$.

Output: the minimal polynomial and the characteristic polynomial of g with respect to f.

1. Find the maximal linearly independent set $B'=\{1,g,g^2,\ldots,g^{r'}\}$.
Find the linear relation between $1,g,\ldots,g^{r'+1}$ and make the minimal polynomial $G(x)$. Return $G(x)$. If $r'=r-1$, then return $G(x)$ as $G_0(x)$.

2. Find the basis $B=\{g_0,g_1,\ldots,g_{r-1}\}$ by adding some elements to B' where $g_1=g$.

3. Compute $b^{(1)}_{i,j}$ and $G_0(x)=\det(xI-M_1)$. Return $G_0(x)$.

In the rest of this section we present the preprocess of finding roots by using the difference between $G(x)$ and $G_0(x)$. Assume that $G_0(x)$ is decomposed to distinct power parts $G_i(x)$, $1 \leqq i \leqq t$, i.e. $G_0(x)=G_1(x)(G_2(x))^2\ldots(G_t(x))^t$ and $GCD(G_i,G_j)=1$ for $1 \leqq i<j \leqq t$. Then the following occurs by lemma 4.4.

Lemma 4.7. $G(x)=G_1(x)G_2(x)\ldots G_t(x)$.

So if $G(x)$ differs from G_0, we can use $G(x)$ to decompose $G_0(x)$ by the following way. This algorithm need not differentiate G, so we can avoid the case $dG/dx=0$.

Algorithm Distinct Power Decomposition of G_0.

Input: the characteristic polynomial G_0 and the minimal polynomial G.

Output: distinct power parts G_i of G_0.

Initialize: $H_0=G_0$ and $K_0=G$.

Recursion: $H_i=H_{i-1}/K_{i-1}$.

$K_i=GCD(K_{i-1},H_i)$.

$G_i=K_{i-1}/K_i$.

Now we show the usage of the distinct power parts G_i of G_0 as a preprocess of

(3) If g is separable, then $GCD(f(x),g(x)-s)$ is irreducible for any root s of $G(x)$. We notice that $G(x)$ and $G_0(x)$ are completely splited in F.

Now we present a method determing the characteristic polynomial $G_0(x)$ of g with respect to f. (We notice that if g is separable, then $G_0(x)=G(x)$.) Let $\{g_0,g_1,g_2,g_3,\ldots,g_{r-1}\}$ be a basis of Kernel(Π-I) where $g_0=1$ and $g_1=g$. Then there are $c_{i,j}$'s in F such that $g_i=c_{i,j}$ mod h_j for $0 \leqq i \leqq r-1$ and $1 \leqq j \leqq r$. We notice that $c_{0,i}=1$ and $c_{1,i}=c_i$ for $1 \leqq i \leqq r$. Moreover since g_ig_j belongs to Kernel(Π-I), there are $b^{(i)}_{j,k}$'s in F such that $g_ig_j=\sum_{k=0}^{r-1} b^{(i)}_{j,k}g_k$ mod f for $0 \leqq i,j \leqq r-1$. So matrices M_i are defined by $M_i=(b^{(i)}_{j,k})_{0 \leq j,k \leq r-1}$. Then M_i's are r r matrices. We show the following theorem.

<u>Theorem 4.6.</u> $\det(xI-M_i)=\prod_{j=1}^{r}(x-c_{i,j})$.
Therefore $\det(xI-M_i)$ is the characteristic polynomial of g_i with respect to f.

Proof. There is a one to one correspondence between Kernel(Π-I) and a r-dimensional vector space W over F as follows;
A polynomial H in Kernel(Π-I) corresponds to a vector $\underline{H}=(H_0,H_1,\ldots,H_{r-1})$ in W such that $H=\sum_{i=0}^{r-1} H_ig_i$.
Then we show that Hg_i corresponds to $\underline{H}M_i$.
Because $Hg_i=\sum_{j=0}^{r-1} H_jg_jg_i=\sum_{j=0}^{r-1} H_j(\sum_{k=0}^{r-1} b^{(i)}_{j,k}g_k)=\sum_{k=0}^{r-1} (\sum_{j=0}^{r-1} H_jb^{(i)}_{j,k})g_k$.
This implies that Hg_i corresponds to $\underline{H}M_i$.

