Clemson University
TigerPrints

All Theses

Theses

5-2016

# Results on Common Left/Right Divisors of Skew Polynomials

Travis Baumbaugh
*Clemson University*, tbaumba@clemson.edu

# Results on Common Left/Right Divisors of Skew Polynomials

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Master of Science
Mathematical Science

by
Travis Baumbaugh
May 2016

Accepted by:
Dr. Felice Manganiello, Committee Chair
Dr. Shuhong Gao
Dr. Gretchen Matthews

# Abstract

Since being introduced by Oystein Ore in his 1933 paper, “Theory of Non-Commutative Polynomials” [6], non-commutative, skew, or Ore polynomials have been studied extensively. One prominent application of skew polynomials is in the generation of codes. This paper covers some key facets of the structure of skew polynomials and aims to find a divisor polynomial for two given polynomials that satisfies certain properties of divisibility.

# Acknowledgments

I would like to thank my advisor, Dr. Felice Manganiello of the Mathematical Science Department at Clemson University for pushing me to develop the original research in this paper. Dr. Manganiello was instrumental in guiding the research to achievable goals and improving the style and content of this paper.

I would also like to thank my brother, Brandyn Baumbaugh for providing a second pair of eyes with which to look for mistakes.

# Table of Contents

# Chapter 1

# Introduction

As seen in [1], skew polynomials can be used to generate codes. In certain circumstances, as outlined in [2], such codes have properties similar to cyclic codes. The main focus of this paper was inspired by a search for polynomial $p(x)$ of minimal degree in a skew polynomial ring $R$ that is in the intersection of the right ideal of a polynomial $f(x)$ and the left ideal of a polynomial $g(x)$ for use in a new coding methodology.

Certainly $f(x)g(x)$ is in the intersection of these ideals, but it may not be the polynomial of least degree. If some polynomial $d(x)$ can be found which is of maximal degree such that $f(x) = f'(x)d(x)$ and $g(x) = d(x)g'(x)$, then we can write

$$f(x)g(x) = \quad f'(x) \quad d(x) \quad d(x) \quad g'(x),$$

where there is some redundancy "between" the polynomials. Indeed, we may write

$$\begin{aligned} f(x) &= \quad f'(x) \quad d(x) \\ g(x) &= \qquad\qquad\; d(x) \quad g'(x) \\ p(x) &= \quad f'(x) \quad d(x) \quad g'(x), \end{aligned}$$

where we can visualize that $p(x)$ is divisible on the left by $f(x)$ and on the right by $g(x)$, so $p(x)$ is in the intersection of ideals. It is hoped that by taking advantage of the overlap of $d(x)$, this is the smallest such polynomial. Thus, the goal becomes finding such $d(x)$, which we refer to as the greatest common left-right divisor (gclrd) of $f(x)$ and $g(x)$. This problem took on a life of its own, motivating a search for structure between the right and left roots of certain types of polynomials. It is the aim of this paper to examine some results toward an algorithm for computing the gclrd of two polynomials.

In Chapter 2, we review some of what was already known about skew polynomials. The basic structure of skew polynomial rings is laid out, along with definitions for the greatest common right divisor and greatest common left divisor as extensions of the concept of gcd for commutative polynomials, as well as similar extensions for the lcm. The formula for evaluation of skew polynomials is also provided, along with a discussion of independent sets of roots.

Chapter 3 covers our original developments toward the greatest common left-right divisor. First, left evaluation is examined as a modification of right evaluation along with corresponding formulations of the left evaluation of products and interpolation. Then special cases of polynomials in which a known formula for a nontrivial polynomial which is a right divisor of $f(x)$ and a left divisor of $g(x)$ are presented. Finally, a condition necessary for a certain construction to share left and right roots is given.

This is followed in Chapter 4 by a description of implementing skew polynomial multiplication in the MAGMA programming language. The functions written to manipulate skew polynomials and aid the search for the gclrd are outlined. Finally, Chapter 5 reviews the results so far and lays out paths for further study of the gclrd.

# Chapter 2

# Background

## 2.1 Introduction to Skew Polynomials

Skew polynomials were introduced by Oystein Ore in his 1933 paper, "Theory of Non-Commutative Polynomials" [6].

**Definition 2.1.** Let $K$ be any division ring, let $\sigma : K \to K$ be an injective homomorphism and let $\delta$ be a $\sigma$-derivation; that is, $\delta : K \to K$ is a homomorphism with respect to addition such that $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$ for all $a, b \in K$. Then let $R$ be the set of polynomials of the form $f(x) = \sum_{i=0}^{n} a_i x^i$, where $n \in \mathbb{N}$ and $a_i \in K$ for $i \in \{0, 1, \dots, n\}$. Under standard polynomial addition and with multiplication determined by the rule

$$xa = \sigma(a)x + \delta(a) \tag{2.1}$$

for all $a \in K$, this forms a ring of skew polynomials over $K$, which we write as $R = K[x; \sigma, \delta]$.

The following example defines the skew polynomial ring that we will use throughout the manuscript.

**Example 2.1.** Let $K = \mathbb{F}_{2^5} = \mathbb{F}_2[\alpha]/(\alpha^5 + \alpha + 1)$, $\sigma(a) = a^2$, and $\delta \equiv 0$. Then $\alpha$ is a primitive element of $K$. We let $R = K[x; \sigma, \delta]$, which we may also write as $R = K[x; \sigma]$ for brevity, since $\delta \equiv 0$.

We note that in our particular work, not only will $K$ be a division ring, but it will in fact be a field. We will take $K$ to be a degree $m$ extension of a finite field, $\mathbb{F}_q$, so that $K = \mathbb{F}_{q^m}$. This forces $\sigma$ to be an automorphism, and we take $\delta \equiv 0$. In this case, we may write $R = K[x; \sigma]$. The above, however, is the most general definition of skew polynomials, and is sufficient to prove several key properties.

## 2.2 Properties of Skew Polynomials

Since their introduction, several properties have already been determined about skew polynomials, some of which will be outlined here. A skew polynomial ring $R$ is not in general commutative. It is right Euclidean, and if $\sigma$ is surjective, left Euclidean. Ideals of $R$ are principal. Factorization is not unique, but the terms of prime factorizations are pairwise similar [6]. Additionally, skew polynomials can be used to generate codes [1] and skew-cyclic codes [2]. Efficient algorithms exist for computing greatest common divisors and least common multiples [3].

The first important property to note is that unlike traditional polynomials, multiplication of skew polynomials is not commutative in general. If $\sigma$ is not the identity homomorphism, then we must have some $a \in K$ such that $\sigma(a) \neq a$, and it is easy to see that then

$$xa = \sigma(a)x + \delta(a) \neq ax.$$

Using this example, it is easy to see that skew polynomial multiplication is commutative if and only if $\sigma$ is the identity homomorphism and $\delta \equiv 0$, in which case multiplication simplifies to ordinary polynomial multiplication.

**Example 2.2.** In $R = K[x;\sigma,\delta]$ from the previous example,we have that

$$\begin{aligned}(x+\alpha)(x+\alpha^2) &= x^2 + x\alpha^2 + \alpha x + \alpha^3 \\ &= x^2 + \sigma(\alpha^2)x + \alpha x + \alpha^3 \\ &= x^2 + (\alpha^4 + \alpha)x + \alpha^3 \\ &= x^2 + \alpha^{30}x + \alpha^3,\end{aligned}$$

whereas

$$\begin{aligned}(x+\alpha^2)(x+\alpha) &= x^2 + x\alpha + \alpha^2 x + \alpha^3 \\ &= x^2 + \sigma(\alpha)x + \alpha^2 x + \alpha^3 \\ &= x^2 + (\alpha^2 + \alpha^2)x^3_\alpha \\ &= x^2 + \alpha^3.\end{aligned}$$

By repeated application of (2.1), we see that $ax^m \cdot bx^n$ will be a polynomial with degree $m+n$ and with leading coefficient $a\sigma^m(b)$. We see that $\sigma^m(b) = 0$ only if $\sigma^{m-1}(b) = 0$, and so on down to $b = 0$, and since there are no zero divisors in $K$, $a, b \neq 0$ implies $a\sigma(b) \neq 0$. We apply the normal rules of associations and distribution, so this allows us to find the product of any arbitrary polynomials. If $f(x)$ is of degree $n$ and $g(x)$ is of degree $m$, then the degree of the resulting polynomial will be $m+n$, and so the degree of a product is the sum of the degrees of the factors. In fact, this is where the definition of skew polynomial multiplication originates from as a generalization of regular polynomial multiplication.

The following is shown in [6]:

**Lemma 2.1.** *A skew polynomial ring $R$ is a right Euclidean ring and, if $\sigma$ is surjective, a left Euclidean ring.*

*Proof.* We see this by first considering polynomials $f(x)$ of degree $n$ and $g(x)$ of degree $m \leq n$. Then if $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$, we find that the leading term of $x^{n-m}g(x)$ is $\sigma^{n-m}(b_m)x^{n-m}x^m = \sigma^{n-m}(b_m)x^n$. Thus, $a_n\sigma^{n-m}(b_m^{-1})x^{n-m}g(x)$ has leading term

$$\begin{aligned} a_n\sigma^{n-m}(b_m^{-1})\sigma^{n-m}(b_m)x^m &= a_n\sigma^{n-m}(b_m^{-1}b_m)x^n \\ &= a_n\sigma^{n-m}(1)x^n \\ &= a_nx^n. \end{aligned}$$

Since this is the same leading term as $f(x)$, the difference

$$f(x) - a_n\sigma^{n-m}(b_m^{-1})x^{n-m}g(x)$$

has no term of degree $n$ and thus is of degree less than $n$. We may repeat this process with the remaining difference until the degree of the difference is less than $m$ or the remaining polynomial is 0. Collecting the monomial terms used as the polynomial $q_r(x)$ will allow us to write

$$f(x) = q_r(x)g(x) + r_r(x), \tag{2.2}$$

where $\deg r_r(x) < m = \deg g(x)$ or $r_r(x) = 0$. We call this right division and it makes the ring $R$ of skew polynomials right Euclidean, with the Euclidean function being the degree of the polynomial. If $\sigma$ is surjective, then we may also perform left division. That is, for any polynomials $f(x), g(x) \in R$, there exist polynomials $q_l(x), r_l(x), \in R$ such that

$$f(x) = g(x)q_l(x) + r_l(x), \tag{2.3}$$

with either $\deg r_l(x) < \deg g(x)$ or $r_l(x) = 0$. We note that while we can always find an element $k = a_n\sigma^{n-m}(b_m^{-1})$ such that $kx^{n-m}g(x)$ has the same leading term as

$f(x)$, it is not necessarily possible to find an element $k \in K$ such that $g(x)kx^{n-m}$ has the same leading term as $f(x)$. This is because the leading term of $g(x)kx^{n-m}$ is $b_m\sigma^m(k)x^n$, while the leading term of $f(x)$ is $a_nx^n$, so we must have $b_m\sigma^m(k) = a_n$, or $\sigma^m(k) = a_nb_m$. To always have a solution for any $f(x)$ and $g(x)$, $\sigma(k) = a$ must have a solution $k \in K$ for any $a \in K$, and so $\sigma$ must therefore be surjective. If $\sigma$ is surjective, then this will always have a solution, and so left division is possible in the same manner as right division. This makes $R$ left Euclidean as well. □

**Example 2.3.** Using the same $R$ as before, we take

$$f(x) = x^3 + \alpha^{19}x^2 + \alpha^{17}x + \alpha$$

and $g(x) = (x - \alpha^7)$.

