2016

On Skew-Constacyclic Codes

Neville Lyons Fogarty
University of Kentucky, neville.fogarty@gmail.com
Digital Object Identifier: http://dx.doi.org/10.13023/ETD.2016.169

STUDENT AGREEMENT:

I represent that my thesis or dissertation and abstract are my original work. Proper attribution has been given to all outside sources. I understand that I am solely responsible for obtaining any needed copyright permissions. I have obtained needed written permission statement(s) from the owner(s) of each third-party copyrighted matter to be included in my work, allowing electronic distribution (if such use is not permitted by the fair use doctrine) which will be submitted to UKnowledge as Additional File.

I hereby grant to The University of Kentucky and its agents the irrevocable, non-exclusive, and royalty-free license to archive and make accessible my work in whole or in part in all forms of media, now or hereafter known. I agree that the document mentioned above may be made available immediately for worldwide access unless an embargo applies.

I retain all other ownership rights to the copyright of my work. I also retain the right to use in future works (such as articles or books) all or part of my work. I understand that I am free to register the copyright to my work.

REVIEW, APPROVAL AND ACCEPTANCE

The document mentioned above has been reviewed and accepted by the student's advisor, on behalf of the advisory committee, and by the Director of Graduate Studies (DGS), on behalf of the program; we verify that this is the final, approved version of the student's thesis including all changes required by the advisory committee. The undersigned agree to abide by the statements above.

Neville Lyons Fogarty, Student

Dr. Heide Gluesing-Luerssen, Major Professor

Dr. Peter Perry, Director of Graduate Studies

On Skew-Constacyclic Codes

DISSERTATION

A dissertation submitted in partial
fulfillment of the requirements for
the degree of Doctor of Philosophy
in the College of Arts and Sciences
at the University of Kentucky

By
Neville Lyons Fogarty
Lexington, Kentucky

Director: Dr. Heide Gluesing-Luerssen, Professor of Mathematics
Lexington, Kentucky 2016

ABSTRACT OF DISSERTATION

On Skew-Constacyclic Codes

Cyclic codes are a well-known class of linear block codes with efficient decoding algorithms. In recent years they have been generalized to skew-constacyclic codes; such a generalization has previously been shown to be useful. We begin with a study of skew-polynomial rings so that we may examine these codes algebraically as quotient modules of non-commutative skew-polynomial rings. We introduce a skew-generalized circulant matrix to aid in examining skew-constacyclic codes, and we use it to recover a well-known result on the duals of skew-constacyclic codes from Boucher/Ulmer in 2011. We also motivate and define a notion of idempotent elements in these quotient modules. We are particularly concerned with the existence and uniqueness of idempotents that generate a given submodule; we generalize relevant results from previous work on skew-constacyclic codes by Gao/Shen/Fu in 2013 and well-known results from the classical case.

KEYWORDS: Linear block codes, skew-constacyclic codes, skew-polynomial rings, circulants, idempotents

Author's signature: Neville Lyons Fogarty

Date: May 5, 2016

On Skew-Constacyclic Codes

By
Neville Lyons Fogarty

Director of Dissertation: Dr. Heide Gluesing-Luerssen

Director of Graduate Studies: Dr. Peter Perry

Date: May 5, 2016

To beginnings and endings.
And to middles, the unsung heroes.

ACKNOWLEDGMENTS

First and foremost, I would like to thank my advisor, Dr. Heide Gluesing-Luerssen, for her inspiration and patience over the past five years. From the first day of algebra to today, words cannot express how grateful I am for your guidance. Thank you.

Thank you also to the other members of my committee: Drs. Gang Cao, David Leep, Uwe Nagel, and Ruriko Yoshida. You took the time to listen to my presentations and read early drafts of this dissertation. Thank you for your insightful comments and questions.

Goodness knows that I have reached beyond my dissertation committee for advice. Thank you, Drs. Ben Braun, Carl Lee, and Kate Ponto, for always having open doors and being willing to chat about teaching, searching for a job, and everything else I came up with (and always at the worst possible time).

I owe an immense debt to Sheri Rhine and Christine Levitt, both of whom possess encyclopedic knowledge of how to navigate every bureaucratic pitfall graduate school has set in my path. Thank you both for passing on what I image is only a tiny fraction of that knowledge to me.

Thank you to Andrew, Katherine, and Anne Sackman, for helping to keep me sane from afar through countless Skype sessions and games of Mario Kart. What a long, strange trip it's been.

And finally, my parents, Frank and "C" Fogarty, without whom I most assuredly not be where I am today: thank you for all of your love and support. I could not have made it through this without you.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1 Introduction

When we transmit data over a noisy channel (e.g., satellite) to a receiver, we run the risk of our data becoming corrupted. Fixing the channel is not typically an option, so instead we must make our data noise-proof. A naive method of doing this is simply sending the same data multiple times. However, the benefit of the redundancy created may be offset by the cost of sending a lengthy message more than once in full. Indeed in some cases, such as transmissions through space via satellite, sending a message more than once may be entirely impractical. When we encode data onto a compact disc, there is no opportunity for the disk drive to request that data be re-encoded. Instead, we want to choose a method of communicating the information that can preserve the information despite the pitfalls of the medium of data transference, whether they are thermal disturbances in space or fingerprints and scratches on a CD.

The study of algebraic coding theory is about balancing the added redundancy with its costs and finding new ways to efficiently encode and decode information. In 1948, Shannon [27] gave proof of the existence of codes that could be used to ensure the accuracy (up to a specified percentage) of decoded data. His proof, however, was not constructive; codes satisfying this condition were not provided.

In the time since, though, many codes have been developed that do demonstrate Shannon's result. Introduced by Prange in 1957 [26], *cyclic codes* are a particularly nice class of codes known to have nice error-correcting properties if suitably chosen. Cyclic codes correspond exactly to the ideals of the quotient ring $\mathbb{F}_q[x]/(x^n - 1)$. It is usually assumed that n and q are relatively prime; this guarantees that $x^n - 1$ has no repeated factors. It also guarantees that a cyclic code has a unique generating idempotent, which serves as the multiplicative identity in the code viewed as a ring. Cyclic codes also have an efficient decoding algorithm called the Meggitt decoder.

Cyclic codes have been studied extensively; recently, they have been generalized to the class of *skew-constacyclic* codes. Much of the initial work was done by Boucher/Ulmer et al. [3, 5, 7, 8, 11], as well as Abualrub et al. [1], Matsuoka [24], and Gao et al. [14]. We are motivated to study skew-constacyclic codes by discoveries of optimal codes in this class. For example, in [3] and [11], the authors present skew-constacyclic codes whose distance improves upon the largest distance that was known at that time for codes with the same parameters (q, n, k). (Here k gives the dimension of the code as a vector subspace.) Similarly, in [9], some self-dual skew-constacyclic

codes are found that have better distance than previously known self-dual codes with the same parameters. Thus we believe that skew-constacyclic codes are a rich field for further study.

This dissertation studies well-known results from the classical cyclic case to see which ones hold in the skew-constacyclic case. Chapters 2 and 3 lay the groundwork for understanding skew-constacyclic codes. Chapters 4 and 5 focus on dual codes of skew-constacyclic codes. Chapter 6 provides information on idempotents in skew-constacyclic codes.

In Chapter 2, we explore the *skew-polynomial ring*. This ring was introduced by Ore [25] in 1933. In general, a skew-polynomial ring, denoted $\mathbb{F}_q[x;\theta;\delta]$ features an automorphism θ and a θ-derivation δ, where θ and δ describe the relation between ax and xa for coefficients $a \in \mathbb{F}$. For our purposes, we assume that $\delta = 0$ throughout, and simply use the notation $\mathbb{F}[x;\theta]$ for the skew-polynomial ring, as is standard in the literature. We then define *(θ, a)-constacyclic codes* using the quotient module $\mathbb{F}_q[x;\theta]/^{\bullet}(x^n - a)$, paralleling the structure of cyclic codes. Each classical cyclic code corresponds to a divisor of $x^n - 1$; similarly, each (θ, a)-constacyclic code corresponds to a right divisor of $x^n - a$.

Because skew-polynomials do not necessarily have unique irreducible factorizations, a polynomial $x^n - a$ may have a considerable number of right divisors, thus leading to many skew-constacyclic codes. In addition, skew-constacyclic codes over finite fields have been used in other areas of coding theory, shift-register synthesis, and cryptography over recent years; see for example [2, 22, 28, 29, 30, 32].

Since skew-constacyclic codes correspond to right divisors of $x^n - a$, it is critical to understand how to factor $x^n - a$. In Chapter 3, we first discuss ways to manipulate factorizations of $x^n - a$ to obtain new factorizations of $x^n - a$ and of other polynomials of similar form. We will exploit these manipulations in Chapter 4. We also discuss techniques for finding factorizations of $x^n - a$ using a computer algebra system. We conclude this chapter with a generalization of polynomial roots to the skew-polynomial ring.

In Chapter 4, we introduce a *skew-generalized circulant* to describe (θ, a)-constacyclic codes. In the classical cyclic case, the *circulant* of a particular polynomial g is an $n \times n$ square matrix whose ith row contains the coefficients of the polynomial $x^i g$ modulo $(x^n - 1)$, for $i = 0, \ldots, n-1$. The rowspace of the circulant of a right divisor g of $x^n - 1$ gives the cyclic code corresponding to g. This circulant description of classical cyclic codes is well known, and circulants have been extensively studied (see, for instance, [23, p. 501]).

Similarly, our skew-generalized circulant of $g \in \mathcal{R}$ is an $n \times n$ square matrix whose ith row contains the *left* coefficients of the polynomial $x^i g$ modulo $^\bullet(x^n - a)$, for $i = 0, \ldots, n-1$. Skew-generalized circulants do not preserve every useful artifact of classical circulants. The product of two skew-generalized circulants is not necessarily a skew-generalized circulant, nor is the transpose of a skew-generalized circulant necessarily a skew-generalized circulant.

We show, however, that the skew-generalized circulant of a right divisor g of $x^n - a$ behaves particularly nicely. For example, a skew-generalized circulant of a left multiple of a right divisor of $x^n - a$ can be written as the product of two associated skew-generalized circulants. We will also show that if g is a right divisor of $x^n - a$, then the transpose of its skew-generalized circulant is again a skew-generalized circulant. In each of these cases, though, not all skew-generalized circulants are based on the modulus $^\bullet(x^n - a)$.

In [5], Boucher/Ulmer used dot product computations to characterize the dual of a skew-constacyclic code as another skew-constacyclic code. In Chapter 5, we use skew-generalized circulants to recover their results by using the structure of skew-polynomial rings. Using another skew-generalized circulant formula, we obtain anti-isomorphisms between the lattice of right divisors of $x^n - a$, the lattice of right divisors of $x^n - a^{-1}$, the lattice of skew-constacyclic codes in $\mathbb{F}^n$ and the lattice of dual codes.

In Chapter 6, we turn to idempotents. Recall that in a ring, we say that e is an *idempotent* if $e^2 = e$. In the case of the quotient ring $\mathbb{F}_q[x;\theta]/(x^n - 1)$, each idempotent e serves as a generator for some classical cyclic code, and we say that e is a *generating idempotent* of that code. When we want to create a classical cyclic code, factorizing $x^n - 1$ to find divisors can be difficult. On the other hand, idempotents can easily be found with the aid of cyclotomic cosets. Thus it is beneficial to understand generating idempotents for cyclic codes. Provided that n is relatively prime to the characteristic of the field $\mathbb{F}$, one can show that each cyclic code contains a unique generating idempotent. (See, for example, [18].)

The fact that $\mathbb{F}_q[x;\theta]$ is in general only a module and not a ring adds to the technicality for skew-constacyclic codes; we must redefine what it means to be idempotent. We generalize the notion of (generating) idempotents in the classical cyclic case to *(generating) idempotents modulo* $^\bullet(x^n - a)$. In [14], Gao/Shen/Fu laid groundwork for the existence of unique generating idempotents when $x^n - 1$ is central. We extend this to all central $x^n - a$, and concretely give the codes in $\mathbb{F}_q[x;\theta]/^\bullet(x^n - a)$ which are guaranteed to have unique central generating idempotents (along with those idempotents). Further, we give results on the existence of generating idem-

potents for general $x^n - a$ and provide generalizations of other well-known results from the classical cyclic case. For example, we will show that the intersection and sum of two (θ, a)-constacyclic codes are again (θ, a)-constacyclic codes, and we will decompose the vector space $\mathbb{F}_q^n$ into the direct sum of two (θ, a)-constacyclic codes.

Finally, we conclude we data on factorizations of $x^n - a$ over prime power fields of order up to 25. We use this data to provide evidence that there are easy-to-check criteria that characterize skew-constacyclic codes with generating idempotents. We also observe that there are in general a large number of skew-constacyclic codes, and a smaller (but non-trivial) number of nice codes with generating idempotents.

Chapter 2 Skew-Polynomial Rings and Left Quotient Modules

Skew-polynomial rings were introduced by Ore [25] in 1933. In this chapter, we define the skew-polynomial ring, denoted $\mathbb{F}[x;\theta]$, and give its relevant properties. We examine the left quotient module $\mathbb{F}_q[x;\theta]/^{\bullet}(x^n - a)$ and compare it and contrast it with the commutative $\mathbb{F}_q[x]/(x^n - 1)$. Special consideration is given toward the case where $x^n - a$ is central.

We use the quotient module $\mathbb{F}_q[x;\theta]/^{\bullet}(x^n - a)$ to define *(θ, a)-constacyclic codes*, paralleling the structure of cyclic codes. Each cyclic code corresponds to a divisor of $x^n - 1$; similarly, each (θ, a)-constacyclic code corresponds to a right divisor of $x^n - a$.

2.1 Properties of Skew-Polynomial Rings

Let $\mathbb{F}$ be a finite field and $\theta \in \mathrm{Aut}(\mathbb{F})$, that is, θ is an automorphism of $\mathbb{F}$. We consider the skew polynomial ring $\mathcal{R} := \mathbb{F}[x;\theta]$, which is defined as the set $\{\sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N}_0,\ a_i \in \mathbb{F}\}$ endowed with the usual addition, and where multiplication is given by

$$xa = \theta(a)x \text{ for all } a \in \mathbb{F}$$

together with the laws of associativity and distributivity. Then $\mathcal{R}$ is a ring with identity which is non-commutative unless $\theta = \mathrm{id}_{\mathbb{F}}$. Following Boucher/Ulmer [7], we call $\mathcal{R}$ a *skew-polynomial ring of automorphism type*. Despite the non-commutativity, the ring is very similar to ordinary polynomial rings over fields. Some well-known properties are summarized below. Note that the degree of a polynomial $f \in \mathcal{R}$, denoted by $\deg(f)$, does not depend on the side where we collect the coefficients of f since θ is an automorphism. We also define $\deg(0) = -\infty$. Then we have the usual degree formulas, and in particular $\mathcal{R}$ is a domain. It is easy to see that the center of $\mathcal{R}$ is given by

$$Z(\mathcal{R}) = \widehat{\mathbb{F}}[x^m], \quad \text{where } |\theta| = m, \tag{2.1.1}$$

and $\widehat{\mathbb{F}} := \mathrm{Fix}_{\mathbb{F}}(\theta)$ is the fixed field of θ.

Remark 2.1.1 ([25])**.** $\mathcal{R}$ is a left Euclidean domain and a right Euclidean domain. More precisely, we have the following.

(a) (Right division with remainder) For all $f, g \in \mathcal{R}$ with $g \neq 0$ there exist unique polynomials $s, r \in \mathcal{R}$ such that $f = sg + r$ and $\deg(r) < \deg(g)$. If $r = 0$, then g

is a *right divisor* of f, denoted by $g \,|_r\, f$.

(b) For any two polynomials $f_1,\ f_2 \in \mathcal{R}$, not both zero, there exists a unique monic polynomial $d \in \mathcal{R}$ such that $d \,|_r\, f_1,\ d \,|_r\, f_2$ and such that whenever $h \in \mathcal{R}$ satisfies $h \,|_r\, f_1$ and $h \,|_r\, f_2$ then $h \,|_r\, d$. The polynomial d is called the *greatest common right divisor* of f_1 and f_2, denoted by $\mathrm{gcrd}(f_1, f_2)$. It satisfies a *right Bézout identity*, that is,

$$d = uf_1 + vf_2 \quad \text{for some } u,\ v \in \mathcal{R}.$$

We may choose $u,\ v$ such that $\deg(u) < \deg(f_2)$ and, consequently, $\deg(v) < \deg(f_1)$; see [15, Sec. 2].

(c) For any two nonzero polynomials $f_1,\ f_2 \in \mathcal{R}$, there exists a unique monic polynomial $\ell \in \mathcal{R}$ such that $f_i \,|_r\, \ell$, $i = 1, 2$, and such that whenever $h \in \mathcal{R}$ satisfies $f_i \,|_r\, h$, $i = 1, 2$, then $\ell \,|_r\, h$. The polynomial ℓ is called the *least common left multiple* of f_1 and f_2, denoted by $\mathrm{lclm}(f_1, f_2)$. Moreover, we have $\ell = uf_1 = vf_2$ for some $u,\ v \in \mathcal{R}$ with $\deg(u) \leq \deg(f_2)$ and $\deg(v) \leq \deg(f_1)$; this follows from [25, Thm. 8 and Eq. (24)].

(d) For all nonzero $f_1,\ f_2 \in \mathcal{R}$

$$\deg(\mathrm{gcrd}(f_1, f_2)) + \deg(\mathrm{lclm}(f_1, f_2)) = \deg(f_1) + \deg(f_2).$$

Analogous statements hold true for the left hand side.

2.2 The Left Quotient Module

Let now $a \in \mathbb{F}^* := \mathbb{F}\backslash\{0\}$ and $n \in \mathbb{N}$. We will use the notation ${}^\bullet(f) = \mathcal{R}f$ to denote the principal left ideal generated by $f \in \mathcal{R}$. Similarly, we will use $(f)^\bullet = f\mathcal{R}$ to denote the principal right ideal generated by $f \in \mathcal{R}$. Throughout this paper we will be concerned with the quotient module

$$\mathcal{S}_a := \mathcal{R}/{}^\bullet(x^n - a).$$

Note that in general $\mathcal{S}_a$ is not a ring, but simply a left $\mathcal{R}$-module. This naturally induces a left $\mathbb{F}$-vector space structure as well.

The coset $f + \mathcal{R}(x^n - a)$ of $f \in \mathcal{R}$ will be denoted by $\overline{f}$. The left $\mathcal{R}$-module structure implies $t\,\overline{f} = \overline{tf}$ for any $t,\ f \in \mathcal{R}$. From right division with remainder it is clear that every coset in $\mathcal{S}_a$ has a unique representative of degree less than n.

Occasionally we will pay special attention to the case where $\mathcal{S}_a$ is a ring.

Remark 2.2.1. An element $f \in \mathcal{R}$ is called *two-sided* if ${}^\bullet(f) = (f)^\bullet$. In this case the left ideal ${}^\bullet(f)$ is even two-sided and thus $\mathcal{R}/{}^\bullet(f) = \mathcal{R}/(f)^\bullet$ is a ring. It is not hard to see [19, Thm. 1.1.22] that the two-sided elements of $\mathcal{R}$ are exactly the skew-polynomials of the form $cx^t f$, where $c \in \mathbb{F}$ and $t \in \mathbb{N}_0$, and f is in the center $Z(\mathcal{R})$. In particular, a polynomial of the form $x^n - a$, where $a \neq 0$, is two-sided if and only if it is central and this is the case if and only if $|\theta|$ divides n and $a \in \mathrm{Fix}_{\mathbb{F}}(\theta)$. Only in this case is the module $\mathcal{S}_a = \mathcal{R}/{}^\bullet(x^n - a)$ a ring.

Let us return to the general case. The module $\mathcal{S}_a$ is the skew-constacyclic analogue of the quotient ring $\mathbb{F}[x]/(x^n - 1)$ for cyclic codes or, more generally, of $\mathbb{F}[x]/(x^n - a)$ for constacyclic codes. We have the left $\mathbb{F}$-linear isomorphism

$$\mathfrak{p}_a : \mathbb{F}^n \longrightarrow \mathcal{S}_a,\ (c_0, \ldots, c_{n-1}) \longmapsto \overline{\sum_{i=0}^{n-1} c_i x^i}. \tag{2.2.1}$$

It is crucial that the coefficients c_i appear on the left of x, because only this turns $\mathfrak{p}_a$ into an isomorphism of (left) $\mathbb{F}$-vector spaces. This map will relate codes in $\mathbb{F}^n$ to submodules in $\mathcal{S}_a$. We set

$$\mathfrak{v}_a := {\mathfrak{p}_a}^{-1}. \tag{2.2.2}$$

The following facts about submodules of $\mathcal{S}_a$ are straightforward generalizations of the commutative case and are proven in exactly the same way (with the aid of Remark 2.1.1). Just as for left ideals, we use the notation ${}^\bullet(\overline{g})$ for the left submodule of $\mathcal{S}_a$ generated by $\overline{g}$.

Proposition 2.2.2. *Let $\mathcal{M}$ be a left submodule of $\mathcal{S}_a$.*

(1) Then $\mathcal{M} = {}^\bullet(\overline{g})$, where $g \in \mathcal{R}$ is the unique monic polynomial of smallest degree such that $\overline{g} \in \mathcal{M}$. Moreover,

(i) $g \,|_r\, f$ for any $f \in \mathcal{R}$ such that $\overline{f} \in \mathcal{M}$. In particular, $g \,|_r\, (x^n - a)$.

(ii) g is the unique monic right divisor of $x^n - a$ such that ${}^\bullet(\overline{g}) = \mathcal{M}$.

(2) Let $f \in \mathcal{R}$. Then ${}^\bullet(\overline{f}) = {}^\bullet(\overline{g})$, where $g = gcrd(f, x^n - a)$.

We mention in passing that in the central case (see Remark 2.2.1) the ring $\mathcal{S}_a$ is Frobenius. This is a trivial consequence of the fact that $\mathcal{S}_a$ is finite and by Proposition 2.2.2(1) a principal left ideal ring; see [17, Th. 1].

2.3 Constacyclic Codes

Let us return to the general case. The following is now immediate and forms a standard generalization of the classical case of cyclic codes; a short proof is added for completeness. We use the notation $\mathrm{im}\,(M)$ for the rowspace of a matrix M.

Corollary 2.3.1 (see also [7]). *Let $g \in \mathcal{R}$ be a right divisor of $x^n - a$, and let $\deg(g) = r$. Set $\mathcal{M} := {}^{\bullet}(\overline{g})$. Then $\mathcal{M}$ is a left $\mathbb{F}$-vector space of dimension $k := n - r$ with basis $\{\overline{g}, \overline{xg}, \ldots, \overline{x^{k-1}g}\}$. Writing $g = \sum_{i=0}^{r} g_i x^i$, we conclude*

$$\mathfrak{v}_a(\mathcal{M}) = im\,(M),$$

where

$$M = \begin{pmatrix} \mathfrak{v}_a(\overline{g}) \\ \mathfrak{v}_a(\overline{xg}) \\ \vdots \\ \mathfrak{v}_a(\overline{x^{k-1}g}) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_r & & & \\ & \theta(g_0) & \theta(g_1) & \cdots & \theta(g_r) & & \\ & & \ddots & \ddots & & \ddots & \\ & & & \theta^{k-1}(g_0) & \theta^{k-1}(g_1) & \cdots & \theta^{k-1}(g_r) \end{pmatrix} \in \mathbb{F}^{k\times n}. \tag{2.3.1}$$

Proof. Let $hg = x^n - a$. Consider $f\overline{g} \in \mathcal{M}$. Then $\overline{fg} = \overline{sg}$, where $s \in \mathcal{R}$ is the remainder upon right division of f by h. Thus $\deg(s) < \deg(h) = k$ and $\overline{sg}$ is in the span of $\{\overline{g}, \overline{xg}, \ldots, \overline{x^{k-1}g}\}$. Linear independence is clear from the matrix M. □

We close this chapter with the definition of (θ, a)-constacyclicity and an illustrating example. The definition is a special case of [7, Def. 1].

Definition 2.3.2. A subspace $\mathcal{C} \subseteq \mathbb{F}^n$ is called (θ, a)-*constacyclic* if $\mathfrak{p}_a(\mathcal{C})$ is a submodule of $\mathcal{S}_a$. The code $\mathcal{C} \subseteq \mathbb{F}^n$ is called *skew-constacyclic* if it is (θ, a)-constacyclic for some $\theta \in \mathrm{Aut}(\mathbb{F})$ and $a \in \mathbb{F}^*$. The code is called θ-*cyclic* if it is $(\theta, 1)$-*constacyclic*.

It is easy to see [5, Sec. 2] that a subspace $\mathcal{C} \subseteq \mathbb{F}^n$ is (θ, a)-constacyclic if and only if

$$(f_0, \ldots, f_{n-1}) \in \mathcal{C} \Longrightarrow (a\theta(f_{n-1}), \theta(f_0), \ldots, \theta(f_{n-2})) \in \mathcal{C}. \tag{2.3.2}$$

In particular, the $(\mathrm{id}, 1)$-constacyclic codes are exactly the classical cyclic codes.

From the previous results it is clear that any (θ, a)-constacyclic code has a generator matrix of the form M as in (2.3.1) for some $g = \sum_{i=0}^{r} g_i x^i$ and $\theta \in \mathrm{Aut}(\mathbb{F})$. As one can see, the matrix M does not depend on a. This raises the question when a code $\mathcal{C} = \mathrm{im}\, M$ with M as in (2.3.1) is skew-constacyclic and, if so, for which constant a.

This can easily be answered. Indeed, $\mathcal{C} = \operatorname{im} M$ is (θ, a)-constacyclic if and only if $g \,|_r\, (x^n - a)$. The if-part is clear from Corollary 2.3.1, and for the only-if-part one notices that g is, up to a constant factor, the unique non-zero polynomial of smallest degree in $\mathfrak{p}_a(\mathcal{C})$. Thus $g \,|_r\, (x^n - a)$ by Proposition 2.2.2(1). In this context it is also worthwhile to note that if $\{0\} \subsetneq \mathcal{C} \subsetneq \mathbb{F}^n$, the constant a is unique because distinct polynomials $x^n - a$ and $x^n - b$ have no common non-constant right divisors. In other words, if $a \neq b$ then the images $\mathfrak{p}_a(\mathcal{C})$ and $\mathfrak{p}_b(\mathcal{C})$ of a nontrivial subspace $\{0\} \subsetneq \mathcal{C} \subsetneq \mathbb{F}^n$ cannot both be submodules in $\mathcal{S}_a$ and $\mathcal{S}_b$.