Since $h_1,\ldots,h_{r-1}$ and h_r are pairwise prime, there are polynomials $A_j(x)$ and $B_j(x)$ such that $A_jh_1\cdots h_{j-1}h_{j+1}\cdots h_r+B_jh_j=1$ mod f. Set $S_j=A_jh_1\cdots h_{j-1}h_{j+1}\cdots h_r$.
Then $S_j=1$ mod h_j and $S_j=0$ mod h_t for $t \neq j$. Moreover S_j belongs to Kernel(Π-I). So there are $s_{j,k}$'s in F such that $S_j=\sum_{k=0}^{r-1} s_{j,k}g_k$. Set $\underline{S}_j=(s_{j,0},\ldots,s_{j,r-1})$. Consider $\underline{S}_j(M_i-c_{i,j}I)$. Then $\underline{S}_j(M_i-c_{i,j}I)$ corresponds to the polynomial $S_j(x)(g_i(x)-c_{i,j})$ mod f. But it follows that $S_j(x)(g_i(x)-c_{i,j})=0$ mod h_t for $t \neq j$ and $S_j(x)(g_i(x)-c_{i,j})=c_{i,j}-c_{i,j}=0$ mod h_j. So $S_j(x)(g_i(x)-c_{i,j})=0$ mod f. This implies that $\underline{S}_j(M_i-c_{i,j}I)=0$. i.e. $\underline{S}_j$ is an eigen vector of M_i. $S_1,\ldots,S_{r-1}$ and S_r are linearly independent. Hence the set of all eigen values of M_i is $\{c_{i,j};1 \leqq j \leqq r\}$. From this, we conclude this theorem. #

Compute e_i=GCD(f,G_i(g)).

Return G_i(x), e_i(x) and a sign "separable" or "purely inseparable" according to i=1 or not.

Remark 4.10. (1) If the number r of irreducible factors of f is more than the number of elements q of **F**, then g can not be separable for any g in Kernel(Π-I).
(2) If $r \leqq q$, the ratio of separable elements in Kernel(Π-I) is as follows;
$q(q-1)\ldots(q-r+1)/q^r$.

In the next section, we consider the step of Finding Roots and Finding Non-Trivial Factors.

5. Finding Irreducible Factors and Finding Non-trivial Factors. In this section we use the same notations as in previous section. Consider algorithms determining irreducible factors of f by using G(x) or G_i(x) obtained by previous steps. There are many discussions in the problems of finding roots and finding non-trivial factors by GCD(f,*). We do not present a new method of finding roots. But under the assumption that there is an efficient algorithm of finding roots, we discuss our method determining irreducible factors. Moreover we present a method which determines non-trivial factors of f by using non-trivial factors of G. First we show the following;

Algorithm Finding Irreducible Factors of Separable Case.

Input: $f \in F[x]$, $g \in$Kernel(Π-I) and G where (f,g,G) is a separable case.

Output: irreducible factors h_i with degree m of f for $1 \leqq i \leqq$degree G.

1. Find all roots c_i's of G(x) by some finding roots algorithm.

2. Compute h_i=GCD(f,g-c_i) by some GCD-algorithm with a known degree. Return h_i.

Algorithm Finding Factors of Purely Inseparable Case.

Input: $f \in F[x]$, $g \in$Kernel(Π-I), G where (f,g,G) is a purely inseparable case and finding roots. Again "purely inseparability" is defined as follows.

Definition 4.8. g is said to be purely inseparable with respect to f if $G_0=(G_t)^t$ for some $t>1$, i.e. $G_0=(G)^t$ and t is said to be the multiplicity of G. If g is inseparable but not purely inseparable, g is said to be reducible with respect to f.

So there are three cases; separable case, purely inseparable case and reducible case. Then we get the following.

Lemma 4.9. If g is reducible, then we get the non trivial factors $e_i(x)$ of $f(x)$ for non trivial power parts G_i by the following; $e_i=GCD(f,G_i(g))=\prod h_j$ where the product is taken over all h_j such that $G_i(c_j)=0$.
Moreover degree $e_i=m$ degree G_i. (So we can use GCD-algorithms with a known degree.) g is separable with respect to $e_1(x)$ and purely inseparable with respect to e_i with $i>1$.

Proof of lemma 4.9 follows from lemma 4.4 and lemma 4.5. From this, we have the following algorithm.

Algorithm Testing Separability and Finding Non-Trivial Factors.

Input: g in Kernel$(\Pi-I)$.

Output: (a) the minimal polynomial $G(x)$ and a sign "separable" if g is separable,

(b) the minimal polynomial $G(x)$, the multiplicity t and a sign "purely inseparable" if g is purely inseparable and $G_0=G^t$

or (c) each non trivial distinct power part $G_i(x)$, the non trivial factor $e_i(x)$ associated with G_i and a sign associated with e_i and G_i if g is reducible.

1. Compute the minimal polynomial $G(x)$ and the characteristic polynomial $G_0(x)$ of g with respect to f.

2. If $G=G_0$, then return $G(x)$ and a sign "separable".

If $G_0=G^t$ for $t>1$, then return $G(x)$, t and a sign "purely inseparable".

3. Compute the non-trivial distinct power parts G_i of G_0.

References

Berlekamp, E. R. (1967). Factoring Polynomials over Finite Fields. Bell System Tech. J. **46**, 1853-1859.

