Densities over Global Fields, Arithmetic of Subfield Preserving Maps and Applications to Cryptography

Dissertation

zur

Erlangung der naturwissenschaftlichen Doktorwürde

vorgelegt der

Mathematisch-naturwissenschaftlichen Fakultät

der

Universität Zürich

von

Giacomo Micheli

aus

Italien

Promotionkomitee

Prof. Dr. Joachim Rosenthal

Prof. Dr. Valentin Feray

Prof. Dr. Andrew Kresch

Zürich, 2015

Contents

Introduction

In this thesis I report on the work done during my Ph.D. and supervised by Professor Joachim Rosenthal at the University of Zurich.

At this time, most of the chapters are already published in technical journals or submitted. The papers were written in collaboration with many different co-authors and we will indicate in each chapter to which papers the results are related to. The dissertation consists of three parts which reflect our main interests. The first part is devoted to the study of density questions in the case of global fields. Chapter 1 computes the density of coprime m-tuples over the ring of algebraic integers $\mathcal{O}$ of a number field K. This result consists of a generalization of a theorem by Cesaro over the rational integers: the natural density of the set of coprime pairs is $1/\zeta(2)$, where ζ is the Riemann Zeta function. Our definition of density relies on a choice of a $\mathbb{Z}$-basis for the ring of algebraic integers. Nevertheless, the final result is independent of that choice and we get that the density of coprime m-tuples is $1/\zeta_K(m)$, where ζ_K is the Dedekind zeta function of the number field.

Chapter 2 addresses the same problem for an integrally closed subring of a function field (of any genus) over a finite field using a suitable definition of density, which generalizes the one we have in the case of polynomials over finite fields. In this case we use a definition of density based on Moore-Smith convergence [20, Chapter 2] on the set of effective divisors in the complement of the holomorphy set defining the subring. This definition is very natural since it is based on a covering of the integrally closed ring via Riemann-Roch spaces; in addition it reduces to the natural "degree based" density in the case of polynomials over finite fields.

In Chapter 3 we show some applications of a local-to-global principle for densities. Chapter 4 addresses a different density question for the case of subfield preserving maps over finite fields. In particular: given a prime degree extension $\mathbb{F}_{q^p}$ of a finite field $\mathbb{F}_q$, what is the probability

that a polynomial f over the base field $\mathbb{F}_q$ *preserves* the extension? i.e. what is the probability that $f(\mathbb{F}_{q^p} \setminus \mathbb{F}_q) \subseteq \mathbb{F}_{q^p} \setminus \mathbb{F}_q$? We answer this question by solving a more general problem, i.e. giving the explicit monoid structure of subfield preserving maps for any base field $\mathbb{F}_q$ and any extension $\mathbb{F}_{q^m}$. As a corollary we get an interesting answer to our first question, of which a nice instance is when $q = p$: in this case the density of subfield preserving maps approaches $1/e$ as $q = p \to \infty$.

The second part of the dissertation contains results about linear maps over finite fields. Chapter 5 deals with a general question on matrices over any field and we specialize only later to the case of finite fields. As an application of the results, we break a non-commutative key exchange cipher based on matrix rings which has been proposed in several variants in the literature. Later on in the same chapter we focus the attention on the subfield preserving question in the case of linear maps, which we completely answer in Theorem 80. In Chapter 7 we use the previous results to describe the group structure of invertible q-linearized maps over finite fields with coefficients in some intermediate field between the base field $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$.

The third part of the dissertation is devoted to a general construction for multiplicative knapsack schemes. In particular we show some applications of the construction, which consist of function field variants of the Naccache Stern Knapsack Scheme [36]. In Chapter 9 we provide an information rate improvement for this variant.

Throughout the dissertation we preferred to keep all the chapters as independent as possible: in this way, the reader which is interested in a particular result will not be obliged to read the whole thesis up to the point he is willing to understand.

Acknowledgements

I am extremely grateful to my advisor for his help and support in the last two and a half years and for all the guidance he has provided. Working with him remarkably increased my level of confidence and my skills as writer, speaker, teacher and mathematician. I would also like to thank my office mate, co-author and good friend Andrea Ferraguti for his sharp and always illuminating suggestions concerning mathematics, life and *cuisine*. I am also grateful to Antonio De Rosa, Francesco Ghiraldin, Patrick Kühn, Annalisa Massaccesi, Kyle Marshall, Tommaso Mingazzini, Mattia Molinaro, Riccardo Montalto, Marta Pittavino, Jusuf Ramic, Michele Schiavina, Davide Schipani, Luca Spolaor, Salvatore Stuvard, Marko Zivkovic that made my two and a half years at the Institut für Mathematik an amazing experience. Of course, I also thank the SNF grant number 149716 and *Armasuisse*.

A Vittoria

Part I

Densities over Global Fields

Chapter 1

Cesàro Theorem for Number Fields

The results presented in this chapter come from a joint work with Andrea Ferraguti [13].

1.1 Introduction

In 1881 Ernesto Cesàro proved that the natural density of the set of coprime pairs of integers is $1/\zeta(2)$, where ζ is the Riemann zeta function. An analytic proof of this result is presented in the book by Hardy and Wright [15] while a generalization to the case of m-tuples of integers has been given in [37].

If one tries to extend the formulation of the theorem to the case of algebraic integers, one encounters some obstructions from the very beginning. In the next paragraphs the reader can find some of the motivations that led to our approach to the problem, especially concerning the definition of the density for a subset of the ring of algebraic integers $\mathcal{O}$ of a number field K.

Indeed, for the case of $\mathbb{Z}$, there exists a "canonical" way to compute the density of a set $A \subseteq \mathbb{Z}$: this can be in fact defined as the limit in B (if it exists) of the sequence $|A \cap [-B, B[|/(2B)$. This definition extends to the density of a set $A \subseteq \mathbb{Z}^m$ by considering the limit of the sequence $|A \cap [-B, B[^m|/(2B)^m$. This definition characterizes the probability that, given the m-dimensional hypercube of large side B centred in the origin, a uniformly random selected integer point has all relatively prime entries.

What can actually be done in the setting of algebraic integers is to consider the analogous problem for the set of m-tuples of ideals of $\mathcal{O}$ using a suitable definition of density involving the norm function. Very interesting results in this direction can be found in [45]. On the other hand, if we want a proper generalization of Cesàro Theorem to $\mathcal{O}$ (and not to the set of ideals of $\mathcal{O}$) the approach presented in [45] does not apply: indeed, given a large bound B, there might be infinitely many elements of norm at most B (contrary to what happens in the case of $\mathbb{Z}$). Therefore, not only this definition of density for sets of ideals of $\mathcal{O}$ cannot extend to a definition of density for $\mathcal{O}$, but also the analogous probability interpretation that one has over $\mathbb{Z}$ is missing.

A *non canonical* definition for the density of a subset $A \subseteq \mathcal{O}$ is obtained by considering a $\mathbb{Z}$-isomorphism $\psi : \mathcal{O} \to \mathbb{Z}^n$ (n being the degree of the extension $K \supseteq \mathbb{Q}$) and then by computing the density of $\psi(A) \subseteq \mathbb{Z}^n$ as previously described. The resulting density is then dependent on the choice of ψ (that is equivalent to a choice of a $\mathbb{Z}$-basis for $\mathcal{O}$), but extends to $A \subseteq \mathcal{O}^m$ componentwise, as one would expect by considering the limit of the sequence $|\psi(A) \cap [-B, B[^{mn}|/(2B)^{mn}$. Using this definition of density for the set $E \subseteq \mathcal{O}^m$ of coprime m-tuples and a similar strategy to the one presented in [27] for the case of unimodular matrices over $\mathbb{Z}$, something surprising turns out to be true:

- the density d of E can be computed
- d is *independent* on the choice of the embedding ψ (i.e. independent of the choice of the $\mathbb{Z}$-basis for $\mathcal{O}$)
- d equals $1/\zeta_K(m)$, where $\zeta_K(m)$ is the Dedekind zeta function of the number field K.

This completely generalizes Cesàro Theorem to the case of number fields. It is very interesting to note that this result matches the one presented in [45, Theorem 4.1], that was obtained in the context of ideals of $\mathcal{O}$.

Outline of the proof

Let us now briefly describe the strategy we used to compute the above mentioned density in the general case of a subset $E \subseteq \mathbb{Z}^N$. First, we find a family $\{E_t\}_{t\in\mathbb{N}}$ of subsets of $\mathbb{Z}^N$ with the following properties:

- we are able to compute the density of E_t for every t

- $E_{t+1} \subseteq E_t$
- $\bigcap_t E_t = E$.

Then we verify that the family of sets $\{E_t\}_t$ approximates the set E *in density* in the sense that the sequence of densities of $E_t \setminus E$ converges to zero as t runs to infinity. Finally we compute the limit in t of the density of the E_t, obtaining the density of E. The reason why this method works will be clarified later on.

1.1.1 Notation

Let H, H' be subsets of a commutative ring R and I an ideal of R. We say that H is congruent to H' modulo I if the projections of H and H' are equal modulo I. Moreover we will write

$$H \equiv H' \mod I.$$

Let R be a commutative ring, we say that the ideals $I_1, \ldots, I_l$ are coprime if $\sum_j I_j = R$; we extend this notion to elements of R by considering the ideal generated by them. Let K be a number field of degree n and $\mathcal{O}$ its ring of algebraic integers. Let $\mathbb{E} = \{\mathbf{e}_i\}_{i=1}^n$ be a $\mathbb{Z}$-basis for $\mathcal{O}$. Define

$$\mathcal{O}[B, \mathbb{E}] = \left\{ \sum_{i=0}^{n-1} a_i \mathbf{e}_i \mid a_i \in [-B, B[\cap \mathbb{Z} \right\}.$$

Later on in the chapter we will just write $\mathcal{O}[B]$ since the basis will be understood. For p a prime number, we denote by $S_p = \{\mathfrak{p}_1^{(p)}, \ldots, \mathfrak{p}_{\lambda_p}^{(p)}\}$ the set of prime ideals lying over p. Let $d_j^{(p)}$ be the inertia degree of $\mathfrak{p}_j^{(p)}$ (i.e. $\dim_{\mathbb{F}_p}(\mathcal{O}/\mathfrak{p}_j^{(p)})$) and denote by D_p the integer $\sum_{j=1}^{\lambda_p} d_j^{(p)}$. Let d be a positive integer, let us denote by $\mathrm{GF}(p, d)$ the finite field of order p^d. Define

$$R_p := \prod_{j=1}^{\lambda_p} \mathcal{O}/\mathfrak{p}_j^{(p)} \cong \prod_{j=1}^{\lambda_p} \mathrm{GF}(p, d_j^{(p)}).$$

For $z = (z_1, \ldots, z_m)$ an element of $\mathcal{O}^m$, we denote by I_z the ideal generated by the set $\{z_1, \ldots, z_m\}$. If $\mathbb{F}$ is a field we denote by $\mathbb{F}^*$ its multiplicative group.

1.2 A definition for the density of the set of coprime m-tuples

Let $\mathbb{E}$ be a $\mathbb{Z}$-basis for $\mathcal{O}$. Our goal is to define a notion of density (which will in general depend on the choice of $\mathbb{E}$) for a subset T of $\mathcal{O}^m$. We define the *upper density of T with respect to* $\mathbb{E}$ to be

$$\overline{\mathbb{D}}_{\mathbb{E}}(T) = \limsup_{B\to\infty} \frac{|\mathcal{O}[B,\mathbb{E}] \cap T|}{(2B)^{mn}}$$

and the *lower density of T with respect to* $\mathbb{E}$ as

$$\underline{\mathbb{D}}_{\mathbb{E}}(T) = \liminf_{B\to\infty} \frac{|\mathcal{O}[B,\mathbb{E}] \cap T|}{(2B)^{mn}}.$$

We say that T has *density d with respect to* $\mathbb{E}$ if

$$\overline{\mathbb{D}}_{\mathbb{E}}(T) = \underline{\mathbb{D}}_{\mathbb{E}}(T) =: \mathbb{D}_{\mathbb{E}}(T) = d.$$

Whenever this density is independent of the chosen basis $\mathbb{E}$, it is consistent to denote the density of a set T by $\mathbb{D}(T)$ without any subscript.

Remark 1. First observe that $d \in [0,1] \subseteq \mathbb{R}$ by construction. The main idea behind this definition of density is the same that one has over $\mathbb{Z}$: the only difference is that the way in which we cover the entire set (in this case $\mathcal{O}$) is not canonical but depends on the basis $\mathbb{E}$.

Example 2. Let us show with an example that choosing different bases for $\mathcal{O}$ can yield different densities for the same subset $T \subseteq \mathcal{O}$. Let $K = \mathbb{Q}(i)$, so that $\mathcal{O} = \mathbb{Z}[i]$. Let $T = \{x + iy \in \mathcal{O} \colon x, y > 0\}$. If $\mathbb{E} = \{1, i\}$, clearly $|\mathcal{O}[B,\mathbb{E}] \cap T| = (B-1)^2$, which gives $\mathbb{D}_{\mathbb{E}}(T) = 1/4$. On the other hand, choosing as a basis $\mathbb{E}' = \{1, -1+i\} = \{\mathbf{e}_1, \mathbf{e}_2\}$ we have that $T = \{x\mathbf{e}_1 + y\mathbf{e}_2 \in \mathcal{O} \colon x, y > 0,\ x > y\}$. Therefore $|\mathcal{O}[B,\mathbb{E}'] \cap T| = (B-1)(B-2)/2$, which shows that $\mathbb{D}_{\mathbb{E}'} = 1/8$.

Let $E \subseteq \mathcal{O}^m$ be the set of coprime m-tuples, i.e. the elements $z \in \mathcal{O}^m$ for which $I_z = \mathcal{O}$. A corollary of our final result (Theorem 9) is that the density of E is actually independent of the basis $\mathbb{E}$: even if the choice of the covering of $\mathcal{O}^m$ is not canonical (it depends in fact on the chosen $\mathbb{Z}$-basis for $\mathcal{O}$) the density of E *is*.

1.3 Proof of Cesàro Theorem

Let $\mathbb{S}$ be a finite set of prime numbers. Let $E_{\mathbb{S}}$ be the set of m-tuples $z = (z_1, \ldots, z_m)$ in $\mathcal{O}^m$ such that the ideal I_z is coprime with every $p \in \mathbb{S}$.

Remark 3. Equivalently, one checks that

$$E_{\mathbb{S}} = \{z \in \mathcal{O}^m \mid I_z + \mathfrak{p}_j^{(p)} = \mathcal{O} \quad \forall p \in \mathbb{S} \quad \text{and} \quad \forall j \in \{1, \ldots, \lambda_p\}\}$$

by observing that $(p) \subseteq \prod_j \mathfrak{p}_j^{(p)}$ and the $\mathfrak{p}_j^{(p)}$ are maximal.

Let $\psi_p : (\mathcal{O}/(p))^m \to R_p^m = (\prod_{j=1}^{\lambda_p} \mathcal{O}/\mathfrak{p}_j^{(p)})^m$ be the morphism induced by the projection $\mathcal{O}/(p) \twoheadrightarrow \prod_{j=1}^{\lambda_p} \mathcal{O}/\mathfrak{p}_j^{(p)}$. Recall that $D_p = \sum_{j=1}^{\lambda_p} d_j^{(p)}$. In the following lemma and in Proposition 5 we will consider the surjection

$$\pi : \mathcal{O}^m \longrightarrow \left(\prod_{p \in \mathbb{S}} R_p\right)^m =: T$$

induced by the quotient maps $\mathcal{O} \to \mathcal{O}/\mathfrak{p}_j^{(p)}$.

Lemma 4.

$$E_{\mathbb{S}} = \pi^{-1}\left(\prod_{p \in \mathbb{S}} \prod_{j=1}^{\lambda_p} \left(\left(\mathcal{O}/\mathfrak{p}_j^{(p)}\right)^m \setminus \{0\}\right)\right)$$

Proof. Let $z \in E_{\mathbb{S}}$ then $I_z + \mathfrak{p}_j^{(p)} = \mathcal{O}$ for all j, p, hence

$$\mathcal{O} \equiv I_z \qquad \bmod \mathfrak{p}_j^{(p)}$$

then it follows that for each pair (j, p) there is at least one component of z that is different from zero in $\mathcal{O}/\mathfrak{p}_j^{(p)}$, thus $z \in \left(\mathcal{O}/\mathfrak{p}_j^{(p)}\right)^m \setminus \{0\}$ for each reduction. Vice versa, if

$$z \in \pi^{-1}\left(\prod_{p \in \mathbb{S}} \prod_{j=1}^{\lambda_p} \left(\left(\mathcal{O}/\mathfrak{p}_j^{(p)}\right)^m \setminus \{0\}\right)\right)$$

it follows that I_z is always congruent to $\mathcal{O}$ modulo $\mathfrak{p}_i^{(p)}$. □

Proposition 5. *Let q be a positive integer, $\mathbb{E}$ a $\mathbb{Z}$-basis for $\mathcal{O}$, $\mathbb{S}$ a finite set of prime numbers*

and $N = \prod_{p\in\mathbb{S}} p$. *Then*

$$|E_{\mathbb{S}} \cap \mathcal{O}[qN]^m| = (2q)^{mn} \prod_{p\in\mathbb{S}} \left(p^{nm-mD_p} \prod_{j=1}^{\lambda_p} (p^{d_j^{(p)}m} - 1) \right)$$

where $\mathcal{O}[qN]^m$ *is the set of* m*-tuples of elements of* $\mathcal{O}[qN]$.

Proof. The key point is to decompose the map π. For the rest of the proof, the reader may refer to the following diagram:

$$\begin{array}{ccccc} \mathcal{O}^m & \xrightarrow{\pi_N} & (\mathcal{O}/(N))^m & \xrightarrow{\overline{\psi}} & T \\ & & \| & & \| \\ & & (\prod_{p\in\mathbb{S}} \mathcal{O}/(p))^m & \xrightarrow{\psi} & (\prod_{p\in\mathbb{S}} R_p)^m \end{array}$$

where π_N is the quotient map, $\psi = (\dots, \psi_p, \dots)$ and $\overline{\psi}$ is its obvious extension to $(\mathcal{O}/(N))^m$ obtained by applying the Chinese Remainder Theorem to primes in $\mathbb{S}$. Notice then that $\pi = \overline{\psi} \circ \pi_N$. Our strategy to prove the result is to compute the cardinality of the fibers of ψ and the intersection of the fibers of π_N with $\mathcal{O}[qN]$:

- Observe that $\psi_p : (\mathcal{O}/(p))^m \to R_p^m$ is a surjective morphism of $\mathbb{F}_p$-vector spaces, therefore $|\psi_p^{-1}(y_p)| = |\ker(\psi_p)| = p^{nm-mD_p}$ for all $y_p \in R_p^m$. It follows that $|\overline{\psi}^{-1}(y)| = \prod_{p\in\mathbb{S}} |\psi_p^{-1}(y_p)| = \prod_{p\in\mathbb{S}} p^{nm-mD_p}$ for all $y \in (\mathcal{O}/(N))^m$.

- Let $z = (z_j)_j \in (\mathcal{O}/(N))^m$ and $v = (v_j)_j \in \mathcal{O}^m$. Write

  $$z_j = \left(\sum_{t=0}^{n} r_t^j \pi(\mathbf{e}_t) \right)$$

  for some unique $0 \le r_t^j < N$ in $\mathbb{Z}$. Observe that existence and uniqueness of the r_t^j follow from the fact that $\mathcal{O}/(N)$ is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank n with basis $\{\pi(\mathbf{e}_t)\}$. It follows that $\pi_N(v) = z$ if and only if

  $$v_j = \sum_{t=0}^{n} (r_t^j + l_t^j N)\mathbf{e}_t$$

  for some $l_t^j \in \mathbb{Z}$. We conclude then that $|\mathcal{O}[qN]^m \cap \pi_N^{-1}(z)| = (2q)^{mn}$: the r_t^j are fixed by the condition $\pi_N(v) = z$ and $l_t^j \in [-q, q[\cap\mathbb{Z}$ for each index j, t.