Proposition 2.2.2 tells us that, as in the classical commutative case, the (θ, a)-constacyclic codes in $\mathbb{F}^n$ are in bijection with the distinct monic right divisors of $x^n - a$. However, as is well known, skew-polynomials do not factor uniquely into irreducible polynomials (but see also [25, Thm. 1, Page 494]), which often results in a large number of right divisors. We provide the following small example, which will be used again in later sections.

Example 2.3.3. Consider the field $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, where $\alpha^3 = \alpha + 1$, and let θ be the Frobenius homomorphism on $\mathbb{F}_8$, thus $\theta(c) = c^2$ for all $c \in \mathbb{F}_8$. Let $f := x^7 + \alpha$. With the aid of an exhaustive search one finds that f has the monic right divisors

$$
\begin{aligned}
&g^{(0)} = 1, \quad g^{(1)} = x + \alpha, \quad g^{(2)} = x^3 + \alpha^4 x^2 + 1, \quad g^{(3)} = x^3 + \alpha^6 x + 1,\\
&g^{(4)} = x^4 + \alpha x^3 + \alpha^5 x^2 + \alpha, \quad g^{(5)} = x^4 + \alpha^5 x^2 + x + \alpha,\\
&g^{(6)} = x^6 + \alpha^4 x^5 + \alpha^6 x^4 + x^3 + \alpha^4 x^2 + \alpha^6 x + 1, \quad g^{(7)} = x^7 + \alpha.
\end{aligned}
$$

The polynomials $g^{(2)}$, $g^{(3)}$, $g^{(6)}$ are not left divisors of $x^7 + \alpha$, while all others are. Moreover, we have the lattice shown in Figure 2.1 with respect to right division, which in turn provides us with the lattice of the (θ, α)-constacyclic codes $\mathcal{C}^{(i)} := \mathfrak{v}_a\big({}^{\bullet}(\overline{g^{(i)}})\big)$ in $\mathbb{F}_8^7$ with respect to inclusion.

This means, for instance, that $g^{(1)}$ is a right divisor of $g^{(5)}$ and thus $\mathcal{C}^{(5)} \subseteq \mathcal{C}^{(1)}$. The latter implies that $(\mathcal{C}^{(1)})^{\perp} \subseteq (\mathcal{C}^{(5)})^{\perp}$. The lattice of right divisors (in a suitable skew polynomial ring) corresponding to the dual codes will be provided in Section 5.2.

It is worth noting that the codes generated by $g^{(2)}$, $g^{(3)}$, $g^{(4)}$, $g^{(5)}$ are near-MDS (but not MDS), that is, both the code and its dual have defect 1 (recall that the defect of a code is the difference between the Singleton bound and the distance of the code). The codes generated by $g^{(1)}$ and $g^{(6)}$ are trivial MDS codes.

Of course, as in the classical commutative case, general skew-constacyclic codes are not MDS or otherwise optimal. In fact, as has been observed already by Boucher/Ul-

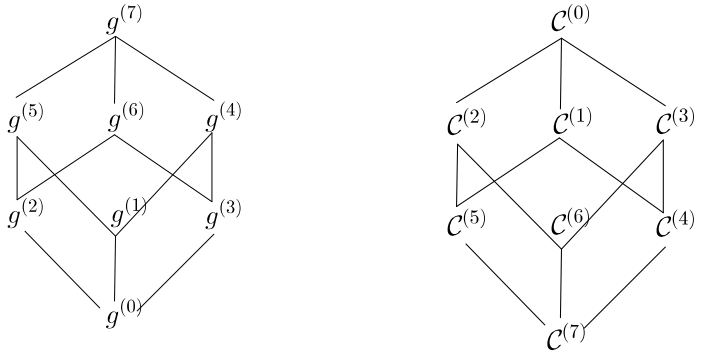

Figure 2.1: Lattice of monic right divisors of $x^7 + \alpha$ and the corresponding codes

mer [8, Tables 1 – 3], for many choices of n there are no skew-constacyclic codes of length n that have the best possible distance among all codes with the same parameters (q, n, k). But at the same time there are plenty of parameters for which skew-constacyclicity leads to the best codes known. Tables can be found in [3, 11].

Chapter 3 Factorizations of $x^n - a$

In the previous chapter, we defined the left quotient module $\mathbb{F}_q[x;\theta]/^\bullet(x^n - a)$ and looked at its submodules. Again in this chapter, we consider the skew-polynomial ring $\mathcal{R} := \mathbb{F}[x;\theta]$ for some fixed $\theta \in \mathrm{Aut}(\mathbb{F})$. We will explore factorizations of $x^n - a$, which in turn gives us characterizations of those submodules using right divisors. In the first section of this chapter, we will manipulate these factorizations to obtain new factorizations, allowing us to relate skew-polynomials that will play critical roles in future chapters. In the second section, we will explore techniques for efficiently factorizing $x^n - a$ using a computer algebra system and discuss the existence of right roots and linear factors of $x^n - a$.

3.1 Manipulating Factorizations of $x^n - a$

In this section we study factorizations of the form $x^n - a = hg$ in $\mathcal{R}$. They give rise to an abundance of further factorizations and lead to various identities for the coefficients of h and g. In order to derive these results we need the following maps.

The natural extension of θ to $\mathcal{R}$ will be denoted by θ as well, thus

$$\theta : \mathcal{R} \longrightarrow \mathcal{R}, \quad \sum_{i=0}^{r} f_i x^i \longmapsto \sum_{i=0}^{r} \theta(f_i) x^i. \tag{3.1.1}$$

As a consequence,

$$xf = \theta(f)x \text{ for all } f \in \mathcal{R}. \tag{3.1.2}$$

In addition, on the ring of skew-Laurent polynomials $\mathbb{F}[x, x^{-1};\theta]$ we consider the map

$$\varphi : \mathbb{F}[x, x^{-1};\theta] \longrightarrow \mathbb{F}[x, x^{-1};\theta], \quad \sum_{i=m}^{n} a_i x^i \longmapsto \sum_{i=m}^{n} x^{-i} a_i. \tag{3.1.3}$$

It gives rise to two reciprocal polynomials, a *left reciprocal* ρ_l and a *right reciprocal* ρ_r, defined as follows:

$$\rho_l : \mathcal{R} \longrightarrow \mathcal{R}, \quad f \longmapsto x^{\deg f}\varphi(f) \text{ and } \rho_r : \mathcal{R} \longrightarrow \mathcal{R}, \quad f \longmapsto \varphi(f)x^{\deg f}. \tag{3.1.4}$$

Explicitly these maps are given by

$$\rho_l\Big(\sum_{i=0}^{t} f_i x^i\Big) = \sum_{i=0}^{t} x^{t-i} f_i = \sum_{i=0}^{t} \theta^i(f_{t-i}) x^i \quad \text{and} \quad \rho_r\Big(\sum_{i=0}^{t} f_i x^i\Big) = \sum_{i=0}^{t} \theta^{i-t}(f_{t-i}) x^i \tag{3.1.5}$$

where $f_t \neq 0$.

The following proposition summarizes the main properties of these maps. The anti-isomorphism in Part (b) appears also in [4, p. 282] for skew-polynomial rings over Galois rings, and the multiplicativity rule for the left reciprocal in Part (h) can also be found in [5, Def. 3, Lem. 1].

Proposition 3.1.1.

(a) θ *is a ring isomorphism of* $\mathcal{R}$.

(b) φ *is a ring anti-isomorphism:* $\varphi(f+f') = \varphi(f) + \varphi(f')$ *and* $\varphi(ff') = \varphi(f')\varphi(f)$ *for all* f, $f' \in \mathbb{F}[x, x^{-1}; \theta]$.

(c) $\rho_r|_{\mathbb{F}} = id_{\mathbb{F}} = \rho_l|_{\mathbb{F}}$.

(d) $\rho_l(f) = \theta^{\deg(f)}(\rho_r(f))$ *for all* $f \in \mathcal{R}$.

(e) $\theta \circ \rho_l = \rho_l \circ \theta$ *and* $\theta \circ \rho_r = \rho_r \circ \theta$.

(f) $\rho_l \circ \rho_l(f) = \theta^{\deg f}(f)$ *and* $\rho_r \circ \rho_r(f) = \theta^{-\deg f}(f)$ *for all* $f \in \mathcal{R}$.

(g) $\rho_r \circ \rho_l = \rho_l \circ \rho_r = id_{\mathcal{R}}$.

(h) $\rho_l(f_1 f_2) = \theta^{k_1}(\rho_l(f_2))\rho_l(f_1)$ *and* $\rho_r(f_1 f_2) = \rho_r(f_2)\theta^{-k_2}(\rho_r(f_1))$ *for all* f_1, $f_2 \in \mathcal{R}$ *and where* $k_i = \deg f_i$.

Proof. (a) and (c) are obvious. The additivity in (b) is clear, and for the multiplicativity it suffices to show that $\varphi(ax^m bx^n) = \varphi(bx^n)\varphi(ax^m)$, which can easily be verified. (d) and (e) are immediate from (3.1.5). For (f) we compute $\rho_l(\rho_l(\sum_{i=0}^t f_i x^i)) = \rho_l(\sum_{i=0}^t \theta^i(f_{t-i})x^i) = \sum_{i=0}^t \theta^i(\theta^{t-i}(f_i))x^i = \theta^t(f)$. Similarly, $\rho_r(\rho_r(\sum_{i=0}^t f_i x^i)) = \rho_r(\sum_{i=0}^t \theta^{i-t}(f_{t-i})x^i) = \sum_{i=0}^t \theta^{i-t}(\theta^{-i}(f_i))x^i = \theta^{-t}(f)$. (g) follows from (d), (e), and (f). For (h) we use (3.1.2) and the previous properties to compute $\rho_l(f_1 f_2) = x^{k_1+k_2}\varphi(f_1 f_2) = x^{k_1+k_2}\varphi(f_2)\varphi(f_1) = x^{k_2}\theta^{k_1}(\varphi(f_2))x^{k_1}\varphi(f_1) = \rho_l(\theta^{k_1}(f_2))\rho_l(f_1)$. The second identity follows from the first one using (d). □

Now we turn to an identity of the form $x^n - a = hg$ and derive various consequences. We introduce the notation

$$\gamma(a, g) := a g_0^{-1} \theta^n(g_0) \text{ for any right divisor } g \text{ of } x^n - a, \tag{3.1.6}$$

where g_0 is the constant coefficient of g. One may note that $\gamma(a,g)$ is the conjugate a^{g_0} in the skew-polynomial ring $\mathbb{F}[x;\theta^n]$ in the sense of [21, Eq. (2.5)].

Theorem 3.1.2 (see also [5, Lem. 2])**.** *Let $g=\sum_{i=0}^{n-k} g_i x^i$, $h=\sum_{i=0}^{k} h_i x^i \in \mathcal{R}$ such that $\deg(h)=k$ and $\deg(g)=n-k$, and let $a\in\mathbb{F}^*$. Define $c=\gamma(a,g)$. Then the following are equivalent.*
(1) $x^n-a=hg$,
(2) $x^n-c=\theta^n(g)h$,
(3) $x^n-\theta^{-n}(c)=g\theta^{-n}(h)$,
Furthermore, if any, hence all, of the above is true then

$$\theta^n(g)a=cg \quad \text{and} \quad a\theta^{-n}(h)=h\theta^{-n}(c). \tag{3.1.7}$$

Proof. (1) $\Rightarrow$ (2) Left-multiplying $x^n-a=hg$ with $\theta^n(g)$ and using $\theta^n(g)x^n=x^n g$, we obtain $(x^n-\theta^n(g)h)g=\theta^n(g)a$. This shows that g is a right divisor of $\theta^n(g)a$. Since both polynomials have the same degree we conclude $cg=\theta^n(g)a$ with c as in the theorem. Now we have $(x^n-\theta^n(g)h)g=cg$, and cancellation of g results in $x^n-c=\theta^n(g)h$, as desired.
(2) $\Rightarrow$ (3) follows by applying θ^{-n}.
(3) $\Rightarrow$ (1) follows from using the implication (1) $\Rightarrow$ (2) along with $g_0h_0=-a$.
It remains to show the identities in (3.1.7). The first one has been derived already in the first part of this proof. For the second one we right-multiply (1) by $\theta^{-n}(h)$ and compute $a\theta^{-n}(h)=x^n\theta^{-n}(h)-hg\theta^{-n}(h)=h(x^n-g\theta^{-n}(h))=h\theta^{-n}(c)$, where the last step follows from (3). □

In the next section, we will elaborate on how the search for all right factors of x^n-a (thus of all (θ,a)-constacyclic codes) can be aided by the above theorem. To do so, we will assume that g has constant term 1.

Definition 3.1.3. An element $f\in\mathcal{R}$ is called *constamonic* if it has constant term 1.

Remark 3.1.4. If g is constamonic, then $c=\gamma(a,g)=ag_0^{-1}\theta^n(g_0)=a1^{-1}\theta^n(1)=a$. In this case, $x^n-a=hg=\theta^n(g)h$.

Comparing left coefficients in the identities in (3.1.7) yields

Corollary 3.1.5. *Let $a\in\mathbb{F}^*$ and $g,\,h\in\mathcal{R}$ such that $x^n-a=hg$ and let $c=\gamma(a,g)$. Write $g=\sum_{i=0}^{n-k} g_i x^i$ and $h=\sum_{i=0}^{k} h_i x^i$. Then*

$$cg_t=\theta^t(a)\theta^n(g_t) \text{ and } a\theta^{-n}(h_t)=h_t\theta^{t-n}(c) \text{ for all } t\geq 0.$$

The following additional identities will be crucial in the next sections when turning to transpositions of circulants and duals of θ-constacyclic codes.

Corollary 3.1.6. *Let $a \in \mathbb{F}^*$ and g, $h \in \mathcal{R}$ such that $x^n - a = hg$ and let $c = \gamma(a, g)$. Define*

$$\widehat{h}^l := \rho_l(\theta^{-n}(h)) \quad \text{and} \quad \widehat{g}^r := \rho_r(\theta^n(g)).$$

Then
(a) $ga^{-1}h = c^{-1}(x^n - c)$,
(b) $-\theta^{k-n}(c^{-1})\theta^k(c^{-1})\widehat{h}^l a\widehat{g}^r = x^n - \theta^k(c^{-1})$,
(c) $-\widehat{g}^r\theta^{k-n}(c^{-1})\widehat{h}^l = x^n - a^{-1}$.

Proof. (a) Using (3.1.7) and (2) of Theorem 3.1.2 we compute $ga^{-1}h = c^{-1}\theta^n(g)h = c^{-1}(x^n - c)$.
(b) Applying ρ_l to (a) yields $-x^n + c^{-1} = \rho_l(ga^{-1}h) = \theta^{n-k}(\rho_l(a^{-1}h))\rho_l(g)$ by virtue of Proposition 3.1.1(h). Applying θ^k and using that $\theta^k(\rho_l(g)) = \rho_r(\theta^n(g)) = \widehat{g}^r$, we obtain $-\theta^n(\rho_l(a^{-1}h))\widehat{g}^r = x^n - \theta^k(c^{-1})$. Hence it remains to show that $\theta^{k-n}(c)\theta^k(c)\theta^n(\rho_l(a^{-1}h)) = \widehat{h}^l a$. First observe that $\theta^n(\rho_l(a^{-1}h)) = \rho_l(\theta^n(a^{-1}h)) = \rho_l(hc^{-1})$ due to (3.1.7). Using again Proposition 3.1.1(h) and once more (3.1.7) we derive $\theta^{k-n}(c)\theta^k(c)\rho_l(hc^{-1}) = \theta^{k-n}(c)\rho_l(h) = \rho_l(h\theta^{-n}(c)) = \rho_l(a\theta^{-n}(h)) = \widehat{h}^l a$, and this establishes (b).
(c) We apply ρ_l to Theorem 3.1.2(1) to obtain $-x^n a + 1 = \rho_l(hg) = \rho_l(\theta^k(g))\rho_l(h)$. Thus, $x^n - a^{-1} = -\widehat{g}^r\rho_l(h)a^{-1} = -\widehat{g}^r\rho_l(a^{-1}h)$. By (3.1.7) we have that $a^{-1}h = \theta^{-n}(h)\theta^{-n}(c^{-1})$, and thus $x^n - a^{-1} = -\widehat{g}^r\rho_l(\theta^{-n}(h)\theta^{-n}(c^{-1})) = -\widehat{g}^r\theta^{k-n}(c^{-1})\widehat{h}^l$, as desired. □

Remark 3.1.7. Let $a \in \mathbb{F}^*$ and g, $h \in \mathcal{R}$ such that $x^n - a = hg$ and let $c = \gamma(a, g)$. Suppose g and h are monic. Then $c = \theta^{n-k}(a)$, which follows from $t = n - k$ in Corollary 3.1.5. As a consequence, the constant $\theta^k(c^{-1})$ in Corollary 3.1.6(b) equals $\theta^n(a^{-1})$ and is thus independent of the choice of g, h and the degree k.

The rest of this section is devoted to a brief discussion of how to find all right divisors of the polynomials of the form $x^n - a$. For the general factorization problem in $\mathbb{F}[x;\theta]$ and fast algorithms we refer to [15, 10].

A major cost saver for finding all right divisors is obtained from Theorem 3.1.2. Indeed, note that if $g_0 = 1$ then $c = a$ and the implication (1) $\Rightarrow$ (2) of that theorem shows that the left divisor h of $x^n - a$ is also a right divisor. Thus, in order to determine all right divisors of $x^n - a$ it suffices to compute all right divisors, g, up to

degree $\lfloor n/2 \rfloor$ with constant term 1; the corresponding left factors, h, will then be the remaining right divisors with degree at least $\lfloor n/2 \rfloor$ (but in general not with constant term 1).

Next, we observe that $x^n - a = hg \iff x^n - ab\theta^n(b^{-1}) = \big(\theta^n(b^{-1})h\big)gb$ for any $a, b \in \mathbb{F}^*$. This is seen by right-multiplying $x^n - a = hg$ by b and left-multiplying by $\theta^n(b^{-1})$. Thus, the map $g \longmapsto gb$ provides us with a bijection between the right divisors of $x^n - a$ and those of $x^n - \hat{a}$, where $\hat{a} = ab\theta^n(b^{-1})$. Note that the map

$$\vartheta : \mathbb{F}^* \longrightarrow \mathbb{F}^*, \ b \longmapsto b\theta^n(b^{-1}) \tag{3.1.8}$$

is a group homomorphism with kernel $\widetilde{\mathbb{F}}^*$, where $\widetilde{\mathbb{F}} = \mathrm{Fix}_{\mathbb{F}}(\theta^n)$. As a consequence, by varying b we obtain for $\hat{a}$ all values in the coset $a(\mathrm{im}\,\vartheta)$ in $\mathbb{F}^*$. This coset is exactly the set of all conjugates of a in $\mathbb{F}[x;\theta^n]$ in the sense of [21]. All of this shows that factorizations of $x^n - a$ provide us easily with factorizations of $|\mathrm{im}\,\vartheta|$ distinct polynomials of the form $x^n - \hat{a}$.

We summarize as follows.

Proposition 3.1.8. *Let $a, b \in \mathbb{F}^*$ and set $\hat{a} := ab\theta^n(b^{-1})$. Let $g \in \mathcal{R}$. Then*

$$g \,|_r\, (x^n - a) \iff (gb) \,|_r\, (x^n - \hat{a}).$$

We will come back to this result in Theorem 4.2.4, where we also relate the corresponding skew-constacyclic codes.

In addition to this result, Corollary 3.1.6 may provide additional information about the right divisors because it relates those of $x^n - a$ to those of $x^n - a^{-1}$. We illustrate all of this by some examples.

Example 3.1.9. (1) Let $\mathrm{char}(\mathbb{F}) = 2$ and $\mathrm{Fix}_{\mathbb{F}}(\theta^n) = \mathbb{F}_2$. Then the map ϑ is surjective and thus the set of right divisors of any $x^n - a$ leads immediately to the set of all right divisors of $x^n - \hat{a}$ for any $\hat{a} \in \mathbb{F}^*$. This is for instance the case for any field $\mathbb{F}_{2^p}$, where p is prime, along with any non-trivial automorphism θ and any n such that $p \nmid n$.

(2) Let $\mathbb{F} = \mathbb{F}_{16}$ and θ be the Frobenius map. Let $n = 6$. Then $\mathrm{Fix}_{\mathbb{F}}(\theta^6) = \mathbb{F}_4$. Thus $\mathrm{im}\,(\vartheta)$ is the unique subgroup of $\mathbb{F}^*$ of order $|\mathbb{F}^*|/|\mathbb{F}_4^*| = 5$. Precisely, with α being a primitive element of $\mathbb{F}$ we have $\mathrm{im}\,\vartheta = \{1, \alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$, and the other two cosets are $\{\alpha, \alpha^4, \alpha^7, \alpha^{10}, \alpha^{13}\}$ and $\{\alpha^2, \alpha^5, \alpha^8, \alpha^{11}, \alpha^{14}\}$. One finds that $x^6 - 1$ has 35 distinct monic right divisors, and hence the same is true for $x^6 - \alpha^{3i}$ for $i = 1, \ldots, 4$. One also finds that the polynomial $x^6 - \alpha$ has no non-trivial right

divisors. Now we may also use Corollary 3.1.6 and conclude that also $x^6 - \alpha^{-1}$ has no non-trivial right divisors. Since $\alpha^{-1} = \alpha^{14}$, we conclude that $x^6 - a$, where a is any element in the last two cosets has no non-trivial right divisors.

(3) Let $\mathbb{F} = \mathbb{F}_9$ and θ be the Frobenius map. Let $n = 4$. Then $\theta^4 = \mathrm{id}$ and thus $\mathrm{im}\,(\vartheta) = \{1\}$. An exhaustive search shows that $x^4 - 2$ has 12 monic right divisors, whereas $x^4 - 1$ has 36 such divisors.

3.2 Finding Factorizations

To find factorizations $x^n - a = hg$, we can use a computer algebra system, such as Maple. Rather than exhaustively searching for all right divisors, we begin by listing all constamonic polynomials of degree at most $\lfloor \frac{n}{2} \rfloor$. (Recall from Def. 3.1.3 that a polynomial is constamonic if and only if its constant term is 1.) Using the computer algebra system, determine which of these polynomials are right divisors of $x^n - a = hg$. Each constamonic right divisor g of degree strictly less than $\lfloor \frac{n}{2} \rfloor$ corresponds to a right divisor of degree strictly greater than $\lfloor \frac{n}{2} \rfloor$. We can determine this high degree right divisor by using Thm. 3.1.2: since $g_0 = 1$, we have that $c = a$. Thus if $x^n - a = hg$, the left divisor h is also a right divisor of $x^n - a$. Note that the constant term of h is $-a$, so h is not necessarily constamonic. Thus if we are looking for all constamonic divisors of $x^n - a$, we should rescale our high degree right divisors by multiplying them by $-a^{-1}$ on the left. To obtain *all* right divisors of $x^n - a$, we must multiply our right divisors by all non-zero constants on the left. Note that rescaling by a constant on the left does not change the code generated by a right divisor.

We present some results on factorizing skew polynomials. First, we examine the case where $n = 2$.

Theorem 3.2.1. *Let $x^2 - a = hg = \tilde{h}\tilde{g} \in \mathbb{F}_q[x;\theta]$, where $g = g_1 x + 1$ and $\tilde{g} = \tilde{g}_1 x + 1$. Then $g\tilde{g} = \tilde{g}g$ if and only if $\tilde{g}_1 = \pm g_1$.*

Proof. ($\Longrightarrow$) Assume that $g\tilde{g} = \tilde{g}g$. We can multiply out either side to get $g\tilde{g} = (g_1 x + 1)(\tilde{g}_1 x + 1) = g_1\theta(\tilde{g}_1)x^2 + (g_1 + \tilde{g}_1)x + 1$ and $\tilde{g}g = (\tilde{g}_1 x + 1)(g_1 x + 1) = \tilde{g}_1\theta(g_1)x^2 + (\tilde{g}_1 + g_1)x + 1$. By comparing coefficients, we see that $g_1\theta(\tilde{g}_1) = \tilde{g}_1\theta(g_1)$, or $g_1\tilde{g}_1^{-1} = \theta(g_1\tilde{g}_1^{-1})$. We will return to this fact shortly.

We have factorizations of $x^n - a$ for some $h_1, \tilde{h}_1 \in \mathbb{F}_q^*$: $x^2 - a = (h_1 x - a)(g_1 x + 1) = h_1\theta(g_1)x^2 + (h_1 - ag_1)x - a$ and $x^2 - a = (\tilde{h}_1 x - a)(\tilde{g}_1 x + 1) = \tilde{h}_1\theta(\tilde{g}_1)x^2 + (\tilde{h}_1 - a\tilde{g}_1)x - a$. Again, by comparing coefficients, we see that $h_1\theta(g_1) = \tilde{h}_1\theta(g_1)$. We also have $h_1 =$

$g_1 a$ and $\tilde{h}_1 = \tilde{g}_1 a$. Making these substitutions, we obtain $g_1 a\theta(g_1) = \tilde{g}_1 a\theta(\tilde{g}_1)$, or $\theta(g_1\tilde{g}_1^{-1}) = \tilde{g}_1 g_1^{-1}$. Therefore $g_1\tilde{g}_1^{-1} = \theta(g_1\tilde{g}_1^{-1}) = \tilde{g}_1 g_1^{-1}$. Equivalently, $g_1^2 = \tilde{g}_1^2$, or $0 = g_1^2 - \tilde{g}_1^2 = (g_1 + \tilde{g}_1)(g_1 - \tilde{g}_1)$. The solutions to this equation are $g_1 = \pm\tilde{g}_1$, as a field has no zero divisors.

($\Longleftarrow$) If $g_1 = \tilde{g}_1$, then $g = \tilde{g}$, so clearly $g\tilde{g} = \tilde{g}g$. So suppose $g_1 = -\tilde{g}_1$. We compute $g\tilde{g}$ and $\tilde{g}g$: $g\tilde{g} = (g_1 x + 1)(-g_1 x + 1) = g_1\theta(-g_1)x^2 + 1 = -g_1\theta(g_1)x^2 + 1$ and $\tilde{g}g = (-g_1 x + a)(g_1 x + 1) = -g_1\theta(g_1)x^2 + 1$, so $g\tilde{g} = \tilde{g}g$, as desired. □

We know that in the standard polynomial ring $\mathbb{F}[x]$, every polynomial has a root in some extension, a fact which is key to factoring polynomials. It is not obvious that the same generalizes to skew polynomial rings, but it does in the following way.