Berlekamp, E. R. (1968). Algebraic Coding Theory, Chap. 6. New York: McGraw-Hill.

Berlekamp, E. R. (1970). Factoring Polynomials over Large Finite Fields. Math. Comp. **24**, 713-735.

Cantor, D. G., Zassenhaus, H. (1981). A New Algorithm for Polynomials over Finite Fields. Math. Comp. **36**, 587-592.

Gunji, H., Arnon, D. (1981). On Polynomial Factorization over Finite Fields. Math. Comp. **36**, 281-287.

Lazard, D. (1979). On Polynomail Factorization. EUROSAM 1979. Springer Lec. Note Comp. Sci. **72**, 126-134.

Moenck, R.T. (1977). On the Efficiency of Algorithms for Polynomial Factoring. Math. Comp. **31**, 235-250.

Rabin, M. (1980). Probabilistic Algorithms in Finite Fields. SIAM J. Comp. **9**, 273-280.

von zur Gathen, J. (1984). Parallel Algorithms for Algebraic Problems. SIAM J. Comp. **13**, 802-824.

Zassenhaus, H. (1969). On Hensel Factorization I. J. Number Theory **1**, 291-311.

the multiplicity $t>1$.

Output: non-trivial factors H_i of f with degree mt for $1 \leqq i \leqq$ degree G.

1. Find all roots c'_i of $G(x)$ by some finding roots algorithm.

2. Compute $H_i = GCD(f, g-c'_i)$ by some GCD-algorithm with a known degree. Return H_i.

Next we show a method determining non-trivial factors of f by non-trivial factor of G. We have the following. (c.f. lemma 4.9)

Lemma 5.1. There is a correspondence from non-trivial factors of G to non-trivial factors of f as follows;
For a non-trivial factor $B(x)$ of $G(x)$, $GCD(f,B(g))$ is a non-trivial factor of f such that $GCD(f,B(g)) = \prod h_i$ where the product is taken over all h_i with $B(c_i)=0$.
Moreover degree $GCD(f,B(g)) = m$ degree B where m=degree h_i if g is separable and $GCD(f,B(g)) = m\ t$ degree B if g is purely inseparable.

Hence we can reduce finding non-trivial factor of f to finding non-trivial factor of G. For example, we modify Cantor-Zassenhaus's method. (c.f. Cantor & Zassenhaus (1981))

Algorithm Finding a Non-Trivial Factor.

Input: $f \in F[x]$, $g \in \mathrm{Kernel}(\pi - I)$ and G.

Output: a non-trivial factor of f.

1. Choose $b(x)$ randomly such that $1 \leqq$ degree $b < r$ = degree G.
2. Compute $B = GCD(G, b^{(q-1)/2}-1)$. If B is not nontrivial,then return to step 1. Otherwise go to next step.
3. Compute $H = GCD(f,B(g))$. Return H as a non-trivial factor of f.

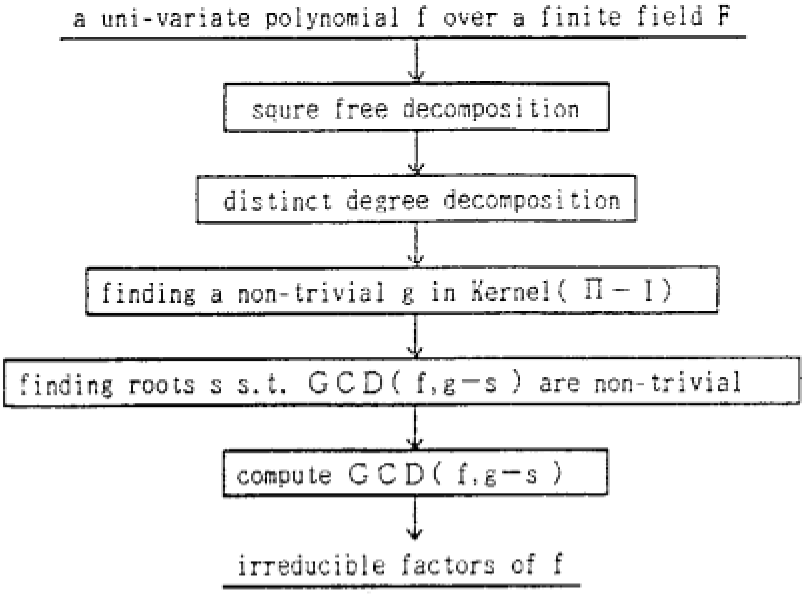

a uni-variate polynomial f over a finite field F
squre free decomposition
distinct degree decomposition
finding a non-trivial g in Kernel(Π − I)
finding roots s s.t. GCD(f,g−s) are non-trivial
compute GCD(f,g−s)
irreducible factors of f

Fig. 1.