We find that

$$f(x) = (x^2 + \alpha^4x + \alpha^4)g(x) + \alpha^5,$$

so we have $q_r(x) = x^2 + \alpha^4x + \alpha^4$ and $r_r(x) = \alpha^5$. On the other hand,

$$f(x) = g(x)(x^2 + \alpha^{15}x + \alpha^{25}),$$

so we have $q_l(x) = x^2 + \alpha^{15}x + \alpha^{25}$ and $r_l(x) = 0$.

**Definition 2.2.** If $r_r(x) = 0$, we say that $g(x)$ divides $f(x)$ on the right and write $g(x)|_rf(x)$. If $r_l(x) = 0$, we say that $g(x)$ divides $f(x)$ on the left and write $g(x)|_lf(x)$.

In the previous example, for instance, we have that $g(x)|_lf(x)$, but $g(x) \not|_r f(x)$.

**Definition 2.3.** The greatest common right divisor (denoted gcrd) of two polynomials $f(x), g(x) \in R$ is the monic polynomial $d_r(x) = \text{gcrd}(f(x), g(x)) \in R$ such that

$d_r(x)|_r f(x)$, $d_r(x)|_r g(x)$, and for any $d'(x) \in R$ such that $d'(x)|_r f(x)$ and $d'(x)|_r g(x)$, we have $d'(x)|_r d_r(x)$.

**Lemma 2.2.** *For any two given polynomials $f(x), g(x) \in R$, there exists a unique* $\mathrm{gcrd}(f(x), g(x))$.

*Proof.* The division algorithm set out above allows us to perform a right Euclidean algorithm to find the gcrd. We start with $f_1(x)$ and $f_2(x)$, equal to $f(x)$ and $g(x)$ such that $\deg f_1(x) \leq \deg f_2(x)$. Then for $i \geq 3$, we perform division of $f_{i-2}(x)$ by $f_{i-1}(x)$, with the quotient being $q_i(x)$ and the remainder being $f_i(x)$. That is,

$$f_{i-2}(x) = q_i(x)f_{i-1}(x) + f_i(x).$$

This process is repeated until we have $f_j(x) = 0$ for some $j \geq 3$. We let $k = j - 1$ and consider the polynomial $f_k(x)$. If the leading coefficient of this polynomial is $a \in \mathbb{F}_{q^m}^* = \mathbb{F}_{q^m} \setminus \{0\}$, then define $d_r(x) = a^{-1}f_k(x)$ so that $d_r(x)$ is monic. We then claim that $d_r(x) = \mathrm{gcrd}(f(x), g(x))$. Since $ad_r(x) = a(a^{-1}f_k(x)) = f_k(x)$, we have that $d_r(x)|_r f_k(x)$. By definition of $k$, we have that

$$\begin{aligned} f_{k-1}(x) &= q_{k+1}(x)f_k(x) + f_{k+1}(x) \\ &= q_{k+1}(x)f_k(x) + 0 \\ &= q_{k+1}(x)f_k(x), \end{aligned}$$

and so $f_k(x)|_r f_{k-1}(x)$. If we have $f_k(x)|_r f_i(x)$ and $f_k(x)|_r f_{i-1}(x)$, then because

$$f_{i-2}(x) = q_i(x)f_{i-1}(x) + f_i(x),$$

and $f_k(x)$ divides both terms on the right, it divides the sum on the right, and so

$f_k(x)|_r f_{i-2}(x)$ as well. This allows us to work back through the sequence of equations to see that $f_k(x)|_r f_1(x)$ and $f_k(x)|_r f_2(x)$.

At this stage, we note that if $a(x)|_r b(x)$ and $b(x)|_r c(x)$, then we can write $b(x) = b'_r(x)a(x)$ and $c(x) = c'_r(x)b(x) = c'_r(x)b'_r(x)a(x)$, and so $a(x)|_r c(x)$. Thus, right divisibility is transitive (the same is true of left divisibility as well). This means that $d_r(x)|_r f_1(x)$ and $d_r(x)|_r f_2(x)$, so $d_r(x)|_r f(g)$ and $d_r(x)|_r g(x)$. We then consider any polynomial $d'(x)$ such that $d'(x)|_r f(x)$ and $d'(x)|_r g(x)$. Then we have that $d'(x)|_r f_1(x)$ and $d'(x)|_r f_2(x)$. We note that if $d'(x)|_r f_{i-2}(x)$ and $d'(x)|_r f_{i-1}(x)$, we may rewrite the equations above as

$$f_i(x) = f_{i-2}(x) - q_i(x)f_{i-1}(x),$$

and so $d'(x)|_r f_i(x)$. Starting with $d'(x)|_r f_1(x)$ and $d'(x)|_r f_2(x)$, this allows us to follow the equations down to $d'(x)|f_k(x)$, and since $d_r(x) = a^{-1}f_k(x)$, we have $d'(x)|_r d_r(x)$. This means that $d_r(x)$ is a monic polynomial such that $d_r(x)|_r d(x)$, $d_r(x)|_r g(x)$, and for any polynomial $d'(x) \in R$ such that $d'(x)|_r f(x)$ and $d'(x)|_r g(x)$, we have $d'(x)|_r d_r(x)$.

Consider any other polynomial $d_2(x)$ satisfying these conditions. Then in particular, $d_2(x)|_r d_r(x)$ and $d_r(x)|_r d_2(x)$, which means that $d_2(x) = d'_2(x)d_r(x)$ and $d_r(x) = d'_r(x)d_2(x) = d'_r(x)d'_2(x)d_r(x)$. By the property that the degree of the product is the sum of the degrees of the factors, we know that $d'_r(x)d'_2(x)$ must be of degree 0, and so $d'_2(x)$ must be of degree 0. This means that $d_2(x)$ is a constant multiple of $d_r(x)$. Thus, if $d_2(x)$ is also monic, it must be $1 \cdot d_r(x) = d_r(x)$, and so $d_r(x)$ is the unique monic polynomial satisfying the conditions stated above. □

**Example 2.4.** If we take

$$f_1(x) = x^3 + \alpha^{23}x^2 + \alpha^2 3x + \alpha^8$$

and

$$f_2(x) = x^3 + \alpha^{28}x^2 + \alpha^{27}x + \alpha^{13},$$

then we find

$$\begin{aligned} f_1(x) &= 1 \cdot f_2(x) + \alpha^{25}x^2 + \alpha^2 x + \alpha^{10} \\ f_2(x) &= (\alpha^{12}x + \alpha^{14})(\alpha^{25}x^2 + \alpha^2 x + \alpha^{10}) + \alpha^{30}x + \alpha \\ \alpha^{25}x^2 + \alpha^2 x + \alpha^{10} &= (\alpha^{27}x + \alpha^9)(\alpha^{30}x + \alpha) + 0, \end{aligned}$$

and so $\mathrm{gcrd}(f_1(x), f_2(x)) = a^{-30}(\alpha^{30}x + \alpha) = x + \alpha^2$

If $\sigma$ is surjective, then the greatest common left divisor $d_l(x)$ of $f_1(x)$ and $f_2(x)$, written $d_l(x) = \mathrm{gcld}(f(x), g(x))$, is defined in the same manner using left division:

**Definition 2.4.** The greatest common left divisor (gcld) of $f(x), g(x) \in R = K[x; \sigma, \delta]$, where $\sigma$ is surjective, is the unique monic polynomial $d_l(x) = \mathrm{gcld}(f(x), g(x))$ such that $d_l(x)|_l f(x)$, $d_l(x)|_l g(x)$, and for any $d'(x)$ such that $d'(x)|_l f(x)$ and $d'(x)|_l g(x)$, we have $d'(x)|_l d_l(x)$.

**Remark.** *We note here that a greatest common left divisor may exist without $\sigma$ being surjective, but without $\sigma$ being surjective, it is not always possible to do left division. Thus the corresponding proof of existence and uniqueness which relies on the Euclidean algorithm is no longer possible.*

We may also speak of the least common left multiple $m_l(x) = \mathrm{lclm}(f(x), g(x))$ of two polynomials $f(x)$ and $g(x)$:

**Definition 2.5.** The least common left multiple (lclm) of $f(x), g(x) \in R$ is the unique monic polynomial $m_l(x) = \text{lclm}(f(x), g(x))$ such that $f(x)|_r m_l(x)$, $g(x)|_r m_l(x)$, and for any $m'(x) \in R$ such that $f(x)|_r m'(x)$ and $g(x)|_r m'(x)$, we have $m_l(x)|_r m'(x)$.

Ore gives an algorithm for computing this polynomial in [6] Theorem 8, but a more computationally efficient algorithm is given in Section 2 of [3]. It is computed as follows: If we let $s_i(x)$ and $t_i(x)$ be the multipliers in the extended Euclidean algorithm then we have

$$\begin{aligned} &s_1(x) = 1 \qquad && s_2(x) = 0 \qquad && s_i(x) = s_{i-2}(x) - q_i(x)s_{i-1}(x) \\ &t_1(x) = 0 && t_2(x) = 1 && t_i(x) = t_{i-2}(x) - q_i(x)t_{i-1}(x), \end{aligned}$$

which guarantee that

$$s_i(x)f_1(x) + t_i(x)f_2(x) = f_i(x)$$

for all $i$ such that $3 \leq i \leq k+1$. In particular, since $f_{k+1}(x) = 0$, we have that $s_{k+1}f_1(x) + t_{k+1}f_2(x) = 0$, and so $s_{k+1}f_1(x)$ is also right divisible by $f_2(x)$, and since the degree is the same as the degree given by Ore, we find that $s_{k+1}f_1(x)$ is the lclm of $f_1(x)$ and $f_2(x)$ up to a constant (as with the gcrd, we define the lclm to be the unique monic polynomial meeting the conditions).