Let us now complete the proof. By Lemma 4 we have that

$$E_{\mathbb{S}} \cap \mathcal{O}[qN]^m = \pi^{-1}\left(\prod_{p\in\mathbb{S}}\prod_{j=1}^{\lambda_p}\left(\left(\mathcal{O}/\mathfrak{p}_j^{(p)}\right)^m \setminus \{0\}\right)\right) \cap \mathcal{O}[qN]^m \tag{1.1}$$

In order to simplify the notation, define

$$H := \psi^{-1}\left(\prod_{p\in\mathbb{S}}\prod_{j=1}^{\lambda_p}\left(\left(\mathcal{O}/\mathfrak{p}_j^{(p)}\right)^m \setminus \{0\}\right)\right)$$

Since $\pi = \psi \circ \pi_N$, Equation 1.1 reads

$$E_{\mathbb{S}} \cap \mathcal{O}[qN]^m = \pi_N^{-1}(H) \cap \mathcal{O}[qN]^m.$$

Therefore

$$|\pi_N^{-1}(H) \cap \mathcal{O}[qN]^m| = (2q)^{mn}|H|$$

and

$$|H| = \prod_{p\in\mathbb{S}}\left(p^{nm-D_p m}\prod_{j=1}^{\lambda_p}\left|\left(\mathcal{O}/\mathfrak{p}_j^{(p)}\right)^m \setminus \{0\}\right|\right).$$

Thus,

$$|E_{\mathbb{S}} \cap \mathcal{O}[B]| = (2q)^{mn}\prod_{p\in\mathbb{S}}\left(p^{nm-mD_p}\prod_{j=1}^{\lambda_p}(p^{d_j^{(p)}m}-1)\right)$$

□

Before we proceed, let us recall the following elementary calculus fact

Lemma 6. *Let $\{a_B\}_{B\in\mathbb{N}}$ be a sequence of real numbers and N a positive integer. Then*

$$\lim_{B\to\infty} a_B = c \Leftrightarrow \lim_{q\to\infty} a_{r+qN} = c \quad \forall r \in \{0,\dots,N-1\}$$

Lemma 7.

$$\mathbb{D}(E_{\mathbb{S}}) = \mathbb{D}_{\mathbb{E}}(E_{\mathbb{S}}) = \prod_{p\in\mathbb{S}}\prod_{j=1}^{\lambda_p}\left(1-\frac{1}{p^{d_j^{(p)}m}}\right) =: D$$

Proof. Let

$$a_B := \frac{|\mathcal{O}[B]^m \cap E_{\mathbb{S}}|}{(2B)^{mn}}$$

Recall that $N = \prod_{p\in\mathbb{S}} p$. Let us first show that $a_{qN} = D$.

$$a_{qN} = \frac{|\mathcal{O}[qN]^m \cap E_{\mathbb{S}}|}{(2qN)^{mn}} =$$

$$= \frac{(2q)^{mn}\prod_{p\in\mathbb{S}} p^{nm-mD_p}\prod_{j=1}^{\lambda_p}(p^{d_j^{(p)}m}-1)}{(2qN)^{mn}}.$$

By cancelling common factors in numerator and denominator and writing D_p according to its definition we get

$$a_{qN} = \prod_{p\in\mathbb{S}} p^{-m\sum_{j=1}^{\lambda_p} d_j^{(p)}} \prod_{j=1}^{\lambda_p}(p^{d_j^{(p)}m}-1)$$

and bringing $p^{-m\sum_{j=1}^{\lambda_p} d_j^{(p)}}$ inside the products it follows that

$$a_{qN} = \prod_{p\in\mathbb{S}}\prod_{j=1}^{\lambda_p}(1-p^{-d_j^{(p)}m}).$$

We are now ready to prove that

$$\lim_{B\to\infty} a_B = D.$$

Thanks to lemma 6 it will be enough to show

$$\lim_{q\to\infty} a_{r+qN} = D.$$

for all $r \in \{0,\dots,N-1\}$. Indeed

$$a_{qN}\cdot\left(\frac{(2qN)}{2r+2qN}\right)^{mn} < a_{r+qN} < a_{(q+1)N}\cdot\left(\frac{(2(q+1)N)}{2r+2qN}\right)^{mn}$$

By passing to the limit in q the claim follows. □

Remark 8. It is immediate to observe that the density of $E_{\mathbb{S}}$ is independent of the chosen basis $\mathbb{E}$.

We are now in a position to formulate and prove Cesàro Theorem for number fields.

Theorem 9. *Let m be a positive integer and K be a number field. Let $\mathcal{O}$ be the ring of integers*

of K. The density of the set E of coprime m-tuples of $\mathcal{O}$ is

$$\mathbb{D}(E) = \frac{1}{\zeta_K(m)}$$

where ζ_K is the Dedekind zeta function of the number field K.

Remark 10. Let $\mathbb{S}_t = \{p_1, \ldots, p_t\}$. The reader should observe that one has the inclusion $E \subseteq E_{\mathbb{S}_t}$ and therefore

$$0 \leq \mathbb{D}_{\mathbb{E}}(E) \leq \overline{\mathbb{D}}_{\mathbb{E}}(E) \leq \mathbb{D}(E_{\mathbb{S}_t}).$$

As a consequence one has that in the case $m = 1$ Theorem 9 follows by passing to the limit $t \to \infty$ in the above inequality and recalling that the Dedekind zeta function of K has a pole at 1. As expected in fact, the group of units of the ring of integers has density zero in any basis. Observe that this is the special case $k = 1$ of [5, Corollary 4.2]. A more extensive description of additive representations of elements in the unit group can be found in [2].

Remark 11. Notice that the argument of 10 does not lead to the conclusion in the case $m > 1$, since it provides just an upper bound (uniform in $\mathbb{E}$) for $\overline{\mathbb{D}}_{\mathbb{E}}(E)$.

Before starting the proof let us recall the following theorem, which we will use as a fundamental tool. We are deeply grateful to Fabrizio Barroero for his suggestion of using it.

Theorem 12. *Let $S \subseteq \mathbb{R}^M$ be a bounded set whose boundary ∂S can be covered by the images of at most W maps $\phi\colon [0,1]^{M-1} \to \mathbb{R}^M$ satisfying Lipschitz conditions*

$$|\phi(x) - \phi(y)| \leq L|x - y|$$

for the Euclidean norm. Then S is measurable. Let $V = vol(S)$.
Let $\Lambda \subseteq \mathbb{R}^M$ be a full-rank lattice and

$$\lambda_1 \coloneqq \inf\{|v|\colon v \in \Lambda \setminus \{0\}\}$$

be its first successive minimum. Then

$$\left| |\Lambda \cap S| - \frac{V}{\det \Lambda} \right| \leq cW \left(\frac{L}{\lambda_1} + 1 \right)^{M-1}$$

for a constant c depending only on M.

Proof. See [25, Lemma 2]. □

Next we are going to deduce from Theorem 12 the particular case that we will use in the proof of Theorem 9.

Proposition 13. *Let K be a number field of degree n with ring of integers $\mathcal{O}$. Let I be an ideal of $\mathcal{O}$. Then*

$$\left| |(I \cap \mathcal{O}[B])^m| - \frac{(2B)^{nm}}{N(I)^m} \right| \leq c \left(\frac{2B}{c_1 N(I)^{1/n}} + 1 \right)^{mn-1}$$

for every $B \in \mathbb{N}$, where $N(I)$ denotes the norm of I and the constants c, c_1 are independent of B and of I.

Proof. Recall that there is a canonical embedding of $\mathcal{O}$ into $\mathbb{R}^n$: if $\sigma_1, \dots, \sigma_r$ are the real embeddings $K \to \mathbb{R}$ and $\sigma_{r+1}, \dots, \sigma_{r+2s} = \sigma_n$ are the complex ones labeled such that $\sigma_{r+i} = \overline{\sigma_{r+s+i}}$, then the map $\tau \colon \mathcal{O} \to \mathbb{R}^n$ defined by $x \mapsto (\sigma_1(x), \dots, \sigma_r(x), \sigma_{r+1}(x), \dots, \sigma_{r+s}(x))$ embeds $\mathcal{O}$ as a full-rank lattice in $\mathbb{R}^n$, where each σ_{r+i} is thought as an embedding into $\mathbb{R}^2$. The map τ induces an embedding $\tau^m \colon \mathcal{O}^m \to \mathbb{R}^{mn}$. The image of $\mathcal{O}$ inside $\mathbb{R}^{mn}$ via τ^m is again a full-rank lattice. Let $\alpha_{\mathbb{E}} : \mathcal{O} \longrightarrow \mathbb{Z}^n$ be the isomorphism of $\mathbb{Z}$-modules given by $\alpha_{\mathbb{E}} \left(\sum_{i=1}^n x_i \mathbf{e}_i \right) = (x_1, \dots, x_n)$. Let $\alpha_{\mathbb{E}}^m \colon \mathcal{O}^m \to \mathbb{Z}^{mn}$ be the isomorphism induced by $\alpha_{\mathbb{E}}$. Consider the following commutative diagram

$$\begin{array}{ccc} \mathcal{O}^m & \xrightarrow{\tau^m} & \mathbb{R}^{mn} \\ \downarrow{\scriptstyle \alpha_{\mathbb{E}}^m} & & \uparrow A \\ \mathbb{Z}^{mn} & \xrightarrow{\iota} & \mathbb{R}^{mn} \end{array}$$

where ι is the inclusion map and A is the unique $\mathbb{R}$-linear map which makes the diagram commute. The idea now is to apply Theorem 12 with $\Lambda = (\iota \circ \alpha_{\mathbb{E}}^m)(I^m) \subseteq \mathbb{R}^{mn}$ and S the cube of side $2B$ centered in the origin, so that $W = 2mn$ and $L = 2B$ in the notation of the theorem. Here by I^m we mean the cartesian product of m copies of I inside $\mathcal{O}^m$.

We first need a lower bound for the first successive minimum of $(\iota \circ \alpha_{\mathbb{E}}^m)(I^m)$. To do this we can clearly assume $m = 1$ since the first successive minimum of a lattice $\Lambda \subseteq \mathbb{R}^n$ coincides with that of $\Lambda^m \subseteq \mathbb{R}^{mn}$. Let v be a vector realizing the first successive minimum of $(\iota \circ \alpha_{\mathbb{E}})(I)$ with respect to the euclidean norm $|\cdot|$. By Lemma 5 of [25], the first successive minimum of $\tau(I)$ is

greater or equal than $N(I)^{1/n}$. Since $A(v) \in \tau(I)$ we have that

$$N(I)^{1/n} \leq \|A(v)\| \leq \|A\||v|$$

where $\|A\|$ is defined by $\sup_{|w|=1} \|A(w)\|$. This shows that the first successive minimum of $(\iota \circ \alpha_{\mathbb{E}})(I)$ is greater or equal than $c_1 N(I)^{1/n}$, where $c_1 \coloneqq 1/\|A\|$ is independent of B and of I. Now the claim follows by applying Theorem 12 together with the fact that

$$\det(\alpha_{\mathbb{E}}^m(I^m)) = \det(\alpha_{\mathbb{E}}(I))^m = [\mathbb{Z}^n : \alpha_{\mathbb{E}}(I)]^m = [\mathcal{O} \colon I]^m = N(I)^m$$

and observing that $|(\iota \circ \alpha_{\mathbb{E}}^m)(I^m) \cap [-B, B[^{mn}| = |I^m \cap \mathcal{O}[B]^m| = |(I \cap \mathcal{O}[B])^m|$. □

Proof of Theorem 9. We already proved the Theorem in the case $m = 1$ in remark 10, therefore let us suppose $m > 1$. Let t be a positive integer, $\mathbb{S}_t$ the set consisting of the first t prime numbers and define $E_t = E_{\mathbb{S}_t}$. Observe that, since $E_t \supseteq E$ we have

$$\overline{\mathbb{D}}_{\mathbb{E}}(E) \leq \overline{\mathbb{D}}(E_t) = \mathbb{D}(E_t).$$

By letting t run to infinity we get

$$\overline{\mathbb{D}}_{\mathbb{E}}(E) \leq \frac{1}{\zeta_K(m)}.$$

In order to show the opposite inequality observe that

$$\mathbb{D}(E_t) - \overline{\mathbb{D}}_{\mathbb{E}}(E_t \setminus E) \leq \underline{\mathbb{D}}_{\mathbb{E}}(E).$$

Therefore, it is enough to prove that $\lim_{t \to \infty} \overline{\mathbb{D}}_{\mathbb{E}}(E_t \setminus E) = 0$. For a prime ideal $\mathfrak{p} \subseteq \mathcal{O}$, the t-th prime number p_t and M an integer, let us introduce the following notation

- $\mathfrak{p} \succ N$ if and only if $\mathfrak{p}$ lies over a prime greater than N (Notice that, with this notation, one has that $\mathfrak{p} \succ p_t$ implies $\mathfrak{p} + (p_i) = \mathcal{O}$ for every $i \leq t$).
- $M \succ \mathfrak{p}$ if and only if the rational prime lying under $\mathfrak{p}$ is less than M.

With this notation one has

$$E_t \setminus E \subseteq \bigcup_{\mathfrak{p} \in \mathcal{P} \colon \mathfrak{p} \succ p_t} \mathfrak{p}^m \subseteq \mathcal{O}^m$$

where $\mathfrak{p}^m$ is the set m-tuples of elements of $\mathcal{O}$ having all entries in $\mathfrak{p}$. It follows that

$$(E_t \setminus E) \cap \mathcal{O}[B]^m \subseteq \bigcup_{\mathfrak{p}\in\mathcal{P}:\ CB^n \succ \mathfrak{p} \succ p_t} (\mathfrak{p} \cap \mathcal{O}[B])^m$$

for C a positive constant independent of B. The upper bound $CB^n \succ \mathfrak{p}$ comes from the following observation: for a fixed basis, the norm function is a polynomial of degree n in the coefficients (with respect to the basis $\mathbb{E}$) of the elements of $\mathcal{O}$. Therefore $N(\mathcal{O}[B]) \subseteq [-CB^n, CB^n]$ for a constant C depending only on the chosen basis. On the other hand, if an element of $\mathcal{O}[B]$ is in $\mathfrak{p}$ then its norm is divisible by the rational prime p lying under $\mathfrak{p}$. This shows that there cannot exist primes $\mathfrak{p} \succ CB^n$ containing a nonzero element of $\mathcal{O}[B]$. We have then

$$\overline{\mathbb{D}}_{\mathbb{E}}(E_t \setminus E) \leq \limsup_{B\to\infty} \left| \bigcup_{\mathfrak{p}\in\mathcal{P}:\ CB^n \succ \mathfrak{p} \succ p_t} \mathfrak{p}^m \cap \mathcal{O}[B]^m \right| \cdot (2B)^{-nm} \leq$$

$$\leq \limsup_{B\to\infty} \sum_{\mathfrak{p}\in\mathcal{P}:\ CB^n \succ \mathfrak{p} \succ p_t} |\mathfrak{p} \cap \mathcal{O}[B]|^m \cdot (2B)^{-nm}.$$

By Proposition 13, $|\mathfrak{p}\cap\mathcal{O}[B]|^m = |(\mathfrak{p}\cap\mathcal{O}[B])^m| \leq \dfrac{(2B)^{mn}}{N(\mathfrak{p})^m} + c\left(\dfrac{2B}{c_1 N(\mathfrak{p})^{1/n}} + 1\right)^{mn-1}$. Therefore

$$\limsup_{B\to\infty} \sum_{\mathfrak{p}\in\mathcal{P}:\ CB^n \succ \mathfrak{p} \succ p_t} |\mathfrak{p} \cap \mathcal{O}[B]|^m \cdot (2B)^{-nm} \leq$$

$$\leq \limsup_{B\to\infty} \sum_{\mathfrak{p}\in\mathcal{P}:\ CB^n \succ \mathfrak{p} \succ p_t} \frac{1}{N(\mathfrak{p})^m} + c\left(\frac{2B}{c_1 N(\mathfrak{p})^{1/n}} + 1\right)^{mn-1} \cdot (2B)^{-nm} \leq$$

$$\leq \limsup_{B\to\infty} \sum_{p:\ CB^n > p > p_t} \frac{n}{p^m} + cn\left(\frac{2B}{c_1 p^{1/n}} + 1\right)^{mn-1} \cdot (2B)^{-nm} =: L_t$$

where the last inequality holds because for every prime $\mathfrak{p}$ of $\mathcal{O}$ one has that $N(\mathfrak{p}) \geq p$ for p the rational prime lying under it and above a fixed rational prime lie at most n distinct primes of $\mathcal{O}$.

Choose now a constant $c_1' \leq c_1$ (independent of B) for which $\dfrac{1}{C^{1/n}} \geq \dfrac{c_1'}{2}$. Notice that the sum that appears in L_t is taken over primes p such that $CB^n > p$, which shows that

$$B > \frac{1}{C^{1/n}} p^{1/n} \geq \frac{c_1'}{2} p^{1/n}.$$

It follows $\frac{2B}{c_1' p^{1/n}} \geq 1$ and then $\dfrac{2B}{c_1' p^{1/n}} + 1 \leq 2\dfrac{2B}{c_1' p^{1/n}}$. Therefore L_t is bounded by

$$\limsup_{B\to\infty} \sum_{p:\, CB^n > p > p_t} \frac{n}{p^m} + cn\left(\frac{4B}{c_1' p^{1/n}}\right)^{mn-1} \cdot (2B)^{-nm} = \sum_{p:\, CB^n > p > p_t} \frac{n}{p^m} + \frac{c'}{B \cdot p^{m-1/n}}$$

for some other constant c' independent of B and p. Now observe that

$$\limsup_{B\to\infty} \sum_{p:\, CB^n > p > p_t} \frac{n}{p^m} \leq \sum_{p > p_t} \frac{n}{p^m}$$

tends to zero when $t \to \infty$ because the series $\displaystyle\sum_p \frac{1}{p^m}$ is convergent, while for the other term one has that

$$\limsup_{B\to\infty} \sum_{CB^n > p > p_t} \frac{c'}{B \cdot p^{m-1/n}} \leq \limsup_{B\to\infty} \frac{c'}{B} \sum_{CB^n > p > p_t} \frac{1}{p} = 0$$

since $\sum_{p < CB^n} \frac{1}{p}$ is asymptotic to $\log\log(CB^n)$.

□

The following corollary produces the classical generalization of Cesàro Theorem to the case of m-tuples of integers (presented in [37]).

Corollary 14 (Extended Cesàro Theorem)**.** *The density of coprime m-tuples of integers is $\frac{1}{\zeta(m)}$, where ζ is the Riemann zeta function.*

Proof. Follows directly from Theorem 9 by setting $K = \mathbb{Q}$. □

Remark 15. Observe that the results of Theorem 9 are coherent with the expectations. The obtained density is in fact independent of the basis: by symmetry, indeed, all proofs can be done by using another basis $\mathbb{B}$, obtaining the same result. In addition, Theorem 9 extends Cesàro Theorem for algebraic integers in the following sense: over $\mathbb{Z}$ one can equivalently consider the density of the set of coprime m-tuples of integers or coprime m-tuples of ideals of $\mathbb{Z}$ without any relevant distinction. If one is willing to do the same in the case of algebraic integers, one has to choose in which context one wants to consider the problem: in the context of m-tuples of ideals, the results in [45] are satisfying while in the setting of m-tuples of algebraic integers, Theorem 9 answers the question. Curiously, even if the set up of the problem is very different, the resulting densities match.

