Complete Factorization Of Skew-Polynomial Over Finite Fields

Saiyue Lyu

Skew-polynomial ring is one of the most classic and earliest examples in non-commutative algebra, which is first introduced by Noether and Schmeidler (1920) and later well studied by Ore (1933). The skew-polynomials have been found useful in solving differential equations, Coding theory and Control theory. This project first gives a review of basic concepts of skew-polynomial rings and then tries to investigate the complete factorization of skew-polynomials over finite fields based on Giesbrecht's paper in 1998.

1. Basic Definitions

Definition 1.1. *An endomorphism σ of ring R is a morphism from R to itself.*

A $\sigma-$derivation δ on R is a R-linear map from R to itself such that the modified Leibniz's law is satisfied, i.e. $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$ for any $a, b \in R$.

Definition 1.2. *Let R be a ring, σ an endomorphism of R and δ a σ-derivation on R. A skew-polynomial ring $R[x;\sigma,\delta]$ is defined as*

$$R[x;\sigma,\delta] = \{\sum_{i=0}^{n} r_i x^i,\ r_i \in R\}$$

with standard addition and multiplication defined such that

$$xa = \sigma(a)x + \delta(a)\ \forall a \in R$$

There are two typical cases :

1. If $\sigma = id$, the identity endomorphism on R, then $R[x;\delta]$ is called differential operator ring or skew-polynomial ring with derivation type, which is first introduced by Schlessinger.

2. If $\delta = 0$, then $R[x;\sigma]$ is called skew-polynomial ring with endomorphism type, which is first introduced by Hilbert.

In this report, we limit R to be a finite field $F \cong \mathbb{F}_q$, where $q = p^k$ is a power of prime p for some $k \in \mathbb{N}$. And we only consider the endomorphism type skew-polynomial $R[x;\sigma]$ with $\delta = 0$. Moreover we take the endomorphism to be also an isomorphism, i.e. σ is a field automorphism on F. Then the multiplication on $R[x;\sigma]$ is defined as

$$xa = \sigma(a)x,\ \forall a \in F$$

Iterating this rule for n times, we have

$$ax^n bx^m = a\sigma^n(b)x^{n+m},\ \forall a \in F$$

Definition 1.3. *Let R be a commutative ring with characteristic p, where p is a prime. The Frobenius endomorphism F is defined such that $F(a) = r^p$ for any $r \in R$*

Let α generate the multiplicative group of F. Since $F \cong \mathbb{F}_q$ is finite, then every nonzero element of F is a power of α. If $\sigma(\alpha) = \alpha^i$ for some i, then σ maps α^j to α^{ij}, i.e. σ raises all elements to the i power, for some i. So for the automorphism σ we have

$$\sigma(a) = a^{p^\xi}, \text{ for some } \xi \in \mathbb{N}$$

which is actually an iterated Frobenius map of F.

Example 1.4. *For $f = a_2x^2 + a_1x + a_0$, $g = b_1x + b_0 \in F[x;\sigma]$, we have the computations:*

$$\begin{aligned}
f + g &= a_2x^2 + (a_1 + b_1)x + (a_0 + b_0) \\
f \cdot g &= (a_2x^2 + a_1x + a_0) \cdot (b_1x + b_0) \\
&= a_2x^2 \cdot b_1x + a_2x^2 \cdot b_0 + a_1x \cdot b_1x + a_1x \cdot b_0 + a_0 \cdot b_1x + a_0 \cdot b_0 \\
&= a_2\sigma^2(b_1)x^3 + \big(a_2\sigma^2(b_0) + a_1\sigma(b_1)\big)x^2 + \big(a_1\sigma(b_0) + a_0b_1\big)x + a_0b_0 \\
g \cdot f &= (b_1x + b_0)(a_2x^2 + a_1x + a_0) \\
&= \sigma(a_2)b_1x^3 + \big(\sigma(a_1)b_1 + a_2b_0\big)x^2 + \big(\sigma(a_0)b_1 + a_1b_0\big)x + a_0b_0
\end{aligned}$$

From these computations, we see that $f \cdot g \neq g \cdot f$, $F[x;\sigma]$ is indeed non-commutative.

Consider any $f, g \in F[x;\sigma]$, note σ does not affect the power of x, so we have deg(fg) = deg(gf) = deg(f) + deg(g), which is the same as in $F[x]$, so we can conclude $F[x;\sigma]$ is also integral. Note that $F[x]$ is Euclidean, thus a PID (Principle Ideal Domain) and a UFD (Unique Factorization Domain), but $F[x;\sigma]$ is not a UFD in general with the below example introduced by Caruso and Le Borgne.

Example 1.5. *Let $F = \mathbb{F}_8 \cong \mathbb{F}_2[\alpha]$, where α is the solution of $\alpha^3 + \alpha + 1 = 0$. The σ is defined such that $\sigma(a) = a^2, \forall a \in F$, then consider the following skew-polynomial (which has 20 different factorizations actually)*

$$\begin{aligned}
f &= x^5 + x^4 + \alpha x^3 + \alpha^6x^2 + \alpha^3x + \alpha^2 \\
&= (x^2 + \alpha^5x + \alpha) \cdot (x + \alpha) \cdot (x + 1) \cdot (x + 1) \\
&= (x^2 + \alpha^5x + \alpha) \cdot (x + \alpha^6) \cdot (x + \alpha^2) \cdot (x + 1)
\end{aligned}$$

$F[x;\sigma]$ is actually a principle left ideal ring with a right Euclidean algorithm (proved later), so as usual, we have the following definition.

Definition 1.6. *A non-zero $f \in F[x;\sigma]$ is irreducible if whenever $f = gh$ for some non-zero $g, h \in F[x;\sigma]$, then either deg(g) = 0 or deg(h) = 0.*

Then any $f \in F[x;\sigma]$ can be written as a product of irreducible skew-polynomials. The factorization may not be unique as seen in above example and the order of factors may not be change due to the special multiplication rule. So we consider two factoring problems.