**Example 2.5.** If we use the previous example, then we find that

$$\begin{aligned} &s_3(x) = 1 - 1 \cdot 0 = 1 \\ &s_4(x) = 0 - (\alpha^{12}x + \alpha^{14}) \cdot 1 = \alpha^{12}x + \alpha^{14} \\ &s_5(x) = 1 - (\alpha^{27}x + \alpha^{9})(\alpha^{12}x + \alpha^{14}) = \alpha^{20}x^2 + \alpha^{19}x + \alpha^{12}, \end{aligned}$$

which means

$$\begin{aligned}\mathrm{lclm}(f_1(x), f_2(x)) &= s_5(x)f_1(x)\\ &= (\alpha^{20}x^2 + \alpha^{19}x + \alpha^{12})(x^3 + \alpha^{23}x^2 + \alpha^23x + \alpha^8)\\ &= \alpha^{20}x^5 + \alpha^{20}.\end{aligned}$$

We may similarly define a polynomial lcrm of $f(x)$ and $g(x)$ based on left divisibility if left division is available.

**Definition 2.6.** The least common right multiple (lcrm) of $f(x), g(x) \in R = K[x;\sigma,\delta]$, where $\sigma$ is surjective, is the unique monic polynomial $m_r(x) = \mathrm{lcrm}(f(x), g(x))$ such that $f(x)|_l m_r(x)$, $g(x)|_l m_r(x)$, and for any $m'(x) \in R$ such that $f(x)|_l m'(x)$ and $g(x)|_l m'(x)$, we have $m_r(x)|_l m'(x)$.

The computation of this lcrm is analogous to the computation of the lclm, but with the extended left Euclidean algorithm.

## 2.3 Right Evaluation

To understand the root structure of skew polynomials, we first wish to define evaluation for skew polynomials. For a commutative polynomial $f(x) \in K[x]$, the process of evaluating $f(x)$ at $a \in K$ (denoted $f(a)$) is as simple as "plugging in" the value $a$ in place of every $x$ in a polynomial and then carrying out the proper operations. However, for a skew polynomial, this results in a value that isn't necessarily the remainder of right division by $(x-a)$. In particular, this means a polynomial divisible by $(x-a)$ on the right may not be 0 when evaluated at $a$, a property that we desire of the evaluation. Thus, we use an alternate definition of evaluation.

**Definition 2.7.** For any polynomial $f(x) \in R$ and any $a \in K$, by using right division we may write $f(x) = q_r(x)(x-a) + r$. Here, $r = 0$ or $\deg r < \deg(x-a) = 1$, so $\deg r = 0$ and $r$ is a constant. Then the evaluation of $f(x)$ on the right at $a$ is $f(a)_r = r$. Likewise, if $\sigma$ is surjective, then left division is possible and we may write $f(x) = (x-a)q_l(x) + s$, where $s = 0$ or $s$ is a constant, and the evaluation of $f(x)$ on the left at $a$ is $f(a)_l = s$.

To summarize, $f(x)$ evaluated at $a$ on the right should be $r$, the remainder of the right division of $f(x)$ by the polynomial $(x-a)$.

**Example 2.6.** We return to the example where

$$f(x) = x^3 + \alpha^{19}x^2 + \alpha^{17}x + \alpha.$$

Since we had that

$$f(x) = (x^2 + \alpha^4 x + \alpha^4)(x - \alpha^7) + \alpha^5,$$

we have $f(\alpha^7)_r = \alpha^5$. On the other hand, we have that

$$f(x) = (x - \alpha^7)(x^2 + \alpha^{15}x + \alpha^{25}) + 0,$$

and so $f(\alpha^7)_l = 0$.

A formula for such evaluation without carrying out division is described in [4], and we repeat it here with our notation.

**Theorem 2.3.** *We define recursively*

$$N_0(a) = 1$$

$$N_{i+1}(a) = \sigma(N_i(a))a + \delta(N_i(a))$$

*for all $a \in K$ and $i \geq 1$. For any $a \in K$ and any polynomial $f(x) = \sum_{i=0}^{d} b_i x^i \in R$, we have $f(a)_r = \sum_{i=0}^{d} b_i N_i(a)$.*

This means that $f(a)_r$ as computed above is the remainder of dividing $f(x)$ on the right by $(x - a)$, as desired. The proof of this is in [4] and is as follows:

*Proof.* For any $k \geq 0$, we have $(x-a)|_r(x^k - N_k(a))$. This is trivially true for $k = 0$, as $tx^0 - N_0(a) = 1 - 1 = 0$, and so it is trivially divisible by $(x - a)$. Then we may use induction, assuming it is true for some $k \geq 0$ and see that

$$\begin{aligned}
x^{k+1} - N_{k+1}(a) &= x^{k+1} - \sigma(N_k(a))a - \delta(N_k(a)) \\
&= x^{k+1} - \sigma(N_k(a))a + (\sigma(N_k(a))x - \sigma(N_k(a))x) - \delta(N_k(a)) \\
&= x^{k+1} + \sigma(N_k(a))(x-a) - (\sigma(N_k(a))x + \delta(N_k(a))) \\
&= \sigma(N_k(a))(x-a) + x^{k+1} - xN_k(a) \\
&= \sigma(N_k(a))(x-a) + x(x^k - N_k(a)).
\end{aligned}$$

From our hypothesis, $(x-a)|_r(x^k - N_k(a))$, so both terms on the last line are divisible on the right by $(x-a)$. This proves that $(x-a)|_r(x^k - N_k(a))$ for any $k \geq 0$. We then note that $f(x) - f(a)_r = \sum_{i=0}^{d} b_i x^i - \sum_{i=0}^{n} b_i N_i(a) = \sum_{i=0}^{d} b_i(x^i - N_i(a))$. By applying what we just proved to each term in the sum, we find that $(x-a)|_r(f(x) - f(a)_r)$, so we may write $f(x) - f(a)_r = q_r(x)(x-a)$, which means $f(x) = q_r(x)(x-a) + f(a)_r$. Since $f(a)_r = 0$ or has degree 0, that means it is indeed the remainder of division of $f(x)$ by $(x - a)$ on the right, as we desire. □

We will generally take $\delta \equiv 0$, and since we operate with $K = \mathbb{F}_{q^m}$, a finite field, $\sigma$ must be an automorphism. We in fact take $\sigma$ to be the Frobenius automorphism.

That is, for any $a \in K$, $\sigma(a) = a^q$. Combined with the above, we see that

$$\begin{aligned} N_0(a) &= 1 \\ N_{i+1}(a) &= N_i(a)^q a, \end{aligned}$$

and this allows us to solve the recursion as $N_i(a) = a^{\frac{q^i-1}{q-1}}$. We use the notation $[\![i]\!] = \frac{q^i-1}{q-1}$ to write this more compactly as $N_i(a) = a^{[\![i]\!]}$. Then we can compactly write

$$f(a)_r = \sum_{i=0}^{n} b_i a^{[\![i]\!]}.$$

## 2.4 Evaluation of Products

Much as simply replacing $x$ with $a$ does not necessarily result in the proper evaluation of a skew polynomial, if we have $h(x) = f(x)g(x)$, it is not necessarily the case that $h(a)_r = f(a)_r g(a)_r$. We thus seek a formula that can be used for the evaluation of products of polynomials. As in [4], we first define, for any element $a \in K$ and any other element $c \in K \setminus \{0\}$:

$$a^c = (\sigma(c)a + \delta(c))c^{-1}. \tag{2.4}$$

Then for any other $d \in K \setminus \{0\}$, we see that

$$\begin{aligned} (a^c)^d &= (\sigma(d)[\sigma(c)a + \delta(c)]c^{-1} + \delta(d))d^{-1} \\ &= (\sigma(d)[\sigma(c)a + \delta(c)]c^{-1} + \delta(d)cc^{-1})d^{-1} \\ &= (\sigma(d)\sigma(c)a + \sigma(d)\delta(c) + \delta(d)c)(dc)^{-1} \\ &= (\sigma(dc)a + \delta(dc))(dc)^{-1} \\ &= a^{dc}. \end{aligned}$$

We say that $a, b \in K$ are $(\sigma, \delta)$-conjugate if there is some $c \in K \setminus \{0\}$ such that $a^c = b$, and this is an equivalence relation on the elements of $K$, so it partitions $K$ into conjugacy classes of elements that are all $(\sigma, \delta)$-conjugate to each other.