Definition 3.2.2. Let $\mathbb{K}$ be an extension of $\mathbb{F}_q$. An element $\alpha \in \mathbb{K}$ is called a *right root* of $f \in \mathbb{F}[x;\theta]$ if $x - \alpha$ is a right divisor of $f \in \mathbb{K}[x;\theta]$.

Let $f = \sum_{i=0}^{n} f_i x^i \in \mathbb{F}_q[x;\theta = \mathrm{Frob}^r]$, and let $\mathbb{F}_q$ have characteristic p. We want to check if $(x - \alpha)$ is a right divisor of f for some α in an field extension $\mathbb{K}$ of $\mathbb{F}_q$. Thus we examine $f = g(x - \alpha) + s$, with $g \in \mathbb{K}[x;\theta]$ and $s \in \mathbb{K}$.

Notice that we can write $\theta^j(\alpha) = \alpha^{p^{rj}}$. Define

$$N_0(\alpha) := 1, \quad N_i(\alpha) := \alpha^{\sum_{j=0}^{i-1} p^{rj}} \text{ for } i \geq 1. \tag{3.2.1}$$

Observe that the product $\prod_{j=0}^{i-1} \theta^j(\alpha) = N_i(\alpha)$. Then one can easily show (as in [19, (1.3.10)]), that $s = \sum_{i=0}^{n} f_i N_i(\alpha)$. To that end, α is a right root of f if and only if $s = \sum_{i=0}^{n} f_i N_i(\alpha) = 0$.

Theorem 3.2.3. *Every skew polynomial $f \in \mathbb{F}_q[x;\theta]$ has a right root in some extension field.*

Proof. Let $f = \sum_{i=0}^{n} f_i x^i \in \mathbb{F}_q[x;\theta = \mathrm{Frob}^r]$ be given. Put $\tilde{f} := \sum_{i=0}^{n} f_i N_i(y) \in \mathbb{F}_q[y]$, the usual commutative ring. Then $\tilde{f}$ has a root α (in the commutative sense) in some (perhaps trivial) extension of $\mathbb{F}_q$. Then we have the equivalence: $\sum_{i=0}^{n} f_i N_i(\alpha) = 0 \Longleftrightarrow$ α is a right root of f. □

Using this theorem, we can easily find constamonic linear right divisors of $(x^n - a)$.

Corollary 3.2.4. *Let $x^n - a \in \mathbb{F}_q[x; \theta = Frob^r]$, where $\mathbb{F}_q$ has characteristic p. Then $(g_1 x + 1) \,|_r \, (x^n - a)$ if and only if $-g_1^{-1}$ is an Nth root of a, where $N = \sum_{i=0}^{n-1} p^{ri}$.*

Proof. Let $f = x^n - a$ and take $-g_1^{-1}$ as α in the equivalences in the proof of Theorem 3.2.3. Assume $(g_1 x + 1) \,|_r \, (x^n - a)$, or equivalently $(x + g_1^{-1}) \,|_r \, (x^n - a)$. By definition, this is equivalent to $-g_1^{-1}$ being a right root of $(x^n - a)$. Equivalently, by the proof of Theorem 3.2.3, $N_n(-g_1^{-1}) - a = 0$, hence $(-g_1^{-1})^N = a$. Thus $-g_1^{-1}$ is an Nth root of a. □

Chapter 4 Circulants

In the previous chapter, we explored ways to factor $x^n - a$. In this chapter, we begin by defining a *skew-generalized circulant* to describe (θ, a)-constacyclic codes. A skew-constacyclic code can be written as the row space of a circulant matrix. This generalizes the well-known circulant description of classical cyclic codes. We will show that our circulant is additive, and under certain conditions, it is multiplicative.

Special attention is paid to the circulant of a right divisor g of $x^n - a$, which behaves particularly nicely. For example, a circulant of a left multiple of a right divisor of $x^n - a$ can be written as the product of two associated skew-generalized circulants. Importantly, if g is a right divisor of $x^n - a$, then the transpose of its circulant is again a circulant, a fact that we will use in the next chapter.

4.1 Definition and Properties

In this section, we associate with each coset $\overline{f} \in \mathcal{S}_a = \mathcal{R}/^\bullet(x^n - a)$ a certain skew-generalized circulant matrix. This is a matrix in $\mathbb{F}^{n\times n}$ defined in such a way that its rows reflect the module structure in $\mathcal{S}_a$ and its row space is, up to the isomorphism $\mathfrak{p}_a$, the left submodule of $\mathcal{S}_a$ generated by $\overline{f}$. The situation becomes particularly nice when $x^n - a$ is central, in which case this circulant provides a ring embedding of $\mathcal{S}_a$ as a subring in $\mathbb{F}^{n\times n}$.

As before, let $\mathcal{R} = \mathbb{F}[x;\theta]$ and $\mathcal{S}_a = \mathcal{R}/^\bullet(x^n - a)$ for some fixed $a \in \mathbb{F}^*$. Recall the left $\mathbb{F}$-isomorphism $\mathfrak{p}_a$ and its inverse $\mathfrak{v}_a$ from (2.2.1) and (2.2.2). These maps give rise to the following type of circulant matrices. For the special (central) case where $\mathcal{S}_a = \mathcal{S}_1 = \mathbb{F}_{q^n}[x;\theta]/^\bullet(x^n - 1)$ with $\theta(x) = x^q$, these matrices also appear in the context of linearized polynomials and are known as Dickson matrices; see [31, p. 80]

Definition 4.1.1. The (θ, a)-*circulant* of the coset $\overline{f} \in \mathcal{S}_a$ is defined as

$$M_a^\theta(\overline{f}) := \begin{pmatrix} \mathfrak{v}_a(\overline{f}) \\ \mathfrak{v}_a(x\overline{f}) \\ \vdots \\ \mathfrak{v}_a(x^{n-2}\overline{f}) \\ \mathfrak{v}_a(x^{n-1}\overline{f}) \end{pmatrix} \in \mathbb{F}^{n\times n}. \tag{4.1.1}$$

Thus we have a map

$$M_a^\theta : \mathcal{S}_a \longrightarrow \mathbb{F}^{n\times n}, \quad \overline{f} \longmapsto M_a^\theta(\overline{f}).$$

A matrix in $\mathbb{F}^{n\times n}$ is called a *skew-generalized circulant* or simply a *circulant* if it is a (θ, a)-circulant for some $\theta \in \mathrm{Aut}(\mathbb{F})$ and $a \in \mathbb{F}^*$.

Explicitly, the circulant of $\overline{f}$ is given as follows. Without loss of generality assume $\deg(f) < n$ and thus $f = \sum_{i=0}^{n-1} f_i x^i$. For any $i \in \mathbb{N}_0$ and $\gamma \in \mathbb{F}$ we have $\overline{x\gamma x^i} = \overline{\theta(\gamma)x^{i+1}}$ and hence $\overline{x\gamma x^{n-1}} = \overline{\theta(\gamma)x^n} = \overline{\theta(\gamma)a}$. This leads to

$$M_a^\theta(\overline{f}) = \begin{pmatrix} f_0 & f_1 & f_2 & \dots & f_{n-2} & f_{n-1} \\ a\theta(f_{n-1}) & \theta(f_0) & \theta(f_1) & \dots & \theta(f_{n-3}) & \theta(f_{n-2}) \\ a\theta^2(f_{n-2}) & \theta(a)\theta^2(f_{n-1}) & \theta^2(f_0) & \dots & \theta^2(f_{n-4}) & \theta^2(f_{n-3}) \\ \vdots & \vdots & \ddots & & \vdots & \vdots \\ a\theta^{n-2}(f_2) & \theta(a)\theta^{n-2}(f_3) & \theta^2(a)\theta^{n-2}(f_4) & \dots & \theta^{n-2}(f_0) & \theta^{n-2}(f_1) \\ a\theta^{n-1}(f_1) & \theta(a)\theta^{n-1}(f_2) & \theta^2(a)\theta^{n-1}(f_3) & \dots & \theta^{n-2}(a)\theta^{n-1}(f_{n-1}) & \theta^{n-1}(f_0) \end{pmatrix}. \tag{4.1.2}$$

In other words, $M_a^\theta(\overline{f}) = (M_{ij})_{i,j=0,\dots,n-1}$, where

$$M_{ij} = \begin{cases} \theta^i(f_{j-i}), & \text{if } i \le j, \\ \theta^j(a)\theta^i(f_{n+j-i}), & \text{if } i > j. \end{cases} \tag{4.1.3}$$

For example,

$$M_a^\theta(\overline{x}) = \begin{pmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ a & & & & \end{pmatrix} \quad \text{and} \quad M_a^\theta(\overline{x^2}) = \begin{pmatrix} & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ a & & & & \\ & \theta(a) & & & \end{pmatrix}.$$

Remark 4.1.2. (a) The map M_a^θ is injective and additive, i.e.,

$$M_a^\theta(\overline{f} + \overline{f'}) = M_a^\theta(\overline{f}) + M_a^\theta(\overline{f'}) \text{ for all } f,\, f' \in \mathcal{R}.$$

(b) $M_a^\theta(c\overline{f}) = M_b^\theta(\overline{c})M_a^\theta(\overline{f})$ for all $c \in \mathbb{F}$ and $f \in \mathcal{R}$ and all $b \in \mathbb{F}^*$. This follows

directly from the definition along with the fact that

$$M_b^\theta(\overline{c}) = \begin{pmatrix} c & & & \\ & \theta(c) & & \\ & & \ddots & \\ & & & \theta^{n-1}(c) \end{pmatrix} \text{ for any } b \in \mathbb{F}^*. \tag{4.1.4}$$

As a consequence, M_a^θ is not $\mathbb{F}$-linear (unless $\theta = \mathrm{id}_\mathbb{F}$), but it is $\mathrm{Fix}_\mathbb{F}(\theta)$-linear.

(c) The map M_a^θ is not multiplicative, that is, $M_a^\theta(\overline{ff'}) \neq M_a^\theta(\overline{f})M_a^\theta(\overline{f'})$ in general. This simply reflects the fact that $\mathcal{S}_a$ is not a ring.

As a particular case of Part (c) above, we observe that the identity $hg = x^n - a$ does not imply $M_a^\theta(\overline{h})M_a^\theta(\overline{g}) = 0$. (For an example take the right divisor $g = x+\alpha^5$ of $x^5 - \alpha \in \mathbb{F}_8[x;\theta]$, where θ is the Frobenius homomorphism and $\alpha^3 + \alpha + 1 = 0$.) The situation becomes much nicer when $x^n - a$ is central, as we will see in Theorem 4.1.6. For the general case we will establish a certain product formula later in Theorem 4.2.3.

The next result shows that the row space of the circulant of $\overline{f}$ corresponds to the left submodule ${}^\bullet(\overline{f})$ under the isomorphism $\mathfrak{v}_a$.

Proposition 4.1.3. *We have*

$$\mathfrak{p}_a(uM_a^\theta(\overline{f})) = \mathfrak{p}_a(u)\overline{f} \text{ for all } u \in \mathbb{F}^n \text{ and } f \in \mathcal{R}.$$

As a consequence, $\mathrm{im}\, M_a^\theta(\overline{f}) = \mathfrak{v}_a({}^\bullet(\overline{f}))$.

Proof. Writing $u = (u_0, \ldots, u_{n-1})$, we can compute $uM_a^\theta(\overline{f}) = \sum_{i=0}^{n-1} u_i \mathfrak{v}_a(x^i\overline{f}) = \mathfrak{v}_a(\mathfrak{p}_a(u)\overline{f})$. This proves the first statement. The containment "$\subseteq$" of the second statement is an immediate consequence. As for "$\supseteq$" consider $\overline{hf} \in {}^\bullet(\overline{f})$ for some $h \in \mathcal{R}$. If we can show that $\overline{hf} = \overline{kf}$ for some $k \in \mathcal{R}$ with $\deg(k) < n$, then the first part yields $\mathfrak{v}_a(\overline{hf}) = \mathfrak{v}_a(\overline{kf}) = \mathfrak{v}_a(\overline{k})M_a^\theta(\overline{f})$, as desired. For the existence of such k, let $uf = v(x^n - a) = \mathrm{lclm}(f, x^n - a)$ with some $u, v \in \mathcal{R}$ and where $\deg(u) \leq n$. Such polynomials exist due to Remark 2.1.1(c). Using right division with remainder we obtain $h = qu + k$ for some q, $k \in \mathcal{R}$ with $\deg(k) < n$. Then $\overline{hf} = \overline{quf + kf} = \overline{qv(x^n - a) + kf} = \overline{kf}$, as desired. □

The last proposition and Proposition 2.2.2(2) provide us with the following.

Corollary 4.1.4. *(a) Let f, $g \in \mathcal{R}$. Then $\mathrm{im}\, M_a^\theta(\overline{f}) \subseteq \mathrm{im}\, M_a^\theta(\overline{g}) \iff g \,|_r\, f$.*
(b) Let $f \in \mathcal{R}$ and $g = \mathrm{gcrd}(f, x^n - a)$. Then $\mathrm{im}\, M_a^\theta(\overline{f}) = \mathrm{im}\, M_a^\theta(\overline{g})$.

Note that $\operatorname{im} M_a^\theta(\overline{f}) \subseteq \operatorname{im} M_a^\theta(\overline{g})$ if and only if $M_a^\theta(\overline{f}) = QM_a^\theta(\overline{g})$ for some $Q \in \mathbb{F}^{n\times n}$. Therefore, using the notation $\cdot \,|_r\, \cdot$ for "is a right divisor of" in both the rings $\mathcal{R}$ and $\mathbb{F}^{n\times n}$, statement (a) above may be rephrased as

$$g \,|_r\, f \iff M_a^\theta(\overline{g}) \,|_r\, M_a^\theta(\overline{f}), \tag{4.1.5}$$

that is, g is a right divisor of f in the ring $\mathcal{R}$ if and only if $M_a^\theta(\overline{g})$ is a right divisor of $M_a^\theta(\overline{f})$ in the ring $\mathbb{F}^{n\times n}$. In other words, M_a^θ induces an isomorphism between the lattice of monic polynomials in $\mathcal{R}$ with right division and the lattice of associated (skew-generalized) circulants in $\mathbb{F}^{n\times n}$ with right division. In Theorem 4.2.3 we will see that if g is a right divisor of $x^n - a$, then the matrix Q above may be chosen as a particular circulant as well. However, if g is not a right divisor of $x^n - a$, then the matrix Q cannot be chosen as a circulant in general (see Example 4.2.7).

Combining Corollary 2.3.1, Propositions 2.2.2, 4.1.3, and Corollary 4.1.4 we obtain the following description of (θ, a)-constacyclic codes.

Theorem 4.1.5. *Let $g \in \mathcal{R}$ be a right divisor of $x^n - a$ of degree $n - k$. Then the circulant $M_a^\theta(\overline{g})$ has rank k and its first k rows form a basis of the (θ, a)-constacyclic code $\mathfrak{v}_a({}^\bullet(\overline{g}))$. As a consequence, the (θ, a)-constacyclic codes in $\mathbb{F}^n$ are exactly the subspaces of the form $\operatorname{im} M_a^\theta(\overline{g})$, where g is a monic right divisor of $x^n - a$. Different such divisors result in different codes. We call g the generator polynomial of the code $\operatorname{im} M_a^\theta(\overline{g})$.*

In the case where $x^n - a$ is central (see Remark 2.2.1) we obtain a particularly nice situation for the circulants. It generalizes the isomorphism in [31, Thm. 4.3] (see also Thm. 2.1 therein), which covers the case where $\mathcal{S}_a = \mathbb{F}_{q^n}[x;\theta]/{}^\bullet(x^n - 1)$ with $\theta(x) = x^q$ for all $x \in \mathbb{F}_{q^n}$.

Theorem 4.1.6. *Let $x^n - a$ be central; thus $\mathcal{S}_a$ is a ring. Then*

$$M_a^\theta(\overline{fg}) = M_a^\theta(\overline{f})M_a^\theta(\overline{g}) \text{ for all } f,\, g \in \mathcal{R}.$$

Hence M_a^θ is a ring isomorphism between $\mathcal{S}_a$ and the subring $M_a^\theta(\mathcal{S}_a) \subseteq \mathbb{F}^{n\times n}$.

Proof. Note first that the product $\overline{f}\,\overline{g}$ is well-defined and equals $\overline{fg}$ thanks to the centrality of $x^n - a$; see Remark 2.2.1. Thus, with the aid of Proposition 4.1.3 we obtain $\mathfrak{p}_a\big(uM_a^\theta(\overline{f})M_a^\theta(\overline{g})\big) = \mathfrak{p}_a\big(uM_a^\theta(\overline{f})\big)\overline{g} = \mathfrak{p}_a(u)\overline{f}\,\overline{g} = \mathfrak{p}_a(u)\overline{fg} = \mathfrak{p}_a(uM_a^\theta(\overline{fg}))$ for all $u \in \mathbb{F}^n$. Since $\mathfrak{p}_a$ is an isomorphism, this yields the desired result. □

Using identities pertaining to factorizations of $x^n - a$, we can look at relationships of particularly nice circulants.

4.2 Circulants of right divisors of $x^n - a$

As before, we consider the skew-polynomial ring $\mathcal{R} := \mathbb{F}[x;\theta]$ for some fixed $\theta \in \mathrm{Aut}(\mathbb{F})$. Recall from the paragraph right after Remark 4.1.2 that in general $x^n - a = hg$ does not imply $M_a^\theta(\overline{h})M_a^\theta(\overline{g}) = 0$. In this section we will prove instead a specific product formula for (skew-generalized) circulants of right divisors of $x^n - a$ that will be sufficient for our investigation of skew-constacyclic codes. Moreover, we will show that the transpose of such a circulant is a circulant again.

Throughout, let $a \in \mathbb{F}^*$. In order to compute modulo the left ideal ${}^\bullet(x^n - a)$ we will need the following lemma.

Lemma 4.2.1. *In the left $\mathcal{R}$-module $\mathcal{S}_a = \mathcal{R}/{}^\bullet(x^n - a)$ we have*

$$\overline{x^{tn+j}} = \Big(\prod_{l=0}^{t-1} \theta^{ln+j}(a)\Big)\overline{x^j} \quad \textit{for all } t \in \mathbb{N},\ j = 0, \ldots, n-1.$$

Proof. For $t = 1$ we compute $\overline{x^{n+j}} = \overline{x^j(x^n - a + a)} = \overline{x^j a} = \overline{\theta^j(a)x^j}$, as desired. The rest follows similarly using induction on t. □

We now turn to circulants of left multiples of $\overline{g}$, where g is a right divisor of $x^n - a$. Before presenting the general result, let us first compute the circulant of $x\overline{g}$ in terms of the circulant of $\overline{g}$.

Example 4.2.2. Let $x^n - a = hg$. Then $x^n = \theta^n(g)h + c$ by Theorem 3.1.2(2) and where $c = \gamma(a, g)$; see (3.1.6). This yields

$$\overline{x^n g} = \overline{\theta^n(g)hg + cg} = \overline{cg} \text{ in } \mathcal{S}_a,$$

and therefore

$$M_a^\theta(\overline{xg}) = \begin{pmatrix} \mathfrak{v}_a(x\overline{g}) \\ \mathfrak{v}_a(x^2\overline{g}) \\ \vdots \\ \mathfrak{v}_a(x^n\overline{g}) \end{pmatrix} = \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ c & & & \end{pmatrix} \begin{pmatrix} \mathfrak{v}_a(\overline{g}) \\ \mathfrak{v}_a(x\overline{g}) \\ \vdots \\ \mathfrak{v}_a(x^{n-1}\overline{g}) \end{pmatrix} = \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ c & & & \end{pmatrix} M_a^\theta(\overline{g}).$$

Note that this can be written as $M_a^\theta(\overline{xg}) = M_c^\theta(\overline{x})M_a^\theta(\overline{g})$, where $\overline{x} := x +^\bullet (x^n - c) \in \mathcal{S}_c$, while, as before, $\overline{g} = g +^\bullet (x^n - a) \in \mathcal{S}_a$.

The product formula for circulants in the previous example can be generalized. From now on we have to consider circulants for different bases and therefore use the convention that for a circulant $M_b^\theta(\overline{f})$ the coset $\overline{f}$ is taken in $\mathcal{S}_b$, thus $\overline{f} = f +^\bullet (x^n - b)$. Recall the notation $\gamma(a, g)$ from (3.1.6).

Theorem 4.2.3. *Let $x^n - a = hg$ and $f \in \mathcal{R}$. Then*

$$M_a^\theta(\overline{fg}) = M_c^\theta(\overline{f})M_a^\theta(\overline{g}), \text{ where } c = \gamma(a, g).$$

Note that if $|\theta|$ divides n, then $c = a$ and thus $M_a^\theta(\overline{fg}) = M_a^\theta(\overline{f})M_a^\theta(\overline{g})$ for all $f \in \mathcal{R}$. For the case where $x^n - a$ is central we have proven the same formula already for general g in Theorem 4.1.6.

Proof. Due to Remark 4.1.2 it suffices to show the statement for $f = x^i$ for any $i \in \mathbb{N}_0$. Write $i = tn + j$, where $0 \le j < n$. Then Lemma 4.2.1 yields $\overline{x^i} = d\overline{x^j}$, where $d := \prod_{l=0}^{t-1} \theta^{ln+j}(c)$. Thus, again Remark 4.1.2(b) shows that we may restrict ourselves to the case $0 \le i < n$. Now we compute

$$M_c^\theta(\overline{x^i})M_a^\theta(\overline{g}) = \begin{pmatrix} & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & \ddots \\ & & & & & & & 1 \\ c & & & & & & & \\ & \theta(c) & & & & & & \\ & & \ddots & & & & & \\ & & & \theta^{i-1}(c) & & & & \end{pmatrix} \begin{pmatrix} \mathfrak{v}_a(\overline{g}) \\ \mathfrak{v}_a(\overline{xg}) \\ \vdots \\ \mathfrak{v}_a(\overline{x^{i-1}g}) \\ \mathfrak{v}_a(\overline{x^ig}) \\ \mathfrak{v}_a(\overline{x^{i+1}g}) \\ \vdots \\ \mathfrak{v}_a(\overline{x^{n-1}g}) \end{pmatrix}$$

$$= \begin{pmatrix} \mathfrak{v}_a(\overline{x^ig}) \\ \mathfrak{v}_a(\overline{x^{i+1}g}) \\ \vdots \\ \mathfrak{v}_a(\overline{x^{n-1}g}) \\ \mathfrak{v}_a(\overline{cg}) \\ \mathfrak{v}_a(\overline{\theta(c)xg}) \\ \vdots \\ \mathfrak{v}_a(\overline{\theta^{i-1}(c)x^{i-1}g}) \end{pmatrix}.$$

Using $\theta^l(c)x^l = x^l c$ as well as $c = x^n - \theta^n(g)h$ from Theorem 3.1.2(2), the cosets modulo the left ideal ${}^\bullet(x^n - a)$ satisfy $\overline{\theta^l(c)x^l g} = \overline{x^l cg} = \overline{x^l(x^n g - \theta^n(g)hg)} = \overline{x^{n+l}g}$ for $l = 0, \ldots, i-1$. Hence the last matrix is $M_a^\theta(\overline{x^i g})$, which is what we wanted. □

The leftmost matrix in above identity will be needed again. Clearly this matrix is invertible, and one easily verifies that

$$\left(M_b^\theta(\overline{x^i})^\intercal\right)^{-1} = M_{b^{-1}}^\theta(\overline{x^i}) \text{ for all } i = 0, \ldots, n-1 \text{ and any } b \in \mathbb{F}^*. \tag{4.2.1}$$

Before we move on to discuss the transpose of a circulant, we take a brief digression and consider the situation of Proposition 3.1.8 again.

Theorem 4.2.4. *Let $x^n - a = hg$ and $b \in \mathbb{F}^*$. Then $gb\,|_r\,(x^n - \hat{a})$, where $\hat{a} = \gamma(a, b^{-1}) = ab\theta^n(b^{-1})$, and*

$$M_{\hat{a}}^\theta(\overline{gb}) = M_a^\theta(\overline{g})M_{\hat{a}}^\theta(\overline{b}).$$

As a result, the skew-constacyclic codes $\mathfrak{v}_a({}^\bullet(\overline{g}))$ and $\mathfrak{v}_{\hat{a}}({}^\bullet(\overline{gb}))$ are scale-equivalent, that is, they differ only by rescaling each codeword coordinate with a fixed nonzero constant. In particular, the codes have the same Hamming weight enumerator and Hamming distance.

Proof. The first statement is due to Proposition 3.1.8. As for the circulants, we have trivially $b\,|_r\,(x^n - \hat{a})$ and $\gamma(\hat{a}, b) = a$. Thus Theorem 4.2.3 yields the desired identity. The scale-equivalence follows from the fact that $M_{\hat{a}}^\theta(\overline{b})$ is a non-singular diagonal matrix. □

Example 4.2.5. Consider the situation of Example 3.1.9(1) in which the map ϑ from (3.1.8) is surjective. The above tells us that it suffices to study θ-cyclic codes, and thus the right divisors of $x^n - 1$, because each (θ, a)-constacyclic code is scale-equivalent to a θ-cyclic one.

We return now to general circulants and show that if g is a right divisor of $x^n - a$ then the transpose of $M_a^\theta(\overline{g})$ is a circulant, see (1) below. While this is an interesting result by itself, for us the version in (2) relating the transpose to a different circulant is more powerful. This is so because the polynomial $a\widehat{g}^r$ appearing in (2) is a right divisor of $x^n - \theta^k(c^{-1})$, see Corollary 3.1.6(b), while $g^\#$ in (1) is not a right divisor of $x^n - c^{-1}$ (not even in the classical commutative case and with $a = c = 1$). As for Part (2) below note that left multiplication of $M_a^\theta(\overline{g})$ by $M_c^\theta(\overline{x^k})$ is simply a reordering

and rescaling of the rows of $M_a^\theta(\overline{g})$; see the proof of Theorem 4.2.3. Part (3) is essentially a special case of (2) and is exactly the form needed to show that the dual of a skew-constacyclic code is a skew-constacyclic code again (see Theorems 4.2.8 and 5.1.1).

Theorem 4.2.6. *Let $x^n - a = hg$, where $\deg(h) = k$, and let $c = \gamma(a, g)$. As in Corollary 3.1.6 let $\widehat{g}^r = \rho_r(\theta^n(g))$ and $\widehat{h}^l = \rho_l(\theta^{-n}(h))$. Then*
(1) $M_a^\theta(\overline{g})^\mathsf{T} = M_{c^{-1}}^\theta(\overline{g^\#})$, where $g^\# = a\widehat{g}^r x^k - cg_0(x^n - c^{-1})$,
(2) $M_c^\theta(\overline{x^k})M_a^\theta(\overline{g}) = M_{\theta^k(c^{-1})}^\theta(\overline{a\widehat{g}^r})^\mathsf{T}$,
(3) $M_{\theta^{k-n}(c^{-1})}^\theta(\overline{x^{n-k}})M_{a^{-1}}^\theta(\overline{\widehat{h}^l}) = M_c^\theta(\overline{a^{-1}h})^\mathsf{T}$.