- **Complete Factorization.** Given any non-constant $f \in F[x;\sigma]$, find irreducible $f_1, \cdots, f_k \in F[x;\sigma]$ such that $f = f_1 \cdots f_k$.

- **Bi-Factorization.** Given any non-constant non-zero $f \in F[x;\sigma]$ and a positive integer $d < \deg(f)$, determine if there exists $g, h \in F[x;\sigma]$ such that $f = gh$ and deg h =d. If so, find such g and h.

In commutative case, these two problems are equivalent while in the skew-polynomial rings, there are not. In this report, we take a close look at **Complete Factorization**.

The first resultful contribution for algorithms of factoring a skew-polynomial appears in Giesbrecht's paper, which uses associate algebra as a key tool. Let K be the maximum subfield of F fixed by $\sigma \in Aut(F)$ with $[K : \mathbb{F}_p] = s$, i.e. K can be viewed as a vector space over $\mathbb{F}_p$ of dimension s. Since $[\mathbb{F}_{p^s} : \mathbb{F}_p] = s$, then we have $K \cong \mathbb{F}_{p^s} \cong \mathbb{F}_p[x]/(g_K)$ for some irreducible $g_K \in \mathbb{F}_p[x]$ with degree s. And there exists a basis $B_K = \{1, y, y^2, \cdots, y^{s-1}\}$ where $y \equiv x \mod g_K$. The corresponding iterated Frobenius map σ is of the form that $\sigma(a) = \tau^l(a) = a^{p^{sl}}$ for some $l < [F : K] = t$ and τ is the only automorphism of F/K fixing K. By the maximality of K, $\gcd(t, l) = 1$. Similarly for $K/\mathbb{F}_p$, we can also view $F \cong K[x]/(h_F)$ for some irreducible $h_F \in K[x]$ and there exists a basis for F, $B_F = \{1, z, z^2, \cdots, z^{t-1}\}$ where $z \equiv x \mod h_F$, i.e. we have the following diagram

$$\mathbb{F}_p \underbrace{\le}_{s} \mathbb{F}_p[x]/(g_K) \;\cong\; \mathbb{F}_{p^s} \;\cong\; K \underbrace{\le}_{t} K[x]/(h_F) \;\cong\; F$$

We then view $F[x;\sigma]$ as an associate K-algebra with basis $\{h_F^i x^j, 0 \le i < t, j \ge 0\}$. We then can describe any input using K, so we consider cost in terms of operations in K.

2. Addition, Multiplication, Division and Modular Equivalence

Definition 2.1.

- *For any $f, g : \mathbb{R}^+ \to \mathbb{R}^+$, we say if $f = \tilde{O}(g)$ and only if there exists a constant $c > 0$ such that $f = O\big(g(\log g)^c\big)$.*
- *We define function $M : \mathbb{N}^+ \to \mathbb{R}^+$ to be a multiplication time for $K[x]$, if polynomials in F of degree $< n$ can be multiplicated using at most $M(n)$ operations in K. Harvey and Vander found in 2019 that $M(n) \in O(n \log n)$.*
- *We define function $MM : \mathbb{N}^+ \to \mathbb{R}^+$ to be a multiplication time for $K[x]^{n \times n}$, if two $n \times n$ matrices can be multiplicated using at most $MM(n)$ operations in K. Coppersmith and Winograd found in 1990 that $MM(n) \in O(n^{2.376})$.*

Theorem 2.2 (Addition). *For any $f, g \in F[x;\sigma]$, $f + g$ takes $O(n)$ operations in F or $O(nt)$ operations in K, where $n = \max($ $deg\ f,\ deg\ g$ $)$.*

Proof. For any $f, g \in F[x;\sigma]$, we can write

$$f = \sum_{0 \le i \le n_1} a_i x^i \ ,\ g = \sum_{0 \le j \le n_2} b_i x^i \text{ where } a_0, \cdots, a_{n_1}, b_0, \cdots, b_{n_2} \in F$$

Then $f + g$ is the same as the standard addition, which takes $O(n)$ operations in F. ∎

There are many different ways to do multiplications, the classical one introduced by Giesbrecht uses the explicit formula for the coefficients of the product.

Theorem 2.3 (Multiplication). *For any $f, g \in F[x;\sigma]$, fg takes $O\big(n_1 n_2 M(t) + n_2 t M(t) \log t\big)$ or $\tilde{O}(n_1 n_2 t + n_2 t^2)$ operations in K, where n_1, n_2 are the degrees of f, g.*

Proof. For any $f, g \in F[x;\sigma]$, we can compute their product as

$$fg = \Big(\sum_{0\le i\le n_1} a_i x^i\Big)\cdot\Big(\sum_{0\le j\le n_2} b_i x^i\Big) = \sum_{i=0}^{n_1+n_2}\Big(\sum_{j=0}^{i} a_j\sigma^j(b_{i-j})\Big)x^i$$

For any coefficient b, we can use von zur Gathen and Shoup's algorithm to compute all conjugates $b, \tau(b), \cdots, \tau^{t-1}(a)$ of any element a in F over K using $O(tM(t)\log t)$ operations in K, so we can compute images of all power of σ in $O(n_1 tM(t)\log t)$. Then we can compute $n_1 n_2$ products in F, so in total it takes $O\big(n_1 n_2 M(t) + n_2 tM(t)\log t\big)$ or $\tilde{O}(n_1 n_2 t + n_2 t^2)$ operations in K. ■

Caruso and Le Borgne pointed out that this can be actually improved to $\tilde{O}\big(n_1 n_2 t\log q\cdot(\log q + t^{\epsilon}\cdot(\log q)^{O(1)})\big)$ for all $\epsilon > 0$ where q is the cardinality of K by using fast modular composition introduced by Kedlaya and Umans in 2008.