Using this notion, we have the following:

**Theorem 2.4.** *If $h(x) = f(x)g(x)$ where $f(x), g(x) \in R$, then for any $a \in K$, if $g(a)_r = 0$, $h(a)_r = 0$, but if $g(a)_r \neq 0$, we have $h(a)_r = f(a^{g(a)_r})_r g(a)_r$.*

*Proof.* First, in the case $g(a)_r = 0$, we have $(x-a)|_r g(x)$, and since $g(x)|_r h(x)$, we also get $(x-a)|_r h(x)$ by transitivity of right divisibility, and thus $h(a)_r = 0$ as well. Otherwise, we take $c = g(a)_r$ and have that $c \neq 0$, so $c \in K \setminus \{0\}$, and if we let $b = a^c$, then we have

$$\begin{aligned}
(x-b)c &= xc - bc \\
&= \sigma(c)x + \delta(c) - a^c c \\
&= \sigma(c)x + \delta(c) - (\sigma(c)a + \delta(c))c^{-1}c \\
&= \sigma(c)x + \delta(c) - \sigma(c)a - \delta(c) \\
&= \sigma(c)(x-a).
\end{aligned}$$

If we then write that $g(x) = q_1(x)(x-a) + c$ and $f(x) = q_2(x)(x-b) + f(b)_r$, then because we may use this to write

$$\begin{aligned}
h(x) &= f(x)g(x) \\
&= f(x)q_1(x)(x-a) + f(x)c \\
&= f(x)q_1(x)(x-a) + q_2(x)(x-b)c + f(b)_r c \\
&= f(x)q_1(x)(x-a) + q_2(x)\sigma(c)(x-a) + f(b)_r c \\
&= [f(x)q_1(x) + q_2(x)\sigma(c)](x-a) + f(b)_r c,
\end{aligned}$$

the remainder of dividing $h(x)$ on the right by $(x-a)$ is $f(b)_r c = f(a^c)c = f(a^{g(a)})g(a)$, which means $h(a)_r = f(a^{g(a)})g(a)$. □

When we again consider the specific case that $K = \mathbb{F}_{q^m}$ with $\sigma(a) = a^q$ and $\delta \equiv 0$, then we have that

$$\begin{aligned} a^c &= (\sigma(c)a + \delta(c))c^{-1} \\ &= (c^q a + 0)c^{-1} \\ &= c^q a c^{-1} \\ &= a c^{q-1}. \end{aligned}$$

## 2.5 Factorization

We note here that in general, a skew polynomial ring $R$ is not a unique factorization ring. In fact, many different factorizations may be possible, as the following example shows

**Example 2.7.** We let $f(x) = x^4 + \alpha^{17}x^3 + \alpha^{16}x^2 + \alpha^9 x + \alpha^3$ and find that the following are all of the factorizations of $f(x)$ into monic irreducible factors:

$$\begin{gathered} (x+\alpha) \quad (x+\alpha^2) \quad (x^2+x+1) \\ (x+\alpha^{24}) \quad (x+\alpha^{10}) \quad (x^2+x+1) \\ (x+\alpha^{12}) \quad (x+\alpha^{22}) \quad (x^2+x+1) \\ (x+\alpha) \quad (x^2+\alpha^{20}x+\alpha^{18}) \quad (x+\alpha^{15}) \\ (x+\alpha^{24}) \quad (x^2+\alpha^{9}x+\alpha^{24}) \quad (x+\alpha^{17}) \\ (x+\alpha^{12}) \quad (x^2+\alpha^{26}x+\alpha^{2}) \quad (x+\alpha^{20}) \\ (x^2+\alpha^{19}x+\alpha^{13}) \quad (x+\alpha^{6}) \quad (x+\alpha^{15}) \\ (x^2+\alpha^{19}x+\alpha^{13}) \quad (x+\alpha^{4}) \quad (x+\alpha^{17}) \\ (x^2+\alpha^{19}x+\alpha^{13}) \quad (x+\alpha) \quad (x+\alpha^{20}) \end{gathered}$$

We note that in the example, each factorization has two factors of degree 1 and one of degree 2. This is not an accident. We introduce some terminology and a theorem from [6] to see why.

**Definition 2.8.** A polynomial $p(x) \in R$ that is monic and irreducible; that is, $p(x)$ has no monic factors other than 1 and $p(x)$, is said to be prime.

**Definition 2.9.** For any two polynomials $f(x), g(x) \in R$, $\mathrm{lclm}(f(x), g(x))$ is divisible by $g(x)$, and the polynomial $f'(x) = \mathrm{lclm}(f(x), g(x))/g(x)$ is called the transform of $f(x)$ by $g(x)$.

**Definition 2.10.** If $f(x), g(x) \in R$ are relatively prime ($\mathrm{gcrd}(f(x), g(x)) = 1$) and $f'(x)$ is the transform of $f(x)$ by $g(x)$, then $\deg(f'(x)) = \deg(f(x))$, and we say that $f'(x)$ is similar to $f(x)$.

With these definitions in place, we restate Theorem 1 from Chapter 2 of [6]:

**Theorem 2.5.** *Every monic polynomial has a representation as the product of prime factors. Two different decompositions of the same polynomial have the same number of prime factors and the factors are similar in pairs.*

This result is actually stronger than we need here, but in particular, since similar polynomials have the same degree and any two factorizations have terms that are similar in pairs, any two factorizations have terms that may be paired up which have the same degree, and so they must have the same number of factors with any given degree.

## 2.6 Closures

At this point, it is important to speak of the closure of a set of elements of $K$. First, we must define the left and right minimal polynomials of such a set.

**Definition 2.11.** The right minimal polynomial of a set $Z = \{a_1, a_2, \ldots, a_n\}$, with $a_i \in K$ for $i \in \{1, \ldots, n\}$ is the monic polynomial $\mu_{Z,r}(x) \in R$ of minimal degree such that $\mu_{Z,r}(a_i)_r = 0$ for all $i \in \{1, \ldots, n\}$. Similarly, the left minimal polynomial of $Z$ is the monic polynomial $\mu_{Z,l}(x) \in R$ of minimal degree such that $\mu_{Z,l}(a_i)_l = 0$ for all $i \in \{1, \ldots, n\}$.

We will see how to find such a polynomial in the next section. Now that the minimal polynomial has been defined, define the closure of a set of elements.

**Definition 2.12.** The right closure of $Z = \{a_1, a_2, \ldots, a_n\}$, denoted $\overline{Z}^r$, is the set of all $k \in K$ such that $\mu_{Z,r}(k)_r = 0$, and likewise the left closure, $\overline{Z}^l$ of $Z$ is the set of all $k \in K$ such that $\mu_{Z,l}(k)_l = 0$.

**Example 2.8.** If we continue to work in the same ring $R$ as before and consider the set $Z = \{\alpha^2, \alpha^3\}$, we find the polynomial $\mu_{Z,r}(x) = x^2 + \alpha^{15}x + \alpha^{25}$, and since the right roots of this polynomial are $\alpha^2$, $\alpha^3$, and $\alpha^{20}$, we have that $\overline{Z}^r = \{\alpha^2, \alpha^3, \alpha^{20}\}$. Since $Z \neq \overline{Z}^r$, we say that $Z$ is not closed on the right. We also find $\mu_{Z,l}(x) = x^2 + \alpha^{26}x + \alpha^{26}$, and the left roots of this polynomial are $\alpha^2$, $\alpha^3$, and $\alpha^{16}$, so $\overline{Z}^l = \{\alpha^2, \alpha^3, \alpha^{16}\}$. This also means $Z$ is not closed on the left.

As seen in the example, other than the elements of $Z$, there is no guarantee of other elements in $\overline{Z}^r$ being in $\overline{Z}^l$.

With these definitions in place, we may also define the independence of a set.

**Definition 2.13.** A set $Z = \{a_1, a_2, \ldots, a_n\}$ is called right independent if for any $i \in \{1, \ldots, n\}$, $\mu_{Z \setminus \{a_i\},r}(a_i)_r \neq 0$. Similarly, $Z$ is left independent if $\mu_{Z \setminus \{a_i\},l}(a_i)_l \neq 0$ for all $i \in \{1, \ldots, n\}$.

## 2.7 Interpolation

Using the formula for evaluation of products, we can interpolate polynomials with a given set of roots. Let $a_1, a_2, \ldots, a_n$ be elements of $K$. Let $f_1(x) = x - a_1$. Then clearly $f_1$ has only $a_1$ as a root, since $f_1(a_1)_r = 0$. Then for $2 \leq i \leq n$, we calculate $c_i = f_{i-1}(a_i)_r$. If $c_i = 0$, then we take $f_i(x) = f_{i-1}(x)$, but if $c_i \neq 0$, we take $f_i(x) = (x - a_i^{c_i})f_{i-1}(x) = (x - a_i c_i^{q-1})f_{i-1}(x)$. Since $(x - a_i^{c_i})$ evaluated at $a_i^{c_i}$ is 0, we have that $f_i(a_i)_r = 0$. By this construction, we will have that $f_i(x)$ has $a_1, a_2, \ldots, a_i$ as roots. This can be continued up to $i = n$ to construct the polynomial $f_n(x)$ with all of $a_1, \ldots, a_n$ as roots.

**Theorem 2.6.** *The polynomial $f_n(x)$ constructed above is the right minimal polynomial $\mu_{Z,r}(x)$ for $Z = \{a_1, a_2, \ldots, a_n\}$.*

*Proof.* We proceed by induction. First, if we take $Z_1 = \{a_1\}$, then $f_1(x) = (x - a_1)$ has degree 1. Any polynomial of degree 0 will be a constant, which when evaluated at $a_1$ will be nonzero. The zero polynomial is not monic, so the monic polynomial of minimal degree with $a_1$ as a root must have degree at least 1. Since $\deg(f_1(x)) = 1$, $f_1(x)$ is the minimal polynomial. We then assume that for some $1 \leq m < n$, $f_m(x)$ is the minimal polynomial of $Z_m = \{a_1, \ldots, a_m\}$, so $f_m(x) = \mu_{Z_m,r}(x)$. If $f_m(a_{m+1})_r = 0$, then by definition of $\mu_{Z_m,r}(x)$, no nonzero polynomial of lesser degree can have all of $Z_m$ as right roots, and so no lesser degree polynomial can have $Z_m \cup \{a_{m+1}\}$ as roots. Since $f_m(a_{m+1})_r = 0$, and $f_m(x) = \mu_{Z_m,r}(x)$ is monic, it therefore is the minimal polynomial of $Z_{m+1} = Z_m \cup \{a_{m+1}\}$. In this case we defined $f_{m+1}(x) = f_m(x)$, and so we indeed have $f_{m+1}(x) = \mu_{Z_{m+1},r}(x)$.

If we instead have $f_m(a_{m+1}) \neq 0$, then if we let $d = \deg(f_m)$, by our assumption, no polynomial of degree less than $d$ has all of $Z_m$ as right roots. If a polynomial $f_m'(x)$ of degree $d$ had all of $Z_{m+1}$ as right roots, then multiplying by the inverse of the leading coefficient will generate a monic polynomial with all of $Z_m$ as right roots (in addition to $a_{m+1}$). By the divisibility property of the minimal polynomial, this must be $\mu_{Z_m,r}(x) = f_m(x)$, but this contradicts $a_i$ not being a root of $f_m(x)$, and so no polynomial of degree $d$ has all of $Z_{m+1}$ as right roots. Since in this case $f_{m+1}(x)$ is of degree $d+1$ and has all of $Z_{m+1}$ as right roots, and is monic because it is a product of two monic polynomials, we must have that $f_{m+1}(x) = \mu_{Z_{m+1},r}(x)$. Thus, in either case $f_{m+1}(x) = \mu_{Z_{m+1},r}(x)$, and so by induction, $f_n(x) = \mu_{Z,r}(x)$. □

# Chapter 3

# Partial Results toward the GCLRD

Now that the necessary parts of the existing framework of skew polynomials have been laid out, it is possible to discuss the work that has been done specifically for this paper. In this chapter, unless indicated otherwise, we will assume that the field $K$ is finite, so $K = \mathbb{F}_{q^m}$ for some prime power $q$ and some integer $m \geq 1$. We further assume that $\sigma(a) = a^q$ for any $a \in K$ (this is the Frobenius automorphism), and that $\delta \equiv 0$. In this case we may write $R = \mathbb{F}_{q^m}[x;\sigma]$. Furthermore, we see that $\sigma^{-1}$ is is defined by $\sigma^{-1}(a) = a^{q^{m-1}}$.