Proof. (1) Write $g = \sum_{i=0}^{n-k} g_i x^i$ and set $g_i = 0$ for $i = n-k+1, \ldots, n-1$. Due to (4.1.3) we have $M_a^\theta(\overline{g}) = (M_{ij})_{i,j=0,\ldots,n-1}$, where

$$M_{ij} = \begin{cases} \theta^i(g_{j-i}), & \text{if } i \le j, \\ \theta^j(a)\theta^i(g_{n+j-i}), & \text{if } i > j. \end{cases} \tag{4.2.2}$$

On the other hand, $\widehat{g}^r = \rho_r(\theta^n(g)) = \sum_{i=0}^{n-k} \theta^{i+k}(g_{n-k-i})x^i$, and thus we have $a\widehat{g}^r x^k = \sum_{i=k}^{n} a\theta^i(g_{n-i})x^i$. Using that $cg_0 = a\theta^n(g_0)$, this leads to

$$g^\# = \sum_{i=0}^{n-1} s_i x^i, \quad \text{where } s_0 = g_0 \text{ and } s_i = a\theta^i(g_{n-i}) \text{ for } i > 0.$$

Note that $s_i = 0$ for $i = 1, \ldots, k-1$. By (4.1.3), $M_{c^{-1}}^\theta(\overline{g^\#}) = (P_{ij})_{i,j=0,\ldots,n-1}$, where

$$P_{ij} = \begin{cases} \theta^i(s_{j-i}) = \theta^i(a)\theta^j(g_{n-j+i}), & \text{if } i < j, \\ \theta^i(s_0) = \theta^i(g_0), & \text{if } i = j, \\ \theta^j(c^{-1})\theta^i(s_{n+j-i}) = \theta^j(c^{-1})\theta^i(a)\theta^{n+j}(g_{i-j}), & \text{if } i > j. \end{cases}$$

This shows immediately that $P_{ij} = M_{ji}$ for all $i \le j$. The remaining case, that is, $P_{ij} = M_{ji}$ for $i > j$, is equivalent to the identities $g_t = c^{-1}\theta^t(a)\theta^n(g_t)$ for all $t := i - j > 0$. But the latter have been established in Corollary 3.1.5.
(2) On the one hand, $M_c^\theta(\overline{x^k})M_a^\theta(\overline{g}) = M_a^\theta(\overline{x^k g})$ due to Theorem 4.2.3. On the other hand, for $M_{\theta^k(c^{-1})}^\theta(\overline{a\widehat{g}^r})^\mathsf{T}$ we may use part (1) because $a\widehat{g}^r$ is a right divisor of $x^n - \theta^k(c^{-1})$ due to Corollary 3.1.6(b). Thus $M_{\theta^k(c^{-1})}^\theta(\overline{a\widehat{g}^r})^\mathsf{T} = M_{b^{-1}}^\theta(\overline{(a\widehat{g}^r)^\#})$, where $b = \gamma\big(\theta^k(c^{-1}), a\widehat{g}^r\big)$ and $(a\widehat{g}^r)^\#$ is according to (1). The constant coefficient of $a\widehat{g}^r$ is

$a\theta^k(g_{n-k})$ and hence

$$b = \gamma\big(\theta^k(c^{-1}), a\widehat{g}^r\big) = \theta^k(c^{-1})a^{-1}\theta^k(g_{n-k}^{-1})\theta^n(a)\theta^{n+k}(g_{n-k}) = a^{-1}, \tag{4.2.3}$$

where the last step follows from the fact that the product of the last three factors is $\theta^k(c)$ due to Corollary 3.1.5. This shows that $M^\theta_{\theta^k(c^{-1})}(\overline{a\widehat{g}^r})^\mathsf{T} = M^\theta_a(\overline{(a\widehat{g}^r)^\#})$; it remains to prove that $\overline{(a\widehat{g}^r)^\#} = \overline{x^k g}$ in $\mathcal{S}_a$. By definition, $\overline{(a\widehat{g}^r)^\#} = \overline{\theta^k(c^{-1})\rho_r(\theta^n(a\widehat{g}^r))x^k}$. Making use of Proposition 3.1.1(d),(f),(h) we compute

$$\begin{aligned}\rho_r(\theta^n(a\widehat{g}^r))x^k &= \rho_r\big(\theta^n(a)\rho_r(\theta^{2n}(g))\big)x^k = \rho_r\circ\rho_r(\theta^{2n}(g))\theta^{k-n}(\theta^n(a))x^k\\ &= \theta^{k-n}(\theta^{2n}(g))\theta^k(a)x^k = x^k\theta^n(g)a.\end{aligned}$$

Now (3.1.7) leads to $\theta^k(c^{-1})\rho_r(\theta^n(a\widehat{g}^r))x^k = x^k c^{-1}\theta^n(g)a = x^k g$, as desired.
(3) follows from (2): first $\widehat{h}^l$ is a right divisor of $x^n - a^{-1}$ due to Corollary 3.1.6(c); secondly $\gamma(a^{-1}, \widehat{h}^l) = a^{-1}\big(\widehat{h}_0^l\big)^{-1}\theta^n(\widehat{h}_0^l) = \theta^{k-n}(c^{-1})$ due to Corollary 3.1.5 and because $\widehat{h}_0^l = \theta^{-n}(h_k)$; and finally $a^{-1}\widehat{\widehat{h}^l}^r = a^{-1}\rho_r(\theta^n(\rho_l(\theta^{-n}(h)))) = a^{-1}h$, as desired. □

Theorems 4.2.3 and 4.2.6, true for right divisors g of $x^n - a$, do not hold for more general polynomials.

Example 4.2.7. Let $\mathcal{R} = \mathbb{F}_8[x;\theta]$, where θ is the Frobenius homomorphism, thus $\theta(\lambda) = \lambda^2$ for all $\lambda \in \mathbb{F}_8$. Let $\alpha \in \mathbb{F}_8^*$ be the primitive element satisfying $\alpha^3 = \alpha + 1$. Consider the polynomial $f := x^5 - \alpha^2$, hence $n = 5$ and $a = \alpha^2$. Then $h := \alpha^6 + x + \alpha^2x^2 + \alpha^6x^3 + x^4$ is a left divisor of f, but not a right divisor. In this case $M_a^\theta(\overline{h})$ is in $\mathrm{GL}_5(\mathbb{F}_8)$, and one can easily check that $M_a^\theta(\overline{xh})M_a^\theta(\overline{h})^{-1}$ is not a circulant of the form $M_b^\theta(\overline{s})$ for any $s \in \mathcal{R}$ and any $b \in \mathbb{F}_8^*$. This means that there is no identity of the form $M_a^\theta(\overline{xh}) = M_b^\theta(\overline{s})M_a^\theta(\overline{h})$, illustrating that Theorem 4.2.3 does not generalize. Moreover, the transpose $M_a^\theta(\overline{h})^\mathsf{T}$ is not a circulant either.

We conclude the section with the following product formula for various circulants related to the factorization $x^n - a = hg$. In the next chapter, it will be translated into a duality result for skew-constacyclic codes.

Theorem 4.2.8. *Let $x^n - a = hg$, and as in Corollary 3.1.6 let $\widehat{h}^l = \rho_l(\theta^{-n}(h))$. Then*

$$M_a^\theta(\overline{g})M_c^\theta(\overline{a^{-1}h}) = M_a^\theta(\overline{g})M_{a^{-1}}^\theta(\overline{\widehat{h}^l})^\mathsf{T} = 0, \text{ where } c = \gamma(a,g).$$

Proof. For the first product we aim at using Theorem 4.2.3 and thus need to check the requirements. By Theorem 3.1.2(2) the polynomial $a^{-1}h$ is a right divisor of $x^n - c$.

Moreover, $\gamma(c, a^{-1}h) = c(a^{-1}h_0)^{-1}\theta^n(a^{-1}h_0) = cah_0^{-1}\theta^n(h_0)\theta^n(a^{-1}) = a$ by Corollary 3.1.5. Hence we may use Theorem 4.2.3 and this yields $M_a^\theta(\overline{g})M_c^\theta(\overline{a^{-1}h}) = M_c^\theta(\overline{ga^{-1}h})$. But the last matrix is zero because $\overline{ga^{-1}h} = \overline{0}$ in $\mathcal{S}_c$ due to Corollary 3.1.6(a). The rest follows from Theorem 4.2.6(3). □

Chapter 5 Dualization of Skew-Constacyclic Codes

In the previous chapter, we developed a skew-generalized circulant to describe a skew-constacyclic code by using the structure of skew-polynomial rings. We begin this chapter by recovering a result from Boucher/Ulmer: the dual code of a skew-constacyclic code is also a skew-constacyclic code. In particular, we rely on Theorem 4.2.8 on the transposes of circulants. Following this, we use another circulant formula to obtain anti-isomorphisms between the lattice of right divisors of $x^n - a$, the lattice of right divisors of $x^n - a^{-1}$, the lattice of skew-constacyclic codes in $\mathbb{F}^n$ and the lattice of dual codes.

5.1 Main Theorem

Let $\mathcal{R} := \mathbb{F}[x;\theta]$ for some fixed $\theta \in \mathrm{Aut}(\mathbb{F})$. The previous sections lead to the following result, which was first presented and proven in a different form by Boucher/Ulmer in [6, Thm. 8] and [5, Thm. 1].

Theorem 5.1.1. *Let $a \in \mathbb{F}^*$ and $\mathcal{C} \subseteq \mathbb{F}^n$ be a (θ, a)-constacyclic code. Then there exists a unique monic polynomial $g \in \mathcal{R}$ such that $x^n - a = hg$ for some $h \in \mathcal{R}$ and $\mathcal{C} = im\, M_a^\theta(\overline{g}) = \mathfrak{v}_a({}^\bullet(\overline{g}))$. In this case $\mathcal{C}^\perp$ is (θ, a^{-1})-constacyclic and $\mathcal{C}^\perp = im\, M_{a^{-1}}^\theta(\overline{\widehat{h}^l}) = \mathfrak{v}_{a^{-1}}({}^\bullet(\overline{\widehat{h}^l}))$, where $\widehat{h}^l = \rho_l(\theta^{-n}(h))$.*

Proof. The first part about $\mathcal{C}$ is in Theorem 4.1.5 and Proposition 4.1.3. As for the dual code, note first that $\mathrm{rk}(M_a^\theta(\overline{g})) = n - \deg(g) = \deg(h) = \deg(\widehat{h}^l) = n - \mathrm{rk}(M_{a^{-1}}^\theta(\overline{\widehat{h}^l}))$. Since Theorem 4.2.8 yields $M_a^\theta(\overline{g}) M_{a^{-1}}^\theta(\overline{\widehat{h}^l})^\intercal = 0$ we conclude that $\mathrm{im}\, M_a^\theta(\overline{g})$ and $\mathrm{im}\, M_{a^{-1}}^\theta(\overline{\widehat{h}^l})$ are mutually dual codes. □

Now we recover [6, Prop. 13] about self-dual codes (see also [9, Prop. 5]).

Corollary 5.1.2. *If there exists a self-dual (θ, a)-constacyclic code in $\mathbb{F}^n$, then n is even and $a = \pm 1$.*

5.2 The Lattices of Skew-Constacyclic Codes

We are now in a position to formulate the interplay between right divisors of $x^n - a$ and the associated codes as well as their duals in terms of lattice (anti-)isomorphisms.

For $a \in \mathbb{F}^*$ define the sets

$$\begin{aligned}\mathcal{D}_a &:= \{g \in \mathcal{R} \mid g \,|_r\, (x^n - a),\ g \text{ monic}\},\\ \mathcal{I}_a &:= \{I \subseteq \mathcal{S}_a \mid I \text{ is a submodule of } \mathcal{S}_a\},\\ \mathcal{T}_a &:= \{\mathcal{C} \subseteq \mathbb{F}^n \mid \mathcal{C} \text{ is } (\theta, a)\text{-constacyclic}\}.\end{aligned}$$

Clearly, $(\mathcal{D}_a,\ |_r\ )$, $(\mathcal{I}_a, \subseteq)$, $(\mathcal{T}_a, \subseteq)$ are lattices. Consider the maps

$$\begin{array}{ccccc} \mathcal{D}_a & \xrightarrow{\sigma_a} & \mathcal{T}_a & \xrightarrow{\mathfrak{p}_a} & \mathcal{I}_a \\ g & \longmapsto & \operatorname{im} M_a^\theta(\overline{g}) & \longmapsto & \mathfrak{p}_a\big(\operatorname{im} M_a^\theta(\overline{g})\big) \end{array} \tag{5.2.1}$$

Because of Corollary 4.1.4(a) and Theorem 4.1.5, the map σ_a is a lattice anti-isomorphism, while $\mathfrak{p}_a$ is a lattice isomorphism thanks to Proposition 4.1.3.

We now turn to the dual situation. Let $x^n - a = hg$ with monic polynomials $g, h \in \mathcal{R}$.

Theorem 5.2.1. *Define the map $\delta_a : \mathcal{D}_a \longrightarrow \mathcal{D}_{a^{-1}},\ g \longmapsto \theta^{-\deg(g)}(-a^{-1}g_0)\widehat{h}^l$, where g_0 is the constant coefficient of g and, as before, set $\widehat{h}^l := \rho_l\big(\theta^{-n}(h)\big)$. Moreover, define $\tau_a : \mathcal{T}_a \longrightarrow \mathcal{T}_{a^{-1}},\ \mathcal{C} \longmapsto \mathcal{C}^\perp$, and let σ_a be as in* (5.2.1)*. Consider the diagram*

$$\begin{array}{ccc} \mathcal{D}_a & \xrightarrow{\delta_a} & \mathcal{D}_{a^{-1}} \\ \downarrow{\scriptstyle \sigma_a} & & \downarrow{\scriptstyle \sigma_{a^{-1}}} \\ \mathcal{T}_a & \xrightarrow{\tau_a} & \mathcal{T}_{a^{-1}} \end{array}$$

Then all maps are lattice anti-isomorphisms and the diagram commutes. In other words, if $\mathcal{C} = im\, M_a^\theta(\overline{g})$ for some $g \in \mathcal{D}_a$, then $\mathcal{C}^\perp = im\, M_{a^{-1}}^\theta(\overline{\delta_a(g)}) = im\, M_{a^{-1}}^\theta(\overline{\widehat{h}^l})$.

Proof. First of all, $\delta_a(g)$ is indeed a right divisor of $x^n - a^{-1}$ thanks to Corollary 3.1.6(c), and it is monic because the leading coefficient of $\widehat{h}^l$ is $\theta^{-\deg(g)}(-ag_0^{-1})$, as one can easily verify. Next, Theorem 5.1.1 yields that the diagram commutes. This in turn implies that δ_a is a lattice anti-isomorphism because σ_a, τ_a, $\sigma_{a^{-1}}$ are. □

Now we can present the dual lattices to those in Example 2.3.3.

Example 5.2.2. Consider again the field $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, where $\alpha^3 = \alpha + 1$, and let θ be the Frobenius homomorphism on $\mathbb{F}_8$. In Example 2.3.3 we presented all monic right divisors of $x^7 + \alpha$. Using the map δ_α we obtain all right divisors of $x^7 + \alpha^{-1} = x^7 + \alpha^6$.

Setting $\tilde{h}^{(i)} := \delta_\alpha(g^{(i)})$ for $i = 0, \ldots, 7$, we obtain

$$\tilde{h}^{(0)} = x^7 + \alpha^6, \quad \tilde{h}^{(1)} = x^6 + \alpha^3 x^5 + \alpha x^4 + x^3 + \alpha^3 x^2 + \alpha x + 1,$$
$$\tilde{h}^{(2)} = x^4 + \alpha^2 x^2 + x + \alpha^6, \quad \tilde{h}^{(3)} = x^4 + \alpha^6 x^3 + \alpha^2 x^2 + \alpha^6, \quad \tilde{h}^{(4)} = x^3 + \alpha x + 1$$
$$\tilde{h}^{(5)} = x^3 + \alpha^3 x^2 + 1, \quad \tilde{h}^{(6)} = x + \alpha^6, \quad \tilde{h}^{(7)} = 1.$$

From the above we know that $(\mathcal{C}^{(i)})^\perp = \sigma_\alpha(\tilde{h}^{(i)})$, and thus we obtain the lattices given in Figure 5.1. They are dual to those in Figure 2.1.

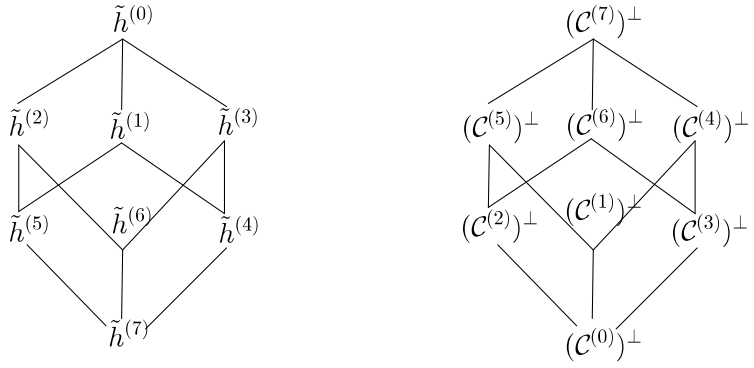

Figure 5.1: Lattice of monic right divisors of $x^7 + \alpha^{-1}$ and the corresponding codes

We now turn to the notion of a check polynomial for skew-constacyclic codes.

Proposition 5.2.3. *Let $x^n - a = hg$ and $c = \gamma(a, g)$. Then the map*

$$\psi : \mathcal{S}_a \longrightarrow \mathcal{S}_{\theta^{-n}(c)}, \ \overline{f} \longmapsto \overline{f\theta^{-n}(h)}$$

is a well-defined $\mathcal{R}$-module homomorphism with $\ker \psi = {}^\bullet(\overline{g})$.

Proof. Theorem 3.1.2(3) gives us both well-definedness and the containment $\ker \psi \supseteq {}^\bullet(\overline{g})$, and $\mathcal{R}$-linearity is clear. For $\ker \psi \subseteq {}^\bullet(\overline{g})$ note that $f\theta^{-n}(h) = t(x^n - \theta^{-n}(c))$ for some $t \in \mathcal{R}$ implies $f\theta^{-n}(h) = tg\theta^{-n}(h)$ and thus $f \in {}^\bullet(g)$ by right cancellation in $\mathcal{R}$. □

The last result justifies to call $\theta^{-n}(h)$ the *check polynomial* of the code $\mathcal{C} = \mathfrak{v}_a({}^\bullet(\overline{g}))$. The only thing to keep in mind that the check equation is carried out modulo $x^n - \theta^{-n}(c)$. This generalizes [7, Lem. 8] (see also [14, Thm. 2.1(iii)]), where a central polynomial $x^n - 1$ is considered. In that case θ^n is the identity on $\mathcal{R}$ and

thus $\theta^{-n}(h) = h$. In particular, all of this generalizes the classical commutative case where h is the check polynomial of $\mathcal{C}$ [23, Ch. 7, §4].

We close with a brief summary of the central case. The results bear some resemblance with those obtained for cyclic convolutional codes in [16]; see especially Theorem 7.5 therein. The last part of (4) appears already in [24, Cor. 1] by Matsuoka, where even skew-polynomial rings over arbitrary finite rings are considered.

Theorem 5.2.4. *Let n be such that $\theta^n = |_{r\,\mathcal{R}}$ and consider $x^n - a$ for some $a \in Fix_{\mathbb{F}}(\theta)$, hence $x^n - a$ is central. Suppose $x^n - a = hg$. Then*
(1) M_a^θ induces an injective ring homomorphism from $\mathcal{S}_a$ into $\mathbb{F}^{n\times n}$.
(2) $x^n - a = gh$.
(3) $M_a^\theta(\overline{g})M_a^\theta(\overline{h}) = M_a^\theta(\overline{h})M_a^\theta(\overline{g}) = 0$.
(4) We have left $\mathcal{R}$-module homomorphisms

$$\psi_h : \mathcal{S}_a \longrightarrow \mathcal{S}_a,\ \overline{f} \longmapsto \overline{fh} \quad \text{and} \quad \psi_g : \mathcal{S}_a \longrightarrow \mathcal{S}_a,\ \overline{f} \longmapsto \overline{fg}.$$

Moreover, $\ker \psi_h = {}^\bullet(\overline{g}) = ann_l((\overline{h})^\bullet)$, the left annihilator of the right ideal generated by h. In the same way, $\ker \psi_g = {}^\bullet(\overline{h}) = ann_l((\overline{g})^\bullet)$. In this sense h is the check polynomial of the code $\mathcal{C} = \mathfrak{v}_a({}^\bullet(\overline{g}))$.
(5) We have right $\mathcal{R}$-module homomorphisms

$$\psi'_h : \mathcal{S}_a \longrightarrow \mathcal{S}_a,\ \overline{f} \longmapsto \overline{hf} \quad \text{and} \quad \psi'_g : \mathcal{S}_a \longrightarrow \mathcal{S}_a,\ \overline{f} \longmapsto \overline{gf},$$

and $\ker \psi'_h = (\overline{g})^\bullet = ann_r({}^\bullet(\overline{h}))$, the right annihilator of the left ideal generated by h, and $\ker \psi'_g = (\overline{h})^\bullet = ann_r({}^\bullet(\overline{g}))$.
(6) Let $\mathcal{C} = \mathfrak{v}_a({}^\bullet(\overline{g}))$ and $h = \sum_{i=0}^k h_i x^i$. Then

$$\mathcal{C}^\perp = \mathfrak{v}_{a^{-1}}({}^\bullet(\overline{\rho_l(h)})),\ \text{where } \rho_l(h) = h_k + \theta(h_{k-1})x + \ldots + \theta^k(h_0)x^k.$$

One may regard (5) and (6) as the counterpart to (4) in terms of ideals.

Proof. (1) is in Theorem 4.1.6. (2) follows from Theorem 3.1.2 because $\gamma(a, g) = a$ for all right divisors g of $x^n - a$. (3) is a consequence of (1) and (2). (4) is a special case of Proposition 5.2.3, and (5) follows by symmetry. (6) is a special case of Theorem 5.1.1. □

In this context it is worth pointing out that if $x^n - a$ is central and $x^n - a = hg$ then g and h need not even be two-sided: for instance, in $\mathbb{F}_4[x;\theta]$ with θ being the

Frobenius homomorphism, we have the identity $x^4-1=(x^2+\alpha x+\alpha^2)(x^2+\alpha x+\alpha)$, and neither factor is two-sided. Furthermore, if x^n-a is a product of three or more factors, the factors do not commute arbitrarily. This can be seen with $x^6-1=(x+1)(\alpha^2x^2+1)(\alpha x^3+\alpha x^2+x+1)\neq(\alpha x^3+\alpha x^2+x+1)(\alpha^2x^2+1)(x+1)$ in $\mathbb{F}_4[x;\theta]$. It is well known that every two-sided element can be factored into a product of two-sided maximal elements, and in this case the factors commute [19, Sec. 1.2]. Further information about the case where $a=1$ and x^n-1 is central can be found in [14].

Chapter 6 Idempotents

In this chapter, we turn to idempotent elements of our quotient module. We begin by generalizing the idea of idempotents and generating idempotents from the cyclic case to our skew-constacyclic case. After some brief examples demonstrating the quirks of idempotents modulo ${}^{\bullet}(x^n - a)$, we restrict ourselves to the case where $x^n - a$ is central. We generalize a result from [14], in which Gao/Shen/Fu showed the existence of unique central generating idempotents modulo ${}^{\bullet}(x^n - 1)$ (where $x^n - 1$ is central). We extend this to all central $x^n - a$, and give a formula for the unique central generating idempotent of a skew-constacyclic code generated by a central divisor of $x^n - a$.

We then remove the restriction that $x^n - a$ be central and give results on the existence of generating idempotents of skew-constacyclic codes, including an explicit formula for a generating idempotent in a particularly nice case. Evidence is provided to demonstrate that this nice case occurs non-trivially. We end the chapter with generalizations of other well-known results from the classical cyclic case on intersections and sums of codes.

6.1 Preliminaries

We continue to consider the skew-polynomial ring $\mathcal{R} := \mathbb{F}_q[x;\theta]$ for some fixed $\theta \in \mathrm{Aut}(\mathbb{F}_q)$. The generator polynomial is not the only polynomial that can be used to generate a particular skew-constacyclic code.

In the cyclic case, when $\gcd(n, q) = 1$, a code $\mathcal{C}$ has a unique generating idempotent $\overline{e}$, where $e \in \mathbb{F}_q[x]$. That is, $\overline{e} = \overline{e}^2$ in $\mathbb{F}_q[x]/(x^n - 1)$ and $\mathcal{C} = \mathfrak{v}_1((\overline{e}))$ [18, p. 132]. We wish to generalize this concept to skew-constacyclic codes. But we need to proceed with care, because in contrast to the commutative case idempotency of cosets is in general not a well-defined notion.

Example 6.1.1. (1) Consider $x^9 - 1 \in \mathbb{F}_4[x;\theta = \mathrm{Frob}]$, where $\omega^2 + \omega = 1$. One can check that the polynomial $e := \omega^2x^8 + \omega^2x^7 + \omega x^6 + \omega^2x^5 + \omega^2x^4 + \omega x^3 + \omega^2x^2 + \omega^2x + \omega^2$ satisfies $e^2 - e \in {}^{\bullet}(x^9 - 1)$. Define $\tilde{e} := e + x^9 - 1$. By construction, $\tilde{e} \in \overline{e}$. However, $\tilde{e}^2 - \tilde{e} \notin {}^{\bullet}(x^9 - 1)$. In general, just because one polynomial in a coset is an idempotent modulo ${}^{\bullet}(x^n - a)$, this does not mean that every polynomial in the same coset is also an idempotent modulo ${}^{\bullet}(x^n - a)$.

(2) Consider $x^4 - \omega \in \mathbb{F}_4[x; \theta = \text{Frob}]$, where $\omega^2 + \omega = 1$. One can check that polynomial $e := \omega x^4 + \omega x^3 + \omega^2 x^2 + \omega^2 x + 1$ satisfies $e^2 - e \in {}^\bullet(x^4 - w)$. We see that $e \in \overline{\omega x^3 + \omega^2 x^2 + \omega^2 x + \omega}$, but $\omega x^3 + \omega^2 x^2 + \omega^2 x + \omega$ is *not* idempotent modulo ${}^\bullet(x^4 - \omega)$.