Chapter 2

Cesàro Theorem for Function Fields

In this chapter we provide the function field analogue of the result presented in the previous one. This is a joint work with Reto Schnyder [33].

2.1 Introduction

Let $\mathbb{F}_q$ be a finite field with q elements and let F be an algebraic function field[1] having full constant field $\mathbb{F}_q$. Let $\mathcal{C}$ be the set of places of F and $\mathcal{S} \subsetneq \mathcal{C}$ be a non-empty proper subset. The holomorphy ring of $\mathcal{S}$ is $H = \bigcap_{P \in \mathcal{S}} \mathcal{O}_P$, where $\mathcal{O}_P$ is the valuation ring of the place P.

In what follows we will say that an m-tuple of elements of H is coprime if its components generate the unit ideal in H (in analogy to the case of the ring of integers in [13]). In this chapter we define a notion of density for subsets of H^m, using Moore-Smith convergence for nets [20, Chapter 2]. We then wish to study the density of the set of coprime m-tuples in H, considered as a subset of H^m.

The special case $F = \mathbb{F}_q(x)$ and $H = \bigcap_{P \neq P_\infty} \mathcal{O}_P = \mathbb{F}_q[x]$ has been studied for $m = 2$ in [50] and more generally in [14]. We will explain how to interpret the densities presented in these papers as particular cases of our general framework. In fact, using the Riemann-Roch Theorem and the absolute convergence of the zeta function of F, we are able to show that the density of

[1] In this chapter we will mostly use the language and notation of [49].

coprime m-tuples of elements of a holomorphy ring exists and is equal to $\frac{1}{\zeta_H(q^{-m})}$, where ζ_H is the zeta function of the holomorphy ring.

Finally, we provide an example in the case of the affine ring of coordinates of an elliptic curve to show a concrete application of the main result.

2.1.1 Notation

Let $F/\mathbb{F}_q$ be an algebraic function field with full constant field $\mathbb{F}_q$, let g be the genus of F, and let $\mathcal{C}$ be the set of its places. Let H be the holomorphy ring of a nonempty set of places $\mathcal{S} \subsetneq \mathcal{C}$. For a fixed positive integer m, we wish to study the set of coprime m-tuples of elements of the ring H. Let us denote this set by U:

$$U \coloneqq \{f = (f_1, \ldots, f_m) \in H^m \mid I_f = H\},$$

where I_f denotes the ideal of H generated by the set $\{f_1, \ldots f_m\}$.

Define furthermore $\mathcal{D} \coloneqq \{D \in \mathrm{Div}(F) \mid D \geq 0 \wedge \mathrm{supp}(D) \subseteq \mathcal{C} \setminus \mathcal{S}\}$, the set of positive divisors supported away from $\mathcal{S}$. It follows that

$$H = \bigcup_{D \in \mathcal{D}} \mathcal{L}(D),$$

where $\mathcal{L}(D)$ denotes the Riemann-Roch space associated to a divisor D. Recall that we have a bijection between the set of places $\mathcal{S}$ and the maximal ideals of H given by $P \mapsto P \cap H =: P_H$ (see for example [49, Proposition 3.2.9]). In analogy to the natural density of integers, we define the *superior density* of a subset $L \subseteq H^m$ as

$$\overline{\mathbb{D}}(L) \coloneqq \limsup_{D \in \mathcal{D}} \frac{|L \cap \mathcal{L}(D)^m|}{|\mathcal{L}(D)^m|}. \tag{2.1}$$

This limit can be defined via Moore-Smith convergence [20, Chapter 2]. To be precise, the set of divisors $\mathcal{D}$ with the usual partial order $\leq$ is a directed set, so the map from $\mathcal{D}$ to the topological space $\mathbb{R}$ defined as

$$D \mapsto \frac{|L \cap \mathcal{L}(D)^m|}{|\mathcal{L}(D)^m|}$$

is a net. Now, since $\mathbb{R}$ is Hausdorff, the definition in (2.1) is well posed. Analogously one can

define the *inferior density* as

$$\underline{\mathbb{D}}(L) \coloneqq \liminf_{D\in\mathcal{D}} \frac{|L \cap \mathcal{L}(D)^m|}{|\mathcal{L}(D)^m|}.$$

Moreover, whenever $\overline{\mathbb{D}}(L) = \underline{\mathbb{D}}(L)$, we call this value the *density* of L and denote it by $\mathbb{D}(L)$.

2.2 The density of U

Recall that the zeta function of the function field F is given by

$$\zeta_F(T) \coloneqq \prod_{P\in\mathcal{C}} \left(1 - T^{\deg(P)}\right)^{-1}$$

for $0 < T < q^{-1}$. Analogously, we define the zeta function of the holomorphy ring H corresponding to the set of places $\mathcal{S}$ as

$$\zeta_H(T) \coloneqq \prod_{P\in\mathcal{S}} \left(1 - T^{\deg(P)}\right)^{-1}.$$

We will now state our main result.

Theorem 16. *The density of the set of coprime tuples of length $m \geq 2$ of the holomorphy ring H is $\frac{1}{\zeta_H(q^{-m})}$.*

Proof. We first enumerate the set of places of $\mathcal{S} = \{Q_1, Q_2, \dots, Q_t, \dots\}$. Let us define

$$U_t \coloneqq \{f = (f_1, \dots f_m) \in H^m \mid I_f \nsubseteq (Q_i)_H \quad \forall i \in \{1, \dots, t\}\}$$

and notice that $U_t \supseteq U$. Observe that the condition $I_f \nsubseteq (Q_i)_H$ is equivalent to the fact that for each i there exists at least one f_j that does not belong to Q_i. Consider now the projection $\pi\colon H \to H/((Q_1)_H \cdots (Q_t)_H)$ and observe that

$$H/((Q_1)_H \cdots (Q_t)_H) \cong \prod_{i=1}^{t} H/(Q_i)_H \cong \prod_{i=1}^{t} \mathbb{F}_{q^{\deg Q_i}},$$

by the Chinese remainder theorem over the ideals $(Q_i)_H$. This gives us a homomorphism

$$\phi\colon H \longrightarrow \prod_{i=1}^{t} \mathbb{F}_{q^{\deg Q_i}},$$

which we can extend to m-tuples by

$$\widehat{\phi}\colon H^m \longrightarrow \prod_{i=1}^{t} \mathbb{F}_{q^{\deg Q_i}}^m.$$

By construction, this homomorphism satisfies

$$U_t = \widehat{\phi}^{-1}\left(\prod_{i=1}^{t}(\mathbb{F}_{q^{\deg Q_i}}^m \setminus \{0\})\right). \tag{2.2}$$

Consider now a divisor $D \in \mathcal{D}$. We wish to count the number of elements in $U_t \cap \mathcal{L}(D)^m$. First, we will show that ϕ maps $\mathcal{L}(D)$ surjectively onto $\prod_{i=1}^{t} \mathbb{F}_{q^{\deg Q_i}}$ if $\deg D$ is large enough.

For this, note that the image of $\mathcal{L}(D)$ under π is $\mathcal{L}(D)/(\mathcal{L}(D) \cap ((Q_1)_H \cdots (Q_t)_H))$. The space

$$\mathcal{L}(D) \cap ((Q_1)_H \cdots (Q_t)_H) = \mathcal{L}(D) \cap Q_1 \cap \cdots \cap Q_t$$

consists of all elements in $\mathcal{L}(D)$ with at least a root at each Q_i, so it is equal to $\mathcal{L}(D - \sum_{i=1}^{t} Q_i)$. (Note that the Q_i cannot be in the support of D.) Hence, its dimension as an $\mathbb{F}_q$-vector space is $\ell(D - \sum_{i=1}^{t} Q_i)$, which is equal to $\deg D - \sum_{i=1}^{t} \deg Q_i + 1 - g$ if $\deg D$ is large enough by Riemann-Roch Theorem. On the other hand, the dimension of $\mathcal{L}(D)$ is then $\ell(D) = \deg D + 1 - g$, and so the image has dimension $\sum_{i=1}^{t} \deg Q_i$, the same as $\prod_{i=1}^{t} \mathbb{F}_{q^{\deg Q_i}}$.

We can now count the elements of $U_t \cap \mathcal{L}(D)^m$ using (2.2). As we have just seen, the dimension of the kernel of ϕ restricted to $\mathcal{L}(D)$ is $\ell(D - \sum_{i=1}^{t} Q_i)$, so each element of $\prod_{i=1}^{t}(\mathbb{F}_{q^{\deg Q_i}}^m \setminus \{0\})$ is the image under $\widehat{\phi}$ of exactly $q^{m\ell(D - \sum_{i=1}^{t} Q_i)}$ elements of $U_t \cap \mathcal{L}(D)^m$. Hence we get

$$\frac{|U_t \cap \mathcal{L}(D)^m|}{|\mathcal{L}(D)^m|} = q^{m(\ell(D - \sum_{i=1}^{t} Q_i) - \ell(D))} \cdot \prod_{i=1}^{t}(q^{m \deg Q_i} - 1) = \prod_{i=1}^{t}(1 - q^{-m \deg Q_i})$$

if $\deg D$ is large enough. It follows that the density of U_t is well-defined and equals

$$\mathbb{D}(U_t) = \lim_{D \in \mathcal{D}} \frac{|U_t \cap \mathcal{L}(D)^m|}{|\mathcal{L}(D)^m|} = \prod_{i=1}^{t}(1 - q^{-m \deg Q_i}).$$

Since $U \subseteq U_t$, it follows that $\overline{\mathbb{D}}(U) \leq \mathbb{D}(U_t)$.

To get an estimate in the other direction, let us write $(\mathcal{L}(D) \cap U) \cup (\mathcal{L}(D) \cap (U_t \setminus U)) = \mathcal{L}(D) \cap U_t$. We have

$$\underline{\mathbb{D}}(U) = \liminf_{D \in \mathcal{D}} \frac{|U \cap \mathcal{L}(D)^m|}{q^{m\ell(D)}} \geq \lim_{D \in \mathcal{D}} \frac{|U_t \cap \mathcal{L}(D)^m|}{q^{m\ell(D)}} - \limsup_{D \in \mathcal{D}} \frac{|(U_t \setminus U) \cap \mathcal{L}(D)^m|}{q^{m\ell(D)}},$$

hence we have the inequalities

$$\mathbb{D}(U_t) \geq \overline{\mathbb{D}}(U) \geq \underline{\mathbb{D}}(U) \geq \mathbb{D}(U_t) - \limsup_{D \in \mathcal{D}} \frac{|(U_t \setminus U) \cap \mathcal{L}(D)^m|}{q^{m\ell(D)}}. \tag{2.3}$$

Now, passing to the limit in t we get that $\lim_{t \to \infty} \mathbb{D}(U_t) = 1/\zeta_H(q^{-m})$. Therefore it remains to prove that

$$\lim_{t \to \infty} \limsup_{D \in \mathcal{D}} \frac{|(U_t \setminus U) \cap \mathcal{L}(D)^m|}{q^{m\ell(D)}} = 0.$$

In order to prove the last claim, let us denote by $\mathcal{Q}_t$ the set $\{Q_1, \ldots, Q_t\}$, and notice

$$U_t \setminus U \subseteq \bigcup_{P \in \mathcal{S} \setminus \mathcal{Q}_t} \{A \in H^m \mid I_A \subseteq P_H\} = \bigcup_{P \in \mathcal{S} \setminus \mathcal{Q}_t} P_H^m,$$

where by P_H^m we mean the Cartesian product of m copies of the ideal P_H. Fix now a divisor $D \in \mathcal{D}$. It follows that

$$(U_t \setminus U) \cap \mathcal{L}(D)^m \subseteq \bigcup_{P \in \mathcal{S} \setminus \mathcal{Q}_t} (P_H \cap \mathcal{L}(D))^m = \bigcup_{P \in \mathcal{S} \setminus \mathcal{Q}_t} \mathcal{L}(D - P)^m = \bigcup_{\substack{P \in \mathcal{S} \setminus \mathcal{Q}_t \\ \deg P \leq \deg D}} \mathcal{L}(D - P)^m.$$

The last equality holds because $\mathcal{L}(D - P) = 0$ if $\deg D - \deg P < 0$. With this containment, we can now estimate the last term of (2.3):

$$\begin{aligned}
\limsup_{D \in \mathcal{D}} \frac{|\mathcal{L}(D) \cap (U_t \setminus U)|}{q^{m\ell(D)}} &\leq \limsup_{D \in \mathcal{D}} \Big| \bigcup_{\substack{P \in \mathcal{S} \setminus \mathcal{Q}_t \\ \deg P \leq \deg D}} \mathcal{L}(D - P)^m \Big| \cdot q^{-m\ell(D)} \\
&\leq \limsup_{D \in \mathcal{D}} \sum_{\substack{P \in \mathcal{S} \setminus \mathcal{Q}_t \\ \deg P \leq \deg D}} \Big| \mathcal{L}(D - P)^m \Big| \cdot q^{-m\ell(D)} \\
&= \limsup_{D \in \mathcal{D}} \sum_{\substack{P \in \mathcal{S} \setminus \mathcal{Q}_t \\ \deg P \leq \deg D}} q^{m(\ell(D-P) - \ell(D))}
\end{aligned}$$

Now observe that we have $\ell(D) \geq \deg(D) + 1 - g$ and $\ell(D - P) \leq \deg(D - P) + 1$, since $\deg(D - P) \geq 0$ [49, Eq. 1.21 and Theorem 1.4.17]. It follows that the above is less or equal to

$$\limsup_{\substack{D \in \mathcal{D} \\ \deg P \leq \deg D}} \sum_{P \in \mathcal{S} \setminus \mathcal{Q}_t} q^{m(g - \deg P)} = \limsup_{d \to \infty} q^{gm} \sum_{\substack{P \in \mathcal{S} \setminus \mathcal{Q}_t \\ \deg P \leq d}} (q^{-m})^{\deg P} = q^{gm} \sum_{P \in \mathcal{S} \setminus \mathcal{Q}_t} (q^{-m})^{\deg P}.$$

Observe that $\sum_{P \in \mathcal{S} \setminus \mathcal{Q}_t} q^{-m \deg P}$ is the tail of a subseries of the zeta function of F evaluated at $q^{-m} < q^{-1}$, which is absolutely convergent (see for example [35, Chapter 3]). As t goes to infinity, it converges to 0, from which our claim follows. □

2.3 Consequences

The reader should observe that in Theorem 16 both $\mathcal{S}$ and $\mathcal{C} \setminus \mathcal{S}$ could possibly be infinite and the result will still hold. Nevertheless, the density depends on the zeta function of the holomorphy ring, which may be hard to compute. First of all notice that this is not the case when $\mathcal{S}$ is finite since under this condition ζ_H is a finite product. The following immediate corollary covers the case in which $\mathcal{C} \setminus \mathcal{S}$ is finite.

Corollary 17. *Let F be a function field, $\mathcal{S}$ a set of places of F and H the holomorphy ring of $\mathcal{S}$. Let $L_F(T)$ be the L-polynomial of F. Then*

$$\zeta_H(q^{-m}) = \frac{L_F(q^{-m})}{(1 - q^{-m})(1 - q^{-m+1})} \prod_{P \in \mathcal{C} \setminus \mathcal{S}} \left(1 - \frac{1}{q^{\deg(P)m}}\right).$$

Proof. The corollary follows from Theorem 16, the definition of ζ_H and the expression of the zeta function of F in terms of the L-polynomial. □

Remark 18. Observe now that in the case where $\mathcal{C} \setminus \mathcal{S}$ is finite, the density of coprime m-tuples of H essentially only depends on the degrees of the places in $\mathcal{C} \setminus \mathcal{S}$ and the L-polynomial of the function field, which again only depends on the $\mathbb{F}_{q^i}$-rational points of the curve associated to the function field for $i \in \{1, \ldots, g\}$ (see for example [49, Corollary 5.1.17]).

2.3.1 An example

Let $\mathbf{char}(\mathbb{F}_q) \neq 2, 3$ for simplicity. Let $a, b \in \mathbb{F}_q$ and $p(x, y) = y^2 - x^3 - ax - b$ be a polynomial defining an elliptic curve E over $\mathbb{F}_q$. Let us define

$$A(E) \coloneqq \mathbb{F}_q[x, y]/(p(x, y)).$$

Let $E(\mathbb{F}_q)$ denote the set of (projective) $\mathbb{F}_q$-rational points of E (i.e. the places of degree one of the function field of E).

Corollary 19. *The density of m-tuples of coprime elements of $A(E)$ is*

$$\mathbb{D}(U) = \frac{1 - q^{-m+1}}{1 + a_q q^{-m} + q^{-2m+1}} \tag{2.4}$$

where $a_q = q + 1 - |E(\mathbb{F}_q)|$.

Proof. Observe that the zeta function of an elliptic curve is

$$\zeta_E(T) = \frac{1 + a_q T + qT}{(1 - qT)(1 - T)}.$$

The result follows from Theorem 16 applied to the holomorphy ring $A(E) = \bigcap_{P \neq P_\infty} \mathcal{O}_P$ where P_∞ is the place at infinity of E with respect to $p(x, y)$. □

Remark 20. The reader should notice again that (2.4) depends only on the number of $\mathbb{F}_q$-rational points of E, since the genus of E equals one. The probabilistic interpretation of Corollary 19 is the following: select uniformly at random m elements of $A(E)$ of degree at most N, then the probability that they generate the unit ideal in $A(E)$ approaches $\dfrac{1 - q^{-m+1}}{1 + a_q q^{-m} + q^{-2m+1}}$ as $N \to \infty$.

2.3.2 The case $F = \mathbb{F}_q(x)$

In the remaining part of this section we show how the result of [14] about $\mathbb{F}_q[x]$ fits in our framework. We denote by P_∞ the place at infinity of the function field $\mathbb{F}_q(x)$.

The reader should observe that the definition of density for $\mathbb{F}_q[x]$ given in [14, 50] agrees with ours for $H = \mathbb{F}_q[x] = \bigcap_{P \neq P_\infty} \mathcal{O}_P$, so we have [50, Theorem 1] as a corollary with $m = 2$. More generally, we obtain the result in [14] for unimodular rows over $\mathbb{F}_q[x]$:

Corollary 21. *Let $m > 1$ be an integer. The density of unimodular rows of length m over $\mathbb{F}_q[x]$ is*

$$\mathbb{D}(U) = 1 - \frac{1}{q^{m-1}}$$

Proof. It is enough to notice that the zeta function of the function field $\mathbb{F}_q(x)$ (i.e. the zeta function of the projective line) is

$$\zeta_{\mathbb{F}_q(x)}(T) = \frac{1}{(1-T)(1-qT)}$$

and then the zeta function of the holomorphy ring $\mathbb{F}_q[x] = \bigcap_{P \neq P_\infty} \mathcal{O}_P$ is

$$\zeta_{\mathbb{F}_q[x]}(T) = \frac{1}{1-qT}.$$

The claim follows by inverting the expression above and evaluating at q^{-m}. □

Chapter 3

Density of Eisenstein Polynomials from a local to global principle

In this short chapter we prove some of the results of [17] using a powerful lemma in [42]. Let $A \subseteq \mathbb{Z}^d$, we define the *natural density of A*

$$\rho(A) := \lim_{B\to\infty} \frac{|A \cap [-B, B[^d|}{(2B)^d}.$$

Let μ_p be the p-adic measure on $\mathbb{Z}_p^d$ and μ_∞ the Lebesgue measure on $\mathbb{R}^d$.