## 3.1 Left Evaluation

We have previously defined right evaluation and left evaluation, and we have seen a formula for right evaluation. We wish to find a similar formula for left evaluation; that is, we wish to define some recursive formula for $M_i(a)$ such that we may write $f(a)_l = \sum_{i=0}^{n} b_i M_i(a)$ and have $f(a)_l$ be the remainder of dividing $f(x)$ on the left by $(x - a)$. Assuming that $\sigma$ is an automorphism, we may make use of $\sigma^{-1}$. In a natural similarity to the case for right evaluation, we have the following theorem.

**Theorem 3.1.** *We define recursively*

$$M_0(a) = 1$$
$$M_{i+1}(a) = a\sigma^{-1}(M_i(a)) - \delta(\sigma^{-1}(M_i(a)))$$

*for all $a \in K$ and $i \geq 1$. For any $a \in K$ and any polynomial $f(x) = \sum_{i=0}^n b_i x^i \in R$, we rewrite $f(x) = \sum_{i=0}^n x^i b_i' \in R$ and have $f(a)_l = \sum_{i=0}^n M_i(a) b_i'$.*

*Proof.* We wish to show that $(x-a)|_l(x^k - M_k(a))$ for all $k \geq 0$. Again, for $k = 0$, this is trivial, as $x^0 - M_0(a) = 1 - 1 = 0$, and $(x-a)|_l 0$. Then we again use induction, assuming that for some $k \geq 0$, we know that $(x-a)|_l(x^k - M_k(a))$. We then consider

$$\begin{aligned}
x^{k+1} - M_{k+1}(a) &= x^{k+1} - a\sigma^{-1}(M_k(a)) + \delta(\sigma^{-1}(M_k(a))) \\
&= x^{k+1} - a\sigma^{-1}(M_k(a)) + (x\sigma^{-1}(M_k(a))) \\
&\quad -x\sigma^{-1}(M_k(a))) + \delta(\sigma^{-1}(M_k(a))) \\
&= (x-a)\sigma^{-1}(M_k(a)) + x^{k+1} - [x\sigma^{-1}(M_k(a)) - \delta(\sigma^{-1}(M_k(a)))] \\
&= (x-a)\sigma^{-1}(M_k(a)) + x^{k+1} - [\sigma(\sigma^{-1}(M_k(a)))x \\
&\quad +\delta(\sigma^{-1}(M_k(a))) - \delta(\sigma^{-1}(M_k(a)))] \\
&= (x-a)\sigma^{-1}(M_k(a)) + (x^k - M_k(a))x.
\end{aligned}$$

From our induction hypothesis, $(x-a)|_l(t^k - M_k(a))$, and so both terms on the last line are divisible on the left by $(x-a)$, which means $(x-a)|_l(x^{k+1} - M_{k+1}(a))$, and by induction, $(x-a)|_l(x^k - M_k(a))$ for all $k \geq 0$. This means that if we rewrite $f(x)\sum_{i=0}^n b_i x^i$ as $f(x) = \sum_{i=0}^n x^i b_i'$ (which is possible since $\sigma$ is invertible), and let $f(a)_l = \sum_{i=0}^n M_i(a) b_i'$, we find that

$$f(x) - f(a)_l = \sum_{i=0}^n x^i b_i' - \sum_{i=0}^n M_i(a) b_i' = \sum_{i=0}^n (x^i - M_i(a)) b_i',$$

and applying what we just proved to each term of the sum as before, we find that $(x-a)|_l(f(x)-f(a)_l)$. This means we may write $f(x)-f(a)_l = (x-a)q_l(x)$, or $f(x) = (x-a)q_l(x)+f(a)_l$. Since $f(a)_l$ has degree 0, we know that $f(a)_l$ is thus the remainder of division of $f(x)$ by $(x-a)$ on the left, which is the property we desire of a left evaluator. □

### 3.1.1 Left Evaluation of Products and Interpolation

Just as we were able to find a formula for the evaluation of a product of two polynomials on the right, we can find a formula for the evaluation of a product on the left. For any $a \in K$ and any $c \in K \setminus \{0\}$, we can define

$$^{c}a = \sigma^{-1}(c)ac^{-1} = c^{q^{m-1}-1}a. \tag{3.1}$$

**Theorem 3.2.** *If $h(x) = f(x)g(x)$, then for any $a \in K$, if $f(a)_l = 0$, then $h(a)_l = 0$, but if $f(a)_l \neq 0$, we have $h(a)_l = f(a)_l g(^{f(a)_l}a)_l$. Moreover, if $Z = \{a_1, \ldots, a_n\} \subseteq K$, let $g_1(x) = x - a_1$, and for $2 \leq i \leq n$, calculate $d_i = g_{i-1}(a_i)_l$. If $d_i = 0$, take $g_i(x) = g_{i-1}(x)$, and take $g_i(x) = g_{i-1}(x)(x - {}^{d_i}a_i)$ otherwise. Then $g_n$ is the minimal polynomial of $Z$.*

The proof of these is analogous to the proof for right evaluation of products and right minimal polynomials.

### 3.1.2 Left Evaluation as Right Evaluation

We note that the structures of $f(a)_r$ and $f(a)_l$ are very similar, and so we attempt to write $f(a)_l$ as $g(a)_r$, for some polynomial $g(x)$ related to $f(x)$. This leads us to the following result.

**Theorem 3.3.** *Let $K$ be a field. If we define $\sigma' = \sigma^{-1}$ and $\delta' = -\delta \circ \sigma^{-1}$, then $R' = K[x; \sigma', \delta']$ is a skew polynomial ring, and for any polynomial $f(x) = \sum_{i=0}^{d} b_i x^i$ rewritten as $f(x) = \sum_{i=0}^{d} b_i x^i = \sum_{i=0}^{d} x^i b_i' \in R$ and any $a \in K$, $f(a)_l = f'(a)_r$, where $f'(x) \in R'$ is the polynomial $f'(x) = \sum_{i=0}^{d} b_i' x^i$.*

*Proof.* We see that $\sigma^{-1}$ is already an endomorphism of $K$. We then wish to show that $-\delta \circ \sigma^{-1}$ is a $\sigma^{-1}$-derivation. First, we need to show that it is an additive homomorphism of $K$. We find that

$$\begin{aligned} -\delta(\sigma^{-1}(a+b)) &= -\delta(\sigma^{-1}(a) + \sigma^{-1}(b)) \\ &= -\delta(\sigma^{-1}(a)) - \delta(\sigma^{-1}(b)) \end{aligned}$$

because $\sigma^{-1}$ is an automorphism and $\delta$ is a homomorphism. Thus, we find that $-\delta \circ \sigma^{-1}$ is an additive homomorphism of $K$. Next, we check

$$\begin{aligned} -\delta(\sigma^{-1}(ab)) &= -\delta(\sigma^{-1}(a)\sigma^{-1}(b)) \\ &= -\left[\sigma(\sigma^{-1}(a))\delta(\sigma^{-1}(b)) + \delta(\sigma^{-1}(a))\sigma^{-1}(b)\right]. \end{aligned}$$

Here, we run into a problem in that this doesn't appear to fit the general form of a $\sigma^{-1}$-derivation. However, since $K$ is not only a division ring but a field, and thus commutative, we get

$$\begin{aligned} -\delta(\sigma^{-1}(ba)) &= -\delta(\sigma^{-1}(ab)) \\ &= -\left[\sigma(\sigma^{-1}(a))\delta(\sigma^{-1}(b)) + \delta(\sigma^{-1}(a))\sigma^{-1}(b)\right] \\ &= -\left[\delta(\sigma^{-1}(b))a + \sigma^{-1}(b)\delta(\sigma^{-1}(a))\right] \\ &= \sigma^{-1}(b)(-\delta(\sigma^{-1}(a))) + (-\delta(\sigma^{-1}(b)))a. \end{aligned}$$

Thus, if we let $\sigma' = \sigma^{-1}$ and $\delta' = -\delta \circ \sigma^{-1}$, we have

$$\delta'(ba) = \sigma'(b)\delta'(a) + \delta'(b)a$$

for all $a, b \in K$, which means $\delta'$ is a $\sigma'$-derivation. We can then find that

$$\begin{aligned} M_0(a) &= 1 \\ M_{k+1}(a) &= a\sigma^{-1}(M_k(a)) - \delta(\sigma^{-1}(M_k(a))) \\ &= \sigma'(M_k(a))a + \delta'(M_k(a)), \end{aligned}$$

which we can see means $M_k(a) = N'_k(a)$, where $N'_k(a)$ is the function used in right-evaluation of polynomials in $R' = K[x; \sigma', \delta']$. We then furthermore note that we have

$$f(a)_l = \sum_{i=0}^{n} M_i(a)b'_i = \sum_{i=0}^{n} b'_i M_i(a) = \sum_{i=0}^{n} b'_i N'_i(a) = f'(a)_r$$

That is, left-evaluation of $f(x)$ at $a$ in $R$ is the right-evaluation of the polynomial $f'(x)$ at $a$ in $R'$, where $f'$ is the polynomial with left-coefficients equal to the right-coefficients of $f(x)$ when it is transformed to have only right-coefficients. □

## 3.2 The GCLRD

For any two polynomials $f(x)$ and $g(x)$ in $R$, we wish to define a polynomial divisor that is somehow the largest polynomial "between" $f(x)$ and $g(x)$. We define the set $H = \{h(x) \in R : h(x)|_r f(x) \text{ and } h(x)|_l g(x)\}$. The temptation is to define the greatest common left-right divisor (gclrd) as the polynomial $d(x) \in R$ such that

1. $d(x) \in H$

2. $\forall h(x) \in H$, $h(x)|_r d(x)$ and $h(x)|_l d(x)$,

so that the definition is similar to that of the gcrd and the gcld; that is, if $d'(x)|_r f(x)$ and $d'(x)|_l g(x)$, we have $d'(x)|_r d(x)$ and $d'(x)|_l d(x)$. However, an example shows why this definition is not appropriate.