They also showed that we can also modify **Karatsuba's algorithm** over skew-polynomial ring if we only compute multiplication of polynomials with degree $\le t$ using Giesbrecht's algorithm and compute higher degree multiplication by recursion. Here is Karatsuba for skew-polynomials :

```
Algorithm 1: KaratsubaSkew
    Input: $f, g \in F[x;\sigma]$ with $n_1 = \deg(f)$, $n_2 = \deg(g)$
    Output: $fg \in F[x;\sigma]$
    $t = [F : K]$;
    if $\max(n_1, n_2) \le t$ then
        return GiesbrechtMultiplication($f, g$);
    end
    $d = \lfloor\frac{\max(n_1,n_2)}{2t}\rfloor$;
    Rewrite $f = f_0 + x^{dt}f_1$ and $g = g_0 + x^{dt}g_1$;
    $h_0$ = KaratsubaSkew $(f_0, g_0)$;
    $h_2$ = KaratsubaSkew $(f_1, g_1)$;
    $h_1$ = KaratsubaSkew $(f_0 + f_1, g_0 + g_1) - h_0 - h_2$;
    return $h_0 + x^{dt}h_1 + x^{2dt}h_2$;
```

Let $f, g \in F[x;\sigma]$. Write $f = f_0 + x^{dt}f_1$ and $g = g_0 + x^{dt}g_1$, where $d = \lfloor\frac{\max(n_1,n_2)}{2t}\rfloor$. Note x^{2dt} lies in the center of $F[x;\sigma]$, then we can write

$$fg = h_0 + x^{dt}h_1 + x^{2dt}h_2$$

where $h_0 = f_0 g_0, h_1 = f_0 g_1 + f_1 g_0, h_2 = f_1 g_1$. Then we can get fg by doing 3 multiplications $h_0 = f_0 g_0, h_2 = f_1 g_1$ and $(f_0 + f_1)(g_0 + g_1)$ to get $h_1 = (f_0 + f_1)(g_0 + g_1) - h_0 - h_2$. In total we can get a complexity of around $O(n^{1.58}t^{1.41})$, where $n = \max(n_1, n_2)$.

Caruso and Le Borgne also introduced two more methods for multiplication. One is to reduce it to commutative case by applying σ^i to all coefficients of g to get a deduced G_i, then $fg = \sum_{i=0}^{n_1} a_i G_i x^i$, which takes $O(nt^2)$. The other is to use the structure of matrix (details omitted here), which takes $\tilde{O}\big(n\frac{MM(t)}{t} + nt\log q + n^{1+\epsilon}t\cdot(\log q)^{o(1)}\big)$ for all $\epsilon > 0$. SO we have the following complexity table :

Algorithm for Multiplication	Operations in K
Giesbrecht	$\tilde{O}(n_1 n_2 t + n_2 t^2)$
Improved Giesbrecht	$\tilde{O}\big(n_1 n_2 t \log q \cdot (\log q + t^{\epsilon} \cdot (\log q)^{O(1)})\big)$
Karatsuba	$O(n^{1.58} t^{1.41})$
Reduction to Commutative	$O(nt^2)$
Matrix	$\tilde{O}\big(n\frac{MM(t)}{t} + nt\log q + n^{1+\epsilon} t \cdot (\log q)^{o(1)}\big)$

Note that ”Reduction to Commutative” assumes that multiplication in commutative ring can be done in quasi-linear time. And although ”Matrix” achieves best asymptotical theoretical complexity, it is inefficient when $n < t^2$ and it is not easy to implement due to a complex algebraic structure. So it might be better to choose **Karatsuba** for multiplication.

Theorem 2.4 (Right Division Existence). *For any $f, g \in F[x;\sigma]$, there exists $q, r \in F[x;\sigma]$ such that $f = qg + r$, i.e. $F[x;\sigma]$ is right Euclidean. Moreover, $F[x;\sigma]$ is a principal left ideal with a right Euclidean division algorithm.*

Proof. Assume deg $(f) = n_1 \geq n_2 =$ deg (g).

The leading term of $x^{n_1-n_2}g$ is $\sigma^{n_1-n_2}(b_{n_2})x^{n_1-n_2}x^{n_2} = \sigma^{n_1-n_2}(b_{n_2})x^{n_1}$, then we can compute the leading term of $a_{n_1}\sigma^{n_1-n_2}(b_{n_2}^{-1})x^{n_1-n_2}g$, which is $a_{n_1}\sigma^{n_1-n_2}(b_{n_2}^{-1}b_{n_2})x^{n_1} = a_{n_1}x^{n_1}$.

Note the leading term of f is also $a_{n_1}x^{n_1}$, so the difference $f - a_{n_1}\sigma^{n_1-n_2}(b_{n_2}^{-1})x^{n_1-n_2}g$ has degree $< n_1$. Therefore just as in the standard division algorithm, we can repeat the procedure to reduce the degree until it is $< n_2$ or the remaining difference is just 0, this allows us to find required q, r.

The existence of right division algorithm (described below) ensures the existence of right Euclidean algorithm, which implies $F[x;\sigma]$ is a principal left ideal ring. ∎

Note that if σ is surjective, $F[x;\sigma]$ is also left Euclidean, i.e. for any $f, g \in F[x;\sigma]$, there exists $q, r \in F[x;\sigma]$ such that $f = gq + r$.

Here is the right division algorithm for skew-polynomials

Algorithm 2: RightDivisionSkew

```
Input: $f, g \in F[x;\sigma]$ with $n_1 = $ deg $(f) \geq n_2 = $ deg $(g)$
Output: $q, r \in F[x;\sigma]$ such that $f = qg + r$ with deg $(r) <$ deg $(g)$
$t = [F : K]$;
$f^{(n_1)} = f$;
$h^{(n_1)} = a_{n_1}\sigma^{n_1-n_2}(b_{n_2}^{-1})x^{n_1-n_2}$;
for $n_1 \geq i \geq n_2$ do
    $\bar{a}_i = $ Coefficient $(x^i, f^{(i)})$;
    $h^{(i)} = \bar{a}_i\sigma^{i-n_2}(b_{n_2}^{-1})x^{i-n_2}$;
    $f^{(i-1)} = f^{(i)} - h^{(i)}g$;
end
$q = h^{n_1} + \cdots + h^{n_2}$;
$r = f^{(n_2-1)}$;
return $(q, r)$;
```

Note that to avoid notation of fraction, the algorithm uses $\sigma^{n_1-n_2}(b_{n_2}^{-1})$ instead of $\frac{1}{\sigma^{n_1-n_2}(b_{n_2})}$ since they are equal as σ is an automorphism.