Definition 6.1.2. An element $e \in \mathcal{R}$ is said to be an *idempotent modulo* ${}^\bullet(x^n - a)$ if $e^2 - e \in {}^\bullet(x^n - a)$. We say that it is a *generating idempotent of* ${}^\bullet(\overline{g})$ if, in addition, ${}^\bullet(\overline{g}) = {}^\bullet(\overline{e})$.

If our polynomial $x^n - a$ is central, then idempotency of a coset is well-defined, as we see in the following proposition.

Proposition 6.1.3. *Let $x^n - a \in Z(\mathcal{R})$ and let $e \in \mathcal{R}$ be an idempotent modulo ${}^\bullet(x^n - a)$. Then $\tilde{e} \in \overline{e}$ is also an idempotent modulo ${}^\bullet(x^n - a)$.*

Proof. Since $\tilde{e} \in \overline{e}$, we can write $\tilde{e} = e + t(x^n - a)$ for some $t \in \mathcal{R}$. Then

$$\begin{aligned}\tilde{e}^2 - \tilde{e} &= (e + t(x^n - a))((e + t(x^n - a)) - ((e + t(x^n - a)) \\ &= e^2 + et(x^n - a) + t(x^n - a)e + t(x^n - a)t(x^n - a) - e - t(x^n - a) \\ &\equiv e^2 + t(x^n - a)e - e = e^2 + et(x^n - a) - e \equiv e^2 - e \equiv 0 \mod {}^\bullet(x^n - a).\end{aligned}$$

Thus $\tilde{e}$ is also an idempotent modulo ${}^\bullet(x^n - a)$. □

So in the central case, if we want to search for idempotents modulo ${}^\bullet(x^n - a)$ in some left ideal ${}^\bullet(\overline{g})$, we may restrict ourselves to checking left multiples of g with degree less than n. All idempotents of greater degree will be equivalent to one of these smaller degree idempotents.

We present a small result on idempotents in the classical cyclic case to further aid in illustrating the differences between the classical and skew-constacyclic cases. The following proposition is given for the general constacyclic case (*not* skew-constacyclic); for the cyclic result, take $a = 1$.

Proposition 6.1.4. *Let $\overline{e}$ be a non-zero idempotent in $\mathbb{F}_q[x]/(x^n - a)$ and $u \in \mathbb{F}_q^*$. Then $\overline{ue}$ is an idempotent in $\mathbb{F}_q[x]/(x^n - a)$ if and only if $u = 1$.*

Proof. We have that $e^2 - e \in (x^n - a)$. Then

$$\begin{aligned}\overline{(ue)^2 - ue} &= \overline{u^2e^2 - ue} = \overline{u^2e^2 - u^2e + u^2e - ue} \\ &= \overline{u^2(e^2 - e) + (u^2 - u)e} = \overline{(u^2 - u)e}.\end{aligned}$$

Then $\overline{ue}$ is a idempotent if and only if $\overline{(u^2-u)e} = \overline{0}$. Because $u \in \mathbb{F}^*$, we know that $u^2 - u \in \mathbb{F}$ is not a zero divisor. Since $\overline{e} \neq \overline{0}$, we have $\overline{(u^2-u)e} = \overline{0}$ exactly when we have $u^2 - u = 0$, or $u = 1$. □

In contrast with the classical cyclic case, we present a concrete example from the skew-constacyclic case to demonstrate some of the ways in which idempotents behave differently.

Example 6.1.5. Let $x^4 - 1 \in \mathcal{R} := \mathbb{F}_9[x; \theta = \text{Frob}]$, where $\omega^2 + \omega = 1$, and consider $g = x^3 + x^2 + x + 1$, which is a right divisor of $x^4 - 1$. Observe that $x^4 - 1 \in Z(\mathcal{R})$, but g is not central. Note also that $\gcd(n, q) = 1$ as is desired in the classical cyclic case.

One can easily examine the left multiples of g with degree less than 4 to see which ones are idempotents modulo $^\bullet(x^4 - 1)$. From Prop. 6.1.3, we know that all idempotents of greater degree are equivalent to one of these polynomials modulo $^\bullet(x^n - a)$. We find the following non-zero idempotents modulo $^\bullet(x^4 - 1)$: $g, \omega g, \omega^3 g$. Unlike in the classical cyclic case (see Prop. 6.1.4), idempotents may be non-trivial constant left multiples of each other.

Further, each of these three idempotents is a generating idempotent of $^\bullet(\overline{g})$. Thus we know that in the skew-cyclic case, there may be multiple generating idempotents, and not just a unique one as in the classical cyclic case.

Example 6.1.6. (1) Recall that in Example 6.1.1(1), we saw that there is a polynomial e such that $e^2 - e \in {}^\bullet(x^9 - 1) \subset \mathbb{F}_4[x; \theta = \text{Frob}]$, but there exists an $\tilde{e} \in \overline{e}$ such that $\tilde{e}^2 - \tilde{e} \notin {}^\bullet(x^9 - 1)$. There are eight right divisors of $x^9 - 1$ (including 1 and $x^9 - 1$), and there is exactly one generating idempotent e corresponding to each divisor such that every polynomial in $\overline{e}$ is also an idempotent. There are also four idempotents modulo $^\bullet(x^9 - 1)$ of degree less than 9 that do *not* have this nice property: not every polynomial in its coset is an idempotent.

(2) Consider $x^4 - \omega \in \mathbb{F}_4[x; \theta = \text{Frob}]$, where $\omega^2 + \omega = 1$. One can check that the only idempotents modulo $^\bullet(x^4 - \omega)$ of degree less than 4 are 0 and 1. However, there are twelve idempotents modulo $^\bullet(x^4 - \omega)$ of degree 4. Six of these idempotents are elements of either $\overline{0}$ or $\overline{1}$; the remaining six are not. And as there were no other idempotents of degree less than 4, we know that these six idempotents do not correspond to idempotent cosets. We see that we can have idempotents of degree n or greater that do not correspond to lower degree idempotents.

In some cases, we can quickly show that an idempotent's coset contains only idempotents modulo ${}^\bullet(x^n - a)$ by examining the relationship between θ, n, a, and the idempotent, as we will see in the following proposition. The following is a generalization of Proposition 6.1.3.

Proposition 6.1.7. *Let $x^n - a \in \mathcal{R}$ and let $e \in \mathcal{R}$ be an idempotent modulo ${}^\bullet(x^n - a)$. If $ae = \theta^n(e)a$, then every $\tilde{e} \in \overline{e}$ is also an idempotent modulo ${}^\bullet(x^n - a)$.*

Proof. Let e be an idempotent modulo ${}^\bullet(x^n - a)$ with $ae = \theta^n(e)a$. Let $\tilde{e} \in \overline{e}$; we can write $\tilde{e} = e + s(x^n - a)$ for some $s \in \mathcal{R}$. We compute

$$\begin{aligned}\tilde{e}^2 - \tilde{e} &= (e + s(x^n - a))^2 - (e + s(x^n - a)) \\ &= e^2 + es(x^n - a) + s(x^n - a)e + (s(x^n - a))^2 - e - s(x^n - a) \\ &= s(x^n - a)e + t(x^n - a)\end{aligned}$$

for some $t \in \mathcal{R}$. Thus $\tilde{e}^2 - \tilde{e} \in {}^\bullet(x^n - a)$ exactly when $(x^n - a) \mid_r s(x^n - a)e$. We have

$$s(x^n - a)e = sx^n e - sae = s\theta^n(e)x^n - s\theta^n(e)a = s\theta^n(e)(x^n - a),$$

so $\tilde{e}$ is an idempotent modulo ${}^\bullet(x^n - a)$. □

6.2 The Central Case

Though we will not need it until Proposition 6.2.7, throughout this section, let $x^n - a \in Z(\mathcal{R})$ with $a \neq 0$. Further, let $m := |\theta|$. Recall that $Z(\mathcal{R}) = \widehat{\mathbb{F}}[x^m]$, where $\widehat{\mathbb{F}} := \mathrm{Fix}_{\mathbb{F}}(\theta)$ is the fixed field of θ. Thus $m \mid n$ and $a \in \widehat{\mathbb{F}}$. Equivalently, $S_a := \mathcal{R}/{}^\bullet(x^n - a)$ is a ring. In this section, we will adapt [14, Thm. 2.11] to find idempotents modulo ${}^\bullet(x^n - a)$.

Recall that in Remark 2.2.1, we defined an element $f \in \mathcal{R}$ to be *two-sided* if ${}^\bullet(f) = (f)^\bullet$. Further, f is two-sided if and only if for all $g \in \mathcal{R}$, there exists $\tilde{g} \in \mathcal{R}$ such that $gf = f\tilde{g}$, and there exists $\hat{g}$ such that $fg = \hat{g}f$.

Thus for a two-sided element f, the left ideal ${}^\bullet(f)$ is two-sided, and we simply write (f). Note that central elements are two sided. From [19, Thm. 1.1.22], we have that if $f \in \mathcal{R}$ is two-sided, then it has the form $f = c\hat{f}x^t$, where $c \in \mathbb{F}_q, t \in \mathbb{N}_0$, and $\hat{f} \in Z(\mathcal{R})$. One can easily check that if f, g are two-sided elements, then their product fg is also two-sided. However, two-sided elements do not in general commute. (Consider, for example, $f = x$ and $g = ax$, where $a \notin \widehat{\mathbb{F}}$.) Recall that $\mathcal{R}$ is a left

principal ideal domain; since each two-sided ideal is also a left ideal, each two-sided ideal is also principal.

Proposition 6.2.1. *If $f, g \in \mathcal{R}$ are two-sided, then gcrd(f,g) = gcld(f,g).*

Proof. Because f is two-sided, any left multiple of f can also be written as a right multiple of f, and vice versa. The same applies for g. Thus given the Bézout identity $\gcrd(f,g) = uf + vg$ for some $u, v \in \mathcal{R}$, we also have $\gcrd(f,g) = f\hat{u} + g\hat{v}$ for some $\hat{u}, \hat{v} \in \mathcal{R}$. So $\gcld(f,g) \,|_l \gcrd(f,g)$. On the other hand, given the Bézout identity $\gcld(f,g) = fs + gt$ for some $s, t \in \mathcal{R}$, we also have $\gcld(f,g) = \hat{s}f + \hat{t}g$ for some $\hat{s}, \hat{t} \in \mathcal{R}$. So $\gcrd(f,g) \,|_r \gcld(f,g)$. Since $\gcrd(f,g)$ and $\gcld(f,g)$ are both monic, $\gcrd(f,g) = \gcld(f,g)$. □

Later, it will be useful to factor a two-sided element into two-sided factors. The following theorem leads to a useful tool: the quotient of a two-sided element and one of its two-sided divisors is also two-sided.

Theorem 6.2.2. *Let $f, h \in Z(\mathcal{R})$ with $f = hg = gh$ for some $g \in \mathcal{R}$. Then $g \in Z(\mathcal{R})$ as well. Hence $Z(\mathcal{R}) \cap (h) = Z(\mathcal{R})h$.*

Proof. Suppose g has a non-zero term of degree that is not a multiple of m. Let ax^t be the term of least such degree in g. Let bx^{sm} be the non-zero term of least degree in h. Consider the product of these two terms: $bx^{sm}ax^t = abx^{sm+t}$. Since each term was non-zero and $\mathbb{F}[x;\theta]$ is a domain, $abx^{sm+t} \neq 0$. No other term of degree $sm+t$ arises in the product of h and g, as all terms of h have degrees that are multiples of m, and any term of greater degree in g would need to be multiplied with a non-zero term of h with degree less than sm, which does not exist. Thus abx^{sm+t} is a term of f. But $m \nmid (sm+t)$, so f is not central, a contradiction. Thus every non-zero term of g has degree divisible by m.

Now suppose that g has a term with coefficients not in $\widehat{\mathbb{F}} := \mathrm{Fix}_{\mathbb{F}}(\theta)$. Let ax^t be the term of least degree such that $a \notin \widehat{\mathbb{F}}$. Let s be the degree of the non-zero term of least degree in h. Write $g = \sum_{i=0}^{\deg(g)} g_i x^i$ and $h = \sum_{j=0}^{\deg(h)} h_j x^j$. Then the term of f with degree $s+t$ is $\sum_{i+j=s+t} h_j x^j g_i x^i = \sum_{i+j=s+t} g_i h_j x^{s+t} = ah_s x^{s+t} + \sum_{\substack{i+j=s+t \\ i<t}} g_i h_j x^{s+t}$. Since each $g_i \in \widehat{\mathbb{F}}$ for $i < t$, we have that $\sum_{\substack{i+j=s+t \\ i<t}} g_i h_j \in \widehat{\mathbb{F}}$. But since $a \notin \widehat{\mathbb{F}}$ and $h_s \in \widehat{\mathbb{F}}$, we have $ah_s \notin \widehat{\mathbb{F}}$, and even $(ah_s + \sum_{\substack{i+j=s+t \\ i<t}} g_i h_j) \notin \widehat{\mathbb{F}}$. But this is a contradiction, as each coefficient of f must be in $\widehat{\mathbb{F}}$. Thus every coefficient of g is in $\widehat{\mathbb{F}}$. So $g \in \widehat{\mathbb{F}}[x^m] = Z(\mathcal{R})$.

For $Z(\mathcal{R}) \cap (h) = Z(\mathcal{R})h$, this gives us the containment $Z(\mathcal{R}) \cap (h) \subseteq Z(\mathcal{R})h$, and the containment $Z(\mathcal{R}) \cap (h) \supseteq Z(\mathcal{R})h$ is trivial. □

Corollary 6.2.3. *Let $f \in \mathcal{R}$ be a non-zero two-sided element with $f = hg$. Then g is two-sided if and only if h is two-sided.*

Proof. We show that if h is two-sided, then g is as well. Since f and h are two-sided, we may write $f = c\hat{f}x^t$ and $h = d\hat{h}x^s$ for some $c, d \in \mathbb{F}^*$ and $\hat{f}, \hat{h} \in Z(\mathcal{R})$ with non-zero constants. Thus $f = hg$ implies that $c\hat{f}x^t = d\hat{h}x^s g$, or $d^{-1}c\hat{f}x^t = \hat{h}x^s g$. We can write $g = x^l\tilde{g}$ for some $\tilde{g}$ with a non-zero constant. Then $t = s + l$. So $x^t\theta^{-t}(d^{-1}c)\hat{f} = d^{-1}c\hat{f}x^t = \hat{h}x^s x^l\tilde{g} = x^s x^l\hat{h}\tilde{g}$. By left cancellation, $\theta^{-t}(d^{-1}c)\hat{f} = \hat{h}\tilde{g}$. Since $\hat{f}$ and $\hat{h}$ are central, then Theorem 6.2.2 gives us that $\theta^{-t}(dc^{-1})\tilde{g}$ is central. So $g = x^l\tilde{g} = x^l\theta^{-t}(d^{-1}c)(\theta^{-t}(dc^{-1})\tilde{g})$ is two-sided.

The other direction follows in a similar fashion. □

There is a particular class of two-sided elements that we will consider: two-sided maximal elements.

Definition 6.2.4. A two-sided element $f^* \in \mathcal{R}$ is said to be *two-sided maximal* if (f^*) is a two-sided maximal ideal in $\mathcal{R}$.

Note that (0) is never a two-sided *maximal* ideal, as it is contained in the ideal generated by any other two-sided element. For example, $(0) \subset (x)$.

Proposition 6.2.5. *The two-sided maximal elements in $\mathcal{R}$ are exactly those two-sided elements with no proper two-sided factors in $\mathcal{R}$.*

Proof. First, let $f \in \mathcal{R}$ be a two-sided element with no non-trivial factorization into two-sided element. Suppose there exists a two-sided element $g \in \mathcal{R}$ such that $(f) \subseteq (g)$. Then $g \mid f$. Since f has no proper two-sided factors, either $g = cf$ or $g = c$ for some $c \in \mathbb{F}^*$. Thus either $(g) = (f)$ or $(g) = \mathcal{R}$, so (f) must be a maximal ideal. Thus f is a two-sided maximal element.

On the other hand, let $f^* \in \mathcal{R}$ be a two-sided maximal element. Suppose $f^* = f_1^* f_2^*$ is a proper factorization of f^* into non-unit two-sided elements. Then $(f^*) \subset (f_1^*) \subset \mathcal{R}$. This contradicts the fact that f^* is two-sided maximal; thus f^* has no proper two-sided factors. □

Thus we see that finding two-sided maximal elements in $\mathcal{R}$ amounts to finding the two-sided elements with no proper two-sided factors.

We can characterize a class of two-sided elements that do commute with each other.

Proposition 6.2.6. *If f^* and g^* are two-sided maximal elements in $\mathcal{R}$ with non-zero constant terms, then f^* and g^* commute.*

Proof. Let f^*, g^* be as described. Then ${}^\bullet(f^*)^\bullet(g^*) = {}^\bullet(g^*)^\bullet(f^*)$ by [19, Lem. 1.2.16], which states that any two two-sided maximal ideals commute. So ${}^\bullet(f^*g^*) = {}^\bullet(g^*f^*)$, and since $f^*g^* \in {}^\bullet(f^*g^*)$, we have $f^*g^* = cg^*f^*$ for some $c \in \mathcal{R}$. By degree, c must be a non-zero constant. However, since the constant terms of f^*g^* and g^*f^* are the same, $c = 1$. Thus $f^*g^* = g^*f^*$ as desired. □

In the following proposition, we introduce the condition that $\gcd(n, q) = 1$. This condition guarantees that $x^n - a \in \mathbb{F}_q[x]$ has no repeated irreducible factors (see, for example, [18], Section 4.1); we will exploit this fact by converting our central skew-polynomials into standard polynomials. This assumption will reappear throughout the rest of this section for that purpose, but we will call attention to it where it is needed.

As mentioned at the beginning of this section, we assume that $x^n - a \in Z(\mathcal{R})$ with $a \in \mathbb{F}^*$ for the duration of this section.

Proposition 6.2.7. *Suppose $m \mid n$ and $\gcd(n, q) = 1$. Then $x^n - a$ can be factorized as $x^n - a = f_1^* f_2^* \cdots f_t^*$, where the f_i^*'s are distinct and pairwise coprime two-sided maximal polynomials.*

Recall that in Proposition 6.2.1 we showed that the greatest common left divisor and greatest common right divisor of two two-sided elements are the same. Thus in this case, being left coprime and right coprime are the same, and we just write coprime.

Proof. Since $x^n - a \in Z(\mathcal{R})$ is two-sided and not a unit, [19, Thm. 1.2.17'] gives us that it can be factorized as $x^n - a = f_1^* f_2^* \cdots f_t^*$, where each f_i^* is a two-sided maximal element. Since $x^n - a$ has a non-zero constant term, so must each f_i^*. Then each $f_i^* \in \mathbb{F}_q[x^m]$.

Now, set $\tilde{n} := n/m$ and $y := x^m$. Then in $\mathbb{F}_q[y; \theta] = \mathbb{F}_q[y]$, we have $y^{\tilde{n}} - a = \tilde{f}_1^* \tilde{f}_2^* \cdots \tilde{f}_t^*$, where $\tilde{f}_i^*$ is simply f_i^* with y substituted in for x^m. Since $\gcd(n, q) = 1$, so does $\gcd(\tilde{n}, q) = 1$. Hence $y^{\tilde{n}} - a$ is separable, and thus $\tilde{f}_1^*, \ldots, \tilde{f}_t^*$ are distinct.

Then, substituting x^m back in for y, we see that the original two-sided maximal factors $f_1^*, f_2^*, \cdots, f_t^*$ are distinct. Further, since each (f_i^*) is maximal, f_i^* and f_j^* are coprime for all $i \neq j$. □

As used in the previous proof, each two-sided element has a factorization into two-sided maximal elements that is unique (up to order and unit factors). Recall also from Proposition 6.2.6 that two-sided elements with non-zero constant terms commute. In particular, factors of $x^n - a$ must have non-zero constants; thus its two-sided maximal factors commute.

However, we can convert these two-sided maximal factors into central elements to make computations easier, as we will see in Proposition 6.2.9.

Definition 6.2.8. If $f \in Z(\mathcal{R})$ is two-sided maximal, call it *central maximal*.

From 6.2.5, it follows that as a two-sided maximal element has no proper two-sided factors, a central maximal element has no proper central factors.

Proposition 6.2.9. *Suppose $x^n - a \in Z(\mathcal{R})$ has a factorization into two-sided maximal elements $x^n - a = f_1 f_2 \cdots f_t$. Then we also have a factorization $x^n - a = \hat{f}_1 \hat{f}_2 \cdots \hat{f}_t$ into monic central maximal elements, where $\hat{f}_i = d_i f_i$ for some constant $d_i \in \mathbb{F}^*$.*

Proof. Each f_i is two-sided, so it can be written as $f_i = c_i \hat{f}_i x^{t_i}$, with $c_i \in \mathbb{F}^*$, monic $\hat{f}_i \in Z(\mathcal{R})$, and $t_i \in \mathbb{N}_0$. Since each $f_i \,|_r\, (x^n - a)$, the constant term of each f_i is non-zero. Thus $t_i = 0$ for all i. Then $f_i = c_i \hat{f}_i$, or $\hat{f}_i = c_i^{-1} f_i$. Then we write $x^n - a = c_1 \hat{f}_1 \cdots c_t \hat{f}_t = (\prod_{i=1}^{t} c_i) \hat{f}_1 \cdots \hat{f}_t$. Since each $\hat{f}_i$ is monic and $x^n - a$ is monic, $\prod_{i=1}^{t} c_i = 1$. Thus $x^n - a = \hat{f}_1 \cdots \hat{f}_t$. Further, $(\hat{f}_i) = (f_i)$, so each $\hat{f}_i$ is indeed central maximal. □

Thus we can convert our factorization from Prop. 6.2.7 into a factorization of distinct and pairwise coprime *central maximal* elements. (The fact that the central maximal elements are distinct and pairwise coprime is carried over by the construction in Prop. 6.2.9.) Thus when $\gcd(n, q) = 1$, we have a unique factorization (up to order) of pairwise coprime monic central maximal elements:

$$x^n - a = f_1^* f_2^* \cdots f_t^*. \tag{6.2.1}$$

In addition, we will consider the product of all but one of these central maximal elements. For a fixed factorization as in (6.2.1), put

$$\hat{f}_i^* := f_1^* f_2^* \cdots f_{i-1}^* f_{i+1}^* \cdots f_t^*. \tag{6.2.2}$$

Since these elements are all central, $\hat{f}_i^*$ is well-defined regardless of our choice of ordering. Note also that $\hat{f}_i^* f_i^* = f_i^* \hat{f}_i^* = x^n - a$. Further, $\gcrd(\hat{f}_i^*, f_i^*) = 1$ because $x^n - a$ has no repeated right roots in any extension field since $\gcd(n, q) = 1$.

Finding this central maximal factorization can be accomplished concretely by first searching for all monic right divisors of $x^n - a$ as previously described. One can then identify which factors are central by checking if they are elements of $\mathrm{Fix}_{\mathbb{F}}(\theta)[x^m]$. Finally, one can determine which of those central factors are central *maximal* by determining which ones have no non-trivial central factors themselves. (One needs only to test the central factors that have been previously found, as for a central element to right divide a right divisor g of $x^n - a$, it must also right divide $x^n - a$ itself.) Thus one can truly find the factorization in the following theorems, which generalize [14, Thm. 2.11].

Recall that in Section 2.2, we defined left quotient module $\mathcal{S}_a := \mathcal{R}/^{\bullet}(x^n - a)$, and demonstrated that $\mathcal{S}_a$ is even a ring exactly when $x^n - a$ is central. We now turn to our attention to the quotient ring $\mathcal{S}_a$.

Theorem 6.2.10 (see also [14, Thm. 2.11])**.** *Let* $\gcd(n, q) = 1$. *Let* $x^n - a$ *be factorized as in (6.2.1) and (6.2.2). Since* $\gcrd(\hat{f}_i^*, f_i^*) = 1$, *there exist polynomials* $b_i, c_i \in Z(\mathcal{R})$ *such that* $b_i \hat{f}_i^* + c_i f_i^* = 1$ *with* $\deg(b_i) < \deg(f_i^*)$. *Define* $e_i := b_i \hat{f}_i^* \in Z(\mathcal{R})$. *Thus* $\deg(e_i) < n$. *Then* $(\overline{e_i}) = (\overline{\hat{f}_i^*}) \subseteq \mathcal{S}_a$ *is a ring with identity* $\overline{e_i}$. *In particular,* $\overline{e_i}^2 = \overline{e_i}$.

Proof. Immediately, $(\overline{e_i}) \subseteq (\overline{\hat{f}_i^*})$. On the other hand, using $\overline{f_i^*}\,\overline{\hat{f}_i^*} = \overline{0}$ and centrality, we have $\overline{\hat{f}_i^*} = \overline{\hat{f}_i^*(b_i \hat{f}_i^* + c_i f_i^*)} = \overline{\hat{f}_i^* b_i \hat{f}_i^* + \hat{f}_i^* c_i f_i^*} = \overline{\hat{f}_i^* b_i \hat{f}_i^* + c_i \hat{f}_i^* f_i^*} = \overline{\hat{f}_i^* b_i \hat{f}_i^*}$ in $\mathcal{S}_a$, which implies that $(\hat{f}_i^*) \subseteq (\overline{e_i})$. Thus $(\overline{e_i}) = (\overline{\hat{f}_i^*})$.

It is a standard result in ring theory that an idempotent serves as the identity in the ring it generates, but we prove this in our case for completeness. Let $\overline{g e_i}$ be an element in $(\overline{e_i}) \subseteq \mathcal{S}_a$. We have $\overline{e_i}\,\overline{g e_i} = \overline{(1 - c_i f_i^*) g e_i} = \overline{g e_i - c_i f_i^* g b_i \hat{f}_i^*} = \overline{g e_i - c_i g b_i f_i^* \hat{f}_i^*} = \overline{g e_i}$. Taking $g := 1$, we see that $\overline{e_i}\,\overline{e_i} = \overline{e_i}$. As such, $\overline{g e_i}\,\overline{e_i} = \overline{g}\,\overline{e_i}\,\overline{e_i} = \overline{g e_i}$. So indeed, $\overline{e_i}$ is the identity of the ring $(\overline{e_i})$. □

Theorem 6.2.11 (see also [14, Thm. 2.11])**.** *Let* $\gcd(n, q) = 1$. *Let* $x^n - a$ *be factorized as in (6.2.1) and (6.2.2). Since* $\gcrd(\hat{f}_i^*, f_i^*) = 1$, *there exist polynomials* $b_i, c_i \in Z(\mathcal{R})$ *such that* $b_i \hat{f}_i^* + c_i f_i^* = 1$. *Define* $e_i := b_i \hat{f}_i^* \in Z(\mathcal{R})$. *Then:*

(1) $\overline{e_1}, \overline{e_2}, \ldots, \overline{e_t}$ *are mutually orthogonal non-zero elements in* $\mathcal{S}_a$, *i.e.,* $\overline{e_i}\,\overline{e_j} = 0$ *for all* $i \neq j$.