Lemma 22. *Suppose $U_\infty \subseteq \mathbb{R}^d$ is such that $\mathbb{R}^+ \cdot U_\infty = U_\infty$, $\mu_\infty(\partial U_\infty) = 0$. Let $U_\infty^1 = U_\infty \cap [-1,1]^d$ and $s_\infty = \mu_\infty(U_\infty^1)$. Let $U_p \subseteq \mathbb{Z}_p^d$, $\mu_p(\partial U_p) = 0$ and $s_p = \mu_p(U_p)$. Let $M_\mathbb{Q}$ be the set of places of $\mathbb{Q}$. Moreover, suppose that*

$$\lim_{M\to\infty} \rho(\{a \in \mathbb{Z}^d : \ a \in U_p \text{ for some finite prime } p \text{ greater than } M\}) = 0. \tag{3.1}$$

Let $P : \mathbb{Z}^d \longrightarrow 2^{M_\mathbb{Q}}$ defined as $P(a) = \{v \in M_\mathbb{Q} : \ a \in U_v\}$. Then we have

1. *$\sum_v s_v$ converges*
2. *for $T \subseteq 2^{M_\mathbb{Q}}$, $\nu(T) := \rho(P^{-1}(T))$ exists and defines a measure on $2^{M_\mathbb{Q}}$, which is concentrated at the finite subsets of $M_\mathbb{Q}$.*

3. Let S be a finite subset of $M_{\mathbb{Q}}$, then

$$\nu(\{S\}) = \prod_{v \in S} s_v \prod_{v \notin S} (1 - s_v).$$

Proof. For the proof, see [42, Lemma 20]. □

Let E be the set of monic Eisenstein polynomials of fixed degree $d > 1$ i.e.

$$E = \{x^d + \sum_{i=0}^{d-1} a_i x^i \mid \exists\, p \text{ prime} : p | a_i \; \forall i \in \{0, \ldots, d-1\} \quad \text{and } p^2 \nmid a_0\}$$

Theorem 23. *The set of monic Eisenstein polynomials of degree d has natural density*

$$1 - \prod_{p:prime} \left(1 - \frac{p-1}{p^{d+1}}\right).$$

Proof. With a small abuse of notation we regard at E as subset of $\mathbb{Z}^d$. Set $U_\infty = \varnothing$ and

$$U_p := (p\mathbb{Z}_p \setminus p^2\mathbb{Z}_p) \times p\mathbb{Z}_p \times \cdots \times p\mathbb{Z}_p \subseteq \mathbb{Z}_p^d$$

Condition (2) of the lemma is easily verified by the convergence of

$$\sum_{p:\text{prime}} \frac{1}{p^d}$$

for $d > 1$. In addition, the measure s_p of U_p is $(p-1)/p^{d+1}$. The key observation is that $P^{-1}(\{\varnothing\})$ equals the complement of E. It follows that

$$\rho(E) = 1 - \rho(P^{-1}(\{\varnothing\})) = 1 - \prod_{p:prime} \left(1 - \frac{p-1}{p^{d+1}}\right).$$

□

Let

$$\overline{E} = \{\sum_{i=0}^{d} a_i x^i \mid \exists\, p \text{ prime} : p | a_i \; \forall i \in \{0, \ldots, d-1\}, \quad p^2 \nmid a_0 \text{ and } p \nmid a_d\}$$

be the set of non-monic Eisenstein polynomials. We have

Theorem 24. *The set of non-monic Eisenstein polynomials of degree d has natural density*

$$1 - \prod_{p:prime} \left(1 - \frac{(p-1)^2}{p^{d+2}}\right).$$

Proof. Set again $U_\infty = \varnothing$ and

$$U_p = (p\mathbb{Z}_p \setminus p^2\mathbb{Z}_p) \times p\mathbb{Z}_p \times \cdots \times p\mathbb{Z}_p \times \mathbb{Z}_p \setminus p\mathbb{Z}_p \subseteq \mathbb{Z}_p^{d+1}.$$

Again, condition (2) of the lemma is easily verified for $d \geq 2$. Moreover,

$$\mu_p(U_p) = \left(\frac{1}{p} - \frac{1}{p^2}\right) \frac{1}{p^{d-1}} \left(1 - \frac{1}{p}\right) = \frac{(p-1)^2}{p^{d+2}} =: s_p.$$

Observing that $P^{-1}(\{\varnothing\})$ equals the complement of $\overline{E}$ we get the claim:

$$\rho(\overline{E}) = 1 - \rho(P^{-1}(\{\varnothing\})) = 1 - \prod_{p:\text{prime}} \left(1 - \frac{(p-1)^2}{p^{d+2}}\right).$$

□

Chapter 4

On q-canonical m-subfield preserving polynomials

In this Chapter we study the monoid structure of subfield preserving maps together with densities arising from this context. This is a joint work with Davide Schipani [32].

4.1 Introduction

Let q be a prime power and m a natural number. In [4] the structure of the group consisting of permutation polynomials [24] of $\mathbb{F}_{q^m}$ having coefficients in the base field $\mathbb{F}_q$ was made explicit. We start observing that, if f is a permutation of $\mathbb{F}_{q^m}$ with coefficients in $\mathbb{F}_q$ then

$$f(\mathbb{F}_q) = \mathbb{F}_q \quad \text{and} \quad \forall\, d, s \mid m \qquad f(\mathbb{F}_{q^d} \setminus \mathbb{F}_{q^s}) = \mathbb{F}_{q^d} \setminus \mathbb{F}_{q^s}.$$

Indeed for any integer $s \geq 1$, since f has coefficients in $\mathbb{F}_q$ and $\mathbb{F}_{q^s}$ is a field, we have $f(\mathbb{F}_{q^s}) \subseteq \mathbb{F}_{q^s}$. Being f also a bijection, this is also an equality. The property above follows then directly (see also [4, Lemma 2]).

It is natural now to ask which are the polynomials f, having coefficients in $\mathbb{F}_q$, such that

$$f(\mathbb{F}_q) \subseteq \mathbb{F}_q \quad \text{and} \quad \forall\, d, s \mid m \qquad f(\mathbb{F}_{q^d} \setminus \mathbb{F}_{q^s}) \subseteq \mathbb{F}_{q^d} \setminus \mathbb{F}_{q^s}. \tag{4.1}$$

Let us call T_q^m the set of such polynomials. We remark that this is a monoid under compo-

sition and its invertible elements $(T_q^m)^*$ consist of the group of permutation polynomials with coefficients in $\mathbb{F}_q$ mentioned above. In this chapter we give the explicit semigroup structure of T_q^m, obtaining the main result of [4] (i.e. the group structure mentioned above) as a corollary. The explicit semigroup structure will allow us to compute the probability that a polynomial chosen uniformly at random having coefficients in $\mathbb{F}_q$ satisfies condition (4.1). This will imply the following remarkable results:

- Given p prime, for q relatively large, the density of T_q^p is approximately zero.
- Given q, for p relatively large prime, the density of T_q^p is approximately one.
- For $q = p$ large prime the density of T_p^p is approximately $1/e$.

4.2 Preliminary definitions

Definition 25. We say $f : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ to be *subfield preserving* if

$$f(\mathbb{F}_q) \subseteq \mathbb{F}_q \quad \text{and} \quad \forall\, d, s \mid m \qquad f(\mathbb{F}_{q^d} \setminus \mathbb{F}_{q^s}) \subseteq \mathbb{F}_{q^d} \setminus \mathbb{F}_{q^s}. \tag{4.2}$$

Moreover, we will say f to be *q-canonical* if its polynomial representation has coefficients in $\mathbb{F}_q$ (or simply *canonical* when q is understood).

Remark 26. One of the reason why we use the term *canonical* to address the property of having coefficients in a subfield is that, under this property, the induced application $\tilde{f}$ of $f(x)$ is always well defined no matter what irreducible polynomial we choose for the representation of the finite field extension $\mathbb{F}_{q^m}$.

Denote by $\mathcal{L}_{\mathbb{F}_{q^m}}$ the set of all subfield preserving polynomials.

Remark 27. If we drop the condition on the coefficients, the semigroup structure becomes straightforward:

$$\mathcal{L}_{\mathbb{F}_{q^m}} \cong \bigtimes_{k|m} M_{[k\pi(k)]}.$$

with $\pi(k)$ being the number of monic irreducible polynomials of degree k over $\mathbb{F}_q$ and $M_{[n]}$ being the set of all maps from $\{1, \ldots, n\}$ to itself.

Remark 28. Clearly not all subfield preserving polynomials are canonical, which can also be checked by a cardinality count with the results later in this chapter.

In the rest of the chapter we will need the following lemma, whose proof can be easily adapted from [4].

Lemma 29. *Let $f : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ be a map. Then $f \in \mathbb{F}_q[x]$ if and only if $f \circ \varphi_q = \varphi_q \circ f$ where $\varphi_q(x) = x^q$.*

Indeed the set of functions we are looking at consists of $T_q^m = \mathcal{L}_{\mathbb{F}_{q^m}} \cap \mathcal{C}_{\varphi_q}$ where $\mathcal{C}_{\varphi_q} := \{f : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m} \mid f \circ \varphi_q = \varphi_q \circ f\}$.

4.3 Combinatorial underpinning

Let S be a finite set and $\psi : S \to S$ a bijection. For any $T \subseteq S$, let

$$\mathcal{K}_\psi(T) := \{f : T \to T \mid \forall x \in T \quad f \circ \psi(x) = \psi \circ f(x)\}.$$

For any partition $\mathcal{P}$ of S into sets P_k, let

$$M_S(\mathcal{P}) := \{f : S \to S \mid \forall\ k \quad f(P_k) \subseteq P_k\}.$$

When $\mathcal{P} = \{S\}$ is the trivial partition, we will denote $M_S(\{S\}) = M_S$ namely the monoid of applications from S to itself.

For any bijection $\phi : S \to S$, define ϕ_k for any k as the composition of the cycles of ϕ of length k, and set $\phi_k = (\varnothing)$ if ϕ has no cycles of length k. Let W denote the set $\{1, \ldots, |S|\}$, then $\phi = \prod_{k \in W, \phi_k \neq (\varnothing)} \phi_k$. If $\mathrm{supp}(\phi_k)$ denotes the set of elements moved by ϕ_k, then ϕ induces a partition $\mathcal{P}_\phi$ on $S = \bigcup_{k \in W} S_k$, with $S_k = \mathrm{supp}(\phi_k)$, for $k \geq 2$, and S_1 being the set of fixed points of ϕ.

Lemma 30.

$$M_S(\mathcal{P}_\phi) \cap \mathcal{K}_\phi(S) \cong \bigtimes_{k \in W, \phi_k \neq (\varnothing)} \mathcal{K}_{\phi_k}(S_k)$$

Proof. Clearly any $f \in \mathcal{K}_{\phi_k}(S_k)$ can be extended to S as the identity and then the extension $\bar{f}$

belongs to $\mathcal{K}_\phi(S) \cap M_S(\mathcal{P}_\phi)$. Indeed we have a natural injection

$$\bigtimes_{k \in W, \phi_k \neq (\varnothing)} \mathcal{K}_{\phi_k}(S_k) \hookrightarrow M_S(\mathcal{P}_\phi) \cap \mathcal{K}_\phi(S).$$

This is also a surjection: in fact let $f \in M_S(\mathcal{P}_\phi) \cap \mathcal{K}_\phi(S)$ and define

$$f_k(x) := \begin{cases} f(x) & \text{if } x \in S_k, \\ x & \text{otherwise.} \end{cases}$$

Since $M_S(\mathcal{P}_\phi) \cap \mathcal{K}_\phi(S) \subseteq M_S(\mathcal{P}_\phi)$, then $f_k(S_k) \subseteq S_k$ which implies

$$f_k\big|_{S_k} \in \mathcal{K}_{\phi_k}(S_k).$$

As the S_k form a partition, the composition of all the f_k coincides with f. □

Now, for $n, k \in \mathbb{N}$ let U_n^k be a set with kn elements and ψ a bijection of U_n^k having n cycles of length k. Let us put indices on the elements of the set in the following way: let a_{ij} be the j-th element of the i-th cycle, with $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, k\}$.

Let $[h]$ denote $\{1, \ldots, h\}$ for a natural number h. We say $\lambda : [h] \to [h]$ to be a cyclic shift of $[h]$ if $\lambda(j + \ell) = \lambda(j) + \ell$ modulo h for any $j, \ell \in [h]$.

Let $\gamma_1, \ldots, \gamma_n$ be cyclic shifts of $[k]$ and $\sigma : [n] \to [n]$ a map. We construct then $f_\sigma^\gamma : U_n^k \to U_n^k$ as follows:

$$f_\sigma^\gamma(a_{ij}) := a_{\sigma(i)\gamma_i(j)}.$$

Theorem 31. *$g \in \mathcal{K}_\psi(U_n^k) \Leftrightarrow \exists\ \gamma := (\gamma_1, \ldots, \gamma_n)$, γ_i cyclic shifts of $[k]$, and $\exists\ \sigma : [n] \to [n]$ map such that $g = f_\sigma^\gamma$.*

Proof. Suppose first $g \in \mathcal{K}_\psi(U_n^k)$. Then

$$g(a_{ij}) = g(\psi^{j-1}(a_{i1})) = \psi^{j-1}(g(a_{i1})).$$

Define $\sigma(i) := [g(a_{i1})]_1$ and $\gamma_i(j) := [g(a_{ij})]_2$, where the subscripts $[x]_1$ and $[x]_2$ refer to the two indices of $x \in U_n^k$ in the representation a_{ij} above.

Observe that for all $i \in [n]$, γ_i is a cyclic shift, indeed it holds modulo k:

$$\gamma_i(j+\ell) = [g(a_{i\ j+\ell})]_2 = [g(\psi^\ell(a_{ij}))]_2 =$$

$$[\psi^\ell(g(a_{ij}))]_2 = [g(a_{ij})]_2 + \ell = \gamma_i(j) + \ell.$$

Moreover remark that

$$g(a_{ij}) = g(\psi^{j-1}(a_{i1})) = \psi^{j-1}(g(a_{i1})) = \psi^{j-1}(a_{\sigma(i)\gamma_i(1)}) =$$

$$a_{\sigma(i)\ \gamma_i(1)+j-1} = a_{\sigma(i)\gamma_i(j)} = f^\gamma_\sigma(a_{ij}).$$

Let us prove now the other implication:

$$\psi(f^\gamma_\sigma(a_{ij})) = \psi(a_{\sigma(i)\gamma_i(j)}) = a_{\sigma(i)\ \gamma_i(j)+1} =$$

$$a_{\sigma(i)\gamma_i(j+1)} = f^\gamma_\sigma(a_{i\ j+1}) = f^\gamma_\sigma(\psi(a_{ij}))$$

for all $i \in [n]$ and $j \in [k]$. □

4.3.1 Semidirect product of monoids

We now recall the definition of semidirect product of monoids

Definition 32. Let M, N be monoids and let $\Gamma : M \to \mathrm{End}(N)$ with $m \mapsto \Gamma_m$ be an antihomomorphism of monoids (i.e. $\Gamma_{m_1 m_2} = \Gamma_{m_2} \circ \Gamma_{m_1}$). We define $M \ltimes_\Gamma N$ as the monoid having support $M \times N$ and operation $*$ defined by the formula

$$(m_1, n_1) * (m_2, n_2) = (m_1 m_2, \Gamma_{m_2}(n_1)\, n_2)$$

Remark 33. It is straightforward to verify that the associative property holds.

We will now prove an easy lemma that will be useful in Section 4.4. For any monoid H let us denote by H^* the group of invertible elements of H.

Lemma 34. *Let $M \ltimes G$ be a semidirect product of monoids where G is a group. Then*

$$(M \ltimes G)^* = M^* \ltimes G$$

Proof. The inclusion $(M \ltimes G)^* \subseteq M^* \ltimes G$ is trivial, since if $(m, g) \in (M \ltimes G)^*$ then there exists (m', g') such that

$$(m, g) * (m', g') = (e_1, e_2)$$

so $mm' = e_1$ identity element of M. Let us now prove $(M \ltimes G)^* \supseteq M^* \ltimes G$. Let $(m, g) \in M^* \ltimes G$, then its inverse is $(m^{-1}, \Gamma_{m^{-1}}(g^{-1}))$. □

We are now ready to prove the main proposition of this section as a corollary of Theorem 31.

We first observe that the set of cyclic shifts of $[k]$ is clearly isomorphic to C_k, the cyclic group of order k, and each cyclic shift can be identified by its action on 1.

Corollary 35.

$$\mathcal{K}_\psi(U_n^k) \cong M_{[n]} \ltimes_\Gamma C_k^n$$

where Γ is defined by

$$\Gamma(\sigma)(\gamma) := \Gamma_\sigma(\gamma) := \gamma_\sigma := (\gamma_{\sigma(1)}, \ldots, \gamma_{\sigma(n)})$$

for any $\gamma \in C_k^n$.

Proof. The reader should first observe

$$\Gamma_\mu(\gamma_{\sigma(1)}, \ldots, \gamma_{\sigma(n)}) = (\gamma_{\sigma(\mu(1))}, \ldots, \gamma_{\sigma(\mu(i))}, \ldots, \gamma_{\sigma(\mu(n))})$$

for any $\sigma, \mu \in M_{[n]}$. This can be easily seen by denoting $\gamma_{\sigma(i)} =: g_i$. Therefore, Γ is an antihomomorphism, as we wanted:

$$\Gamma(\sigma\mu)(\gamma) = \gamma_{\sigma\mu} = (\gamma_{\sigma(\mu(1))}, \ldots, \gamma_{\sigma(\mu(i))}, \ldots, \gamma_{\sigma(\mu(n))}) =$$

$$\Gamma_\mu(\gamma_{\sigma(1)}, \ldots, \gamma_{\sigma(n)}) = \Gamma_\mu \circ \Gamma_\sigma(\gamma).$$

Let

$$\Delta : M_{[n]} \ltimes C_k^n \longrightarrow \mathcal{K}_\psi(U_n^k)$$

$$(\sigma, \gamma) \mapsto f_\sigma^\gamma.$$

Δ is clearly a bijection by Theorem 31. It is also an automorphism since

$$\Delta((\overline{\sigma}, \overline{\gamma}) * (\sigma, \gamma))(a_{i,j}) = \Delta(\overline{\sigma}\sigma, \overline{\gamma}_\sigma \gamma)(a_{i,j}) = f_{\overline{\sigma}\sigma}^{\overline{\gamma}_\sigma \gamma}(a_{i,j}) =$$

$$a_{\overline{\sigma}\sigma(i), \overline{\gamma}_{\sigma(i)}\gamma_i(j)} = f_{\overline{\sigma}}^{\overline{\gamma}}(a_{\sigma(i),\gamma_i(j)}) = f_{\overline{\sigma}}^{\overline{\gamma}} \circ f_\sigma^\gamma(a_{i,j}) =$$

$$\big(\Delta(\overline{\sigma}, \overline{\gamma}) \circ \Delta(\sigma, \gamma)\big)(a_{i,j})$$

for all $i \in [n]$ and all $j \in [k]$. □

4.4 Semigroup structure of T_q^m

Consider now T_q^m and notice that, since $M_{\mathbb{F}_{q^m}}(\mathcal{P}_{\varphi_q}) = \mathcal{L}_{\mathbb{F}_{q^m}}$ and $\mathcal{K}_{\varphi_q}(\mathbb{F}_{q^m}) = \mathcal{C}_{\varphi_q}$, then we have

$$T_q^m = \mathcal{L}_{\mathbb{F}_{q^m}} \cap \mathcal{C}_{\varphi_q} = M_{\mathbb{F}_{q^m}}(\mathcal{P}_{\varphi_q}) \cap \mathcal{K}_{\varphi_q}(\mathbb{F}_{q^m}). \tag{4.3}$$

Indeed the condition

$$f(S_k) \subseteq S_k$$

for each S_k in the partition induced by φ_q is equivalent to the subfield preserving requirement (4.2), being

$$S_1 = \mathbb{F}_q \quad \text{and} \quad S_k = \bigcap_{a|k,\, a \neq k} \left(\mathbb{F}_{q^k} \setminus \mathbb{F}_{q^a}\right) \quad \text{for } k \geq 2.$$

Any element α in a cycle of length d is associated to the irreducible polynomial $\prod_{i=0}^{d-1} (x - \alpha^{q^i}) \in \mathbb{F}_q[x]$, so there is a bijection between the cycles of φ_q of length d and the monic irreducible polynomials of degree d over $\mathbb{F}_q$, whose cardinality is

$$\pi(d) = \frac{1}{d} \sum_{j\,|d} \mu(d/j) q^j$$

with μ being the Moebius function. Now, write

$$\varphi_q = \prod_{k \mid m} \phi_k$$

similarly as above with $\phi = \varphi_q$ and label the elements of the finite field as follow: $a_{i,j}^{(k)}$ is the j-th element living in the i-th k-cycle.