Example 2.5. *Let $F = \mathbb{F}_{2^5} \cong \mathbb{F}_2[\alpha]/(\alpha^5 + \alpha + a)$, where α is a primitive element of K. The σ is defined such that $\sigma(a) = a^2, \forall a \in F$. Consider*

$$f = x^3 + \alpha^{19}x^2 + \alpha^{17}x + \alpha, \quad g = x - \alpha^7$$

Using above algorithm, we can find that

$$q = x^2 + \alpha^4 x + \alpha^4, \quad r = \alpha^5$$

I.e. $f = (x^2 + \alpha^4 x + \alpha^4)g + \alpha^5$

Theorem 2.6 (Right Division Cost). *For any $f, g \in F[x;\sigma]$ with $n_1 \geq n_2$, perform right division to find q, r takes $O\big(n_2(n_1 - n_2)M(t) + n_2 tM(t)\log t\big)$ or $\tilde{O}\big(n_2(n_1 - n_2)t + n_2 t^2\big)$ operations in K.*

Proof. Computing the conjugates takes $O\big(n_2 tM(t)\log t\big)$ operations in K. At each iteration, computing $f^{(i-1)}$ takes n_2 operations, there are $\leq n_1 - n_2$ iterations in total. So right division takes $O\big(n_2(n_1 - n_2)M(t) + n_2 tM(t)\log t\big)$ operations in K. ∎

Caruso and Le Borgne uses a different algorithm to compute the right division which uses the Newton iteration and reciprocal polynomials. Their algorithm takes $\tilde{O}(n_1 t^2)$ operations in K but it involves approximation in the skew-power series ring.

Just as in commutative ring, we then can define modular equivalence once we have division.

Definition 2.7. *For any $f, g \in F[x;\sigma]$ with $n_1 \geq n_2$, we say g divides f on the right if right division algorithm finds $r = 0$.*

Definition 2.8 (Modular Equivalence). *For any $f_1, f_2, g \in F[x;\sigma]$, we say $f_1 \equiv f_2 \mod g$ is and only if there exists $q \in F[x;\sigma]$ such that $f_1 - f_2 = qg$.*

Theorem 2.9. *Modular equivalence defined above is an equivalence relation in $F[x;\sigma]$.*

Proof. We check relexivity, symmetricity, transitivity in $F[x;\sigma]$.

- it is clear $f \equiv f \mod g$.
- if $f_1 \equiv f_2 \mod g$, then $f_1 - f_2 = qg$, then $f_2 - f_1 = (-q)g$, thus $f_2 \equiv f_1 \mod g$.
- if $f_1 \equiv f_2 \mod g$ and $f_2 \equiv f_3 \mod g$, then $f_1 - f_2 = q_1 g$ and $f_2 - f_3 = q_2 g$, we add these together to get $f_1 - f_3 = (q_1 + q_2)g$ where $q_1 + q_2 \in F[x;\sigma]$, then $f_1 \equiv f_3 \mod g$. ∎

We have seen that factorization of skew-polynomials is not unique in general. With modular equivalence, we then can consider how two factorizations as a product of irreducible factors are related. This is the main structure theorem on complete factorization in $F[x;\sigma]$ proved by Ore in 1933.

Theorem 2.10 (Ore). *If $f \in F[x;\sigma]$ achieves two different complete factorizations, i.e.*

$$f = f_1 \cdots f_{m_1} = g_1 \cdots g_{m_2}$$

Then $m_1 = m_2$ and there exists a permutation π of $\{1, \cdots, m_1\}$ such that for all $1 \leq i \leq m_1$, deg (f_i) = deg $(g_{\pi(i)})$.

A more general version of the above theorem saying that f_i is similar to $g_{\pi(i)}$ instead of deg $(f_i) = $ deg $(g_{\pi(i)})$. "Similar" is also an equivalence relation defined as : f and g are similar if there exists $p, q \in F[x;\sigma]$ such that $\mathrm{gcrd}(f, q) = 1 = \mathrm{gcld}(g, p)$ and $pf = gq$. This definition is based on gcrd (the greatest common right divisor) and gcld (the greatest common left divisor), which will be discussed later.

Example 2.11. *Back to Example 1.5 with same F,*

$$\begin{aligned} f &= x^5 + x^4 + \alpha x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha^2 \\ &= (x^2 + \alpha^5 x + \alpha) \cdot (x + \alpha) \cdot (x + 1) \cdot (x + 1) \\ &= (x^2 + \alpha^5 x + \alpha) \cdot (x + \alpha^6) \cdot (x + \alpha^2) \cdot (x + 1) \end{aligned}$$

If we write up all its 20 factorizations, we will find that all degree-1 polynomials in thoes factorizations are similar to each other and all degree-1 polynomials in thoes factorizations are similar to each other, which gives us two similar class :

$$\begin{aligned} S_1 &= \{x + 1, x + \alpha, x + \alpha^2, x + \alpha^3, x + \alpha^4, x + \alpha^5, x + \alpha^6\} \\ S_2 &= \{x^2 + \alpha^6 x + \alpha^3, x^2 + \alpha^5 x + \alpha^6, x^2 + \alpha^5 x + \alpha, x^2 + \alpha^2 x + \alpha^4, x^2 + \alpha^2 x + 1, x^2 + x + \alpha^2, x^2 + x + \alpha\} \end{aligned}$$

3. Common Divisors, Multiples and Decomposition

Just as in the commutative case, the existence of right division also leads to the existence of right Euclidean algorithm for skew-polynomial ring, then we can define the greatest common right divisor and the least common left multiples.