(2) $\overline{e_1} + \overline{e_2} + \cdots + \overline{e_t} = \overline{1}$ *in* $\mathcal{S}_a$.

(3) $\mathcal{S}_a = (\overline{e_1}) \oplus (\overline{e_2}) \oplus \cdots \oplus (\overline{e_t})$.

(4) For each $i = 1, 2, \ldots, t$, *the map* $\psi : \mathcal{R}/(f_i^*) \longrightarrow (\overline{e_i})$, $g + (f_i^*) \longmapsto \overline{ge_i}$, *is a well-defined isomorphism of rings.*

(5) $\mathcal{S}_a \cong \mathcal{R}/(f_1^*) \oplus \mathcal{R}/(f_2^*) \oplus \cdots \mathcal{R}/(f_t^*)$ *as rings.*

Proof. (1) Suppose $\overline{e_i} = \overline{0}$ for some $i \in \{1, 2, \ldots, t\}$, i.e., $b_i\hat{f}_i^* \in (x^n - a)$ in $\mathcal{R}$. Then $b_i\hat{f}_i^* \in (f)_i^*$. Thus $1 = b_i\hat{f}_i^* + c_if_i^* \in (f_i^*)$, a contradiction. Hence for each $i \in \{1, 2, \ldots, t\}, \overline{e_i} \neq \overline{0}$. For $i \neq j, e_ie_j = b_i\hat{f}_i^*b_j\hat{f}_j^* = b_ib_j\hat{f}_i^*\hat{f}_j^* \in (x^n - a)$, so $\overline{e_i}\,\overline{e_j} = 0$.

(2) For any $i = 1, \ldots, t$ and $i \neq j$, we see that each $\hat{f}_j^*$ is a left multiple of f_i^*, as is $b_i\hat{f}_i^* - 1 = c_if_i^*$. Thus we have $b_1\hat{f}_1^* + \cdots + b_t\hat{f}_t^* - 1 \in (f_i^*)$ for all $i \in \{1, 2, \ldots, t\}$, and the f_i^*'s are pairwise coprime. Therefore $b_1\hat{f}_1^* + \cdots + b_t\hat{f}_t^* - 1 \in (x^n - a)$, the product of the f_i^*'s. Thus $\overline{e_1} + \cdots + \overline{e_t} = \overline{1} \in \mathcal{S}_a$.

(3) This is a standard result in ring theory, but we provide a proof for completeness. Let $\overline{g} \in \mathcal{S}_a$. Then $\overline{g}$ can be represented as $\overline{g} = \overline{ge_1} + \overline{ge_2} + \cdots + \overline{ge_t}$ by (2). Since $ge_i \in (e_i)$ and our choice of $\overline{g}$ was arbitrary, $\mathcal{S}_a = (\overline{e_1}) + (\overline{e_2}) + \cdots + (\overline{e_t})$. For the directness of the sum, assume that $\overline{g_1} + \overline{g_2} + \cdots + \overline{g_t} = \overline{0}$, where each $\overline{g_i} \in (\overline{e_i})$. Multiplying by e_i on the right (or left) and using (1), we get $\overline{0} = \overline{g_1e_i} + \overline{g_2e_i} + \cdots + \overline{g_te_i} = \overline{g_ie_i} = \overline{g_i}$, for $i \in \{1, 2, \ldots, t\}$. So each $\overline{g_i} = \overline{0}$, and our sum is direct: $\mathcal{S}_a = (\overline{e_1}) \oplus (\overline{e_2}) \oplus \cdots \oplus (\overline{e_t})$.

(4) First, we show that ψ is a well-defined map. Suppose that $g + (f_i^*) = g' + (f_i^*) \in \mathcal{R}/(f_i^*)$. Then $g - g' \in (f_i^*)$; write $g - g' = df_i^*$ for some $d \in \mathcal{R}$. Then $\overline{(g - g')e_i} = \overline{(g - g')b_i\hat{f}_i^*} = \overline{df_i^*b_i\hat{f}_i^*} = \overline{db_if_i^*\hat{f}_i^*} = \overline{0}$. Thus ψ is a well-defined map.

Next, we check that ψ is indeed a ring homomorphism. Let $g, g' \in \mathcal{R}$. We easily see that ψ respects addition: $\psi(g + (f_i^*) + g' + (f_i^*)) = \psi(g + g' + (f_i^*)) = \overline{(g + g')e_i} = \overline{ge_i} + \overline{g'e_i} = \psi(g + (f_i^*)) + \psi(g' + (f_i^*))$. Further, we confirm that ψ respects multiplication: $\psi((g + (f_i^*))(g' + (f_i^*))) = \psi(gg' + (f_i^*)) = \overline{gg'e_i} = g\overline{g'e_i}$. Using Theorem 6.2.10, we see that $g\overline{g'e_i} = g\overline{e_ig'e_i} = \overline{ge_ig'e_i} = \overline{g_ie}\,\overline{g'e} = \psi((g + (f_i^*)))\psi((g' + (f_i^*)))$, as desired. Finally, we see that indeed $\psi(1 + (f_i^*)) = \overline{e_i}$, so ψ is a ring homomorphism.

Clearly ψ is a surjective ring homomorphism. For injectivity, let $g + (f_i^*) \in \mathcal{R}/(f_i^*)$ satisfy $\overline{ge_i} = \overline{0}$. Then $ge_i \in (x^n - a) \subseteq (f_i^*)$. Since f_i^* and $e_i = b_i\hat{f}_i^*$ are relatively prime, $g \in (f_i^*)$, or put differently, $g + (f_i^*) = (f_i^*)$. Thus the kernel of ψ is trivial. Hence ψ is injective, and thus an isomorphism.

(5) This follows immediately from (3) and (4). □

Remark 6.2.12. Each of the e_i in Theorems 6.2.10 & 6.2.11 is an idempotent modulo ${}^\bullet(x^n - a)$; this follows directly from Theorem 6.2.10. Remember that these two theorems only apply when $x^n - a \in Z(\mathcal{R})$ and $\gcd(n, q) = 1$.

In the commutative case, a polynomial $x^n - 1 \in \mathbb{F}_q[x]$ with $\gcd(n, q) = 1$ can be factored into distinct irreducible polynomials $f_1, f_2, \ldots, f_t$. Then the polynomials $\hat{f}_i = (x^n - 1)/f_i$ generate ideals $(\overline{\hat{f}_i})$ of $\mathbb{F}_q[x]/(x^n - 1)$. By [18, Thm. 4.3.8], these are all of the minimal ideals of $\mathbb{F}_q[x]/(x^n - 1)$. Further, the only idempotents in $(\overline{\hat{f}_i})$ are its (unique) generating idempotent $\hat{e_i}$ and 0. Finally, [18, Thm. 4.3.8] also gives us that if e is a nonzero idempotent in $\mathbb{F}_q[x]/(x^n - 1)$, then there is a subset T of $\{1, 2, \ldots, t\}$ such that $e = \sum_{i \in T} \hat{e_i}$ and $(\overline{e}) = \sum_{i \in T} (\overline{\hat{f}_i})$.

In the central non-commutative case, when the right divisor g of $x^n - a$ is itself central, we obtain a similar result.

Remark 6.2.13. If $f, g \in Z(\mathcal{R})$, then $\gcd(f, g)$ in the ring $Z(\mathcal{R})$ equals the $\operatorname{gcrd}(f, g)$ in $\mathcal{R}$. We see this by carrying out the right Euclidean algorithm in the skew polynomial ring. Because $f, g \in Z(\mathcal{R})$, each quotient and remainder from the algorithm must also be central. By Proposition 6.2.1, we also have $\gcd(f, g) = \operatorname{gcld}(f, g)$.

Proposition 6.2.14. *Let* $\gcd(n, q) = 1$ *and let* $f_1^* f_2^* \cdots f_t^*$ *be a factorization of* $x^n - a$ *into central maximal elements taken from (6.2.1) and let* g *be a proper central right divisor of* $x^n - a$*. Then we can factor* g *as* $g_1^* g_2^* \cdots g_s^*$*, where each* g_i *is some distinct* f_j^**.*

Proof. Since g is a proper central right divisor of $x^n - a$, we can factor it into central maximal elements $g_1^* g_2^* \cdots g_s^*$; each of these central maximal elements must also divide $x^n - a$. Because the central maximal elements that divide $x^n - a$ are distinct, each g_i is some distinct f_j. □

Note that without loss of generality, we can write $g = f_1^* f_2^* \cdots f_s^*$, where each f_i^* is central maximal, and $s < t$. This is because we can reorder the central maximal elements and by the uniqueness of (6.2.1).

Theorem 6.2.15. *Let* g *be a proper central right divisor of* $x^n - a$*, and suppose* $g = f_1^* f_2^* \cdots f_s^*$ *is a factorization of* g *into central maximal elements taken from (6.2.1). Then* $e_g := \sum_{i=s+1}^{t} e_i$ *(as in Theorem 6.2.10) is the unique central generating idempotent of* ${}^\bullet(\overline{g})$ *of degree less than* n*.*

Proof. We have such a factorization of g from Proposition 6.2.14. Observe that $g \mid_r \hat{f}_i^*$ for $s < i \leq t$. Clearly $g = \gcd(\hat{f}_{s+1}^*, \ldots, \hat{f}_t^*)$ in $Z(\mathcal{R})$, and by Remark 6.2.13, $g = \operatorname{gcrd}(\hat{f}_{s+1}^*, \ldots, \hat{f}_t^*)$ in our skew-polynomial ring. Then the elements $\overline{e_{s+1}}, \ldots \overline{e_t} \in {}^\bullet(\overline{g})$ all correspond to idempotent polynomials. Consider the polynomial $e_g := \sum_{i=s+1}^{t} e_i$. Each e_i has degree at most n, so $\deg(e_g) < n$ as well. Using the orthogonality and idempotency of the $\overline{e_i}$'s from Theorems 6.2.10 and 6.2.11, we see that

$$\overline{e_g}^2 = \overline{\left(\sum_{i=s+1}^{t} e_i\right)}^2 = \left(\sum_{i=s+1}^{t} \overline{e_i}\right)^2 = \sum_{i=s+1}^{t} \overline{e_i}^2 = \sum_{i=s+1}^{t} \overline{e_i} = \overline{e_g}.$$

Thus the polynomial e_g is idempotent modulo ${}^\bullet(x^n - a)$.

It remains to show that ${}^\bullet(\overline{e_g}) = {}^\bullet(\overline{g})$. Since $g \mid_r \hat{f}_i^*$ for $s < i \leq t$, we have that $e_g = \sum_{i=s+1}^{t} e_i = \sum_{i=s+1}^{t} b_i \hat{f}_i^*$ is a left multiple of g. Thus ${}^\bullet(\overline{e_g}) \subseteq {}^\bullet(\overline{g})$. Now let $j \in \{s+1, \ldots, t\}$ be given, and set $r := \hat{f}_j^* e_j$. We will again exploit the orthogonality and idempotency of the $\overline{e_i}$'s from Theorems 6.2.10 and 6.2.11, as well as the fact that $\sum_{i=1}^{t} \overline{e_i} = \overline{1}$. Using the fact that $(\overline{\hat{f}_j^*}) = (\overline{e_j})$, and that $\overline{e_j}$ is the identity of this ring, we compute:

$$\overline{\hat{f}_j^* - r e_g} = \overline{\hat{f}_j^* - \hat{f}_j^* e_j \sum_{i=s+1}^{t} e_i} = \overline{\hat{f}_j^* - \hat{f}_j^* e_j^2} = \overline{\hat{f}_j^* - \hat{f}_j^* e_j} = \overline{0}.$$

Thus each $\overline{\hat{f}_j^*} \in {}^\bullet(\overline{e_g})$ for $s+1 \leq j \leq t$. So $\overline{g} = \overline{\operatorname{gcrd}(\hat{f}_{s+1}^*, \ldots, \hat{f}_t^*)} \in {}^\bullet(\overline{e_g})$ as well, so ${}^\bullet(\overline{e_g}) = {}^\bullet(\overline{g})$ as desired.

Finally, we note that since e_g and g are central, ${}^\bullet(\overline{e_g}) = {}^\bullet(\overline{g}) = (\overline{e_g}) = (\overline{g})$. Let $\overline{r e_g s}$ be an element in the ring $(\overline{e_g})$. Multiplying by $\overline{e_g}$ on the left, we see that $\overline{e_g}\,\overline{r e_g s} = \overline{e_g r e_g s} = \overline{r s e_g e_g} = \overline{r s}\,\overline{e_g e_g} = \overline{r s}\,\overline{e_g} = \overline{r e_g s}$. Similarly, if we multiply by $\overline{e_g}$ on the right, we have $\overline{r e_g s}\,\overline{e_g} = \overline{r e_g s e_g} = \overline{r s e_g e_g} = \cdots = \overline{r e_g s}$. Thus $\overline{e_g}$ is the multiplicative identity of $(\overline{g})$. Suppose there exists another central generating idempotent of ${}^\bullet(\overline{g})$ of degree less than n; call it $\hat{e}$. Then by the previous argument, $\overline{\hat{e}}$ is also the multiplicative identity of $(\overline{g})$. By the uniqueness of the multiplicative identity of rings, $\overline{\hat{e}} = \overline{e_g}$, and by the uniqueness of coset representatives of degree less than n, we have $\hat{e} = e_g$. Thus e_g is the unique generating idempotent of ${}^\bullet(\overline{g})$ of degree less than n. $\square$

6.3 The General Case

As we showed in the previous section, we are able to find idempotents in the central case when $\gcd(n, q) = 1$. What about when $x^n - a$ is not central? In many cases, we

will require that $\gcrd(h,g)=1$, with Bézout identity $1=uh+vg$ satisfying $vg=gv$ and $\deg(v)<\deg(h)$. In fact, we make a strong conjecture based on the data in Appendix A that grants us these conditions. We feel confident in this conjecture, but have been unable to prove it.

Conjecture 6.3.1. If $\gcd(n,q)=\gcd(n,|\theta|)=1$ and $x^n-a=hg$ with constamonic g, then:

(1) $\gcrd(h,g)=1$.

(2) Let $1=uh+vg$ with $\deg(u)<\deg(g)$ and $\deg(v)<\deg(h)$. Then $vg=gv$.

Notice that the existence of u,v in Conjecture 6.3.1(2) comes from part (1) of the same conjecture by Remark 2.1.1(b). One can also see that if g is constamonic and $\gcrd(h,g)=1$, then $\lclm(h,g)=x^n-a$. (This is a special case of.) We now look to Appendix A for some particular examples.

Example 6.3.2. (1) Consider $x^5-1\in\mathbb{F}_8[x;\theta=\mathrm{Frob}]$. Observe that $\gcd(n,q)=\gcd(5,8)=1$ and $\gcd(n,|\theta|)=\gcd(5,3)=1$. Indeed, for any factorization $x^5-1=hg$ with $g_0=1,\gcrd(h,g)=1$. There are only two nontrivial right divisors: $x+1$ and $x^4+x^3+x^2+x+1$. For these, $1=(x^3+x)(x+1)+(1)(x^4+x^3+x^2+x+1)$, with $(x^3+x)(x+1)=(x+1)(x^3+1)$ and $(1)(x^4+x^3+x^2+x+1)=(x^4+x^3+x^2+x+1)(1)$. Conjecture 6.3.1 is supported by this example.

(2) Consider $x^{10}-\omega\in\mathbb{F}_4[x;\theta=\mathrm{Frob}]$, where $\omega^2+\omega=1$. Observe that $\gcd(n,q)=\gcd(10,4)=2$ and $\gcd(n,|\theta|)=\gcd(10,2)=2$. Despite not meeting the hypothesis of Conjecture 6.3.1, the conclusions still hold for any factorization $x^{10}-\omega=hg$ with $g_0=1$. Thus while $\gcd(n,q)=\gcd(n,|\theta|)=1$ may be a sufficient condition, it is certainly not necessary.

(3) Consider $x^8-1\in\mathbb{F}_4[x;\theta=\mathrm{Frob}]$, where $\omega^2+\omega=1$. Observe that $\gcd(n,q)=\gcd(8,4)=4$ and $\gcd(n,|\theta|)=\gcd(8,2)=2$. This polynomial satisfies neither the hypothesis nor (in general) the conclusions of Conjecture 6.3.1. For example, consider the factorization $x^8-1=(\omega x^7+x^6+\omega x^5+x^4+\omega x^3+x^2+\omega x+1)(\omega x+1)$. One computes that $\gcrd(\omega x^7+x^6+\omega x^5+x^4+\omega x^3+x^2+\omega x+1,\omega x+1)=x+\omega^2$, and there exist no $u,v\in\mathcal{R}$ such that $1=u(\omega x^7+x^6+\omega x^5+x^4+\omega x^3+x^2+\omega x+1)+v(\omega x+1)$.

(4) Consider $x^5-\omega\in\mathbb{F}_8[x;\theta=\mathrm{Frob}]$, where $\omega^3+\omega=1$. Observe that $\gcd(n,q)=\gcd(5,8)=1$ and $\gcd(n,|\theta|)=\gcd(5,3)=1$. We can factor $x^5-\omega=hg$, where $g=\omega^2x+1$ and $h=\omega^3x^4+\omega x^3+x^2+\omega^3x+\omega$. We have that $\gcrd(h,g)=1$. Set $u=\omega x+\omega^2$ and $v=\omega^3x^4+\omega^3x^3+x^2+\omega^5x+\omega$. Notice that $\deg(u)=\deg(g)$

and $\deg(v) = \deg(h)$. Then we have the identity $1 = uh + vg$. However, $vg = x^5 + \omega^2 x^4 + x^3 + \omega^6 x^2 + \omega^2 x + \omega \neq \omega x^5 + x^4 + \omega^4 x^3 + \omega^5 x^2 + x + \omega = gv$. Thus if we do not use the u and v of low degree as described in Conjecture 6.3.1(2), we do not have $vg = gv$.

(5) As in (4), consider $x^5 - \omega \in \mathbb{F}_8[x; \theta = \text{Frob}]$, where $\omega^3 + \omega = 1$. Rescaling our previous right divisor, we have a factorization $x^5 - \omega = hg$, where $g = x + \omega^5$ and $h = x^4 + \omega^3 x^3 + \omega x^2 + x + \omega^3$. We have that $\text{gcrd}(h, g) = 1$, but notice that g is no longer constamonic. Set $u = \omega^5$ and $v = \omega^5 x^3 + x^2 + \omega^5$. Then we have the identity $1 = uh + vg$ with degree restrictions satisfied. However, $vg = \omega^5 x^4 + \omega x^3 + \omega^6 x^2 + \omega^5 x + \omega^3 \neq \omega^3 x^4 + \omega x^3 + \omega^5 x^2 + \omega^3 x + \omega^3 = gv$. Thus if we do not have g constamonic, we do not have $vg = gv$.

We see in Appendix A that Conjecture 6.3.1 holds in each tested case where it applies; this is a non-trivial number of cases. We can find generating idempotents when these conclusions hold. Notice that we do not rely on $\gcd(n, q) = 1$ or a constamonic right divisor g for this proof, but we instead assume the conclusions of Conjecture 6.3.1.

Theorem 6.3.3. *Let $x^n - a = hg \in \mathcal{R}$ with $1 = uh + vg$ and $vg = gv$ for some $u, v \in \mathcal{R}$. Then vg is a generating idempotent of ${}^\bullet(\overline{g})$.*

Proof. We begin by showing that vg is an idempotent modulo ${}^\bullet(x^n - a)$. From Remark 2.1.1(d), we have $\deg(\text{lclm}(h, g)) = \deg(h) + \deg(g) - \deg(\text{gcrd}(h, g)) = n$. Thus there exist $w, z \in \mathcal{R}$ such that $wh = -zg$ (where $\deg(wh) = n$), or alternatively, $wh + zg = 0$.

Note that $\text{gcld}(w, z) = 1$; this is because if w and z had a common left divisor of degree greater than zero, then $\deg(\text{lclm}(h, g)) < n$, a contradiction. Therefore, there exist $\hat{w}, \hat{z} \in \mathcal{R}$ such that $1 = w\hat{w} + z\hat{z}$. Put $f := u\hat{w} + v\hat{z}$. Then we have

$$\begin{pmatrix} u & v \\ w & z \end{pmatrix} \begin{pmatrix} h & \hat{w} \\ g & \hat{z} \end{pmatrix} = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}. \tag{6.3.1}$$

We can multiply both sides of this equation by the matrix $\left(\begin{smallmatrix} 1 & -f \\ 0 & 1 \end{smallmatrix}\right)$ on the right to get

$$\begin{pmatrix} u & v \\ w & z \end{pmatrix} \begin{pmatrix} h & \hat{w} \\ g & \hat{z} \end{pmatrix} \begin{pmatrix} 1 & -f \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -f \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{6.3.2}$$

Define $\tilde{w} := h(-f) + \hat{w} \cdot 1$ and $\tilde{z} := g(-f) + \hat{z} \cdot 1$. This gives us

$$\begin{pmatrix} u & v \\ w & z \end{pmatrix} \begin{pmatrix} h & \tilde{w} \\ g & \tilde{z} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{6.3.3}$$

Now $\mathcal{R}$ is a right principal ideal domain, and thus is right noetherian. By [20, Prop. 1.13], any right noetherian ring is stably finite, so if $AB = I$, then $BA = I$, where A and B are square matrices with entries in $\mathcal{R}$. This gives us

$$\begin{pmatrix} h & \tilde{w} \\ g & \tilde{z} \end{pmatrix} \begin{pmatrix} u & v \\ w & z \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{6.3.4}$$

We use the matrix identities (6.3.3) and (6.3.4) to show that vg is an idempotent modulo ${}^\bullet(x^n - a)$: $(vg)^2 - vg = (1 - uh)vg - vg = vg - uhvg - vg = -uhvg = u\tilde{w}zg = -v\tilde{z}zg = -v(1-gv)v = -v(1-vg)g = -vuhg \in {}^\bullet(x^n - a)$, i.e., $(vg)^2 - vg \in {}^\bullet(x^n - a)$, so vg is an idempotent modulo ${}^\bullet(x^n - a)$.

To show that vg is a *generating* idempotent modulo ${}^\bullet(x^n - a)$, we show that $\overline{g} \in {}^\bullet(\overline{vg})$. By assumption, $uh + vg = 1$, and since $vg = gv$, we have $uh + gv = 1$. Multiplying by g on the right, we get $uhg + gvg = g$. Thus $g \equiv g(vg) \mod {}^\bullet(x^n - a)$, or $\overline{g} \in {}^\bullet(vg)$. Ergo vg is a generating idempotent modulo ${}^\bullet(x^n - a)$ of ${}^\bullet(\overline{g})$. □

This idempotent vg has some additional nice properties.

Proposition 6.3.4. *Let $x^n - a = hg \in \mathcal{R}$ with $1 = uh + vg$ for some $u, v \in \mathcal{R}$, and let $vg = gv$. Then vg serves as a right identity in ${}^\bullet(\overline{g})$ in the sense that $\overline{fvg} = \overline{f}$ for all $\overline{f} \in {}^\bullet(\overline{g})$.*

Proof. Since $\overline{f} \in {}^\bullet(\overline{g})$, we can write $\overline{f} = \overline{\tilde{f}g}$ for some $\tilde{f} \in \mathcal{R}$. Then $\overline{fvg} = \overline{\tilde{f}gvg} = \overline{\tilde{f}vgg} = \overline{\tilde{f}(1 - uh)g} = \overline{\tilde{f}g - \tilde{f}uhg} = \overline{f - \tilde{f}u(x^n - a)} = \overline{f}$, as desired. □

Remark 6.3.5. Under the same assumptions, vg does *not* necessarily serve as a left identity in ${}^\bullet(\overline{g})$; in general, $\overline{vgf} \neq \overline{f}$ for $\overline{f} \in {}^\bullet(\overline{g})$. Consider, for example, $x^5 - \omega \in \mathbb{F}_9[x; \theta = \text{Frob}]$, where $\omega^2 + \omega = 1$. We can factor $x^5 - \omega = hg$, with $h = 2\omega x^4 + x^3 + \omega x^2 + 2x + 2\omega$ and $g = \omega^3 x + 1$. Using Theorem 6.3.3, $vg = x^4 + \omega^3 x^3 + 2x^2 + 2\omega^3 x + 2$ is a generating idempotent modulo ${}^\bullet(x^5 - \omega)$ of ${}^\bullet(\overline{g})$. If we take $f = 2\omega g$, we can see that that $\overline{vgf} \neq \overline{f}$.

Recall that in Definition 6.1.2 being an idempotent modulo ${}^\bullet(x^n - a)$ is a property of a skew-polynomial $f \in \mathcal{R}$, not of a coset $\overline{f} \in {}^\bullet(\overline{g})$. In general, we do not have that this property is independent of choice of coset representative. However, as we show

next, in the case of the generating idempotent vg that we get from Theorem 6.3.3, any other polynomial in the coset $\overline{vg}$ is also an idempotent modulo ${}^\bullet(x^n - a)$.

Proposition 6.3.6. *Let $x^n - a = hg \in \mathcal{R}$ with $1 = uh + vg$ for some $u, v \in \mathcal{R}$, and let $vg = gv$. Let $e := vg + t(x^n - a)$ for some $t \in \mathcal{R}$. Then e is also a generating idempotent of ${}^\bullet(\overline{g})$. As a consequence, we may call $\overline{vg}$ a generating idempotent of ${}^\bullet(\overline{g})$.*

Proof. Recall that vg is an idempotent modulo ${}^\bullet(x^n - a)$ by Theorem 6.3.3, and thus $vgvg - vg \in {}^\bullet(x^n - a)$. Observe that

$$\begin{aligned}
\overline{e^2} &= \overline{vgvg + vgt(x^n - a) + t(x^n - a)vg + t(x^n - a)t(x^n - a)} \\
&= \overline{vgvg + t(x^n - a)vg} = \overline{vgvg + thgvg} = \overline{vgvg + thvgg} \\
&= \overline{vgvg + th(1 - uh)g} = \overline{vgvg + thg - thuhg} \\
&= \overline{vgvg + t(x^n - a) - thu(x^n - a)} = \overline{vgvg}.
\end{aligned}$$

Then we can easily compute:

$$\overline{e^2 - e} = \overline{e^2} - \overline{e} = \overline{vgvg} - \overline{vg + t(x^n - a)} = \overline{vgvg - vg} = \overline{0}.$$

So $e^2 - e \in {}^\bullet(x^n - a)$, as desired.