**Example 3.1.** Continuing to work in the case case where $K = \mathbb{F}_{2^5}$, with $\alpha$ a primitive element of $K$ and $\sigma(a) = a^2$ for all $a \in K$, we let $f(x) = x^2 + \alpha^{11}x + \alpha^{19}$ and $g(x) = x^3 + \alpha^5 x^2 + \alpha^8 x + \alpha^{27}$. Then the polynomials in $H(f(x), g(x))$ of degree 2 are

$$x^2 + \alpha^{11}x + \alpha^{19}$$
$$\alpha^{26}x^2 + \alpha^6 x + \alpha^{14}$$
$$\alpha^{29}x^2 + \alpha^9 + \alpha^{17}.$$

Unfortunately, none of these is divisible by all of the other elements of $H$ on both sides, so none of these satisfy Property 2 from above. Any polynomial in $H$ of lesser degree is clearly not divisible by any of these three polynomials, and so there is no polynomial satisfying Properties 1 and 2.

We therefore use an alternate definition.

**Definition 3.1.** For any two polynomials $f(x), g(x) \in R$, let the set

$$H = \{h(x) \in R : h(x)|_r f(x) \text{ and } h(x)|_l g(x)\}.$$

A greatest common left-right divisor $d(x)$ of $f(x)$ and $g(x)$ is a polynomial such that $d(x) \in H$, and $\deg(d(x)) \geq \deg(h(x))$ for all $h(x) \in H$. We let $gclrd(f(x), g(x))$ be the set of all such polynomials.

We know that such polynomials exist because trivially $1|_r f(x)$ and $1|_l g(x)$, so $1 \in H$, which means $H$ is nonempty, and the degree of any polynomial in $H$ is at most

$\min\{\deg(f(x)), \deg(g(x))\}$. Thus, examining the set of the degrees of polynomials in $H$, we find that there is a maximum, and any polynomial in $H$ of that degree will satisfy the above definition.

### 3.2.1 Special Cases

There are some special cases where it is possible to give a nice formula for a polynomial sharing the roots of two polynomials. In this section, we assume $f(x), g(x) \in R$ are products of linear factors.

**Exactly Two Common Roots**

Here, we consider a polynomial which is an interpolation of two elements of $K$ which are right roots of $f(x)$ and left roots of $g(x)$.

**Theorem 3.4.** *Let*

$$Z = \{k \in K | f(k)_r = 0 \textit{ and } g(k)_l = 0\}.$$

*Then if* $|Z| = 2$*, and* $Z = \{a_1, a_2\}$ *is independent,*

$$(a_1 - a_2)^{q^2[\![r-1]\!]} \mu_{Z,r} \in H.$$

*Proof.* We have that

$$\mu_{Z,r}(x) = (x - \sigma(a_2 - a_1)a_2(a_2 - a_1)^{-1})(x - a_1)$$

by Theorem 2.6. We let $c = (a_1 - a_2)^{[\![r-1]\!]}$. In this way, $c^{q-1} = (a_1 - a_2)^{q^{m-1}-1}$.

We then see that

$$\begin{aligned}
\mu_{Z,l}(x)c &= (x-a_2)(x-\sigma^{-1}(a_1-a_2)a_1(a_1-a_2)^{-1})c \\
&= (x-a_2)(x-(a_1-a_2)^{q^{m-1}-1}a_1)c \\
&= (x-a_2)\sigma(c)(x-(a_1-a_2)^{q^{m-1}-1}a_1(\sigma(c))^{-1}c) \\
&= (x-a_2)\sigma(c)(x-(a_1-a_2)^{q^{m-1}-1}a_1c^{-(q-1)}) \\
&= (x-a_2)\sigma(c)(x-(a_1-a_2)^{q^{m-1}-1}a_1(a_1-a_2)^{-(q^{m-1}-1)}) \\
&= (x-a_2)\sigma(c)(x-a_1) \\
&= \sigma^2(c)(x-(\sigma^2(c))^{-1}a_2\sigma(c))(x-a_1) \\
&= c^{q^2}(x-(c^{q-1})^{-q}a_2)(x-a_1) \\
&= c^{q^2}(x-((a_1-a_2)^{q^{m-1}-1})^{-q}a_2)(x-a_1) \\
&= c^{q^2}(x-(a_1-a_2)^{-1}(a_1-a_2)^{q}a_2)(x-a_1) \\
&= c^{q^2}(x-(a_1-a_2)^{q-1}a_2)(x-a_1).
\end{aligned}$$

If $2|q$, then we have $a_1-a_2=-(a_1-a_2)=a_2-a_1$. If instead we have that $q$ is odd, then $q-1$ is even, so $(a_1-a_2)^{q-1}=(a_2-a_1)^{q-1}$. This means that the above gives us

$$\begin{aligned}
\mu_{Z,l}(x)c &= c^{q^2}(x-(a_2-a_1)^{q-1}a_2)(x-a_1) \\
&= c^{q^2}(x-\sigma(a_2-a_1)a_2(a_2-a_1)^{-1})(x-a_1) \\
&= (a_1-a_2)^{q^2\llbracket r-1\rrbracket}\mu_{Z,r}(x).
\end{aligned}$$

Since these interpolations are minimal polynomials, they are also the lclm's of the relevant linear factors, and by the divisibility property of the lclm, any right multiple of $\mu_{Z,l}(x)$ by a constant will divide $g(x)$ on the left, and any right multiple of $\mu_{Z,r}(x)$ by a constant will divide $f(x)$ on the right. Thus, this polynomial is in $H$. $\square$

Unfortunately, while this polynomial clearly has each element of $Z$ as both a left and a right root, this does not guarantee that it is the polynomial of greatest degree with this property. In turn, it is not guaranteed that it is the polynomial of largest degree in $H$. For instance, the following is a simple counterexample.

**Example 3.2.** If we let $f(x) = g(x) = x^3 + \alpha^{19}x^2 + \alpha^{14}x + 1$, then it is clear that $f(x)|_r f(x)$ and $f(x)|_l g(x)$, so $f(x) \in H$. Furthermore, it is clear that $f(x)$ has the highest possible degree of any polynomial in $H$, so $f(x) \in \mathrm{gclrd}(f(x), g(x))$. We can verify that $f(x)$ is the right interpolation of $\{\alpha^6, \alpha^{14}, \alpha^{18}\}$, so it is a product of linear factors, and

$$Z_r = \{\alpha^6, \alpha^7, \alpha^{14}, \alpha^{18}, \alpha^{24}, \alpha^{26}, \alpha^{29}\}.$$

Similarly, $g(x)$ is a left interpolation of $\{\alpha^6, \alpha^{14}, \alpha^{16}\}$, so it is a product of linear factors, and

$$Z_l = \{\alpha^6, \alpha^9, \alpha^{11}, \alpha^{12}, \alpha^{14}, \alpha^{16}, \alpha^{25}\}.$$

Thus, we find that $Z = Z_r \cap Z_l = \{\alpha^6, \alpha^{14}\}$, and so $m(x) = (a_1 - a_2)^{q^2[\![r-1]\!]}\mu_{Z,r} \in H$, but $\deg(m(x)) = 2 < 3$, so $m \notin \mathrm{gclrd}(f(x), g(x))$.

### Extensions of Degree Two

If we work in a field $K = \mathbb{F}_{q^m}$ where $m = 2$, then we have that $\sigma(a) = a^q$ for all $a \in K$, and also $\sigma^{-1}(a) = a^{q^{2-1}} = a^q = \sigma(a)$, and so $\sigma^{-1} = \sigma$. If we again consider $\delta \equiv 0$, this allows us to find the following result.

**Theorem 3.5.** *Again let*

$$Z = \{k \in K | f(k)_r = 0 \text{ and } g(k)_l = 0\}.$$

*If $R = \mathbb{F}_{q^2}[x;\sigma]$, then for any two polynomials $f(x), g(x) \in R$, $\mu_{Z,r}(x)|_r \,\mathrm{gcrd}(f(x), \overline{g}(x))$, where if $g(x) = \sum_{i=0}^{d} g_i x^i$, $\overline{g}(x) = \sum_{i=0}^{d} \sigma^i(g_i)x^i$.*

*Proof.* We note that as in Theorem 3.3, $g(a)_l = g'(a)_r$. Here, $g'(x) = \sum_{i=0}^{d} b'_i x^i$, where $g(x) = \sum_{i=0}^{d} b_i x^i = \sum_{i=0}^{d} x^i b'_i$. Since we have that $\delta \equiv 0$, we have that $x^i b'_i = \sigma^i(b'_i) x^i$, and so if $b'_i = \sigma^{-i}(b_i)$, we have $x^i b'_i = b_i x^i$. Since $\sigma^{-1} = \sigma$, we can also write $b'_i = \sigma^i(b_i)$. This means we have $g'(x) = \sum_{i=0}^{d} \sigma^i(b_i) x^i = \overline{g}(x)$. Further, we note that $\overline{g}(x) \in R'$, but $R' = K[x; \sigma^{-1}] = K[x; \sigma] = R$, so $\overline{g}(x) \in R$, and so we may consider $d(x) = \operatorname{gcrd}(f(x), \overline{g}(x))$.

Next, we see that since $g(a)_l = \overline{g}(a)_r$, the right roots of $\overline{g}(x)$ are precisely the left roots of $g(a)$. This means that right roots of $d(x)$ are right roots of $f(x)$ and right roots of $\overline{g}(x)$, and thus left roots of $g(x)$. This means that the right roots of $d(x)$ are in $Z$ by the definition of $Z$. Furthermore, note that any element $a \in Z$ is a right root of $f(x)$, so $(x-a)|_r f(x)$, and is a left root of $g(x)$, and thus a right root of $\overline{g}(x)$, so $(x-a)|_r \overline{g}(x)$. Together, this means that $(x-a)|_r \operatorname{gcrd}(f(x), \overline{g}(x))$. Since this is true for all $a \in Z$, we find that $\mu_{Z,r}(x)|_r \operatorname{gcrd}(f(x), \overline{g}(x))$ by the properties of $\mu_{Z,r}(x)$ being the lclm of all of the factors $(x-a)$. □

It is possible that $\operatorname{gcrd}(f(x), \overline{g}(x))$ has factors that are not in $\mu_{Z,r}(x)$, and so we do not necessarily have equality.