Definition 3.1 (GCRD). *The greatest common right divisor of two polynomials $f, g \in F[x;\sigma]$, denoted as gcrd (f, g), is the monic polynomial $h = $ gcrd $(f, g) \in F[x;\sigma]$ of the highest degree such that h divides f and g, i.e. there exists $f_1, g_1 \in F[x;\sigma]$ with $f = f_1 h$ and $g = g_1 h$. For any $h' \in F[x;\sigma]$ such that h' also divides f and g, we have h' divides h.*

With gcrd defined, here is the right Euclidean algorithm for skew-polynomials :

```
Algorithm 3: RightEuclideanSkew
  Input: $f, g \in F[x;\sigma]$ with $n_1 = \deg(f) \le n_2 = \deg(g)$
  Output: gcrd $(f, g)$
  $f^{(1)} = f$;
  $f^{(2)} = g$;
  for $i \ge 3$ do
      $q^{(i)} = $ RightDivisionSkew $(f^{(i-2)}, f^{(i-1)}).q$;
      $r^{(i)} = $ RightDivisionSkew $(f^{(i-2)}, f^{(i-1)}).r$;
      $f^{(i)} = r^{(i)}$;
      STOP when $f^{(j)} = 0$ for some $j \ge 3$;
  end
  $a = \mathrm{lc}\ (f^{(j-1)})$;
  return $a^{-1} f^{(j-1)}$;
```

RightEuclideanSkew is almost the same as in the standard version. Note a^{-1} makes sure h is monic.

Theorem 3.2 (Uniqueness of gcrd). *For any $f, g \in F[x;\sigma]$, there exists a unique gcrd (f, g).*

Proof. The uniqueness of gcrd is in fact preserved by right Euclidean algorithm. Consider h' satisfying the conditions. Then h' divides and h divides h'. I.e. $h' = sh$ and then $h = th' = tsh$ for some $s, t \in F[x;\sigma]$.This forces degree of ts is 1, thus $h' = h$, which proves the uniqueness. ∎

Now we can consider the skew-polynomial version of Extended Euclidean Algorithm, it looks almost same as the standard version.

Algorithm 4: ExtendedEuclideanSkew

```
Input: $f, g \in F[x;\sigma]$ with $n_1 = \deg(f) \leq n_2 = \deg(g)$
Output: $s, t \in F[x;\sigma]$ such that $sf + tg = \text{gcrd}(f, g)$
$r^{(1)} = f$;
$r^{(2)} = g$;
for $i \geq 3$ do
    $q^{(i)} = \text{RightDivisionSkew}(r^{(i-2)}, r^{(i-1)}).q$;
    $r^{(i)} = \text{RightDivisionSkew}(r^{(i-2)}, r^{(i-1)}).r$;
    $Q^{(i)} = \begin{bmatrix} & 1 \\ 1 & -q^{(i)} \end{bmatrix}$;
    $R^{(i)} = Q^{(i)} \begin{bmatrix} r^{(i-2)} \\ r^{(i-1)} \end{bmatrix} = \begin{bmatrix} r^{(i-1)} \\ r^{(i)} \end{bmatrix}$;
    STOP when $r^{(j)} = 0$ for some $j \geq 3$
end
$s = R_{11}^{(j-1)}$;
$t = R_{12}^{(j-1)}$;
$h = r^{(j-1)}$;
return $s, t, h$;
```

Similarly we can define the least common left multiple.

Definition 3.3 (LCLM). *The least common left multiple of two polynomials $f, g \in F[x;\sigma]$, denoted as lclm (f, g), is the monic polynomial $h =$ lclm $(f, g) \in F[x;\sigma]$ of the lowest degree such that f and g divides h , i.e. there exists $f_1, g_1 \in F[x;\sigma]$ with $h = f_1 f$ and $h = g_1 g$. For any $h' \in F[x;\sigma]$ such that f and g also divides h', we have h divides h'. Similarly, LCLM is unique.*

Note we can find the LCLM also via algorithm 4. Note that $s^{(j)} f + t^{(j)} g = r^{(j)} = 0$, we know $s^{(j)} f = -t^{(j)} g$ is a common multiple of f and g. Also with degree restriction proved by Ore (1933), it forces that lclm $(f, g) = s^{(j)} f = -t^{(j)} g$.

Example 3.4. *Use same F as the Example 2.5.*

Let $f = x^3 + \alpha^{23} x^2 + \alpha^{23} x + \alpha^8$ and $g = x^3 + \alpha^{28} x^2 + \alpha^{27} x + \alpha^{13}$. We compute

$$\begin{aligned}
f &= 1 \cdot g + (\alpha^{25}x^2 + \alpha^2 x + \alpha^{10}) \\
g &= (\alpha^{12}x + \alpha^{14})(\alpha^{25}x^2 + \alpha^2 x + \alpha^{10}) + (\alpha^{30}x + \alpha) \\
\alpha^{25}x^2 + \alpha^2 x + \alpha^{10} &= (\alpha^{27}x + \alpha^9)(\alpha^{30}x + \alpha) + 0 \\
gcrd\,(f,g) &= a^{-30}(\alpha^{30} + \alpha) = x + \alpha^2 \\
lclm\,(f,g) &= (\alpha^{20}x^2 + \alpha^{19}x + \alpha^{12})(x^3 + \alpha^{23}x^2 + \alpha^{23}x + \alpha^8) = \alpha^{20}x^5 + \alpha^{20}
\end{aligned}$$

Theorem 3.5. *For any $f, g \in F[x;\sigma]$ with $n_1 = deg\ (f) \le n_2 = deg\ (g)$, computing gcrd (f,g) and lclm (f,g) takes $O\big(n_1^2 M(t) t \log t\big)$ or $\tilde{O}(n_1^2 t^2)$ operations in K.*

Giesbrecht gave the result in his paper in 1998 and Caruso and Le Borgne got a result of $\tilde{O}(SM(n_1,t))$ in 2015 using the FastExtendedRGCD described as Theorem 11.5 in Modern Computer Algebra by Von Zur Gathen and Gerhard (2003).