Example 36. Let $\mathbb{F}_{2^2} = \mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1)$ consisting of $\{0, 1, \alpha, \alpha + 1\}$. Indeed

$$\varphi_q = \phi_1\phi_2 = (0)(1)(\alpha, \alpha + 1)$$

and then $a_{1,1}^{(1)} = 0$, $a_{2,1}^{(1)} = 1$, $a_{1,1}^{(2)} = \alpha$ and $a_{1,2}^{(2)} = \alpha + 1$.

Theorem 37.

$$T_q^m \cong \bigtimes_{k|m} M_{[\pi(k)]} \ltimes C_k^{\pi(k)} \tag{4.4}$$

Proof. It follows from Lemma 30 and Corollary 35 using the partition induced by the Frobenius morphism. Indeed, using equation 4.3 and Lemma 30 we get

$$T_q^m \cong \bigtimes_{k \in W, \phi_k \neq (\varnothing)} \mathcal{K}_{\phi_k}(S_k).$$

Using now Corollary 35 we get

$$T_q^m \cong \bigtimes_{k|m} M_{[\pi(k)]} \ltimes C_k^{\pi(k)}.$$

More explicitly, the action of $t \in \bigtimes_{k|m} M_{[\pi(k)]} \ltimes C_k^{\pi(k)}$ on an element $a_{i,j}^{(k)} \in S_k \subseteq \mathbb{F}_{q^m}$ is given by

$$t(a_{i,j}^{(k)}) = (\sigma^{(k)}, \gamma^{(k)})(a_{i,j}^{(k)}) = f_{\sigma^{(k)}}^{\gamma^{(k)}}(a_{i,j}^{(k)}) = a_{\sigma^{(k)}(i), \gamma_i^{(k)}(j)}^{(k)}$$

where $\gamma^{(k)}$ and $\sigma^{(k)}$ are the components indexed by k.

□

Corollary 38.

$$(T_q^m)^* \cong \bigtimes_{k|m} \mathcal{S}_{\pi(k)} \ltimes C_k^{\pi(k)}$$

where $\mathcal{S}_{\pi(k)}$ is the permutation group of $\pi(k)$ elements.

Proof. Observe that

$$(T_q^m)^* \cong \bigtimes_{k|m} (M_{[\pi(k)]} \ltimes C_k^{\pi(k)})^*$$

holds trivially. Applying now Lemma 34 yields

$$(T_q^m)^* \cong \bigtimes_{k|m} (M_{[\pi(k)]} \ltimes C_k^{\pi(k)})^* \cong \bigtimes_{k|m} \mathcal{S}_{\pi(k)} \ltimes C_k^{\pi(k)}.$$

□

Corollary 39.

$$|T_q^m| = \prod_{k\,|m} k^{\pi(k)} \pi(k)^{\pi(k)}$$

$$|(T_q^m)^*| = \prod_{k\,|m} k^{\pi(k)} \pi(k)!$$

Remark 40. Corollary 38 corresponds to [4, Theorem 2] and Corollary 39 generalizes the corollary of [4, Theorem 2].

Remark 41. Let us observe that a simpler construction as a direct product for $(T_q^m)^*$ can also be seen as follows:

- First notice that any permutation polynomial over $\mathbb{F}_q$ can be extended to a permutation polynomial over $\mathbb{F}_{q^m}$ with coefficients in $\mathbb{F}_q$ by simply defining it as the identity function on $\mathbb{F}_{q^m} \setminus \mathbb{F}_q$ and Lagrange interpolating over the whole field. The produced permutation polynomial over $\mathbb{F}_{q^m}$ has coefficients in $\mathbb{F}_q$, since it commutes with φ_q, which is easily checked by looking at the base field and the rest separately.
- $(T_q^m)^*$ has then a normal subgroup isomorphic to $\mathcal{S}_q$ consisting of

  $$\{s \in T_q^{m*} \mid s \text{ is the identity on } \mathbb{F}_{q^m} \setminus \mathbb{F}_q\}.$$

- Let

  $$H_q^m := \{h \in (T_q^m)^* \mid h \text{ is the identity on } \mathbb{F}_q\}.$$

  H_q^m is also normal in $(T_q^m)^*$.

- $\mathcal{S}_q \times H_q^m = (T_q^m)^*$. Indeed note first that $H_q^m \cap \mathcal{S}_q = 1$. Now given $f \in (T_q^m)^*$ we have to prove that it can be written as a composition of an element of H_q^m and an element of $\mathcal{S}_q$. Let $s_2 \in \mathcal{S}_q$ such that s_2 restricted to $\mathbb{F}_q$ is f. Let $s_1(x) \in \mathcal{S}_q$ such that s_1 restricted to $\mathbb{F}_q$ is the inverse permutation of the restriction of f to $\mathbb{F}_q$. In other words $f(s_1(x))$ restricted to $\mathbb{F}_q$ is the identity. Observe then that, since $f(s_1(x))$ has also coefficients in $\mathbb{F}_q$, it lives in H_q^m. Verify that $s_2(f(s_1(x))) = f$. And so we have written f as a composition of an element of $\mathcal{S}_q$ and an element of H_q^m.

4.5 Asymptotic density of T_q^m

Let us first compute the asymptotic density of the group of permutation polynomials described in [4] inside the whole group of permutation polynomials, and inside the monoid of the polynomial functions having coefficients in the subfield $\mathbb{F}_q$. We will restrict to the case $\mathbb{F}_{q^p}$, p prime.

Theorem 42. *Consider an element of $\mathbb{F}_q[x]/(x^{q^p} - x)$ chosen uniformly at random. The probability that this is a permutation polynomial tends to 0 as p and/or q tends to ∞.*

Proof. Given Corollary 39, we need to consider

$$L := \lim_{p \vee q \to \infty} \frac{q!(p)^{\frac{q^p-q}{p}} (\frac{q^p-q}{p})!}{q^{q^p}}.$$

By Stirling approximation this is

$$L = \lim_{p \vee q \to \infty} \frac{q!(p)^{\frac{q^p-q}{p}} (\frac{q^p-q}{pe})^{\frac{q^p-q}{p}} \sqrt{2\pi \frac{q^p-q}{p}}}{q^{q^p}}.$$

Now notice that

$$\lim_{p \vee q \to \infty} \left(\frac{q^p - q}{q^p}\right)^{\frac{q^p-q}{p}} = \lim_{p \vee q \to \infty} \left(1 - \frac{1}{q^{p-1}}\right)^{q^{p-1} \cdot \frac{q-q^{2-p}}{p}}$$

By the continuity of the exponential function, this can be written as

$$\lim_{p \vee q \to \infty} e^{\frac{q-q^{2-p}}{p} \ln\left(1-\frac{1}{q^{p-1}}\right)^{q^{p-1}}} = e^{-\lim_{p \vee q \to \infty} \frac{q}{p}}$$

so that

$$L = \lim_{p\vee q\to\infty} \frac{q!(q^p)^{\frac{q^p-q}{p}} e^{-\frac{q}{p}} \sqrt{2\pi\frac{q^p-q}{p}}}{q^{q^p} e^{\frac{q^p-q}{p}}}.$$

$$= \lim_{p\vee q\to\infty} \frac{q! e^{-\frac{q}{p}} \sqrt{2\pi\frac{q^p-q}{p}}}{q^q e^{\frac{q^p-q}{p}}} = 0,$$

as one can easily see by exploring the cases $q \to \infty$ with Stirling and q fixed. □

By observing that $q^p! > q^{q^p}$ definitively for large p and/or q, we have also the following:

Corollary 43. *Consider a permutation of the set $\mathbb{F}_{q^p}$ chosen uniformly at random. The probability that its associated permutation polynomial has coefficients in the subfield $\mathbb{F}_q$ tends to 0 as p and/or q tends to ∞.*

We are now interested in an asymptotic estimate for the density of T_q^p in $\mathbb{F}_q[x]/(x^{q^p} - x)$ for p prime number. We will show in fact that the monoid of canonical subfield preserving polynomials has nontrivial density inside the monoid of polynomial functions having coefficients in the subfield $\mathbb{F}_q$. Given Corollary 39, the probability that an element of $\mathbb{F}_q[x]/(x^{q^p} - x)$ chosen uniformly at random is subfield preserving is

$$\frac{|T_q^p|}{q^{q^p}} = \frac{q^q(q^p - q)^{\frac{q^p-q}{p}}}{q^{q^p}}.$$

Theorem 44. *Consider an element of $\mathbb{F}_q[x]/(x^{q^p} - x)$ chosen uniformly at random. The probability that this is subfield preserving tends to $e^{-\lim_{p\vee q\to\infty}\frac{q}{p}}$ as p and/or q tends to ∞.*

Proof. We need to consider

$$\ell := \lim_{p\vee q\to\infty} \frac{q^q(q^p - q)^{\frac{q^p-q}{p}}}{q^{q^p}}.$$

With similar arguments as in Theorem 42, this transforms to

$$\ell = \lim_{p\vee q\to\infty} \frac{q^q(q^p)^{\frac{q^p-q}{p}}}{q^{q^p}} e^{-\frac{q}{p}} = e^{-\lim_{p\vee q\to\infty}\frac{q}{p}}$$

□

Corollary 45.

- $\lim_{p\to\infty} \frac{|T_q^p|}{q^{q^p}} = 1$, *if q is fixed.*

- $\lim_{q\to\infty} \frac{|T_q^p|}{q^{q^p}} = 0$, *if* p *is fixed.*

Corollary 46. *Let* $q = p$.

$$\lim_{p\to\infty} \frac{|T_p^p|}{p^{p^p}} = 1/e$$

Remark 47. Clearly all the limits above are computed for p and q running over the natural numbers, but they hold in particular for the subsequences of increasing primes p and possible orders of finite fields q.

4.6 Example

Let us consider the structure of T_2^2 as an example. Let α be a root of $x^2 + x + 1 = 0$, so that $\mathbb{F}_{2^2} = \mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1)$. It is easy to check that for each polynomial $f \in L$ with

$$L := \{0, 1, x^2 + x, x^2 + x + 1, x^3, x^3 + 1, x^3 + x^2 + x, x^3 + x^2 + x + 1\}$$

we have $f(\alpha) \in \mathbb{F}_2$. We know that T_2^2 contains 8 polynomials, so that

$$T_2^2 = \frac{\mathbb{F}_2[x]}{(x^4 - x)} \setminus L =$$

$$\{x, x + 1, x^2, x^2 + 1, x^3 + x^2 + 1, x^3 + x, x^3 + x^2, x^3 + x + 1\}.$$

The structure is $C_2 \bigtimes M_2$.

Indeed $C_1^2 \rtimes M_2 = M_2$ and consists of

$$\{x, x^2 + 1, x^3 + x^2, x^3 + x + 1\}$$

that is those functions which fix $\mathbb{F}_4 \setminus \mathbb{F}_2$ and act as M_2 on $\mathbb{F}_2$.

Also $C_2 \rtimes M_1 = C_2$ and consists of

$$\{x, x^2\}$$

that is those functions which fix $\mathbb{F}_2$ and act as C_2 on $\mathbb{F}_4 \setminus \mathbb{F}_2$. This is also H_2^2.

Part II

Linear Maps over Finite Fields

Chapter 5

Linear Spanning sets

The results presented in this chapter come from a joint work with Joachim Rosenthal and Paolo Vettori [34].

5.1 Introduction

We start by stating a purely linear algebra problem:

Problem 48. Let m, n be integers and $\mathbb{F}$ be any field. Let A, S, B be matrices having entries in $\mathbb{F}$ of dimensions $m \times m$, $m \times n$ and $n \times n$ respectively. Give necessary and sufficient conditions for the $\mathbb{F}$-linear span of $\{A^i S B^j\}_{i,j \in \mathbb{N}}$ to be equal to the whole matrix space $\mathbb{F}^{m \times n}$.

A solution to this problem will be provided in Section 5.3.

Starting with Section 5.4 we will assume that the base field $\mathbb{F}$ represents the finite field $\mathbb{F} = \mathbb{F}_q$ having cardinality q. Under these conditions and the conditions that $\gcd(m, n) = 1$ and the characteristic polynomials of the matrices A and B are irreducible we are able to show in Section 5.4 that $\{A^i S B^j\}_{i,j \in \mathbb{N}}$ spans the whole vector space $\mathbb{F}^{m \times n}$ as soon as $S \neq 0$.

In Section 5.5 we will prove that whenever the set $\{A^i S B^j\}_{i,j \in \mathbb{N}}$ spans the whole matrix ring as a vector space over the finite field $\mathbb{F}$, we are able to explicitly compute the cardinality $\mathbb{F}[A]S\mathbb{F}[B]$. A particular instance of this computation (i.e. when S is the identity matrix and A, B have irreducible characteristic polynomial) has already been approached via inequalities in [6].

5.2 Notation and Preliminaries

Let $\mathbb{F}$ be a field and denote by $\langle \mathcal{S} \rangle_{\mathbb{F}}$ the linear span over $\mathbb{F}$ of a set $\mathcal{S}$ of elements in some $\mathbb{F}$-vector space. Entries, rows and columns of matrices are indexed by integers starting from zero; I_n and, respectively, $0_{m \times n}$ denote the $n \times n$ identity matrix and the $m \times n$ zero matrix — indices may be omitted when no ambiguity arises.

Moreover, given $M \in \mathbb{F}^{n \times n}$,

- the **minimal polynomial** μ_M of M is the monic generator of the ideal $\{p(s) \in \mathbb{F}[s] : p(M) = 0\}$;
- the **characteristic polynomial** of M is $\chi_M(s) = \det(sI - M)$;
- $\mathcal{E}_M$ is the set of eigenvalues of M, i.e., the zeros of χ_M in some field extension of $\mathbb{F}$;
- $\mathcal{L}_M^\lambda$ and $\mathcal{R}_M^\lambda$ are the left and, respectively, right eigenspaces of M associated with $\lambda \in \mathcal{E}_M$;
- $\mathcal{L}_M = \bigcup_{\lambda \in \mathcal{E}_M} \mathcal{L}_M^\lambda \setminus \{0\}$ and $\mathcal{R}_M = \bigcup_{\lambda \in \mathcal{E}_M} \mathcal{R}_M^\lambda \setminus \{0\}$ are the sets of left and, respectively, right eigenvectors of M.
- M is **cyclic** (or non-derogatory) if one of the following equivalent conditions holds true:
  - $\mu_M = \chi_M$;
  - M is similar to a companion matrix;
  - each eigenspace of M has dimension 1, i.e., every eigenvector has geometric multiplicity 1.

The definition of the Kronecker product and some of its properties are given next. More details may be found in [21, Section 12.1].

Definition 49. The **Kronecker product** of matrices $M \in \mathbb{F}^{m \times p}$ and $N \in \mathbb{F}^{n \times q}$ is the block matrix

$$M \otimes N = [m_{i,j} N]_{0 \leq i < m, 0 \leq j < p} \in \mathbb{F}^{mn \times pq},$$

representing the tensor product of the linear maps corresponding to M and N. Therefore, it satisfies the property

$$(M \otimes N)(P \otimes Q) = MP \otimes NQ, \tag{5.1}$$

whenever the matrix products on the right side can be computed.

The **(column) vectorization** of M is the (column) vector $\mathbf{col}(M) \in \mathbb{F}^{mp}$ formed by stacking the columns of M. Note that $\mathbf{col} : \mathbb{F}^{m\times p} \to \mathbb{F}^{mp}$ is an isomorphism of $\mathbb{F}$-vector spaces, establishing a correspondence between entry (i, j) of M and entry $i + mj$ of $\mathbf{col}(M)$.

Using this notation, given three matrices M, X, N of suitable dimensions,

$$\mathbf{col}(MXN) = (N^\top \otimes M)\,\mathbf{col}(X). \tag{5.2}$$

5.3 A basis for the vector space of $m \times n$ matrices

Let matrices A, B, and S as in Problem 48 and define

$$\mathscr{V}_{A,B;S} = \langle \{A^i S B^j\}_{i,j\geq 0}\rangle_{\mathbb{F}}.$$

In this and in the following section, conditions will be given that ensure that the dimension of $\mathscr{V}_{A,B;S}$ is maximal, i.e., equal to mn.

Theorem 50. *Let $A \in \mathbb{F}^{m\times m}$, $B \in \mathbb{F}^{n\times n}$, and $S \in \mathbb{F}^{m\times n}$ and consider the following conditions:*

$$\mathscr{V}_{A,B;S} = \mathbb{F}^{m\times n}; \tag{5.3}$$

$$A \text{ and } B \text{ are cyclic}; \tag{5.4}$$

$$uSv \neq 0,\ \forall u \in \mathcal{L}_A, v \in \mathcal{R}_B. \tag{5.5}$$

Then, (5.3) $\Leftrightarrow$ $\big($(5.4) *and* (5.5)$\big)$.

Proof. The proof of the theorem is given in [34]. □

Remark 51. The previous theorem has also an impact in Cryptography since it gives necessary and sufficient conditions for the attack in [31, Section 3] to be performed in *provable* polynomial time.

Example 52. Consider the following matrices, with $m, n \geq 2$:

$$A = \begin{bmatrix} 0 & 0 \\ I_{m-1} & 0 \end{bmatrix} \in \mathbb{F}^{m\times m}, \qquad B = \begin{bmatrix} 0 & I_{n-1} \\ 0 & 0 \end{bmatrix} \in \mathbb{F}^{n\times n}, \qquad S = \begin{bmatrix} 1 & 0 \\ 0 & 0_{(m-1)\times(n-1)} \end{bmatrix} \in \mathbb{F}^{m\times n}.$$

Both A and B are already in (left and right, respectively) Jordan canonical form. Therefore, their only eigenvalue is $\lambda = 0$, they are nilpotent and cyclic with minimal polynomials $\mu_A(s) = s^m$ and $\mu_B(s) = s^n$, and their eigenspaces are generated by $u = \begin{bmatrix} 1 & 0 & \cdots & 0 \end{bmatrix}$ (left eigenvector of A) and $v = \begin{bmatrix} 1 & 0 & \cdots & 0 \end{bmatrix}^\top$ (right eigenvector of B).

Even though S has rank 1, $uSv = 1 \neq 0$, whence conditions (5.4) and (5.5) of Theorem 50 are satisfied. Therefore, $\mathbb{F}$–linear combinations of matrices $E_{i,j} = A^i S B^j$, with $0 \leq i < m$ and $0 \leq j < n$, generate $\mathbb{F}^{m \times n}$ for any field $\mathbb{F}$.

Indeed, it is straightforward to check that each $E_{i,j}$ is one of the mn elements of the canonical basis of $\mathbb{F}^{m \times n}$, having its unique nonzero entry, equal to 1, at position (i, j). In other words, $\mathbf{col}(E_{i,j})$ is the $i + mj$-th vector of the canonical basis of $\mathbb{F}^{mn}$.

To the authors' knowledge, equality (5.3) and the kind of equivalent conditions that were presented in Theorem 50 have not been considered in the literature before (not even when $m = n$: see, for instance, the survey [19] containing a small section about spanning sets of matrix algebras).