Further, $\overline{e} = \overline{vg}$, and by Theorem 6.3.3 we have ${}^\bullet(\overline{e}) = {}^\bullet(\overline{vg}) = {}^\bullet(\overline{g})$. Thus e is a generating idempotent modulo ${}^\bullet(x^n - a)$ of ${}^\bullet(\overline{g})$. □

So, we are able to find generating idempotents if Conjecture 6.3.1 holds. In Example 6.1.6(1), the eight generating idempotents modulo ${}^\bullet(x^9 - 1)$ which correspond to idempotent cosets are the idempotents found using the method in Theorem 6.3.3. And by Proposition 6.3.6, their cosets are idempotent. Notice, though, that these are not unique generating idempotents, as in the same example, there are four other idempotent elements of degree less than 9.

We now attempt to find more generating idempotents. In [18, Thm. 4.3.7], we see that if $\mathcal{C}_1$ and $\mathcal{C}_2$ are cyclic codes from the commutative case with respective generating polynomials $\overline{g_1}$ and $\overline{g_2}$ and generating idempotents $\overline{e_1}$ and $\overline{e_2}$, then $\mathcal{C}_1 \cap \mathcal{C}_2$ is a cyclic code with generator polynomial $\overline{\operatorname{lcm}(g_1, g_2)}$ and generating idempotent $\overline{e_1 e_2}$, and $\mathcal{C}_1 + \mathcal{C}_2$ is a cyclic code with generator polynomial $\overline{\gcd(g_1, g_2)}$ and generating idempotent $\overline{e_1 + e_2 - e_1 e_2}$. It turns out that skew-cyclic codes behave similarly, but not identically with regard to idempotents. In the commutative case, idempotent elements are cosets. Because idempotents are defined generally as polynomials in the skew-cyclic case, our generalization looks at polynomials, not cosets.

Theorem 6.3.7. *Let $x^n - a = h_1 g_1 = h_2 g_2 \in \mathcal{R}$. Put $\mathcal{C}_1 := \mathfrak{v}_a({}^\bullet(\overline{g_1}))$ and $\mathcal{C}_2 := \mathfrak{v}_a({}^\bullet(\overline{g_2}))$. Then:*

(1) $\mathcal{C}_1 \cap \mathcal{C}_2$ is a (θ, a)-constacyclic code generated by $\mathrm{lclm}(g_1, g_2)$.

(2) $\mathcal{C}_1 + \mathcal{C}_2$ is a (θ, a)-constacyclic code generated by $\mathrm{gcrd}(g_1, g_2)$.

Proof. (1) Let $c \in \mathcal{C}_1 \cap \mathcal{C}_2$. Then there exist $t_1, t_2 \in \mathcal{R}$ such that $\mathfrak{p}_a(c) = t_1\overline{g_1} = t_2\overline{g_2}$. Since $\mathfrak{p}_a(c)$ is a left multiple of $\overline{g_1}$ and $\overline{g_2}$, it must be a left multiple of $\overline{\mathrm{lclm}(g_1, g_2)}$. Thus $\mathcal{C}_1 \cap \mathcal{C}_2 \subseteq \mathfrak{v}_a({}^\bullet(\overline{\mathrm{lclm}(g_1, g_2)}))$. On the other hand, let $c \in \mathfrak{v}_a({}^\bullet(\overline{\mathrm{lclm}(g_1, g_2)}))$. Then $\mathfrak{p}_a(c)$ is a left multiple of both $\overline{g_1}$ and $\overline{g_2}$, so $c \in \mathcal{C}_1 \cap \mathcal{C}_2$. Therefore $\mathcal{C}_1 \cap \mathcal{C}_2 = \mathfrak{v}_a({}^\bullet(\overline{\mathrm{lclm}(g_1, g_2)}))$, as desired.

(2) We have the Bézout identity $\mathrm{gcrd}(g_1, g_2) = ug_1 + vg_2$ for some $u, v \in \mathcal{R}$. Then for any $t \in \mathcal{R}, t \cdot \mathrm{gcrd}(g_1, g_2) = tug_1 + tvg_2$, so $\mathfrak{v}_a({}^\bullet(\overline{\mathrm{gcrd}(g_1, g_2)})) \subseteq \mathcal{C}_1 + \mathcal{C}_2$. On the other hand, $\mathrm{gcrd}(g_1, g_2)$ is a right divisor of both g_1 and g_2, so $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathfrak{v}_a({}^\bullet(\overline{\mathrm{gcrd}(g_1, g_2)}))$, and thus $\mathcal{C}_1 + \mathcal{C}_2 \subseteq \mathfrak{v}_a({}^\bullet(\overline{\mathrm{gcrd}(g_1, g_2)}))$. Thus $\mathcal{C}_1 + \mathcal{C}_2 = \mathfrak{v}_a({}^\bullet(\overline{\mathrm{gcrd}(g_1, g_2)}))$. □

But what about idempotents modulo ${}^\bullet(x^n - a)$? In the commutative case, the generating idempotents of $\mathcal{C}_1 \cap \mathcal{C}_2$ and $\mathcal{C}_1 + \mathcal{C}_2$ are $\overline{e_1 e_2}$ and $\overline{e_1 + e_2 - e_1 e_2}$ respectively, where $\overline{e_1}$ and $\overline{e_2}$ are the generating idempotents for $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively [18, Thm. 4.3.7]. Immediately we see that these polynomials do not work in the skew-constacyclic case. We examine two examples:

Example 6.3.8. (1) Consider $x^3 - 1 \in \mathcal{R} = \mathbb{F}_8[x, \theta = \mathrm{Frob}]$, where $\omega^3 + \omega = 1$, which has right divisors $g_1 = \omega x^2 + \omega^5 x + 1$ and $g_2 = \omega^6 x^2 + \omega^2 x + 1$. Let $\mathcal{C}_1 := \mathfrak{v}_a({}^\bullet(\overline{g_1})), \mathcal{C}_2 := \mathfrak{v}_a({}^\bullet(\overline{g_2}))$. (Note that $\mathrm{gcrd}(n, m) = 3$.) By Theorem 6.3.7, $\mathcal{C}_1 \cap \mathcal{C}_2 = \mathfrak{v}_a({}^\bullet(\overline{\mathrm{lclm}(g_1, g_2)}))$. In this example, $\mathrm{lclm}(g_1, g_2) = x^3 - 1$, so $\mathcal{C}_1 \cap \mathcal{C}_2 = \{0\}$. In Appendix A, we see that for any factorization $x^3 - 1 = hg \in \mathcal{R}$ with g constamonic, $\mathrm{gcrd}(h, g) = 1$ and $vg = gv$, where $u, v \in \mathcal{R}$ are the unique polynomials such that $1 = uh + vg$ and $\deg(v) < \deg(h), \deg(u) < \deg(g)$. (Note that this is true despite $\gcd(n, |\theta|) = \gcd(3, 3) = 3$.) Indeed, from g_1 we get $v_1 = 1$, and from g_2 we also get $v_2 = 1$. By Theorem 6.3.3, $v_1 g_1 = g_1$ and $v_2 g_2 = g_2$ are generating idempotents modulo ${}^\bullet(x^3 - 1)$ of ${}^\bullet(\overline{g_1})$ and ${}^\bullet(\overline{g_2})$ respectively. However, $g_1 g_2 \neq g_2 g_1$, so we cannot use the method from the commutative case to compute a *unique* generating idempotent for $\mathcal{C}_1 \cap \mathcal{C}_2$.

Further, one can check that $g_1 g_2$ is not an idempotent modulo ${}^\bullet(x^3 - 1)$. And while $g_2 g_1$ is an idempotent modulo ${}^\bullet(x^3 - 1)$, it is not a *generating* idempotent modulo ${}^\bullet(x^3 - 1)$ of ${}^\bullet(\overline{\mathrm{lclm}(g_1, g_2)})$, as $\overline{g_2 g_1} = \overline{\omega^4 x^2 + \omega x + \omega^3} = \overline{\omega^3 g_1} \notin$

$^\bullet(\overline{\mathrm{lclm}(g_1, g_2)}) = {}^\bullet(\overline{x^3 - 1}) = {}^\bullet(\overline{0})$. So this method cannot in general be used to find generating idempotents.

(2) Consider $x^2 - 1 \in \mathcal{R} = \mathbb{F}_9[x, \theta = \mathrm{Frob}]$, where $\omega^2 + \omega = 1$, which has right divisors $g_1 = 2x + 1$ and $g_2 = \omega^2 x + 1$. Note that $\mathrm{gcrd}(n, m) = 2$.) Let $\mathcal{C}_1 := \mathfrak{v}_a({}^\bullet(\overline{g_1})), \mathcal{C}_2 := \mathfrak{v}_a({}^\bullet(\overline{g_2}))$. By Theorem 6.3.7, $\mathcal{C}_1 + \mathcal{C}_2 = \mathfrak{v}_a({}^\bullet(\overline{\mathrm{gcrd}(g_1, g_2)}))$. In this example, $\mathrm{gcrd}(g_1, g_2) = 1$, so $\mathcal{C}_1 + \mathcal{C}_2 = \mathbb{F}_9^2$. Again, we see in Appendix A that for any factorization $x^2 - 1 = hg \in \mathcal{R}$ with $g_0 = 1, \mathrm{gcrd}(h, g) = 1$ and $vg = gv$, where $u, v \in \mathcal{R}$ are the unique polynomials such that $1 = uh + vg$ and $\deg(v) < \deg(h), \deg(u) < \deg(g)$. (Note that this is true despite $\gcd(n, |\theta|) = \gcd(2, 2) = 2$.) Indeed, from g_1 we get $v_1 = 2$, and from g_2 we also get $v_2 = 2$. By Theorem 6.3.3, $v_1 g_1 = g_1$ and $v_2 g_2 = g_2$ are generating idempotents modulo $^\bullet(x^2 - 1)$ of $^\bullet(\overline{g_1})$ and $^\bullet(\overline{g_2})$ respectively. However, $2g_1 + 2g_2 - 2g_1 2g_2 \neq 2g_2 + 2g_1 - 2g_2 2g_1$, so we are clearly unable to compute a *unique* generating idempotent for $\mathcal{C}_1 + \mathcal{C}_2$ using the method from the commutative case.

Further, one can check that neither $2g_1 + 2g_2 - 2g_1 2g_2$ nor $2g_2 + 2g_1 - 2g_2 2g_1$ is an idempotent modulo $^\bullet(x^2 - 1)$. So this method cannot in general be used to find generating idempotents.

So we see that the constructions $\mathcal{C}_1 \cap \mathcal{C}_2$ and $\mathcal{C}_1 + \mathcal{C}_2$ do not behave so nicely in the skew-constacyclic case. However, we notice in each of these examples, we did not have $\gcd(n, |\theta|) = 1$. Looking at the data in Appendix A, as well as other experiments in Maple, we formulate an additional conjecture.

Conjecture 6.3.9. Let $\gcd(n, q) = \gcd(n, |\theta|) = 1$ and $x^n - a = h_1 g_1 = h_2 g_2$ be two right coprime factorizations with constamonic g_1, g_2. Furthermore let $1 = u_i h_i + v_i g_i$ with $\deg(v_i) < \deg(h_i), \deg(u_i) < \deg(g_i)$ and $v_i g_i = g_i v_i$. Then

(1) $g_1 g_2 = g_2 g_1$.

(2) $v_1 g_1 v_2 g_2 = v_2 g_2 v_1 g_1$.

Briefly, this means that the idempotents from Theorem 6.2.11 for two factorizations of $x^n - a$ commute. With this assumption, we are able to show that the commutative formulation for idempotents modulo $^\bullet(x^n - a)$ partially generalizes to the skew-constacyclic case.

Proposition 6.3.10. *Let e_1, e_2 be idempotents modulo $^\bullet(x^n - a)$ such that $e_1 e_2 = e_2 e_1$. Then*

(1) $e_1 e_2$ is an idempotent modulo $^\bullet(x^n - a)$.

(2) $e_1 + e_2 - e_1 e_2$ is an idempotent modulo $^\bullet(x^n - a)$.

Proof. Let e_1, e_2 be as described.
(1) $(e_1e_2)^2 - e_1e_2 = e_1e_2e_1e_2 - e_1^2e_2 - e_1e_2 + e_1^2e_2 = e_1^2(e_2^2 - e_2) + e_2(e_1^2 - e_1) \in {}^\bullet(x^n - a)$.
(2) We compute:

$$\begin{aligned}(e_1 + e_2 - e_1e_2)^2 - (e_1 + e_2 - e_1e_2) \\ &= e_1^2 + e_1e_2 - e_1^2e_2 + e_2e_1 + e_2^2 - e_2e_1e_2 \\ &\qquad - e_1e_2e_1 - e_1e_2^2 + e_1e_2e_1e_2 - e_1 - e_2 + e_1e_2 \\ &= (e_1^2 - e_1) + (e_2^2 - e_2) + 3e_1e_2 - 2e_1e_2^2 - 2e_1^2e_2 + e_1^2e_2^2 \\ &\equiv -2e_1(e_2^2 - e_2) - e_2(e_1^2 - e_1) + e_1^2(e_2^2 - e_2) \mod {}^\bullet(x^n - a) \\ &\equiv 0 \mod {}^\bullet(x^n - a).\end{aligned}$$

□

While we believe that these idempotents are generating idempotents of their respective codes, it remains to be shown. However, we can show that they are generating idempotents when we reintroduce some familiar hypotheses

Theorem 6.3.11. *Let $x^n - a = h_1g_1 = h_2g_2$, with $1 = u_1h_1 + v_1g_1 = u_2h_2 + v_2g_2$ for some $u_1, v_1, u_2, v_2 \in \mathcal{R}$, where $e_1 := v_1g_1 = g_1v_1$ and $e_2 = v_2g_2 = g_2v_2$ are generating idempotents of ${}^\bullet(\overline{g_1})$ and ${}^\bullet(\overline{g_2})$, respectively. Suppose also that $e_1e_2 = e_2e_1$. Then*
(1) ${}^\bullet(\overline{e_1e_2}) = {}^\bullet(\overline{lclm(g_1, g_2)})$.
(2) ${}^\bullet(\overline{e_1 + e_2 - e_1e_2}) = {}^\bullet(\overline{gcrd(g_1, g_2)})$.

Proof. (1) Notice that e_1e_2 is a left multiple of both g_1 and g_2. Thus ${}^\bullet(\overline{e_1e_2}) \subseteq {}^\bullet(\overline{\mathrm{lclm}(g_1, g_2)})$. Now let $\overline{t} \in {}^\bullet(\overline{\mathrm{lclm}(g_1, g_2)}) = {}^\bullet(\overline{g_1}) \cap {}^\bullet(\overline{g_2}) = {}^\bullet(\overline{e_1}) \cap {}^\bullet(\overline{e_2})$. Then $\overline{t} = \overline{s_1v_1g_1} = \overline{s_2v_2g_2}$ for some $s_1, s_2 \in \mathcal{R}$. Then for some $w \in \mathcal{R}$ we can write $s_1v_1g_1 = s_2v_2g_2 + w(x^n - a)$. We then compute:

$$\begin{aligned}s_1v_1g_1v_2g_2 &= s_2v_2g_2v_2g_2 + w(x^n - a)v_2g_2 = s_2v_2g_2v_2g_2 + wh_2g_2v_2g_2 \\ &= s_2v_2v_2g_2g_2 + wh_2v_2g_2g_2 = s_2v_2(1 - u_2h_2)g_2 + wh_2(1 - u_2h_2)g_2 \\ &= s_2v_2g_2 - s_2v_2u_2h_2g_2 + wh_2g_2 - wh_2u_2h_2g_2 \equiv s_2v_2g_2 \mod {}^\bullet(x^n - a) \\ &\equiv t \mod {}^\bullet(x^n - a).\end{aligned}$$

So $\overline{t} = \overline{s_1e_1e_2} \in {}^\bullet(\overline{e_1e_2})$. Thus ${}^\bullet(\overline{e_1e_2}) = {}^\bullet(\overline{\mathrm{lclm}(g_1, g_2)})$.

(2) Notice that each term of $e_1 + e_2 - e_1e_2 = v_1g_1 + v_2g_2 - v_1g_1v_2g_2$ is clearly right divisible by $\mathrm{gcrd}(g_1, g_2)$. Thus ${}^\bullet(\overline{e_1 + e_2 - e_1e_2}) \subseteq {}^\bullet(\overline{\mathrm{gcrd}(g_1, g_2)})$. We now want to show that $\overline{g_1}, \overline{g_2} \in {}^\bullet(\overline{e_1 + e_2 - e_1e_2})$. Put $s := g_1e_1$ and compute using Propo-

sition 6.3.4:

$$\begin{aligned}
\overline{g_1 - s(e_1 + e_2 - e_1e_2)} &= \overline{g_1 - se_1 - se_2 + se_1e_2} \\
&= \overline{g_1 - g_1e_1e_1 - g_1e_1e_2 + g_1e_1e_1e_2} \\
&= \overline{g_1 - g_1e_1e_1 - g_1e_2e_1 + g_1e_2e_1e_1} \\
&= \overline{g_1 - g_1e_1e_1 - g_1e_2e_1 + g_1e_2e_1} \\
&= \overline{g_1 - g_1e_1e_1} = \overline{g_1 - g_1e_1} \\
&= \overline{g_1 - g_1} = \overline{0}.
\end{aligned}$$

Thus $\overline{g_1} = \overline{s(e_1 + e_2 - e_1e_2)} \in {}^\bullet(\overline{e_1 + e_2 - e_1e_2})$. By taking $s := g_2e_2$, we can similarly show that $\overline{g_2} \in {}^\bullet(\overline{e_1 + e_2 - e_1e_2})$. Thus ${}^\bullet(\overline{g_1}) + {}^\bullet(\overline{g_2}) = {}^\bullet(\overline{\mathrm{gcrd}(g_1, g_2)}) = {}^\bullet(\overline{e_1 + e_2 - e_1e_2})$. □

We have created new (θ, a)-constacyclic codes by intersecting and summing two existing codes. We can also decompose a vector space into the direct sum of two (θ, a)-constacyclic codes and, in certain cases, find their generating idempotents.

Corollary 6.3.12. *Let $x^n - a = hg \in \mathcal{R}$, with g constamonic and gcrd$(h, g) = 1$. Put $\mathcal{C}_g := \mathfrak{v}_a({}^\bullet(\overline{g}))$ and $\mathcal{C}_h := \mathfrak{v}_a({}^\bullet(\overline{h}))$. Then $\mathbb{F}_q^n = \mathcal{C}_g \oplus \mathcal{C}_h$.*

Proof. Notice that since g is constamonic, 3.1.4 gives us that $h \,|_r\, (x^n - a)$. By Theorem 6.3.7(2), $\mathcal{C}_g + \mathcal{C}_h$ is a (θ, a)-constacyclic code generated by $\mathrm{gcrd}(h, g) = 1$. Thus ${}^\bullet(\overline{g}) + {}^\bullet(\overline{h}) = {}^\bullet(\overline{1})$, so $\mathcal{C}_g + \mathcal{C}_h = \mathbb{F}_q^n$.

Further, we inspect the dimensions of our codes: $\dim(\mathcal{C}_g) + \dim(\mathcal{C}_h) = (n - \deg(g)) + (n - \deg(h)) = 2n - (\deg(g) + \deg(h)) = 2n - n = n = \dim(\mathbb{F}_q^n)$, so $\mathcal{C}_g \oplus \mathcal{C}_h = \mathbb{F}_q^n$. □

Remark 6.3.13. (1) Given a factorization $x^n - a = hg$ with $\mathrm{gcrd}(h, g) = 1$ and g constamonic, and $\mathcal{C}_g, \mathcal{C}_h$ defined as above, $\mathcal{C}_h$ is not necessarily the only (θ, a)-constacyclic code $\mathcal{C}$ such that $\mathcal{C}_g \oplus \mathcal{C} = \mathbb{F}_q^n$. For example, consider $x^6 - 1 = hg \in \mathbb{F}_8[x; \theta = \mathrm{Frob}]$ with $g = \omega x^2 + 1$. There are 16 distinct $(\theta, 1)$-constacyclic codes $\mathcal{C}$ such that $\mathcal{C}_g \oplus \mathcal{C} = \mathbb{F}_b^6$, as determined by an exhaustive search.

(2) Given a factorization $x^n - a = hg$ with $\mathrm{gcrd}(h, g) = 1$ and g constamonic, let $u, v \in \mathcal{R}$ such that $1 = uh + vg$. If $vg = gv$, then by Theorem 6.3.3, vg is a generating idempotent modulo ${}^\bullet(x^n - a)$ of ${}^\bullet(\overline{g})$. Similarly, if $uh = hu$, then uh is a generating idempotent modulo ${}^\bullet(x^n - a)$ of ${}^\bullet(\overline{h})$. Note that $vg = gv$ and $uh = hu$ are typically independent conditions. For example, consider $x^9 - \omega = hg \in \mathbb{F}_4[x; \theta =$

Frob] with $g = \omega^2 x + 1$. Then $h = \omega x^8 + x^7 + \omega x^6 + x^5 + \omega x^4 + x^3 + \omega x^2 + x + \omega$, and $u = \omega^2, v = \omega^2 x^7 + \omega^2 x^5 + \omega^2 x^3 + \omega^2 x$ satisfy $1 = uh + vg$. While $vg = gv, uh \neq hu$.

If we restrict ourselves to $x^n - a \in Z(\mathcal{R})$, we can guarantee a relationship between the commutativity of v and g and the commutativity of u and h from Remark 6.3.13(2). In Theorem 6.2.10, we explored what happens in the central case with $\gcd(n, q) = 1$. We now drop the restriction that $\gcd(n, q) = 1$.

Proposition 6.3.14. *Let $x^n - a = hg \in Z(\mathcal{R})$, and let $u, v \in \mathcal{R}$ be such that $1 = uh + vg$. Then $vg = gv$ if and only if $uh = hu$.*

Proof. Suppose $vg = gv$. Then $1 = uh + vg = uh + gv$. Multiplying either side by h on the *left* and g on the *right*, we get $hg = huhg + hgvg$, or equivalently $x^n - a = hu(x^n - a) + (x^n - a)vg$. Since $x^n - a$ is central, we can commute it to the right of each product and remove it via right cancellation. We are left with $1 = hu + vg$. Since $1 = uh + vg$ as well, it follows that $uh = hu$ as desired. The opposite direction follows easily by taking uh for vg and vice versa. □

So in this case, we can easily find either both or neither generating idempotent modulo $^\bullet(x^n - a)$ for $\mathcal{C}_g \oplus \mathcal{C}_h = \mathbb{F}_q^n$ based solely on whether or not $vg = gv$.

Appendix A: Data on Factorizations

The following table gives data on factorizations $x^n - a = hg \in \mathbb{F}_q[x;\theta]$. We are considering only the factorizations in which the right divisor g is constamonic, i.e., it has constant term 1. The first five columns are self-explanatory; they define the parameters q, θ, n, and a. The "Commute" column lists whether or not *all* constamonic right divisors of $x^n - a$ commute with each other pairwise. The "gcrd = 1" column lists whether or not $\text{gcrd}(h, g) = 1$ for *every* factorization $x^n - a = hg$. Regardless of the value of the greatest common right divisor, we can always write the Bézout identity $\text{gcrd}(h, g) = uh = vg$ with $\deg(u) < \deg(g)$ and $\deg(v) < \deg(h)$. The column "$vg = gv$" lists whether or not *all* right divisors g commute with their respective polynomials v from this particular Bézout identity.

The next two columns list the given greatest common right divisors. In the case that both $\gcd(n, q) = 1$ and $\gcd(n, |\theta|) = 1$, the row is listed in boldface; this corresponds exactly to those cases when the hypotheses of Conjecture 6.3.1 are met. Note that in each of these bold rows, both the "gcrd = 1" and "$vg = gv$" columns list "Yes," supporting Conjecture 6.3.1.