GCRD and LCLM are also related to the algebraic structure of $F[x;\sigma]$. Since $F[x;\sigma]$ is a principal left ideal ring by Theorem 2.4, each left ideal of it is generated by one polynomial in $F[x;\sigma]$. We have some similar properties as in the commutative case.

Theorem 3.6. *If $F[x;\sigma]f$ and $F[x;\sigma]g$ are two left ideals generated by $f, g \in F[x;\sigma]$, then*

- *the left ideal $F[x;\sigma]$ gcrd $(f,g) = F[x;\sigma]f + F[x;\sigma]g$;*
- *$F[x;\sigma]f \cap F[x;\sigma]g$ is also a left ideal generated by lclm (f,g).*

Another important operation is decomposition, a polynomial can be decomposed with respect to LCLM.

Definition 3.7. *Just as in commutative cases, we can also define primeness.*

- *Two polynomials $f, g \in F[x;\sigma]$ are co-prime if gcrd (f,g) =1.*
- *$f_1, \cdots, f_l \in F[x;\sigma]$ are mutually co-prime if*

$$gcrd\big(f_i,\ lclm\,(f_1,\cdots,f_{i-1},f_{i+1},\cdots,f_l)\big) = 1,\ \forall 1 \le i \le l$$

Definition 3.8.

- *An LCLM-decomposition of $f \in F[x;\sigma]$ is a list $(f_1,\cdots,f_l) \in F[x;\sigma]^l$ of mutually co-prime polynomials such that $f =$ lclm $(f_1,\cdots,f_l)$.*
- *If $f_1,\cdots,f_l$ are all irreducible, then f is said to be completely irreducible.*
- *$f \in F[x;\sigma]$ is LCLM-indecomposable if f admits no non-trivial LCLM-decompositions.*

Ore (1933) gave the result prove the uniqueness of polynomial decomposition in generalized skew-polynomial ring.

Theorem 3.9 (Ore). *Let $f \in F[x;\sigma]$ be monic and achieves an LCLM-decomposition $(f_1,\cdots,f_l)$, where $f_1,\cdots,f_l$ are LCLM-indecomposable, then*

- *if $f =$ lclm $(g_1,\cdots,g_m)$, where $g_1,\cdots,g_m$ are LCLM-indecomposable and mutually co-prime, then $l = m$ and there exists a permutation π of $\{1,\cdots,l\}$ such that for all $1 \le i \le l$, deg (f_i) = deg $(g_{\pi(i)})$ (f_i is similar to g_i).*
- *if $f_i = f_{i,1}\cdots f_{i,s_i}, \forall 1 \le i \le l$, where each $f_{i,j}$ is irreducible. If $f = h_1\cdots h_k$, where $h_1,\cdots,h_k$ are irreducible, then there exists a bijection $\pi : \{1,\cdots,k\} \to \{(i,j)\}$ such that for all $1 \le t \le k$, deg (h_t) = deg $(f_{\pi(t)})$.*

With all of the above operations and algebraic construction, we now can consider the complete factorization problem.

4. Complete Factorizations

For simiplicity, denote $F[x;\sigma]$ as $\mathcal{S}$. For any non-constant $f \in \mathcal{S}$, we want to achieve a complete factorization of f. Giesbrecht(1998) used associate algebra as a key tool to approach a general result.

Definition 4.1. *An associate algebra $\mathcal{A}$ over K is a K-vector space with compatible operations of addition and multiplication, under which $\mathcal{A}$ is a ring.*

Definition 4.2. *The idealizer of $\mathcal{S}f$ is the largest subalgebra of $\mathcal{S}$ in which $\mathcal{S}f$ is a two-sided ideal. Such an idealizer is given by*

$$I(\mathcal{S}f) = \{u \in \mathcal{S} \,|\, fu \equiv 0 \mod f\}$$

Definition 4.3. *The eigenring $E(\mathcal{S}f)$ of $\mathcal{S}f$ is defined as the quotient $E(\mathcal{S}f) = I(\mathcal{S}f)/\mathcal{S}f$, computing the endomorphisms of $\mathcal{S}f$. It is a finite K-algebra. If deg $(f) = n$, then*

$$E(\mathcal{S}f) \cong \mathcal{A} = \{u \in I(\mathcal{S}f) \,|\, deg\, u < n\} = \{u \in \mathcal{S} \,|\, fu \equiv 0 \mod f,\, deg\, u < n\}$$

where $\mathcal{A}$ is a K-algebra under addition in $\mathcal{S}$ and multiplication in $\mathcal{S}$ reduced modulo f.

Giesbrecht(1998) used a property of $E(\mathcal{S}f)$ that it is a field if and only if f is irreducible to reduct the complete factorization problem to computing non-zero zero divisors in $E(\mathcal{S}f)$.

Theorem 4.4 (McDonald 1974). *The center $\mathcal{C}$ of $\mathcal{S}$ satisfies $\mathcal{C} = K[x^t;\sigma] \subset \mathcal{S}$. In particular, $\mathcal{C}$ is a commutative unique factorization domain.*

Proof. $F[x^t]$ is the subset of $\mathcal{S}$ commuting with h_F defined in section 1.

$K[x]$ is the subset of $\mathcal{S}$ commuting with x.

$\mathcal{S}$ is a K-algebra generated by h_F and x, and $K[x^t] = F[x^t] \cap K[x]$ is the center of $\mathcal{S}$.

Then $\mathcal{C} = K[y]$, where $y = x^t$, which is also a unique factorization domain. ∎

Note that any $\hat{f} \in K[y]$ will generate a two-sided ideal $\mathcal{S}\hat{f}$, and the two-sided ideals in $\mathcal{S}$ are just exactly of the form $\mathcal{S}(\hat{f}x^l)$ for some $\hat{f} \in K[y]$ and $s \in \mathbb{N}$. Then we consider the maximal non-zero two-sided ideals in $\mathcal{S}$, which are $\mathcal{S}x$ and $\mathcal{S}\hat{u}$, where $\hat{u} \neq y$ is irreducible y-polynomial in $K[y]$.