When conditions (5.4) and (5.5) of Theorem 50 are not satisfied, matrices $A^i S B^j$, with $0 \leq i < m$ and $0 \leq j < n$, are linearly dependent. However, something more can be said about the dimension of the space they generate.

The general case demands an extremely complicated notation: only the case of cyclic and diagonalizable matrices A and B will be considered in this chapter.

Theorem 53. *Let $S \in \mathbb{F}^{m \times n}$ and suppose that $A \in \mathbb{F}^{m \times m}$ and $B \in \mathbb{F}^{n \times n}$ are cyclic and diagonalizable. In particular, be $U \in \mathbb{E}^{m \times m}$ and $V \in \mathbb{E}^{n \times n}$ two invertible matrices, in some extension field $\mathbb{E}$ of $\mathbb{F}$, such that UAU^{-1} and $V^{-1}BV$ are diagonal.*

Then, the dimension of $\mathscr{V}_{A,B;S}$, is equal to the number of nonzero entries of USV.

Before proving Theorem 53, we introduce the necessary notation and state a fundamental lemma.

Given $A \in \mathbb{F}^{m \times m}$, $B \in \mathbb{F}^{n \times n}$, and $S \in \mathbb{F}^{m \times n}$, let $r_{i,j} = \mathbf{col}(A^i S B^j)$ and define

$$R_{A,B;S} = \begin{bmatrix} r_{0,0} & r_{1,0} & \cdots & r_{m-1,0} & r_{0,1} & r_{1,1} & \cdots & r_{m-1,n-1} \end{bmatrix} \in \mathbb{F}^{mn \times mn}. \tag{5.6}$$

Then, given $v \in \mathbb{F}^n$, $\operatorname{diag}(v) \in \mathbb{F}^{n \times n}$ is the diagonal matrix defined by the components of v. Moreover, let $\operatorname{diag}(M) = \operatorname{diag}\big(\mathbf{col}(M)\big)$ for any matrix M.

Finally, let $\overline{x}^n = \begin{bmatrix} 1 & x & \cdots & x^{n-1} \end{bmatrix}$ and be $\mathcal{V}^n_{x_1,\ldots,x_k}$ the matrix whose rows are $\overline{x}^n_1, \ldots, \overline{x}^n_k$.

Lemma 54. *Let $A \in \mathbb{F}^{m\times m}$, $B \in \mathbb{F}^{n\times n}$, and $S \in \mathbb{F}^{m\times n}$. Suppose that $u_h \in \mathcal{L}^{\alpha_h}_A$, $0 \le h < s$, and $v_k \in \mathcal{L}^{\beta_k}_B$, $0 \le k < t$, are the rows and, respectively, columns of matrices $U \in \mathbb{E}^{s\times m}$ and $V \in \mathbb{E}^{n\times t}$ in a suitable extension field $\mathbb{E}$ of $\mathbb{F}$. Then,*

$$(V^\top \otimes U)R_{A,B;S} = \operatorname{diag}(USV)(\mathcal{V}^n_{\beta_1,\ldots,\beta_t} \otimes \mathcal{V}^m_{\alpha_1,\ldots,\alpha_s}). \tag{5.7}$$

Proof. Observe that, for any row u_h of U and column v_k of V, there exist $\alpha_h \in \mathcal{E}_A$ and $\beta_k \in \mathcal{E}_B$ such that $u_h \in \mathcal{L}^{\alpha_h}_A$ and $v_k \in \mathcal{R}^{\beta_k}_B$. Thus,

$$(v_k^\top \otimes u_h)\,\mathbf{col}(A^iSB^j) = u_hA^iSB^jv_k = u_hSv_k\,\alpha_h^i\beta_k^j$$

and, from (5.6), it follows that

$$(v_k^\top \otimes u_h)R_{A,B;S} = u_hSv_k\big(\overline{\beta}^n_k \otimes \overline{\alpha}^m_h\big).$$

Stacking up all these equalities, we get equation (5.7). □

Remark 55. Using Lemma 54, implication (5.3) ⇒ (5.5) of Theorem 50 can be proved in a much simpler way.

Indeed, suppose that the nonzero left-eigenvector $u \in \mathcal{L}^\alpha_A$ and right-eigenvector $v \in \mathcal{R}^\beta_B$ satisfy $uSv = 0$. Then, taking $U = u$ and $V = v$ in formula (5.7), we get

$$(v^\top \otimes u)R_{A,B;S} = (uSv)(\overline{\beta}^n \otimes \overline{\alpha}^m) = 0,$$

showing that $R_{A,B;S}$ does not have full rank. Therefore, its columns $\mathbf{col}(A^iSB^j)$ are linearly dependent and the set of matrices A^iSB^j cannot generate $\mathbb{F}^{m\times n}$.

Proof of Theorem 53. Let α_h, $0 \le h < m$ and β_k, $0 \le k < n$, be the left eigenvalues of A associated with the rows of U and, respectively, the right eigenvalues of B associated with the columns of V.

Since A and B are cyclic and diagonalizable, they have no repeated eigenvalues, whence $\mathcal{V}^m_{\alpha_1,\ldots,\alpha_s}$ and $\mathcal{V}^n_{\beta_1,\ldots,\beta_n}$ are invertible Vandermonde matrices.

By Lemma 54, we have that

$$(V^\top \otimes U) R_{A,B;S} = \operatorname{diag}(USV)(\mathcal{V}^n_{\beta_1,\dots,\beta_n} \otimes \mathcal{V}^m_{\alpha_1,\dots,\alpha_s}),$$

where both Kronecker products are invertible. So, $\operatorname{rank} R_{A,B;S} = \operatorname{rank} \operatorname{diag}(USV)$, which is equal to the number of nonzero entries of USV.

Since by definition (5.7), the (column) rank of $R_{A,B;S}$ is equal to the dimension of the space spanned by $A^i S B^j$, the proof is concluded. □

5.4 The irreducible case

For the remainder of the chapter we will assume that $\mathbb{F} = \mathbb{F}_q$ represents the finite field of order q.

The main result of this section will provide a necessary and sufficient condition for matrices A, B having irreducible characteristic polynomial which guarantees that condition (5.3) of Theorem 50 holds true:

Theorem 56. *Let $\mathbb{F}$ be a finite field, $A \in \mathbb{F}^{m\times m}$, $S \in \mathbb{F}^{m\times n}$ and $B \in \mathbb{F}^{n\times n}$. Suppose that A and B have irreducible characteristic polynomials. Then,*

$$\mathscr{V}_{A,B;S} = \mathbb{F}^{m\times n}, \forall S \neq 0 \text{ if and only if } \gcd(m,n) = 1.$$

Proof. Define the $\mathbb{F}$-linear map

$$\begin{aligned} \psi : \quad \mathbb{F}^{m\times n} &\to \mathbb{F}^{m\times n} \\ Z = [z_{i,j}] &\mapsto \textstyle\sum_{\substack{0\le i<m \\ 0\le j<n}} z_{i,j} A^i S B^j \end{aligned} \tag{5.8}$$

and note that $\mathscr{V}_{A,B;S}$ is the image of ψ. Therefore, we need to prove that $\ker \psi = \{0\}, \forall S \neq 0 \Leftrightarrow \gcd(m,n) = 1$. By (5.2) we obtain that

$$\mathbf{col}\left(\psi(Z)\right) = \mathbf{col}\left(\sum_{\substack{0\le i<m \\ 0\le j<n}} z_{i,j} A^i S B^j\right) = \sum_{\substack{0\le i<m \\ 0\le j<n}} z_{i,j} (B^j)^\top \otimes A^i \,\mathbf{col}(S).$$

Hence, by injectivity of **col**, it follows that ψ is injective (for any choice of $S \neq 0$) if and only if

the kernel of matrix $M = \sum_{0 \le i < m, 0 \le j < n} z_{i,j} (B^j)^\top \otimes A^i$ is trivial, i.e., M has no zero eigenvalues whenever $Z \neq 0$.

Observe first that, by the assumptions on A and B, the matrix rings $\mathbb{F}[A]$ and $\mathbb{F}[B]$ are fields. Moreover, all eigenvalue $\alpha \in \mathcal{E}_A$ and $\beta \in \mathcal{E}_B$ have $\mathbb{F}$-linearly independent powers up to degree $m-1$ and, respectively, $n-1$, being $\mathbb{F}(\alpha) \cong \mathbb{F}[A]$ and $\mathbb{F}(\beta) \cong \mathbb{F}[B]$, which are Galois extensions of $\mathbb{F}$ of degree m and, respectively, n.

By a classical result on Kronecker products (see, e.g., [21, Theorem 1, p. 411] for $\mathbb{F} = \mathbb{R}$, whose generalization to finite fields is straightforward) the set of eigenvalues of M is

$$\mathcal{E}_M = \left\{ \sum_{\substack{0 \le i < m \\ 0 \le j < n}} z_{i,j} \alpha^i \beta^j : \alpha \in \mathcal{E}_A, \beta \in \mathcal{E}_B \right\}, \tag{5.9}$$

where all eigenvalues are considered as elements in some common field extension.

So, $\ker \psi = \{0\}$ if and only if each sum in (5.9) is nonzero. In other words, for any two $\alpha \in \mathcal{E}_A$ and $\beta \in \mathcal{E}_B$, the products $\{\alpha^i \beta^j\}_{i<m, j<n}$ are $\mathbb{F}$-linearly independent. By [8, Proposition 5.1 and Theorem 5.5], this condition is equivalent to

$$\mathbb{F}(\alpha) \cap \mathbb{F}(\beta) = \mathbb{F}.$$

Since the intersection of $\mathbb{F}(\alpha)$ and $\mathbb{F}(\beta)$ is the field extension of $\mathbb{F}$ of degree $\gcd(m, n)$ (see [23, Theorem 2.6]), the proof is concluded. □

5.5 The cardinality of subsets of $\mathbb{F}[A]S\mathbb{F}[B]$

In this section we will explicitly compute the cardinality of the set $\mathbb{F}[A]S\mathbb{F}[B]$ whose relevance in Cryptography is discussed in [6, 26]. Define the space of polynomials

$$\mathcal{P}^k[s] = \{p(s) \in \mathbb{F}[s] : \deg p < k\}, \ k = 0, 1, \ldots$$

being, for instance, $\mathcal{P}^0 = \{0\}$ and $\mathcal{P}^1 = \mathbb{F}$.

Note that, given a square matrix M with $d = \deg \mu_M$,

$$\mathcal{P}^0[M] \subset \mathcal{P}^1[M] \subset \cdots \subset \mathcal{P}^{d-1}[M] \subset \mathcal{P}^d[M] = \mathcal{P}^k[M], \ \forall k \ge d.$$

The main objective of this section consists in calculating the cardinality of the set

$$\mathcal{M}_{A,B;S}^{h,k} = \mathcal{P}^h[A]S\mathcal{P}^k[B] \subseteq \mathbb{F}^{m\times n}.$$

Theorem 57. *Let $A \in \mathbb{F}^{m\times m}$, $B \in \mathbb{F}^{n\times n}$, and $S \in \mathbb{F}^{m\times n}$ such that $\mathscr{V}_{A,B;S} = \mathbb{F}^{m\times n}$. Then, for any $0 \leq h \leq m$ and $0 \leq k \leq n$,*

$$\left|\mathcal{M}_{A,B;S}^{h,k}\right| = \frac{(q^h-1)(q^k-1)}{q-1} + 1.$$

In order to demonstrate this statement, some specific notation and one preparatory lemma are needed.

First, for every $h \leq m$, let

$$\mathbb{F}^{h;m} = \{x \in \mathbb{F}^m : x_i = 0, \forall i = h, \ldots, m-1\},$$

being therefore $\mathbb{F}^h \cong \mathbb{F}^{h;m} \subseteq \mathbb{F}^m$. Define, for every $h \leq m$ and $k \leq n$, the bilinear map

$$\begin{aligned} \phi^{h,k} : \mathbb{F}^{h;m} \times \mathbb{F}^{k;n} &\to \mathbb{F}^{m\times n} \\ (x, y) &\mapsto xy^\top \end{aligned} \tag{5.10}$$

and, for the sake of simplicity, denote its image by

$$\Phi^{h,k} = \phi^{h,k}(\mathbb{F}^{h;m} \times \mathbb{F}^{k;n}). \tag{5.11}$$

Lemma 58. *Let A, B, and S as in Theorem 57. Then $\left|\mathcal{M}_{A,B;S}^{h,k}\right| = |\Phi^{h,k}|$.*

Proof. Consider the map ψ defined in (5.8). We claim that $\psi(\Phi^{h,k}) = \mathcal{M}_{A,B;S}^{h,k}$. Actually, for every $M \in \mathcal{M}_{A,B;S}^{h,k}$, there exist $(x, y) \in \mathbb{F}^{h;m} \times \mathbb{F}^{k;n} \subseteq \mathbb{F}^m \times \mathbb{F}^n$ such that

$$M = \left(\sum_{0\leq i<h} x_i A^i\right) S \left(\sum_{0\leq j<k} y_j B^j\right) = \sum_{\substack{0\leq i<m \\ 0\leq j<n}} x_i y_j A^i S B^j = \psi(xy^\top) \in \psi(\Phi^{h,k}).$$

Therefore, $\left|\mathcal{M}_{A,B;S}^{h,k}\right| \leq |\Phi^{h,k}|$. Moreover, when $\mathscr{V}_{A,B;S} = \mathbb{F}^{m\times n}$, ψ is injective and so $\Phi^{h,k} \leftrightarrow \mathcal{M}_{A,B;S}^{h,k}$. □

Observe that this lemma shows that the cardinality of $\mathcal{M}^{h,k}_{A,B;S}$ is independent of the choice of A, B, and S when condition (5.3) is met.

The problem is now reduced to the computation of the cardinality of $\Phi^{h,k}$, defined in (5.11).

Proof of Theorem 57. Consider again the map $\phi^{h,k}$, defined in (5.10), and observe that

$$\mathbb{F}^{h;m} \times \mathbb{F}^{k;n} = (\phi^{h,k})^{-1}(\Phi^{h,k}) = \bigcup_{Z \in \Phi^{h,k}} (\phi^{h,k})^{-1}(Z).$$

Consequently, since the inverse images are disjoint,

$$q^h q^k = |\mathbb{F}^{h;m} \times \mathbb{F}^{k;n}| = \left| \bigcup_{Z \in \Phi^{h,k}} (\phi^{h,k})^{-1}(Z) \right| = \sum_{Z \in \Phi^{h,k}} |(\phi^{h,k})^{-1}(Z)|.$$

To compute the value of the summation, we have to consider two situations.

- When $Z = 0$, $\phi(x, y) = xy^\top = 0$ if and only if all the products of each component of x and each component of y are zero if and only if $x = 0$ and $y = 0$ (1 case), $x = 0$ and $y \neq 0$ ($q^k - 1$ cases), or $x \neq 0$ and $y = 0$ ($q^h - 1$ cases). Therefore, $|\phi^{-1}(0)| = q^h + q^k - 1$.

- If $Z \neq 0$, observe that, by the bilinearity of $\phi^{h,k}$, $\phi^{h,k}(x, y) = \phi^{h,k}(\alpha x, \alpha^{-1} y)$ for every $\alpha \in \mathbb{F} \setminus \{0\}$.

  On the other hand, if $\phi^{h,k}(x, y) = \phi^{h,k}(\tilde{x}, \tilde{y})$ then $\tilde{x} = \alpha x$ and $\tilde{y} = \alpha^{-1} y$ for some $\alpha \neq 0$. Indeed, considering only the indexes i and j such that $x_i y_j = \tilde{x}_i \tilde{y}_j \neq 0$, we get that

  $$\frac{x_i}{\tilde{x}_i} = \frac{\tilde{y}_j}{y_j}.$$

  By the independency of the indices, it follows that $\alpha = \frac{x_i}{\tilde{x}_i} = \frac{\tilde{y}_j}{y_j}$ for every i, j. So, we conclude that $|(\phi^{h,k})^{-1}(Z)| = |\mathbb{F} \setminus \{0\}| = q - 1$.

Putting all together,

$$\begin{aligned} q^h q^k &= |(\phi^{h,k})^{-1}(0)| + \sum_{Z \in \Phi^{h,k} \setminus \{0\}} \left|(\phi^{h,k})^{-1}(Z)\right| \\ &= q^h + q^k - 1 + \sum_{Z \in \Phi^{h,k} \setminus \{0\}} (q-1) = q^h + q^k - 1 + \big(|\Phi^{h,k}| - 1\big)(q-1), \end{aligned}$$

whence

$$|\Phi^{h,k}| = \frac{q^h q^k - q^h - q^k + 1}{q-1} + 1 = \frac{(q^h-1)(q^k-1)}{q-1} + 1.$$

Finally, the claim follows by Lemma 58. □

5.6 Cryptanalysis of a noncommutative key exchange protocol

In this section we give an application of the results previously proved. An interesting development in the direction of a non commutative based scheme is provided in the sided action described in [26] (an attack to a certain instance based on semirings is also presented in [48]). Some cryptosystems relying on those ideas are implemented in [1] and [40] and in the patent US7184551. In this section we provide the cryptanalysis of these three schemes using the results in the previous sections. We first describe the noncommutative key exchange presented in [1] and [40]. Consider the group $\mathrm{GL}_n(\mathbb{F}_q)$ of invertible matrices of order n over the finite field $\mathbb{F}_q$ and $M_1, M_2 \in \mathrm{GL}_n(\mathbb{F}_q)$ such that $M_1 M_2 \neq M_2 M_1$. Let the public key be $(\mathrm{GL}_n(\mathbb{F}_q), M_1, M_2)$.

- Alice chooses $(a_1, a_2) \in \mathbb{Z}^2$ and sends $C_1 = M_1^{a_1} M_2^{a_2}$ to Bob
- Bob chooses $(b_1, b_2) \in \mathbb{Z}^2$ and sends $C_2 = M_1^{b_1} C_1 M_2^{b_2}$ to Alice
- Alice computes $K = M_1^{-a_1} C_2 M_2^{-a_2}$

As a result Alice and Bob can compute the secret key $K = M_1^{b_1} M_2^{b_2}$. The purpose of this section is to show that K can be computed in $O(n^3)$ field operations from C_1 and C_2.

5.6.1 Preliminaries

Cayley-Hamilton Theorem

Let $M \in \mathrm{GL}_n(\mathbb{F}_q)$ and f_M be the characteristic polynomial of M. Then $f_M(M) = 0$. As a result every power of M can be written in terms of a linear combination of $\{1, M, \ldots, M^{n-1}\}$ where n is the order of the matrix. A nice proof of this is presented in [29, p.21].

Solving homogeneous "mixed" multivariate polynomial equations of degree 2

In general solving multivariate polynomial equations is NP-complete [9]. In situations where the number of variables is much smaller than the number of equations there exists a polynomial time algorithm. To be precise: in [9] the authors proposed an "expected" polynomial time algorithm (eXtended Linearization) to solve overdefined polynomial equations when the number of unknowns k and the number of equations m satisfy the inequality $m \geq \varepsilon k^2$ where $\varepsilon \in (0, \frac{1}{2}]$. The expected running time is approximately of $k^{O(\frac{1}{\sqrt{\varepsilon}})}$. A few years after publication of XL, it has been realized that the algorithm can be regarded as a weak form of the F4 algorithm [12]. In our context we will use XL, since it will be more suitable for a direct application. In particular our approach will use a specialized version of XL that can be proved to lead to a polynomial time algorithm that breaks the protocols described in [1] and [40] in the generic condition. For all other cases we refer to the heuristic result in [9] that, for cryptanalytic purposes, will be enough.