**Example 3.3.** If we consider $K = \mathbb{F}_{3^2} = \mathbb{F}_3[\alpha]/(\alpha^2 + 2\alpha + 2)$ such that $\alpha$ is a primitive element of $K$, with $\sigma(a) = a^3$ for all $a \in K$ and once again take $\delta \equiv 0$, then we consider $f(x), g(x) \in R = K[x; \sigma]$, where

$$f(x) = (x+1)(x+\alpha)(x+\alpha^2) = x^3 + \alpha^7 x + \alpha^3$$

and

$$g(x) = (x+\alpha^2)(x+2)(x+\alpha^5) = x^3 + \alpha^5 x + \alpha^3.$$

Clearly $f(x)$ and $g(x)$ are products of linear factors by definition. We then find that

$Z_r = Z_l = \{\alpha^5, \alpha^6\}$, and so $Z = \{\alpha^5, \alpha^6\}$. From this we can compute the minimal polynomial $\mu_{Z,r}(x) = x^2 + 2x + \alpha^3$. We also compute

$$\overline{g}(x) = \sigma^3(1)x^3 + \sigma(\alpha^5)x + \alpha^3 = x^3 + \alpha^7 x + \alpha^3 = f(x),$$

and so $\mathrm{gcrd}(f(x), \overline{g}(x)) = \mathrm{gcrd}(f(x), f(x)) = f(x)$, and we certainly have $\mu_{Z,r}(x)|_r f(x)$, because all right roots of $\mu_{Z,r}$ ar right roots of $f(x)$, but we also clearly do not have equality because the degrees do not match.

### 3.2.2 A Necessary Condition

At this point, we consider a set of elements that is left and right independent and wish to examine a condition that is necessary for some left multiple of right minimal polynomial of these elements to also be a right multiple of the left minimal polynomial. First, however, we note an important result of multiplying a polynomial by a constant on the left.

#### Modifications of Left Roots

Let us study the set of left roots of two polynomials when one is a constant multiple of the other.

**Theorem 3.6.** *If $L = \{a_1, \ldots, a_n\}$ is the set of left roots of $f(x)$, then for any nonzero $b \in K$, the set of left roots of $bf(x)$ is $L' = \{b(\sigma^{-1}(b))^{-1}a_1, \ldots, b(\sigma^{-1}(b))^{-1}a_n\}$.*

*Proof.* We start with $L = \{a_1, \ldots, a_n\}$ as the set of left roots of $f(x)$. This means, for any $i \in \{1, \ldots, n\}$, that $f(a_i)_l = 0$. This in turn means that $f(x) = (x - a_i)q_l(x)$ for some $q_l(x) \in R$.

We then have that

$$\begin{aligned} bf(x) &= b(x-a_i)q_l(x) \\ &= (x\sigma^{-1}(b) - ba_i)q_l(x) \\ &= (x - ba_i(\sigma^{-1}(b))^{-1})\sigma^{-1}(b)q_l(x), \end{aligned}$$

and since $(b(\sigma^{-1}(b))^{-1}a_i - ba_i(\sigma^{-1}(b))^{-1})) = 0$, we have that $bf(b(\sigma^{-1}(b))^{-1}a_i)_l = 0$, and so $b(\sigma^{-1}(b))^{-1}a_i$ is a left root of $bf(x)$. Since this is true for all $i \in \{1, \ldots, n\}$, we have that $L'$ as defined above contains left roots of $bf(x)$.

Now we must show that it is an extensive list. Consider any left root $k \in K$ of $bf(x)$. Then we have that $(x-k)|_l bf(x)$, so

$$\begin{aligned} bf(x) &= (x-k)q_l'(x) \\ &= (x-k)\sigma^{-1}(b)(\sigma^{-1}(b))^{-1}q_l'(x) \\ &= (bx - k\sigma^{-1}(b))(\sigma^{-1}(b))^{-1}q_l'(x) \\ &= b(x - b^{-1}k\sigma^{-1}(b))(\sigma^{-1}(b))^{-1}q_l'(x). \end{aligned}$$

Thus, we may write $f(x) = (x - b^{-1}k\sigma^{-1}(b))(\sigma^{-1}(b))^{-1}q_l'(x)$, so $b^{-1}k\sigma^{-1}(b)$ is a left root of $f(x)$, and thus $b^{-1}k\sigma^{-1}(b) = a_i$ for some $i \in \{1, \ldots, n\}$. Then we have that $k\sigma^{-1}(b) = ba_i$, and $k = b(\sigma^{-1}(b))^{-1}a_i \in L'$. This means that not only are all elements of $L'$ left roots of $bf(x)$, but all left roots of $bf(x)$ are elements of $L'$. Thus $L'$ is the set of left roots of $bf(x)$, as stated. □

### Left Multiple of Right Minimal Polynomial

We are interested in characterizing the polynomials in $\text{gclrd}(\mu_{Z,r}, \mu_{Z,l})$ when $Z = \{a_1, \ldots, a_n\}$. That is, we consider when the left multiple of a right minimal polynomial of a set is simultaneously a right multiple of the left minimal polynomial of the same set. In particular, we consider the set $Z$ to be independent on both sides.

**Theorem 3.7.** *Let $Z = \{a_1, \dots, a_n\} \subset K$ be a set of elements that is left independent and right independent. Then if*

$$b\mu_{Z,r}(x) = \mu_{Z,l}(x)c$$

*for some $b, c \in K$, $b$ must be a solution to*

$$b^{-1}\sigma^{-n}(b) = \prod_{i=2}^{n} \frac{f_{i-1}(a_i)_r^{q-1}}{g_{i-1}(a_i)_l^{q^{m-1}-1}},$$

*and $c = \sigma^{-n}(b)$, where $f_i(x)$ and $g_i(x)$ are as defined in Section* 2.7*.*

*Proof.* Since the elements of $Z$ are left and right independent, when we interpolate $\mu_{Z,r}(x)$ and $\mu_{Z,l}(x)$, we start with $f_1(x) = (x - a_1)$ and $g_1(x) = (x - a_1)$, and have, for $1 < i \leq n$,

$$\begin{aligned} f_i(x) &= (x - \sigma(f_{i-1}(a_i)_r)a_i f_{i-1}(a_i)_r^{-1})f_{i-1}(x) \\ g_i(x) &= g_{i-1}(x)(x - \sigma^{-1}(g_{i-1}(a_i)_l)a_i g_{i-1}(a_i)_l^{-1}). \end{aligned}$$

Then we have $\mu_{Z_r}(x) = f_n(x)$ and $\mu_{Z,l}(x) = g_n(x)$ and consider the constant terms of both $f_n(x)$ and $g_n(x)$. Specifically we let $f_i(x) = \sum_{j=0}^{i} b_{i,j}x^j$ and $g_i(x) = \sum_{j=0}^{i} c_{i,j}x^i$, and then we let $d_i = \frac{b_{i,0}}{c_{i,0}}$.

For $i = 1$, it is clear that $b_{1,0} = -a_1 = c_{1,0}$, and so $d_i = 1$. Then we examine an arbitrary $i > 1$. We see that

$$\begin{aligned} b_{i,0} &= \sigma(f_{i-1}(a_i)_r)a_i f_{i-1}(a_i)_r^{-1} b_{i-1,0} \\ &= f_{i-1}(a_i)_r^q a_i f_{i-1}(a_i)_r^{-1} b_{i-1,0} \\ &= f_{i-1}(a_i)_r^{q-1} a_i b_{i-1,0} \end{aligned}$$

and

$$\begin{aligned}c_{i,0} &= \sigma^{-1}(g_{i-1}(a_i)_l)a_i g_{i-1}(a_i)_l^{-1}c_{i-1,0}\\ &= g_{i-1}(a_i)_l^{q^{m-1}}a_i g_{i-1}(a_i)_l^{-1}c_{i-1,0}\\ &= g_{i-1}(a_i)_l^{q^{m-1}-1}a_i c_{i-1,0},\end{aligned}$$

so we have that

$$\begin{aligned}d_i &= \frac{b_{i,0}}{c_{i,0}}\\ &= \frac{f_{i-1}(a_i)_r^{q-1}a_i b_{i-1,0}}{g_{i-1}(a_i)_l^{q^{m-1}-1}a_i c_{i-1,0}}\\ &= \frac{f_{i-1}(a_i)_r^{q-1}}{g_{i-1}(a_i)_l^{q^{m-1}-1}}d_{i-1}.\end{aligned}$$

This means that $d_i = \frac{f_{i-1}(a_i)_r^{q-1}}{g_{i-1}(a_i)_l^{q^{m-1}-1}}d_{i-1}$, and following this recursive formula, we get that

$$d_n = \prod_{i=2}^{n}\frac{f_{i-1}(a_i)_r^{q-1}}{g_{i-1}(a_i)_l^{q^{m-1}-1}}.$$

Then we note that if $b\mu_{Z,r} = \mu_{Z,l}c$, then $bf_n(x) = g_n(x)c$, and by comparing the coefficients of $x^n$, we must have $c = \sigma^{-n}(b)$. Then comparing the constant coefficients, we have that $bb_{n,0} = c_{n,0}\sigma^{-n}(b)$, so $\frac{b_{n,0}}{c_{n,0}} = b^{-1}\sigma^{-n}(b)$, or $b^{-1}\sigma^{-n}(b) = d_n$ and so $b$ must be a solution to

$$b^{-1}\sigma^{-n}(b) = \prod_{i=2}^{n}\frac{f_{i-1}(a_i)_r^{q-1}}{g_{i-1}(a_i)_l^{q^{m-1}-1}}.$$

□

If $b$ is a solution to this equality, then we have $b\mu_{Z,r}(x) \in \text{gclrd}(\mu_{Z,r}(x), \mu_{Z,l}(x))$, and so this characterizes a special case of the gclrd.

# Chapter 4

# Implementation

To help formulate and test new hypotheses, several algorithms were implemented to ease computation with skew polynomials. Since the MAGMA language is designed to work with algebraic structures already, it was chosen to minimize the amount of work that had to be done from scratch. In particular, once the field $K$ is specified, all of the operations in the finite field are handled intuitively by MAGMA.