Definition 4.5. *The bound of the left ideal $\mathcal{S}f$ is the largest two-sided ideal $\mathcal{O}$ it contains.*

Definition 4.6. *The minimal central left multiple $\hat{g} \in K[y]$ of f is a left multiple of f of the minimal degree.*

Theorem 4.7. *If gcrd $(f,x) = 1$, then $\mathcal{O} = \mathcal{S}\hat{g}$. In general, if $f =$ lclm (g,x^l) for some $l \geq 0$ and some $g \in \mathcal{S}$ co-prime with x and with minimal central left multiple $\hat{g} \in K[y]$, then $\mathcal{O} = \mathcal{S} \cdot \hat{g}x^s$.*

Definition 4.8.

- *An algebra $\mathcal{A}$ is simple if $\{0\}$ and $\mathcal{A}$ are the only two-sided ideals of it.*
- *An algebra is semi-simple if it is a direct sum of simple algebras.*

Theorem 4.9 (Lang 1984). *Let $\mathcal{A}$ be a finite simple algebra of dimension d over K and L be a left ideal in $\mathcal{A}$.*

- *$\mathcal{A}$ is isomorphic to $E^{m\times m}$, where E is the center of $\mathcal{A}$ and $[E:K]=r$, $d=m^2r$.*
- *There exists minimal left ideals $L_1,\cdots,L_m$ of $\mathcal{A}$ such that $\mathcal{A}=L_1\oplus\cdots\oplus L_m$, each L_i has dimension rm as a K-vector space.*
- *Let $L=L_1\oplus\cdots\oplus L_l$ for some $l\le m$, then there exists maximal left ideals $M_1,\cdots,M_m$ of $\mathcal{A}$ and $k\le m$ such that $L=M_1\cap\cdots\cap M_k$ and $M_1\cap\cdots\cap M_m=\{0\}$, also $M_i+(M_1\cap\cdots\cap M_{i-1}\cap M_{i+1}\cap\cdots\cap M_m)=\mathcal{A}$. Each maximal left ideal has dimension $d-rm$ as a K-vector space.*

Consider the $K-$algebra $\mathcal{A}=\mathcal{S}/\mathcal{S}\hat{u}$, then it is a simple algebra and a left principle ideal.

Theorem 4.10. *Left ideals of $\mathcal{A}$ are closed under GCRD and each left ideal J in $\mathcal{A}$ is generated by some unique $g+\mathcal{S}\hat{u}$, $g\in\mathcal{S}$ is monic of minimal degree.*

Proof. Suppose $g_1+\mathcal{S}\hat{u}$ and $g_2+\mathcal{S}\hat{u}$ are in some left ideal J of $\mathcal{A}$, $g_1,g_1\in\mathcal{A}$.

By Extended Euclidean algotrihm, we can find $h_1,h_2\in\mathcal{S}$ such that

$$\begin{aligned} h_1g_1+h_2g_2 &= gcrd(g_1,g_1) \\ (h_1+\mathcal{S}\hat{u})(g_1+\mathcal{S}\hat{u})+(h_2+\mathcal{S}\hat{u})(g_2+\mathcal{S}\hat{u}) &= gcrd(g_1,g_2)+\mathcal{S}\hat{u}\in J \end{aligned}$$

Note that gcrd $(g,\hat{u})+\mathcal{S}\hat{u}\in J$ and g has minimal degree, then g is a right factor of $\hat{u}$. ∎

Definition 4.11. *Such g determined in Theorem 4.11 is called the minimal modular generatir of J.*

Based on above construction, Giesbrecht (1998) proved a property showing the relationship between left ideal in $\mathcal{A}$ and left ideals in $\mathcal{S}$ generated by their minimal modular generators and characterizes the LCLM-decompositions of $f\in\mathcal{S}$, where the minimal central left multiples of f are irreducible as polynomials in y.

Theorem 4.12. *Let J_1,J_2 be non-zero left ideals in $\mathcal{A}$ with minimal modular generators $g_1,g_2\in\mathcal{S}$, then*

- *the left ideal $J_3=J_1\cap J_2$ in $\mathcal{A}$ has minimal generator $g_3 = lclm\ (g_1,g_2)$ when $J_3\neq\{0\}$. If $J_3=\{0\}$, then $\hat{u} = lclm\ (g_1,g_2)$.*
- *the left ideal $J_4=J_1+J_2$ in $\mathcal{A}$ has minimal modular generator $g_4 = gcrd\ (g_1,g_2)$.*

Theorem 4.13 (Giesbrecht 1998). *For $f\in\mathcal{S}$, the eigenring $E(\mathcal{S}f)$ is a finite field if and only if f is irreducible in $\mathcal{S}$.*

Now with Theorem 4.13, we can reduce the complete factorization problem to the problem of determining if a finite dimensional associative algebra $\mathcal{A}$ over a finite field has any non-zero zero divisors. This gives consequence of the following corollary showing that left zero divisors in $\mathcal{A}$ is isomorphic to $E(\mathcal{S}f)$, which can be easily proved by contradiction.

Theorem 4.14. *For $f\in\mathcal{S}$, if $u,v\in\mathcal{A}\smallsetminus\{0\}$ with $uv\equiv 0 \mod f$, then gcrd $(f,u)\neq$ 1.*

Then we have the algorithm for complete factorization of skew-polynomial, which is introduced by Giesbrecht in 1998 :

```
Algorithm 5: CompleteFactorizationSkew
  Input: $f \in F[x;\sigma]$ with $n = \deg(f)$
  Output: a list of $f_1, \cdots, f_k \in F[x;\sigma]$ irreducible such that $f = f_1 \cdots f_k$
  $B_{\mathcal{A}}$ = FindBasis ($\mathcal{A}$);
  if ( $\mathcal{A}$ is a field ) then
      return $f$;
  else
      $u$ = nonzero left divisor of $\mathcal{A}$;
      $h$ = RightEuclideanSkew ($f, u$);
      $g$ = RightDIvisionSkew ($f, h$).q;
      return ( CompleteFactorizationSkew ($g$), CompleteFactorizationSkew ($h$) );
  end
```