Commutative rings of matrices

Let $M_{n\times n}(\mathbb{F}_q)$ be the algebra of $n \times n$ matrices over $\mathbb{F}_q$. Let T be an invertible matrix and define $\mathbb{F}_q[T]$ to be the $\mathbb{F}_q$-algebra generated by T. In other words $\mathbb{F}_q[T]$ is the image of the evaluation map

$$\psi : \mathbb{F}_q[x] \longrightarrow M_{n\times n}(\mathbb{F}_q)$$

$$\psi(p(x)) := p(T).$$

By Cayley-Hamilton theorem it follows that $\mathbb{F}_q[T]$ is a finite dimensional algebra over $\mathbb{F}_q$. The following short lemma will be useful for our purposes.

Lemma 59. *Let* $p(T) \in \mathbb{F}_q[T] \cap \mathrm{GL}_n(\mathbb{F}_q) =: (\mathbb{F}_q[T])^*$ *and*

$$C(T) := \{L \in \mathrm{GL}_n(\mathbb{F}_q) \mid LT = TL\}.$$

Then $p(T)^{-1} \in C(T)$.

Proof.

$$p(T)^{-1}T = (T^{-1}p(T))^{-1} = (p(T)T^{-1})^{-1} = Tp(T)^{-1}$$

□

5.6.2 Performing the attack

The attack described in the following sections makes use of the elementary tools mentioned above and this is intended to show the structural vulnerabilities of the system. Suppose Eve is observing the key exchange, she is then able to get the following information: $\{M_1, M_2, M_1^{a_1}M_2^{a_2}, M_1^{a_1+b_1}M_2^{a_2+b_2}\}$. Eve first observes $M_1^{a_1} \in \mathbb{F}_q[M_1]$ and $M_2^{a_2} \in \mathbb{F}_q[M_2]$ and that $M_1^{a_1}M_2^{a_2}$ is in the image of the application

$$\varphi : \mathbb{F}_q[M_1] \times \mathbb{F}_q[M_2] \longrightarrow M_{n\times n}(\mathbb{F}_q)$$

$$\varphi(h_1(M_1), h_2(M_2)) = h_1(M_1)h_2(M_2).$$

Then, we are able to write $M_1^{a_1}M_2^{a_2} = p(M_1)q(M_2)$, for some $p(x), q(x) \in \mathbb{F}_q[x]$ with

$$p(M_1) = \sum_{i=0}^{n-1} x_i M_1^i\,, \quad q(M_2) = \sum_{j=0}^{n-1} y_j M_2^j$$

and then

$$M_1^{a_1}M_2^{a_2} = \sum_{i=0,\, j=0}^{n-1} x_i y_j M_1^i M_2^j \tag{5.12}$$

where x_i, y_j are indeterminates. Observe that the system is solvable in polynomial time with $m = n^2$, $k = 2n$ and $\varepsilon = \frac{1}{4}$ and expected running time $O(n^2)$ (in the notation of [9]). We pick now *any* solution and write down $p(M_1)$ and $q(M_2)$.

Remark 60. The system given by Equation (5.12) is easy to solve, again even without the knowledge of the algorithm presented in [9] since they consist of n^2 homogeneous equations of degree 2 in $2n$ unknowns where we can perform a Gaussian elimination-like computation on the variables $u_{i,j} := x_i y_j$. We will show those equations with an explicit example in the next subsection. It is also elementary to observe that when the n^2 by n^2 matrix of the linear system

$$\sum_{i,j} u_{i,j} M_1^i M_2^j = M_1^{a_1}M_2^{a_2}$$

is invertible, the attack can be proven to be polynomial by the observation that the $u_{i,j}$ are unique and the system $x_i y_j = u_{i,j}$ admits a solution by construction (that can be found just by substitutions). In particular this happens when we have the non degenerate case, in the

sense that the k-vector space generated by the M^iN^j is the whole matrix ring; a necessary and sufficient condition for this to happen have already been described previously in the chapter.

Remark 61.

- We have at least one solution by the observation $M_1^{a_1}M_2^{a_2} \in \operatorname{img}\varphi$.
- We are not claiming $p(M_1) = M_1^{a_1}$ and $q(M_2) = M_2^{a_2}$. It has been observed in [26] that in order to break the protocol it is enough to find $U \in \mathbb{F}_q[M_1]$ and $V \in \mathbb{F}_q[M_2]$ such that $U = M_1^{a_1}$ and $V = M_2^{a_2}$.
- Since M_1, M_2 are invertible, also $p(M_1)$ and $q(M_2)$ are.
- $M_1^{a_1}M_2^{a_2} = p(M_1)q(M_2)$ implies

$$(p(M_1)^{-1}M_1^{a_1})(M_2^{a_2}q(M_2)^{-1}) = 1.$$

Eve gets the key thanks to the computation

$$p(M_1)^{-1}M_1^{a_1+b_1}M_2^{a_2+b_2}q(M_2)^{-1} =$$

$$p(M_1)^{-1}M_1^{b_1}M_1^{a_1}M_2^{a_2}M_2^{b_2}q(M_2)^{-1} =$$

$$M_1^{b_1}(p(M_1)^{-1}M_1^{a_1})(M_2^{a_2}q(M_2)^{-1})M_2^{b_2} =$$

$$M_1^{b_1}(p(M_1)^{-1}M_1^{a_1}M_2^{a_2}q(M_2)^{-1})M_2^{b_2} =$$

$$M_1^{b_1} \cdot 1 \cdot M_2^{b_2} = M_1^{b_1}M_2^{b_2} = K,$$

where the second equality is due to lemma 59 and the very last one by the solution of the system (5.12).

5.6.3 Cryptanalysis of the public key patented variant of the protocol

In this section we cryptanalise the patent $US7184551$.

Brief description

Public key

- Alice chooses $A, C \in GL_k(\mathbb{Z}_n)$ for $n = pq$ and p, q prime numbers
- $B = CAC$ and $G \in \mathbb{Z}_n[C]$
- Alice publishes (A, B, G)

Encryption

- Bob chooses $D \in \mathbb{Z}_n[G]$
- Bob computes $K = DBD$ and $E = DAD$
- Let M be the message in $GL_k(\mathbb{Z}_n)$
- Bob sends (KM, E)

Decryption

- Alice computes $CEC = K$
- Alice decrypts as $K^{-1}KM$

Cryptanalysis

The idea behind this cryptanalysis is the same as in the previous sections, we just need to make a revision of what it has already been done earlier in this section. In what follows we prove that factoring the modulus is enough to break the protocol, since any latter computation can be performed in polynomial time. Informally, the presented cryptanalysis is meant to show that in $US7184551$ matrices do not provide additional security features than integers. In addition, observe that the protocol is roughly k^2 times more expensive than RSA [43] in terms of memory (where k is the order of the matrices). If $M \in M_{k\times k}(\mathbb{Z}_n)$, let M_p and M_q denote its two reductions modulo p and q respectively. We reduce G, E and A modulo p and write the system

$$E_p = \left(\sum_{j=0}^{k-1} x_j G_p^j\right) A_p \left(\sum_{i=0}^{k-1} x_i G_p^j\right) \tag{5.13}$$

in k unknowns and k^2 homogeneous degree 2 equations over $\mathbb{F}_p^k$. We can assure at least one solution by the construction of $E_p = D_p A_p D_p$, since D_p can be written in terms of low powers

of G. We apply again the algorithm presented in [9] getting one solution for the system in polynomial time with $\varepsilon = 1/2$. This solution identifies a matrix $D' \in \mathbb{F}_p[G] \subseteq \mathbb{F}_p[C]$ such that

$$D'A_pD' = D_pA_pD_p = E_p \mod p.$$

Observe that we get the partial secret key $K_p = K \mod p$ by multiplying B_p on both sides by D'

$$D'B_pD' = D'C_pA_pC_pD' = C_pD'A_pD'C_p = C_pD_pA_pD_pC_p = K_p \mod p. \tag{5.14}$$

We perform the same procedure modulo q getting $D'' \in \mathbb{F}_q[G] \subseteq \mathbb{F}_q[C]$ such that $D''B_qD'' = K_q$. Since we have the computable isomorphism of rings

$$\psi : M_{k\times k}(\mathbb{Z}_n) \longrightarrow M_{k\times k}(\mathbb{F}_p) \oplus M_{k\times k}(\mathbb{F}_q)$$

given by the Chinese Remainder Theorem we are able to recover the secret key K just by taking the preimage of the pair (K_p, K_q) through ψ. Note that $\psi^{-1}(K_p, K_q)$ is exactly K by observing that K_p and K_q are necessarily the reductions of K modulo p and q (by the homomorphism properties of ψ) and then that $K = \psi^{-1}(K_p, K_q)$ since ψ is a bijection. In this procedure it is important to observe that both D' and D'' are guaranteed to exists thanks to the fact that D_p and D_q exist by construction and they are in the algebra generated by G. Once again, recall that D' (resp D'') is not guaranteed to equal D_p (resp. D_q), while K will always be correct thanks to equation (5.14).

Remark 62. Observe that the equations in (5.13) are even easier than the ones in (5.12) since they have the same structure but half of the unknowns. What is again important to observe is that Cayley Hamilton theorem always assures us a solution. In the next subsection we give an example to show how they look like.

Example

Let $n = 61133 = 541 \cdot 113$ and Alice's public key constructed as follows: let C be

$$\begin{pmatrix} 243 & 112 \\ 234 & 233 \end{pmatrix}$$

and

$$A = \begin{pmatrix} 121 & 231 \\ 144 & 242 \end{pmatrix}$$

then

$$CAC = B = \begin{pmatrix} 36124 & 40493 \\ 39554 & 16490 \end{pmatrix}.$$

Then we choose

$$G = 14 \cdot 1 + 3374 \cdot C = \begin{pmatrix} 25167 & 11090 \\ 55920 & 52560 \end{pmatrix}.$$

The public key will be (A, B, G). Bob secret key is constructed as follows: Let

$$D = 34125 \cdot 1 + 7123G = \begin{pmatrix} 56710 & 10234 \\ 36665 & 40513 \end{pmatrix}$$

$$K = \begin{pmatrix} 20609 & 51651 \\ 14785 & 1448 \end{pmatrix}$$

and

$$E = DAD = \begin{pmatrix} 57174 & 14133 \\ 7237 & 20711 \end{pmatrix}.$$

Let M be any message, then Bob sends

$$(KM, E).$$

Eve attacks the system as follows: she reduces E modulo 541 getting

$$E_{541} = \begin{pmatrix} 369 & 67 \\ 204 & 153 \end{pmatrix}.$$

She has now to solve the system

$$(x1 + yG_{541})A_{541}(x1 + yG_{541}) = E_{541}$$

getting for example the solution $(x_0, y_0) = (220, 159)$, so we get $K_{541} = (x_0 1 + y_0 G_{541})B_{541}(x_0 1 + y_0 G_{541})$ and then

$$K_{541} = \begin{pmatrix} 51 & 256 \\ 178 & 366 \end{pmatrix}.$$

Analogously one gets $K_{113} = (x_0 1 + y_0 G_{113})B_{113}(x_0 1 + y_0 G_{113})$ where $(x_0, y_0) = (55, 49)$, getting

$$K_{113} = \begin{pmatrix} 43 & 10 \\ 95 & 92 \end{pmatrix}.$$

By the Chinese Remainder Theorem we get

$$K = \begin{pmatrix} 20609 & 51651 \\ 14785 & 1448 \end{pmatrix}.$$

Chapter 6

Linearized Subfield Preserving maps

In this chapter we address the subfield preserving question of chapter 4 for the case of linear maps over finite fields. The results in this chapter are published in [30].

6.1 Introduction

In [3] the group structure of q-linear permutation polynomials of $\mathbb{F}_{q^m}$ having coefficients over the subfield $\mathbb{F}_{q^d}$ is provided. It is then natural to ask which is the monoid structure of q-linear canonical subfield preserving polynomials (of parameters (q^d, m)). In this chapter, in order to establish that monoid structure, we will use techniques from group and semigroup theory, linear algebra, commutative and non commutative ring theory and module theory. Indeed, the purposes we aim at, are not just getting new results, but also showing that classical finite field theoretic propositions can be easily obtained by using more general frameworks (as it happens for example in the case of Theorem 75, in comparison with the same result in [38, Theorem 3.8] and [38, Theorem 3.1]).

It follows a brief outline of the chapter. In Section 6.1.1 some preliminary definitions and notations are given. In Section 6.2 some elementary linear algebra propositions that will be useful in many of the following sections are proved. In Section 6.2.1 some monoid and group structures relative to restrictions of coefficients to some intermediate extensions between $\mathbb{F}_q$ and

$\mathbb{F}_{q^m}$ are provided.

6.1.1 Notation

Let d be a positive integer and let R be a commutative ring, let us denote by $\mathrm{Mat}_d(R)$ the ring of $d \times d$ matrices having entries in R. Let $\mathrm{GL}_d(R)$ be the multiplicative group of invertible elements of $\mathrm{Mat}_d(R)$ and $\mathrm{GL}_1(R)$ by R^*.

Let M be a module over R, let us denote $\mathrm{End}_R(M)$ the ring of endomorphisms of M as an R-module. Moreover, if G is a group we denote by $\mathrm{Aut}(G)$ the group of automorphisms of G as a group.

If S is any ring (possibly noncommutative), denote by $Z(S)$ the center of S. Let k be a field. In this section, all the vector spaces will be finite dimensional, and, if T is an endomorphism of a k-vector space V, let us denote $p^T_{\mathrm{char}}(x)$ and $p^T_{\mathrm{min}}(x)$ the characteristic polynomial and the minimal polynomial of T, respectively.

The reader should pay attention to the fact that, if $W \subseteq V$ are vector spaces, then we denote by $V \setminus W$ the difference of V and W as sets and by V/W the quotient as vector spaces. Let now $T \in \mathrm{End}_k(V)$ be such that $T(W) \subseteq W$, then we denote the restriction of T to W by $T_{|W}$ and the induced application on V/W as $\pi^V_W(T)$.

6.2 Preliminary definitions

Let V be a finite dimensional k-vector space and W be a subspace of V.

Definition 63. Define:

$$A(V,W) := \{f \in \mathrm{End}_k(V) \mid f(W) \subseteq W\}.$$

$$S(V,W) := \{f \in A(V,W) \mid f(V \setminus W) \subseteq V \setminus W\}.$$

Let now $T \in A(V,W)$ and set

$$C_V(T) := \{f \in \mathrm{End}_k(V) \mid f \circ T = T \circ f\}$$

We say that W is *T-closed* if $\gcd(p^{T_{|W}}_{\mathrm{min}}(x), p^{\pi^V_W(T)}_{\mathrm{min}}(x)) = 1$.

Remark 64. Observe that $A(V,W)$ is obviously a k-algebra and $S(V,W)$ is just a monoid under composition. Moreover we have the following

$$S(V,W) = \{f \in A(V,W) \mid \pi_W^V(f) \in \mathrm{Aut}_k(V/W)\}.$$

For the sake of completeness let us prove the following linear algebra lemma:

Lemma 65. *Let $T \in A(V,W)$ and W being T-closed. Then $p_{\min}^{T_{|W}}(x)p_{\min}^{\pi_W^V(T)}(x) = p_{\min}^T(x)$.*

Proof. First observe that both $p_{\min}^{T_{|W}}(x)$ and $p_{\min}^{\pi_W^V(T)}(x)$ divide $p_{\min}^T(x)$. Now, since they have greatest common divisor equal to 1, then their product divides $p_{\min}^T(x)$. In addition

$$\forall v \in V \quad p_{\min}^{T_{|W}}(T)p_{\min}^{\pi_W^V(T)}(T)(v) = p_{\min}^{T_{|W}}(T)\big(p_{\min}^{\pi_W^V(T)}(T)(v)\big) = 0$$

since $p_{\min}^{\pi_W^V(T)}(T)(v) \in W$.

□

For any $F \in A(V,W)$, let us denote $\pi_W^V(F) = \pi F$ whenever V and W are clear from the context.

Proposition 66. *Let $T \in A(V,W)$ and W be T-closed. Then:*

$$\mathbf{R} := C_V(T) \cap A(V,W) \cong C_W(T_{|W}) \times C_{V/W}(\pi_W^V(T))$$

as k-algebras.

Proof. Let

$$\psi : \mathbf{R} \to C_W(T_{|W}) \times C_{V/W}(\pi_W^V(T))$$

be defined by $\psi(f) := (f_{|W}, \pi f)$; Let us now prove that ψ is an injection. Let $\psi(f) = 0$ for some $f \in \mathbf{R}$. Therefore we have that f satisfies $f(W) = 0$ and $f(V) \subseteq W$. Observe that the operator $p_{\min}^{\pi T}(T_{|W})$ is invertible if and only if it is invertible in $k[T_{|W}]$, which is true, since $\gcd(p_{\min}^{\pi T}(x), p_{\min}^{T_{|W}}(x)) = 1$. Indeed

$$\forall v \in V \quad p_{\min}^{\pi T}(T_{|W})(f(v)) = p_{\min}^{\pi T}(T)(f(v)) = f(p_{\min}^{\pi T}(T)(v)) = 0$$

where the last equality follows since $p_{\min}^{\pi_W^V(T)}(T)(v) \in W$, as we already observed previously. Now, since $p_{\min}^{\pi T}(T_{|W})$ is invertible, we have $f(v) = 0$ for all $v \in V$.

Let now $(f, g) \in C_W(T_{|W}) \times C_{V/W}(\pi_W^V(T))$. In order to prove the surjectivity, we first observe that the morphisms

$$\cdot_{|W} : \mathbf{R} \longrightarrow C_W(T_{|W})$$

and

$$\pi : \mathbf{R} \longrightarrow C_{V/W}(\pi_W^V(T))$$

are both surjective. Thanks to the T-closure of W, it is easy to observe that both $p_{\min}^{\pi T}(T_{|W})$ and $p_{\min}^{T_{|W}}(\pi T)$ are invertible respectively on W and V/W. Let $h \in R$ such that $h_{|W} = f \cdot p_{\min}^{\pi T}(T_{|W})^{-1}$ and let $l \in R$ such that $\pi l = g \cdot p_{\min}^{T_{|W}}(\pi T)^{-1}$. Therefore

$$\psi(h \cdot p_{\min}^{\pi T}(T) + l \cdot p_{\min}^{T_{|W}}(T)) = (h_{|W} \cdot p_{\min}^{\pi T}(T_{|W}), (\pi l) \cdot p_{\min}^{T_{|W}}(\pi T))$$

$$= (f \cdot p_{\min}^{\pi T}(T_{|W})^{-1} p_{\min}^{\pi T}(T_{|W}), g \cdot p_{\min}^{T_{|W}}(\pi T)^{-1}) p_{\min}^{T_{|W}}(\pi T)) = (f, g).$$

□

Proposition 67. *Let $T \in A(V, W)$ and W be T-closed. Then it holds:*

$$C_V(T) \cap S(V, W) \cong C_W(T_{|W}) \times C_{V/W}(\pi_W^V(T))^* \tag{6.1}$$

as monoids.

Proof. Observe that the composition law in the monoid $C_V(T) \cap S(V, W)$ is the same as the multiplication in the algebra $\mathbf{R}$. Moreover we have the canonical embedding $C_V(T) \cap S(V, W) \subseteq C_V(T) \cap A(V, W)$. Therefore the claim is obtained by looking at the image of the LHS of (6.1) through the map ψ defined in Proposition 66. Now, applying Remark 64 we get the thesis. □

We now compute the centralizer algebra of a linear application T satisfying a suitable property.