The final column gives the total number of constamonic right divisors of the given polynomial $x^n - a$. Note that this number is always at least 2, as the polynomials 1 and $-a^{-1}x^n + 1$ are always trivial right divisors of $x^n - a$. We want to know that there are a non-trivial number of factorizations when we have $\gcd(n, q) = 1$ and $\gcd(n, |\theta|) = 1$. For instance, each $x^{15} - a \in \mathbb{F}_4[x;\theta = \text{Frob}]$ has 32 constamonic right divisors. We often see many factorizations of central $x^n - a$. For example, $x^8 - 1 \in Z(\mathbb{F}_9[x;\theta = \text{Frob}])$ has 432 constamonic right divisors. Recall though that in Section 6.2, specifically Theorem 6.2.10 and following, we are only interested in central right divisors of $x^n - a$.

|F|=q	θ	|θ|	n	a	Commute	gcrd=1	vg=gv	gcd(n,q)	gcd(n,|θ|)	# of divisors
4	Frob	2	2	1	No	No	Yes	2	2	5
4	Frob	2	2	w	Yes	Yes	Yes	2	2	2
4	Frob	2	2	w^2	Yes	Yes	Yes	2	2	2
4	**Frob**	**2**	**3**	**1**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
4	**Frob**	**2**	**3**	**w**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
4	**Frob**	**2**	**3**	**w^2**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
4	Frob	2	4	1	No	No	No	4	2	15
4	Frob	2	4	w	Yes	No	Yes	4	2	3
4	Frob	2	4	w^2	Yes	No	Yes	4	2	3
4	**Frob**	**2**	**5**	**1**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
4	**Frob**	**2**	**5**	**w**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
4	**Frob**	**2**	**5**	**w^2**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
4	Frob	2	6	1	No	No	No	2	2	35
4	Frob	2	6	w	Yes	Yes	Yes	2	2	2
4	Frob	2	6	w^2	Yes	Yes	Yes	2	2	2
4	**Frob**	**2**	**7**	**1**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
4	**Frob**	**2**	**7**	**w**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
4	**Frob**	**2**	**7**	**w^2**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
4	Frob	2	8	1	No	No	No	4	2	83
4	Frob	2	8	w	Yes	No	Yes	4	2	5
4	Frob	2	8	w^2	Yes	No	Yes	4	2	5
4	**Frob**	**2**	**9**	**1**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
4	**Frob**	**2**	**9**	**w**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
4	**Frob**	**2**	**9**	**w^2**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
4	Frob	2	10	1	No	No	No	2	2	95
4	Frob	2	10	w	Yes	Yes	Yes	2	2	8
4	Frob	2	10	w^2	Yes	Yes	Yes	2	2	8
4	**Frob**	**2**	**11**	**1**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
4	**Frob**	**2**	**11**	**w**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
4	**Frob**	**2**	**11**	**w^2**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
4	Frob	2	12	1	No	No	No	4	2	495
4	Frob	2	12	w	Yes	No	Yes	4	2	3
4	Frob	2	12	w^2	Yes	No	Yes	4	2	3
4	**Frob**	**2**	**13**	**1**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
4	**Frob**	**2**	**13**	**w**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
4	**Frob**	**2**	**13**	**w^2**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
4	Frob	2	14	1	No	No	No	2	2	605
4	Frob	2	14	w	Yes	Yes	Yes	2	2	8
4	Frob	2	14	w^2	Yes	Yes	Yes	2	2	8
4	**Frob**	**2**	**15**	**1**	**Yes**	**Yes**	**Yes**	**1**	**1**	**32**
4	**Frob**	**2**	**15**	**w**	**Yes**	**Yes**	**Yes**	**1**	**1**	**32**
4	**Frob**	**2**	**15**	**w^2**	**Yes**	**Yes**	**Yes**	**1**	**1**	**32**

|F|=q	θ	|θ|	n	a	Commute	gcrd=1	vg=gv	gcd(n,q)	gcd(n,|θ|)	# of divisors
8	Frob, Frob^2	3	2	1	Yes	No	Yes	2	1	3
8	Frob, Frob^2	3	2	w	Yes	No	Yes	2	1	3
8	Frob, Frob^2	3	2	w^2	Yes	No	Yes	2	1	3
8	Frob, Frob^2	3	2	w^3	Yes	No	Yes	2	1	3
8	Frob, Frob^2	3	2	w^4	Yes	No	Yes	2	1	3
8	Frob, Frob^2	3	2	w^5	Yes	No	Yes	2	1	3
8	Frob, Frob^2	3	2	w^6	Yes	No	Yes	2	1	3
8	Frob, Frob^2	3	3	1	No	Yes	Yes	1	3	16
8	Frob, Frob^2	3	3	w	Yes	Yes	Yes	1	3	2
8	Frob, Frob^2	3	3	w^2	Yes	Yes	Yes	1	3	2
8	Frob, Frob^2	3	3	w^3	Yes	Yes	Yes	1	3	2
8	Frob, Frob^2	3	3	w^4	Yes	Yes	Yes	1	3	2
8	Frob, Frob^2	3	3	w^5	Yes	Yes	Yes	1	3	2
8	Frob, Frob^2	3	3	w^6	Yes	Yes	Yes	1	3	2
8	Frob, Frob^2	3	4	1	Yes	No	Yes	4	1	5
8	Frob, Frob^2	3	4	w	Yes	No	No	4	1	5
8	Frob, Frob^2	3	4	w^2	Yes	No	No	4	1	5
8	Frob, Frob^2	3	4	w^3	Yes	No	No	4	1	5
8	Frob, Frob^2	3	4	w^4	Yes	No	No	4	1	5
8	Frob, Frob^2	3	4	w^5	Yes	No	No	4	1	5
8	Frob, Frob^2	3	4	w^6	Yes	No	No	4	1	5
8	**Frob, Frob^2**	**3**	**5**	**1**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
8	**Frob, Frob^2**	**3**	**5**	**w**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
8	**Frob, Frob^2**	**3**	**5**	**w^2**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
8	**Frob, Frob^2**	**3**	**5**	**w^3**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
8	**Frob, Frob^2**	**3**	**5**	**w^4**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
8	**Frob, Frob^2**	**3**	**5**	**w^5**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
8	**Frob, Frob^2**	**3**	**5**	**w^6**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
8	Frob, Frob^2	3	6	1	No	No	No	2	3	129
8	Frob, Frob^2	3	6	w	Yes	No	Yes	2	3	3
8	Frob, Frob^2	3	6	w^2	Yes	No	Yes	2	3	3
8	Frob, Frob^2	3	6	w^3	Yes	No	Yes	2	3	3
8	Frob, Frob^2	3	6	w^4	Yes	No	Yes	2	3	3
8	Frob, Frob^2	3	6	w^5	Yes	No	Yes	2	3	3
8	Frob, Frob^2	3	6	w^6	Yes	No	Yes	2	3	3
8	**Frob, Frob^2**	**3**	**7**	**1**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
8	**Frob, Frob^2**	**3**	**7**	**w**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
8	**Frob, Frob^2**	**3**	**7**	**w^2**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
8	**Frob, Frob^2**	**3**	**7**	**w^3**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
8	**Frob, Frob^2**	**3**	**7**	**w^4**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
8	**Frob, Frob^2**	**3**	**7**	**w^5**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
8	**Frob, Frob^2**	**3**	**7**	**w^6**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**

|F|=q	θ	|θ|	n	a	Commute	gcrd=1	vg=gv	gcd(n,q)	gcd(n,|θ|)	# of divisors
8	Frob, Frob^2	3	8	1	Yes	No	Yes	8	1	9
8	Frob, Frob^2	3	8	w	Yes	No	No	8	1	9
8	Frob, Frob^2	3	8	w^2	Yes	No	No	8	1	9
8	Frob, Frob^2	3	8	w^3	Yes	No	No	8	1	9
8	Frob, Frob^2	3	8	w^4	Yes	No	No	8	1	9
8	Frob, Frob^2	3	8	w^5	Yes	No	No	8	1	9
8	Frob, Frob^2	3	8	w^6	Yes	No	No	8	1	9
9	Frob	2	2	1	No	Yes	Yes	1	2	6
9	Frob	2	2	w	Yes	Yes	Yes	1	2	2
9	Frob	2	2	w^2	Yes	Yes	Yes	1	2	2
9	Frob	2	2	w^3	Yes	Yes	Yes	1	2	2
9	Frob	2	2	w^4	No	Yes	Yes	1	2	6
9	Frob	2	2	w^5	Yes	Yes	Yes	1	2	2
9	Frob	2	2	w^6	Yes	Yes	Yes	1	2	2
9	Frob	2	2	w^7	Yes	Yes	Yes	1	2	2
9	Frob	2	3	1	Yes	No	Yes	3	1	4
9	Frob	2	3	w	Yes	No	No	3	1	4
9	Frob	2	3	w^2	Yes	No	No	3	1	4
9	Frob	2	3	w^3	Yes	No	No	3	1	4
9	Frob	2	3	w^4	Yes	No	Yes	3	1	4
9	Frob	2	3	w^5	Yes	No	No	3	1	4
9	Frob	2	3	w^6	Yes	No	No	3	1	4
9	Frob	2	3	w^7	Yes	No	No	3	1	4
9	Frob	2	4	1	No	No	No	1	2	36
9	Frob	2	4	w	Yes	Yes	Yes	1	2	2
9	Frob	2	4	w^2	Yes	Yes	Yes	1	2	4
9	Frob	2	4	w^3	Yes	Yes	Yes	1	2	2
9	Frob	2	4	w^4	No	Yes	Yes	1	2	12
9	Frob	2	4	w^5	Yes	Yes	Yes	1	2	2
9	Frob	2	4	w^6	Yes	Yes	Yes	1	2	4
9	Frob	2	4	w^7	Yes	Yes	Yes	1	2	2
9	**Frob**	**2**	**5**	**1**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
9	**Frob**	**2**	**5**	**w**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
9	**Frob**	**2**	**5**	**w^2**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
9	**Frob**	**2**	**5**	**w^3**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
9	**Frob**	**2**	**5**	**w^4**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
9	**Frob**	**2**	**5**	**w^5**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
9	**Frob**	**2**	**5**	**w^6**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
9	**Frob**	**2**	**5**	**w^7**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**

|F|=q	θ	|θ|	n	a	Commute	gcrd=1	vg=gv	gcd(n,q)	gcd(n,|θ|)	# of divisors
9	Frob	2	6	1	No	No	No	3	2	76
9	Frob	2	6	w	Yes	No	Yes	3	2	4
9	Frob	2	6	w^2	Yes	No	Yes	3	2	4
9	Frob	2	6	w^3	Yes	No	Yes	3	2	4
9	Frob	2	6	w^4	No	No	No	3	2	76
9	Frob	2	6	w^5	Yes	No	Yes	3	2	4
9	Frob	2	6	w^6	Yes	No	Yes	3	2	4
9	Frob	2	6	w^7	Yes	No	Yes	3	2	4
9	**Frob**	**2**	**7**	**1**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
9	**Frob**	**2**	**7**	**w**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
9	**Frob**	**2**	**7**	**w^2**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
9	**Frob**	**2**	**7**	**w^3**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
9	**Frob**	**2**	**7**	**w^4**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
9	**Frob**	**2**	**7**	**w^5**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
9	**Frob**	**2**	**7**	**w^6**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
9	**Frob**	**2**	**7**	**w^7**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
9	Frob	2	8	1	No	No	No	1	2	432
9	Frob	2	8	w	Yes	Yes	Yes	1	2	2
9	Frob	2	8	w^2	Yes	Yes	Yes	1	2	4
9	Frob	2	8	w^3	Yes	Yes	Yes	1	2	2
9	Frob	2	8	w^4	No	No	No	1	2	144
9	Frob	2	8	w^5	Yes	Yes	Yes	1	2	2
9	Frob	2	8	w^6	Yes	Yes	Yes	1	2	4
9	Frob	2	8	w^7	Yes	Yes	Yes	1	2	2
16	Frob, Frob^3	4	2	1	No	No	Yes	2	2	5
16	Frob, Frob^3	4	2	w	Yes	Yes	Yes	2	2	2
16	Frob, Frob^3	4	2	w^2	Yes	Yes	Yes	2	2	2
16	Frob, Frob^3	4	2	w^3	No	No	Yes	2	2	5
16	Frob, Frob^3	4	2	w^4	Yes	Yes	Yes	2	2	2
16	Frob, Frob^3	4	2	w^5	Yes	Yes	Yes	2	2	2
16	Frob, Frob^3	4	2	w^6	No	No	Yes	2	2	5
16	Frob, Frob^3	4	2	w^7	Yes	Yes	Yes	2	2	2
16	Frob, Frob^3	4	2	w^8	Yes	Yes	Yes	2	2	2
16	Frob, Frob^3	4	2	w^9	No	No	Yes	2	2	5
16	Frob, Frob^3	4	2	w^10	Yes	Yes	Yes	2	2	2
16	Frob, Frob^3	4	2	w^11	Yes	Yes	Yes	2	2	2
16	Frob, Frob^3	4	2	w^12	No	No	Yes	2	2	5
16	Frob, Frob^3	4	2	w^13	Yes	Yes	Yes	2	2	2
16	Frob, Frob^3	4	2	w^14	Yes	Yes	Yes	2	2	2

|F|=q	θ	|θ|	n	a	Commute	gcrd=1	vg=gv	gcd(n,q)	gcd(n,|θ|)	# of divisors
16	**Frob, Frob^3**	**4**	**3**	**1**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**3**	**w**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**3**	**w^2**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**3**	**w^3**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**3**	**w^4**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**3**	**w^5**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**3**	**w^6**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**3**	**w^7**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**3**	**w^8**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**3**	**w^9**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**3**	**w^10**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**3**	**w^11**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**3**	**w^12**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**3**	**w^13**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**3**	**w^14**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	Frob, Frob^3	4	4	1	No	No	No	4	4	67
16	Frob, Frob^3	4	4	w	Yes	Yes	Yes	4	4	2
16	Frob, Frob^3	4	4	w^2	Yes	Yes	Yes	4	4	2
16	Frob, Frob^3	4	4	w^3	Yes	Yes	Yes	4	4	2
16	Frob, Frob^3	4	4	w^4	Yes	Yes	Yes	4	4	2
16	Frob, Frob^3	4	4	w^5	No	No	Yes	4	4	7
16	Frob, Frob^3	4	4	w^6	Yes	Yes	Yes	4	4	2
16	Frob, Frob^3	4	4	w^7	Yes	Yes	Yes	4	4	2
16	Frob, Frob^3	4	4	w^8	Yes	Yes	Yes	4	4	2
16	Frob, Frob^3	4	4	w^9	Yes	Yes	Yes	4	4	2
16	Frob, Frob^3	4	4	w^10	No	No	Yes	4	4	7
16	Frob, Frob^3	4	4	w^11	Yes	Yes	Yes	4	4	2
16	Frob, Frob^3	4	4	w^12	Yes	Yes	Yes	4	4	2
16	Frob, Frob^3	4	4	w^13	Yes	Yes	Yes	4	4	2
16	Frob, Frob^3	4	5	w^14	Yes	Yes	Yes	1	1	2

|F|=q	θ	|θ|	n	a	Commute	gcrd=1	vg=gv	gcd(n,q)	gcd(n,|θ|)	# of divisors
16	**Frob, Frob^3**	**4**	**5**	**1**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**5**	**w**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**5**	**w^2**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**5**	**w^3**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**5**	**w^4**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**5**	**w^5**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**5**	**w^6**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**5**	**w^7**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**5**	**w^8**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**5**	**w^9**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**5**	**w^10**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**5**	**w^11**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**5**	**w^12**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**5**	**w^13**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	**Frob, Frob^3**	**4**	**5**	**w^14**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
16	Frob^2	2	2	1	No	No	Yes	2	2	7
16	Frob^2	2	2	w	Yes	Yes	Yes	2	2	2
16	Frob^2	2	2	w^2	Yes	Yes	Yes	2	2	2
16	Frob^2	2	2	w^3	Yes	Yes	Yes	2	2	2
16	Frob^2	2	2	w^4	Yes	Yes	Yes	2	2	2
16	Frob^2	2	2	w^5	No	No	Yes	2	2	7
16	Frob^2	2	2	w^6	Yes	Yes	Yes	2	2	2
16	Frob^2	2	2	w^7	Yes	Yes	Yes	2	2	2
16	Frob^2	2	2	w^8	Yes	Yes	Yes	2	2	2
16	Frob^2	2	2	w^9	Yes	Yes	Yes	2	2	2
16	Frob^2	2	2	w^10	No	No	Yes	2	2	7
16	Frob^2	2	2	w^11	Yes	Yes	Yes	2	2	2
16	Frob^2	2	2	w^12	Yes	Yes	Yes	2	2	2
16	Frob^2	2	2	w^13	Yes	Yes	Yes	2	2	2
16	Frob^2	2	2	w^14	Yes	Yes	Yes	2	2	2

|F|=q	θ	|θ|	n	a	Commute	gcrd=1	vg=gv	gcd(n,q)	gcd(n,|θ|)	# of divisors
16	**Frob^2**	**2**	**3**	**1**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**3**	**w**	**Yes**	**Yes**	**Yes**	**1**	**1**	**2**
16	**Frob^2**	**2**	**3**	**w^2**	**Yes**	**Yes**	**Yes**	**1**	**1**	**2**
16	**Frob^2**	**2**	**3**	**w^3**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**3**	**w^4**	**Yes**	**Yes**	**Yes**	**1**	**1**	**2**
16	**Frob^2**	**2**	**3**	**w^5**	**Yes**	**Yes**	**Yes**	**1**	**1**	**2**
16	**Frob^2**	**2**	**3**	**w^6**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**3**	**w^7**	**Yes**	**Yes**	**Yes**	**1**	**1**	**2**
16	**Frob^2**	**2**	**3**	**w^8**	**Yes**	**Yes**	**Yes**	**1**	**1**	**2**
16	**Frob^2**	**2**	**3**	**w^9**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**3**	**w^10**	**Yes**	**Yes**	**Yes**	**1**	**1**	**2**
16	**Frob^2**	**2**	**3**	**w^11**	**Yes**	**Yes**	**Yes**	**1**	**1**	**2**
16	**Frob^2**	**2**	**3**	**w^12**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**3**	**w^13**	**Yes**	**Yes**	**Yes**	**1**	**1**	**2**
16	**Frob^2**	**2**	**3**	**w^14**	**Yes**	**Yes**	**Yes**	**1**	**1**	**2**
16	Frob^2	2	4	1	No	No	No	4	2	33
16	Frob^2	2	4	w	Yes	No	Yes	4	2	3
16	Frob^2	2	4	w^2	Yes	No	Yes	4	2	3
16	Frob^2	2	4	w^3	Yes	No	Yes	4	2	3
16	Frob^2	2	4	w^4	Yes	No	Yes	4	2	3
16	Frob^2	2	4	w^5	No	No	No	4	2	33
16	Frob^2	2	4	w^6	Yes	No	Yes	4	2	3
16	Frob^2	2	4	w^7	Yes	No	Yes	4	2	3
16	Frob^2	2	4	w^8	Yes	No	Yes	4	2	3
16	Frob^2	2	4	w^9	Yes	No	Yes	4	2	3
16	Frob^2	2	4	w^10	No	No	No	4	2	33
16	Frob^2	2	4	w^11	Yes	No	Yes	4	2	3
16	Frob^2	2	4	w^12	Yes	No	Yes	4	2	3
16	Frob^2	2	4	w^13	Yes	No	Yes	4	2	3
16	Frob^2	2	4	w^14	Yes	No	Yes	4	2	3

|F|=q	θ	|θ|	n	a	Commute	gcrd=1	vg=gv	gcd(n,q)	gcd(n,|θ|)	# of divisors
16	**Frob^2**	**2**	**5**	**1**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**5**	**w**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**5**	**w^2**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**5**	**w^3**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**5**	**w^4**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**5**	**w^5**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**5**	**w^6**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**5**	**w^7**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**5**	**w^8**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**5**	**w^9**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**5**	**w^10**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**5**	**w^11**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**5**	**w^12**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**5**	**w^13**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
16	**Frob^2**	**2**	**5**	**w^14**	**Yes**	**Yes**	**Yes**	**1**	**1**	**8**
25	Frob	2	2	1	No	Yes	Yes	1	2	8
25	Frob	2	2	w	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^2	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^3	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^4	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^5	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^6	No	Yes	Yes	1	2	8
25	Frob	2	2	w^7	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^8	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^9	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^10	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^11	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^12	No	Yes	Yes	1	2	8
25	Frob	2	2	w^13	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^14	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^15	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^16	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^17	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^18	No	Yes	Yes	1	2	8
25	Frob	2	2	w^19	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^20	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^21	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^22	Yes	Yes	Yes	1	2	2
25	Frob	2	2	w^23	Yes	Yes	Yes	1	2	2

|F|=q	θ	|θ|	n	a	Commute	gcrd=1	vg=gv	gcd(n,q)	gcd(n,|θ|)	# of divisors
25	**Frob**	**2**	**3**	**1**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^2**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^3**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^4**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^5**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^6**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^7**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^8**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^9**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^10**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^11**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^12**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^13**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^14**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^15**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^16**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^17**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^18**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^19**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^20**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^21**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^22**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**
25	**Frob**	**2**	**3**	**w^23**	**Yes**	**Yes**	**Yes**	**1**	**1**	**4**

|F|=q	θ	|θ|	n	a	Commute	gcrd=1	vg=gv	gcd(n,q)	gcd(n,|θ|)	# of divisors
25	Frob	2	4	1	No	No	No	1	2	64
25	Frob	2	4	w	Yes	Yes	Yes	1	2	2
25	Frob	2	4	w^2	Yes	Yes	Yes	1	2	4
25	Frob	2	4	w^3	Yes	Yes	Yes	1	2	2
25	Frob	2	4	w^4	Yes	Yes	Yes	1	2	4
25	Frob	2	4	w^5	Yes	Yes	Yes	1	2	2
25	Frob	2	4	w^6	No	Yes	No	1	2	28
25	Frob	2	4	w^7	Yes	Yes	Yes	1	2	2
25	Frob	2	4	w^8	Yes	Yes	Yes	1	2	4
25	Frob	2	4	w^9	Yes	Yes	Yes	1	2	2
25	Frob	2	4	w^10	Yes	Yes	Yes	1	2	4
25	Frob	2	4	w^11	Yes	Yes	Yes	1	2	2
25	Frob	2	4	w^12	No	No	No	1	2	64
25	Frob	2	4	w^13	Yes	Yes	Yes	1	2	2
25	Frob	2	4	w^14	Yes	Yes	Yes	1	2	4
25	Frob	2	4	w^15	Yes	Yes	Yes	1	2	2
25	Frob	2	4	w^16	Yes	Yes	Yes	1	2	4
25	Frob	2	4	w^17	Yes	Yes	Yes	1	2	2
25	Frob	2	4	w^18	No	Yes	No	1	2	28
25	Frob	2	4	w^19	Yes	Yes	Yes	1	2	2
25	Frob	2	4	w^20	Yes	Yes	Yes	1	2	4
25	Frob	2	4	w^21	Yes	Yes	Yes	1	2	2
25	Frob	2	4	w^22	Yes	Yes	Yes	1	2	4
25	Frob	2	4	w^23	Yes	Yes	Yes	1	2	2

Bibliography

[1] T. Abualrub, A. Ghrayeb, N. Aydin, and I. Siap. On the construction of skew-quasi-cycic codes. *IEEE Trans. Inform. Theory*, IT-56:2081–2090, 2010.

[2] D. Boucher, P. Gaborit, W. Geiselmann, O. Ruatta, and F. Ulmer. Key exchange and encryption schemes based on non-commutative skew polynomials. In *Proc. PQCrypto*, pages 126–141, 6061, 2010.

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

[4] D. Boucher, P. Solé, and F. Ulmer. Skew constacyclic codes over Galois rings. *Adv. Math. Commun.*, 2:273–292, 2008.

[5] D. Boucher and F. Ulmer. A note on the dual codes of module skew codes. In L. Chen, editor, *Proc. of Cryptography and coding: 13th IMA international conference, IMACC 2011, Oxford, UK*, pages 230–243, 2011.

[6] D. Boucher and F. Ulmer. Codes as modules over skew polynomial rings. In M. G. Parker, editor, *Cryptography and Coding. 12th IMA International Conference. Lecture Notes in Computer Science 5921*, pages 38–55, 2009.

[7] D. Boucher and F. Ulmer. Coding with skew polynomial rings. *J. Symb. Comput*, 44:1644–1656, 2009.

[8] D. Boucher and F. Ulmer. Linear codes using skew polynomials with automorphisms and derivations. *Des. Codes Cryptogr.*, 70:405–431, 2014.

[9] D. Boucher and F. Ulmer. Self-dual skew codes and factorizations of skew polynomials. *J. Symb. Comput.*, 60:47–61, 2014.

[10] X. Caruso and J. Le Borgne. Some algorithms for skew polynomials over finite fields. Preprint, 2012.

[11] L. Chaussade, P. Loidreau, and F. Ulmer. Skew codes of prescribed distance or rank. *Des. Codes Cryptogr.*, 50:267–284, 2009.

[12] P. J. Davis. *Circulant Matrices*. A Wiley-Interscience Publication, New York, 1979.

[13] N. Fogarty and H. Gluesing-Luerssen. A circulant approach to skew-constacyclic codes. *Finite Fields and Their Applications*, 35(0):92 – 114, 2015.

[14] J. Gao, L. Shen, and F. Fu. Skew generalized quasi-cyclic codes over finite fields. *CoRR*, abs/1309.1621, 2013.

[15] M. Giesbrecht. Factoring in skew-polynomial rings over finite fields. *J. Symb. Comput.*, 26:463–486, 1998.

[16] H. Gluesing-Luerssen and W. Schmale. On cyclic convolutional codes. *Acta Applicandae Mathematicae*, 82:183–237, 2004.

[17] T. Honold. Characterization of finite Frobenius rings. *Arch. Math.*, 76:406–415, 2001.

[18] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge Univ. Press, 2003.

[19] N. Jacobson. *Finite Dimensional Division Algebra over Fields*. Springer, New York, 1996.

[20] T. Y. Lam. *Lectures on Modules and Rings*. Graduate Texts in Mathematics. Springer New York, 1999.

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

[22] S. Liu, F. Manganiello, and F. R. Kschischang. Kötter interpolation in skew polynomial rings. *Des. Codes Cryptogr.*, 72:593–608, 2014.

[23] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[24] M. Matsuoka. Mathematical aspects of (θ, δ)-codes with skew-polynomial rings. *Int. Math. Forum*, 5:3203–3210, 2010.

[25] O. Ore. Theory of non-commutative polynomials. *Annals Math.*, 34:480–508, 1933.

[26] E. Prange. *Cyclic error-correcting codes in two symbols*. Electronics Research Directorate, Air Force Cambridge Research Center, September 1957. No. AFCRC-TN-57-103. ASTIA Document No. AD133749.

[27] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27, 1948.

[28] V. Sidorenko and M. Bossert. Fast skew-feedback shift-register synthesis. *Des. Codes Cryptogr.*, 70:55–67, 2014.

[29] V. Sidorenko, L. Jiang, and M. Bossert. Skew-feedback shift-register synthesis and decoding interleaved Gabidulin codes. *IEEE Trans. Inform. Theory*, IT-57:621–632, 2011.

[30] B. Wu. New classes of quadratic bent functions in polynomial forms. In *In 2014 IEEE International Symposium on Information Theory (ISIT)*, pages 1832–1836, 2014.

[31] B. Wu and Z. Liu. Linearized polynomials over finite fields revisited. *Finite Fields Appl.*, 22:79–100, 2013.

[32] Y. Zhang. In *Proceedings of the 2010 International Conference on Computational Science and its applications (ICCSA '10)*, Washington (DC).

Vita

Neville Lyons Fogarty

Place of Birth

- Humble, Texas

Educational Experience

- University of Kentucky, Lexington, KY
  M.A. in Mathematics, May 2014
- Washington & Lee University, Lexington, VA
  B.S. in Mathematics & Economics, May 2010
  magna cum laude

Professional Positions

- Graduate Teaching Assistant, University of Kentucky, 2011-2016

Honors

- OΔK (leadership honor society), UK, inducted Spring 2016
- Graduate School Multi-Year Fellowship, UK, 2011-2014
- John McKenzie Gunn Award in Economics, W&L, 2010
- ΦBK (liberal arts honor society), W&L, inducted Spring 2009
- OΔE (economics honor society), W&L, inducted Spring 2009
- ΠME (mathematics honor society), W&L, inducted Spring 2008
- ΦHΣ (freshman honor society), W&L, inducted Spring 2007

Publications

- N. Fogarty and H. Gluesing-Luerssen. A circulant approach to skew-constacyclic codes. *Finite Fields and Their Applications*, 35(0):92-114, 2015. arXiv:1408.5445.