In MAGMA, the built-in definitions of polynomial rings either take multiplication to be commutative, or treat multivariate multiplication as non-commutative in the variables, but still commutative with respect to multiplication of variables and coefficients. This meant that simply specifying the rule for multiplication of $x \cdot a$ in a predefined polynomial ring structure was not possible. Additionally, there were problems with the order of function declaration that prevented easy overloading of predefined operators.

Thus, in order to represent skew polynomials, we interpreted them as maps applied to sequences of coefficients, as explained in Chapter 1, Section 2 of [5]; That is, we consider the ring $R = \oplus_{i=0}^{\infty} K$, where an element $\{a_i\}_{i=0}^{\infty}$ represents the polynomial $\sum_{i \in \mathbb{N} | a_i \neq 0} a_i x^i$ (this sum is possible because in the direct product, only finitely many terms of the sequence are nonzero). We then consider $x : R \to R$ defined by, for any $\{a_i\}_{i=0}^{\infty} \in R$,

$$(a_0, a_1, \dots) \mapsto (0, \sigma(a_0), \sigma(a_1), \dots);$$

that is, $x(\{a_i\}_{i=0}^{\infty}) = \{b_i\}_{i=0}^{\infty}$, with $b_0 = 0$ and $b_i = \sigma(a_{i-1})$ for $i \geq 1$. These are precisely the coefficients one obtains by multiplying a polynomial by $x$ on the left. Repeated multiplication by $x$ on the left is the same as repeated application of this map. This means that addition may be defined as normal for direct sums, and if we define multiplication in $R$ by converting the first sequence into a polynomial in $x$ and applying it to the second sequence, we find that $R$ is isomorphic to the ring $K[x; \sigma]$ used throughout the paper.

By using MAGMA's functions for working with mappings, this allowed skew polynomial operations to be defined in terms of operations with maps, and the actual map $x$ itself could be defined as part of setting up the skew polynomial ring, eliminating the function declaration problem.

Once this definition was in place, overloading the $*$ and $+$ operators allowed for natural expressions. However, MAGMA outputs the resulting skew polynomial as an abstract mapping from $\oplus_{i=0}^{\infty} K$ to $\oplus_{i=0}^{\infty} K$. To retrieve the coefficients, it is necessary to apply the mapping to the sequence $(1, 0, 0, \dots)$. That is, we multiply on the right by 1. With this translation between a mapping and a sequence of coefficients, it became possible to write algorithms that worked with the coefficients of polynomials without having to worry about specifying the rules for multiplying and adding polynomials (for these operations, polynomials are considered as maps and MAGMA handles the operations).

As in the proof of Lemma 2.1, polynomial division can be broken down into a process of polynomial long division. Starting with $f(x)$ of degree $n$ and $g(x)$ of degree

$m$, the coefficient $a_n\sigma^{n-m}(b_m^{-1})$ is calculated and given as the coefficient for $x^{n-m}$ in the quotient, and the process is continued with the difference $f(x)-a_n\sigma^{n-m}(b_m^{-1})x^{n-m}g(x)$ and so on until the degree of the difference is less than $m$. This algorithm returns the quotient and the remainder. Left division is done in the same manner. In turn, both of these are used to carry out the Euclidean algorithm to find the gcrd and gcld of any two polynomials. Left and right evaluation were implemented as the algorithms would indicate, with the simplification that $\delta \equiv 0$.

The following are the principal functions implemented:

```
OpMap(Coeff): PowSeqEnum -> mapping
```

Converts the sequence of coefficients Coeff into the corresponding operator map

```
[q, r] = rDiv(f, g): mapping,mapping -> mapping,mapping
```

Performs right division, returning operator maps $q$ and $r$ such that $f = qg + r$, with $r = 0$ or $r$ corresponding to a polynomial of lower degree than $g$.

```
[q, r] = lDiv(f, g): mapping,mapping -> mapping,mapping
```

Performs left division, returning operator maps $q$ and $r$ such that $f = gq + r$, with $r = 0$ or $r$ corresponding to a polynomial of lower degree than $g$.

```
rFac(f1, f2): mapping,mapping -> boolean
```

Returns true if $f_1(x)|_r f_2(x)$ and returns false otherwise. Relies on $rDiv$.

```
lFac(f1, f2): mapping,mapping -> boolean
```

Returns true if $f_1(x)|_l f_2(x)$ and returns false otherwise. Relies on $lDiv$.

`Oregcrd(f, g): mapping,mapping -> mapping`

Returns the map corresponding to $d_r(x) = \mathrm{gcrd}(f(x), g(x))$. Employs the standard Euclidean Algorithm.

`Orelclm(f, g): mapping,mapping -> mapping`

Returns the map corresponding to $m_l(x) = \mathrm{lclm}(f(x), g(x))$. Employs the formula elaborated in [3]

`H(f1,f2): mapping,mapping -> list of mappings`

Returns a list of mappings corresponding to the set $H$ of polynomials that divide $f_1(x)$ on the left and $f_2(x)$ on the right. This function currently makes use of brute force.

`reval(f,val): mapping, FinFldElt -> FinFldElt`

Returns the value $f(val)_r$.

`leval(f,val): mapping, FinFldElt -> FinFldElt`

Returns the value $f(val)_l$.

`rroots(f): mapping -> sequence of FinFldElts`

Returns the all $a \in K$ such that $f(a)_r = 0$. Uses brute force.

`lroots(f): mapping -> sequence of FinFldElts`

Returns the all $a \in K$ such that $f(a)_l = 0$. Uses brute force.

```
rinterp(roots): sequence of FinFldElts -> mapping
```

Returns minimal polynomial interpolated on the right from the elements given in the sequence roots.

```
linterp(roots): sequence of FinFldElts -> mapping
```

Returns minimal polynomial interpolated on the left from the elements given in the sequence roots.

Most of these currently make use of brute force techniques as they are sufficiently fast for the size of fields and polynomials being used in this research while also being simple enough to not require devoting extensive time to debugging. Since the fields in use are finite, it is possible to simply evaluate a polynomial at each element of the field to find an exhaustive list of all roots. Similarly, for $f(x)$ of degree $m$ and $g(x)$ of degree $n$, it is possible to form an exhaustive list of all polynomials $h(x)$ up to degree $\min\{m, n\}$ and test if $h(x)|_r f(x)$ and $h(x)|_l g(x)$, resulting in the set $H$.

# Chapter 5

# Conclusion

Here, we briefly review the results so far and consider paths for future work.

## 5.1 Review

With a skew polynomial ring $R = K[x; \sigma, \delta]$ for some field $K$, it is possible to perform right division, and thus the ring is right Euclidean and has the gcrd and lclm as analogues to the gcd and lcm in commutative polynomial rings. Additionally, if $\sigma$ is surjective, the ring is left Euclidean and so has the gcld and lcrm as analogous concepts for left division.

We may always evaluate polynomials and their products on the right, and if $\sigma$ is surjective, we may similarly evaluate polynomials and the products thereof on the left. Not only are skew polynomial rings not commutative, but factorizations are not necessarily unique. They are, however, identical up to similarity, and thus the degrees of factors must be the same.

A set of elements of the field $K$ can be used to define a minimal polynomial, and by examining the roots of such a polynomial, we may speak of the closure of the set of elements, and likewise speak of a set of elements being independent. This may always be done on the right, and as before, if $\sigma$ is surjective, it is also possible to speak of left closures and independence. Using a simple algorithm, we are able to interpolate polynomials to construct the minimal polynomial of given linear factors.

We find that with a modification of the formula for right evaluation and evaluation of products, we obtain the corresponding formulas for left evaluation, and that we are able to view left evaluation as right evaluation in a separate polynomial ring $R' = K[x; \sigma', \delta']$.

When considering a new coding methodology, we encounter the idea of the maximal factor "between" two polynomials. Several particular cases have been examined. When there are exactly two common roots, a polynomial can be found in $H$ which is maximal for a given property, but is demonstrably not always in the gclrd. In extensions of degree 2, $\sigma^{-1} = \sigma$, and so we are able to find a polynomial with guaranteed roots, but are not able to fully characterize this polynomial.

Finally, upon examining a set that is independent on both sides, it is possible to find a condition that is necessary for a left multiple of the minimal polynomial on the right to be a right multiple of the minimal polynomial on the left, and this ties into the gclrd of those two polynomials.

## 5.2 Further Work

Moving forward, there are a couple of key directions to examine. First, there are additional properties that might be proven about skew polynomials. For instance, not only must the degrees of any two factorizations match up to rearrangement, but the polynomial factors themselves must be similar. Examining this concept may generate new leads toward the gclrd.

With the main focus being the gclrd, it is possible that there is a unified way to compute the gclrd that will work regardless of the number of shared roots between the two polynomials or the degree of the field. For specifics, though, more work can be done to examine the two special cases. In particular, it may be possible to characterize when the minimal polynomial of the shared roots is in the gclrd, or when the polynomial found in an extension of degree 2 is not only divisible by the minimal polynomial of the shared roots, but is equal to it, and furthermore when it is in $H$ or the gclrd.

Finally, while the condition found for a set that is independent on both sides to have the minimal polynomials be multiples of each other is a necessary condition, there may be special cases where it is also sufficient. There is also the separate issue of determining precisely when a solution will exist. While some partial progress has been made to that end, there is still significant research to be done in that direction.

# Bibliography

[1] D. Boucher and F. Ulmer. Linear codes using skew polynomials with automorphisms and derivations. *Des. Codes and Cryptogr.*, 70(3):405–431, 2012.

[2] W. Geiselmann D. Boucher and F. Ulmer. Skew-cyclic codes. *AAECC*, 18(4):379–389, 2007.

[3] M. Giesbrecht. Factoring in skew-polynomial rings over finite fields. *J. Symbolic Computation*, 26(4):463–486, 1998.

[4] T.Y. Lam and A. Leroy. Vandermonde and wronskian matrices over division rings. *J. Algebra*, 119(4):308–336, 1988.

[5] H. Li. Basic structural tricks and examples. In *Noncommutative Gröbner bases and filtered-graded transfer*, page 10. Springer-Verlag, 2002.

[6] O. Ore. Theory of non-commutative polynomials. *Ann. Math.*, 34(3):480–508, 1933.