There are three subproblems in algorithm 5, one is to find the basis of $\mathcal{A}$, one other is to determine whether $\mathcal{A}$ is a field, another is to find a zero divisor (if $\mathcal{A}$ is not a field). The subproblem of finding basis can be done by the following algorithm :

```
Algorithm 6: FindBasis
  Input: The simple $K$-algebra $\mathcal{A}$ constructed previously
  Output: A basis $B_{\mathcal{A}}$ of $\mathcal{A}$
  Compute $W = \{g \in \mathcal{S} \mid \deg(g) < n\}$;
  Compute a $K$-linear map $T : W \to W$ (in matrix form) s.t. $T(a) = b \equiv fa \mod f$;
  $N$ = NullSpace ($T$);
  return basis of $N$;
```

Theorem 4.15. *The Findbasis algorithm takes $O\big(n^3 tM(t) + n^2 t^2 M(t) \log t + MM(nt)\big)$ operations in K if we Giesbrecht Multiplication algorithm, and $O\big(n^{2.58} t^{2.41} + MM(nt)\big)$ operations in K if we use KaratsubaSkew (Algorithm 1).*

Proof. Note W is a nt-dimensional K-vector space isomorphic to $\mathcal{S}/\mathcal{S}f$,

the basis of W is easily seen to be (h_F determined in section 1)

$$\{h_F^i x^j \mid 0 \leq i < t, 0 \leq j < n\}$$

Thus $\mathcal{A} \cong$ NullSpace (T).

So we need to compute each $fh_F^i x^j \mod f$, which takes $O\big(n^3 tM(t) + n^2 t^2 M(t) \log t\big)$ by Theorem 2.3. Computing the null space will take $O\big(MM(nt)\big)$.

It can improved to $O(n^{2.58} t^{2.41})$ if we use KaratsubaSkew. ■

The subproblem to determine whether $\mathcal{A}$ is a field is solved by Ronyai (1987), who proved that it can be reduced to factoring polynomials in $\mathbb{F}_p[x]$ of degree $(nst)^{O(1)}$ ($[f : \mathbb{F}_p] = st$ in section 1) with $(nt \log q)^{O(1)}$ operations in K. Factoring in $\mathbb{F}_p[x]$ can be solved by a faster Las Vegas type probabilistic algorithm in $O\big(nt\chi + MM(nt) + M(nt)\log(nt)\log q\big)$ operations in K, where χ operations in K are required to multiply twp elements of $\mathcal{A}$. Then after we have determined $\mathcal{A}$ is not a field, it takes $O\big(n^3 tM(t) + n^2 t^2 M(t) \log t + MM(nt) + M(nt)\log(nt)\log q\big)$ operations to find a zero divisor in $\mathcal{A}$. This can be improved to $O\big(n^{2.58} t^{2.41} + MM(nt) + M(nt)\log(nt)\log q\big)$ if Karatsuba is used for multiplications.

Theorem 4.16 (Complete Factorization Cost). *For any $f \in \mathcal{S}$ with degree n, CompleteFactorizationSkew finds a complete factorization of f using a Las Vegas type algorithm with $O\big(n^4tM(t) + n^3t^2M(t)\log t + nMM(nt) + nM(nt)\log(nt)\log q\big)$ operations in K if using classical multiplication algorithm or $O\big(n^{3.58}t^{3.41} + nMM(nt) + nM(nt)\log(nt)\log q\big)$ operations in K if using Karatsuba for multiplication.*

5. Conclusion and Further Works

In non-commutative cases, factoring can be very difficult. But we can try to use the algebraic structure trying to reduce it to the commutative cases. The first significant result is due to Giesbrecht (1998), who used associate algebra reducing the numerical factoring problem to a algebraic problem in the commutative case. Caruso and Le Borgne (2015) developed a faster algorithm using Azumaya algebras, and parts of their improvement on basic operations have been mentioned in section 2 and 3. The total average cost of their faster algorithm for factoring a skew-polynomial of degree n is

$$\tilde{O}\big(nt^3\log q + n\log^q + n^{1+\epsilon}(\log q)^{1+o(1)}\big) + F(n,K)$$

where $F(n,K)$ is the cost of factoring a commutative polynomial of degree n over the finite field K.

The Bi-Factorization with two-sided ideals problem can also be solved using the same technique involving associate algebra with a probabilistic algorithm in $O\big(n^4tM(t) + n^3t^2M(t)\log t + nMM(nt) + nM(nt)\log(nt)\log q\big)$ operations in K, details are not covered in this short report.

Many probabilistic analysis are not covered in this report, further problems to work on about skew-polynomials can be that the probability of a skew-polynomial to be irreducible, the probability of a skew-polynomial to be square free and the probability of a skew-polynomial to be smooth.

References

[1] Oystein Ore. *Theory of non-commutative polynomials.* Ann. of Math. (2) 34 (1933), no. 3, 480–508. MR 1503119

[2] Mark Giesbrecht. *Factoring in skew-polynomial rings over finite fields.* J. Symbolic Comput. 26 (1998), no. 4, 463–486. MR 1646671 (99i:16053)

[3] Xavier Caruso and Jérémy Le Borgne. *A new faster algorithm for factoring skew polynomials over finite fields.* J. Symbolic Comput. 79 (2017), no.2, 411-443.

[4] Joachim Von Zur Gathen and Jurgen Gerhard. *Modern computer algebra, 2ed.* Cambridge University Press, New York, NY, USA, 2003.

[5] Kiran S. Kedlaya and Christopher Umans. *Fast modular composition in any characteristic.* Foundations of Computer Science, IEEE Annual Symposium on 0 (2008), 146–155.

[6] Travis Baumbaugh. *Results on Common Left/Right Divisors of Skew Polynomials.* Master Thesis (2016)

[7] B. McDonald. *Finite RIngs with Identity.* Marcel Dekker, Inc. (New York), 1974.

[8] L. Ronyai. *Simple algebra are difficult.* 19th ACM Symp. on Theory of Comp., pp. 398-408, New York, 1987.