Proposition 68. *Let U be a vector space and $T \in \operatorname{End}_k(U)$ such that $U \cong k[T]^d$ as a $k[T]$-module for some $d \in \mathbb{N}$. Then $C_U(T) \cong \operatorname{Mat}_d(k[T])$ as $\mathbb{F}_q$ algebras.*

Proof. By the standard theory of modules over rings we have

$$\mathrm{End}_{k}(U) \supseteq C_U(T) = \mathrm{End}_{k[T]}(U) \cong \mathrm{End}_{k[T]}(k[T]^d) = \mathrm{Mat}_d(k[T]).$$

□

6.2.1 Coefficients constraints for monoid structures

In this section we set up the problem we want to solve in terms of the linear algebra setting we developed before. Let q be a power of a prime p, $m \in \mathbb{N}^*$ and d be a divisor of m. Write $m = dp^t n$ where $\gcd(p, n) = 1$ and $n' := p^t n$.

Definition 69. Let d and m be positive integers such that $d|m$. We say that the extension $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^m}$ is *degenerate* if $p = \mathrm{char}(\mathbb{F}_q)$ divides m/d.

Let $\mathbb{F}_{q^m}$ be the finite field of order q^m and ϕ_q be the Frobenius morphism. Let $V = \mathbb{F}_{q^m}$ and $W = \mathbb{F}_{q^{dp^t}}$ considered as $\mathbb{F}_q$-vector spaces. Let us fix an $\mathbb{F}_q$-normal basis $\mathbf{B}$ for $\mathbb{F}_{q^m}$, i.e. a basis of the form

$$\mathbf{B} := \{\alpha, \alpha^q, \dots \alpha^{q^{m-1}}\}.$$

The existence of such a basis is guaranteed by the normal basis theorem [24, Theorem 2.35]. For $j \in \{0, \dots, d-1\}$, define

$$\mathbf{B}_j = \{\alpha^{q^j}, \alpha^{q^{j+d}}, \dots, \alpha^{q^{j+(n'-1)d}}\}$$

and V_j as the $\mathbb{F}_q$-span of $\mathbf{B}_j$.

Remark 70. It is elementary to observe that

$$V = \bigoplus_{j=0}^{d-1} V_j$$

as $\mathbb{F}_q$-vector spaces and also as $\mathbb{F}_q[\phi_{q^d}]$-modules.

Denote by W_j the $\mathbb{F}_q$-vector space $V_j \cap \mathbb{F}_{q^{dp^t}}$.

Lemma 71. *A basis for W_j consists of*

$$\mathbf{H}_j = \{\sum_{k=0}^{n-1} \alpha^{q^{j+kdp^t+id}}\}_{i\in\{0,\ldots,p^t-1\}}.$$

Proof. Let U_j be the span of $\mathbf{H}_j$. Clearly $U_j \subseteq W_j$ since the elements of $\mathbf{H}_j$ belong to W_j, therefore, if the set $\mathbf{H} = \bigsqcup_{j=0}^{d-1} \mathbf{H}_j$ consists of $p^t d$ linearly independent vectors we finished: Indeed, since $\mathbb{F}_{q^{dp^t}} = \bigoplus_{j=0}^{d-1} W_j$, no inclusion $U_j \subseteq W_j$ can be proper. It remains then to prove the linear independence of the vectors in $\mathbf{H}$. Assume

$$\sum_{j=0}^{d-1}\sum_{i=0}^{p^t-1} l_{i,j} \sum_{k=0}^{n-1} \alpha^{q^{j+kdp^t+id}} = 0.$$

We now prove that all the indices $j + kdp^t + id$ are distinct for any $k \in \{0, \ldots, n-1\}$ and any $j \in \{0, \ldots, d-1\}$, the result will follow since the α^{q^s}'s are independent for $s \in \{0, \ldots m-1\}$. Consider the index γ for which we have

$$\gamma = j + kdp^t + id = \overline{j} + \overline{k}dp^t + \overline{i}d.$$

γ has a unique remainder j in the division by d, it follows $j = \overline{j}$. Now we cancel out j and then d in the equation above; we now use the same argument to see that $k = \overline{k}$ and then $i = \overline{i}$. □

Notice that W_j has dimension p^t for all j's

Remark 72. Now, using the previous lemma we can observe that

$$V/W = \bigoplus_{j=0}^{d-1} V_j/W_j$$

as $\mathbb{F}_q$-vector spaces and also as $\mathbb{F}_q[\phi_{q^d}]$-modules.

Definition 73. Let $d|m$. Define

$$\mathscr{L}(q,d,m) := \{f : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^m} \mid f(z) = \sum_{i=0}^{m-1} a_i z^{q^i},\ a_i \in \mathbb{F}_{q^d}\}.$$

Remark 74. Observe that $\mathscr{L}(q,d,m)$ is isomorphic to $C_V(\phi_{q^d})$ since the coefficient property is given by the property of commuting with ϕ_{q^d}, see for example [4]. The linearity property follows

easily, since all $\mathbb{F}_q$- linear maps from $\mathbb{F}_{q^m}$ to itself consist exactly of the q-linearized polynomials up to degree q^{m-1}.

Let us now give a quick proof of [3, Theorem 3.1] using module theory. We have to warn the reader that the original proof of [3, Theorem 3.1] by Carlitz et al. is claimed by F. Özbudak to be not correct in [38, Theorem 3.8], where a long but nice proof of the same result is presented. We in fact show that, in the context of module theory, the proof of the same theorem is straightforward. Recall that $n' = np^t$ (with $\gcd(n, p^t) = 1$) and then $m = n'd$.

Theorem 75. *$C_{\mathbb{F}_{q^m}}(\phi_{q^d}) \cong \mathrm{Mat}_d\left(\mathbb{F}_q[z]/(z^{n'}-1)\right)$ as $\mathbb{F}_q$-algebras. In particular we have*

$$\mathscr{L}(q,d,m) \cong \mathrm{Mat}_d(\mathbb{F}_q[z]/(z^{n'}-1)).$$

Proof. Let $R := \mathbb{F}_q[z]/(z^{n'}-1)$. First observe that $R \cong \mathbb{F}_q[\phi_{q^d}]$ since $z^{n'}-1$ is the minimal polynomial for ϕ_{q^d}. It is enough to check that for every $j \in \{0,\ldots,d-1\}$ we have $R \cong V_j$ as $\mathbb{F}_q[\phi_{q^d}]$ modules, it will then follow that

$$R^d \cong \bigoplus_{j=0}^{d-1} V_j$$

as an $\mathbb{F}_q[\phi_{q^d}]$ module, so that we can apply Proposition 68 with $U = \mathbb{F}_{q^m}$ and $T = \phi_{q^d}$.

The required j-th isomorphism is given by

$$\xi_j : R \longrightarrow V_j$$

$$\xi_j(1) := \alpha^{q^j}$$

$$\xi_j(p(z)) := p(\phi_{q^d})(\alpha^{q^j}).$$

It is elementary to check that ξ_j is an isomorphism of R-modules. □

Corollary 76. *It holds:*

$$C_{\mathbb{F}_{q^m}/\mathbb{F}_{q^{dp^t}}}(\phi_{q^d}) \cong \mathrm{Mat}_d\left(\frac{\mathbb{F}_q[z]}{\left(\sum_{i=0}^{n-1} z^i\right)^{p^t}}\right).$$

Proof. Let $R' = \frac{\mathbb{F}_q[z]}{\left(\sum_{i=0}^{n-1} z^i\right)^{p^t}}$. Observe that W_j is an R-submodule of V_j with the same action as Theorem 75. Let ξ_j be as in Theorem 75, define the surjection

$$\overline{\xi}_j : R \longrightarrow V_j/W_j$$

with $\overline{\xi}_j(p(z)) = [p(\phi_{q^d})(\alpha^{q^j})]$. We now prove that $\overline{\xi}_j$ is also well defined (with the same action) on R': Indeed, notice that the kernel of $\overline{\xi}_j$ contains $\left(\sum_{i=0}^{n-1} z^i\right)^{p^t}$, since $\overline{\xi}_j\left(\sum_{i=0}^{n-1} z^{ip^t}\right) \in \mathbb{F}_{q^{dp^t}}$ as it is clear from the formula:

$$\left[\overline{\xi}_j\left(\sum_{i=0}^{n-1} z^{ip^t}\right)\right]^{q^{dp^t}} - \overline{\xi}_j\left(\sum_{i=0}^{n-1} z^{ip^t}\right) = \phi_{q^{dp^t}}\left(\overline{\xi}_j\left(\sum_{i=0}^{n-1} z^{ip^t}\right)\right) - \overline{\xi}_j\left(\sum_{i=0}^{n-1} z^{ip^t}\right)$$

$$= \overline{\xi}_j\left(z^{p^t}\sum_{i=0}^{n-1} z^{ip^t}\right) + \overline{\xi}_j\left(-\sum_{i=0}^{n-1} z^{ip^t}\right)$$

$$= \overline{\xi}_j\left(z^{p^t}\sum_{i=0}^{n-1} z^{ip^t} - \sum_{i=0}^{n-1} z^{ip^t}\right) = \overline{\xi}_j(z^m - 1) = 0.$$

Therefore we can now observe that the morphism

$$\overline{\xi}_j^* : R' \longrightarrow V_j/W_j$$

is surjective (since $\overline{\xi}_j$ is) and injective (since $\dim_{\mathbb{F}_q}(R') = \dim_{\mathbb{F}_q}(V_j/W_j)$). Thus, by Remark 72 we get

$$V/W = \bigoplus_{j=0}^{d-1} V_j/W_j = (R')^d$$

as an $\mathbb{F}_q[\phi_{q^d}]$ module. It follows

$$C_{\mathbb{F}_{q^m}/\mathbb{F}_{q^{dp^t}}}(\phi_{q^d}) \cong \mathrm{Mat}_d\left(\frac{\mathbb{F}_q[z]}{\left(\sum_{i=0}^{n-1} z^i\right)^{p^t}}\right)$$

using Proposition 68.

□

Recall that $m = n'd$.

Definition 77. Define $\mathcal{L}(q^d, n')$ as the set

$$\{f : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m} \mid f(\mathbb{F}_{q^d}) \subseteq \mathbb{F}_{q^d},\ f(\mathbb{F}_{q^{di}} \setminus \mathbb{F}_{q^{dj}}) \subseteq \mathbb{F}_{q^{di}} \setminus \mathbb{F}_{q^{dj}} \text{ for } i, j | n'\}.$$

We say that f is q^d-*canonical linearized subfield preserving* if it belongs to the set $\mathscr{T}(q, d, m) := \mathcal{L}(q^d, n') \cap \mathscr{L}(q, d, m)$.

Remark 78. Observe that $\mathscr{T}(q, d, m)$ is a monoid under composition since $\mathcal{L}(q^d, n')$ and $\mathscr{L}(q, d, m)$ are.

Let now $W' = \mathbb{F}_{q^d}$. Before going into the proof of the main theorem, let us give a characterization of the subfield preserving setting in the case of linearized polynomials with coefficients in a subfield.

Lemma 79. *Let $f \in \mathbb{F}_{q^d}[x]$ be $\mathbb{F}_q$-linear. Then it holds*

$$f \in \mathscr{T}(q, d, m) \iff \pi^V_{W'} f \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^m}/\mathbb{F}_{q^d}).$$

Proof. First observe that f is well defined (for any $l \in \mathbb{N}$) over $\mathbb{F}_{q^{dl}}/\mathbb{F}_{q^d}$, since it has coefficients over $\mathbb{F}_{q^d}$ and then $f(\mathbb{F}_{q^d}) \subseteq \mathbb{F}_{q^d}$. Clearly $f \in \mathscr{T}(q, d, m)$ implies $f(\mathbb{F}_{q^m} \setminus \mathbb{F}_{q^d}) \subseteq \mathbb{F}_{q^m} \setminus \mathbb{F}_{q^d}$ by definition of $\mathscr{T}(q, d, m)$. Let $[\alpha] \in \mathbb{F}_{q^m}/\mathbb{F}_{q^d}$: if $\pi f([\alpha]) = 0$ then $f(\alpha) \in \mathbb{F}_{q^d}$, that implies $[\alpha] = 0$.

Let now f be such that $\pi^V_{W'} f \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^m}/\mathbb{F}_{q^d})$ and assume (by contradiction) that

There exist $l, s \in \mathbb{N}$ dividing n' and $\alpha \in \mathbb{F}_{q^{dl}} \setminus \mathbb{F}_{q^{ds}}$ such that $f(\alpha) \in \mathbb{F}_{q^{ds}}$.

Therefore, reading the previous proposition modulo $\mathbb{F}_{q^d}$ we get

There exist $l, s \in \mathbb{N}$ dividing n' and $\alpha \in \frac{\mathbb{F}_{q^{dl}}}{\mathbb{F}_{q^d}} \setminus \frac{\mathbb{F}_{q^{ds}}}{\mathbb{F}_{q^d}}$ such that $[f(\alpha)] \in \frac{\mathbb{F}_{q^{ds}}}{\mathbb{F}_{q^d}}$.

Now, since $\pi f \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^m}/\mathbb{F}_{q^d})$ then $\pi f \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^{ds}}/\mathbb{F}_{q^d})$ which implies that there exists $\beta \in \frac{\mathbb{F}_{q^{ds}}}{\mathbb{F}_{q^d}}$ such that

$$\pi f([\beta]) = \pi f([\alpha]).$$

but $[\alpha] \neq [\beta]$ by construction, since they lie in different field extensions. The contradiction then follows from the fact that $\pi_{W'}^{V} f \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^m}/\mathbb{F}_{q^d})$. $\square$

We now combine the propositions above to obtain the monoid structure of $\mathscr{T}(q,d,m)$.

Theorem 80. *Let $\mathbb{F}_q$ be a finite field of characteristic p. Let $t,d,n \in \mathbb{N}$ $m = ndp^t$ and* $\gcd(n,p) = 1$. *It holds*

- *if $t = 0$ then*

$$\mathscr{T}(q,d,m) \cong \mathrm{Mat}_d\left(\frac{\mathbb{F}_q[z]}{(z-1)}\right) \times \mathrm{GL}_d\left(\frac{\mathbb{F}_q[z]}{\left(\sum_{i=0}^{n-1} z^i\right)}\right)$$

  as monoids.

- *if $t \geq 1$ then*

$$\mathscr{T}(q,d,m) \cong \mathrm{GL}_d\left(\frac{\mathbb{F}_q[z]}{(z-1)^{p^t}}\right) \times \mathrm{GL}_d\left(\frac{\mathbb{F}_q[z]}{\left(\sum_{i=0}^{n-1} z^i\right)^{p^t}}\right) \cong$$

$$\mathrm{GL}_d\left(\frac{\mathbb{F}_q[z]}{(z^{n'}-1)}\right)$$

  as groups.

Remark 81. The theorem above states something very strong:
In any degenerate case, there exists no linearized, subfield preserving polynomial with coefficients over $\mathbb{F}_{q^d}$ that is not invertible.
Indeed, the property of preserving the subfields assures the full invertibility of the associated linear function.

Proof of Theorem 80: First case: $t = 0$. In this case set $W' = W = \mathbb{F}_{q^d}$, $n = n'$ and $T = \phi_{q^d}$. Let us prove first $S(V,W) \cap C_V(T) = \mathscr{T}(q,d,m)$: If $f \in S(V,W) \cap C_V(T)$ then

$$f \in C_V(T) = \mathbb{F}_{q^d}[x]/(x^{q^m} - x)$$

(by definition) and $\pi_W^V f \in \mathrm{Aut}(V/W)$ by Remark 64. Indeed, by Lemma 79, $f \in \mathscr{T}(q,d,m)$. Now, using Proposition 67, we have

$$\mathscr{T}(q,d,m) = S(V,W) \cap C_V(T) \cong C_W(T_{|W}) \times C_{V/W}(\pi_W^V(T))^*.$$

Using now Corollary 76 for $C_{V/W}(\pi_W^V(T))^*$ and Theorem 75 for $C_W(T_{|W})$ we get

$$\mathscr{T}(q,d,m) \cong \mathrm{Mat}_d\left(\frac{\mathbb{F}_q[z]}{(z-1)}\right) \times \mathrm{GL}_d\left(\frac{\mathbb{F}_q[z]}{\left(\sum_{i=0}^{n-1} z^i\right)}\right).$$

Second case: $t \geq 1$. Set now $V = \mathbb{F}_{q^m}$, $W = \mathbb{F}_{q^{dp^t}}$ and $T = \phi_{q^d}$. Consider the isomorphism of monoids (obtained as above, using Proposition 67, Theorem 75 and Corollary 76)

$$\Omega : S(V,W) \cap C_V(T) \longrightarrow \mathscr{L}(q,d,p^t d) \times \mathrm{GL}_d\left(\frac{\mathbb{F}_q[z]}{\left(\sum_{i=0}^{n-1} z^i\right)^{p^t}}\right).$$

Observe that we have the following inclusion:

$$\mathscr{T}(q,d,m) \subseteq S(V,W) \cap C_V(T).$$

It follows that the isomorphism Ω induces an injection of monoids

$$\Omega : \mathscr{T}(q,d,m) \hookrightarrow \mathscr{L}(q,d,p^t d) \times \mathrm{GL}_d\left(\frac{\mathbb{F}_q[z]}{\left(\sum_{i=0}^{n-1} z^i\right)^{p^t}}\right).$$

Let

- $\mathbf{p} : \mathscr{L}(q,d,p^t d) \times \mathrm{GL}_d\left(\frac{\mathbb{F}_q[z]}{\left(\sum_{i=0}^{n-1} z^i\right)^{p^t}}\right) \to \mathscr{L}(q,d,p^t d)$ be the projection on the first component.
- $\mathbf{Res}_W : \mathscr{T}(q,d,m) \longrightarrow \mathscr{T}(q,d,p^t d)$ be the restriction morphism induced by the inclusion $\mathbb{F}_{q^{dp^t}} \subseteq \mathbb{F}_{q^m}$ to .
- $\iota : \mathscr{T}(q,d,p^t d) \hookrightarrow \mathscr{L}(q,d,p^t d)$ be the inclusion map.

With all this data we construct the following commutative diagram in the category of monoids:

$$\begin{array}{ccc} \mathscr{T}(q,d,m) & \xrightarrow{\Omega} & \mathscr{L}(q,d,p^t d) \times \mathrm{GL}_d\left(\frac{\mathbb{F}_q[z]}{\left(\sum_{i=0}^{n-1} z^i\right)^{p^t}}\right) \\ \Big\downarrow{\scriptstyle \mathbf{Res}_W} & & \Big\downarrow{\scriptstyle \mathbf{p}} \\ \mathscr{T}(q,d,p^t d) & \xrightarrow{\iota} & \mathscr{L}(q,d,p^t d) \end{array}$$

Let us first show that, *if*

$$\iota(\mathscr{T}(q,d,p^t d)) = \mathscr{L}(q,d,p^t d)^*$$

we finished: in fact, in this case, consider

$$\begin{array}{ccc} \mathscr{T}(q,d,m) & \xrightarrow{\Omega} & \mathscr{L}(q,d,p^t d)^* \times \mathrm{GL}_d\left(\frac{\mathbb{F}_q[z]}{\left(\sum_{i=0}^{n-1} z^i\right)^{p^t}}\right) \\ \Big\downarrow \mathbf{Res}_W & & \Big\downarrow \mathbf{p} \\ \mathscr{T}(q,d,p^t d) & \xrightarrow{\iota} & \mathscr{L}(q,d,p^t d)^* \end{array}$$

Moreover, we have that, for any two rings R and S, $\mathrm{GL}_d(R\times S) = \mathrm{GL}_d(R)\times\mathrm{GL}_d(S)$, it follows:

$$\mathscr{L}(q,d,p^t d)^* \times \mathrm{GL}_d\left(\frac{\mathbb{F}_q[z]}{\left(\sum_{i=0}^{n-1} z^i\right)^{p^t}}\right) = \mathrm{GL}_d\left(\frac{\mathbb{F}_q[z]}{(z^{n'}-1)}\right)$$

therefore

$$\mathscr{T}(q,d,m) \cong \mathrm{GL}_d\left(\frac{\mathbb{F}_q[z]}{(z^{n'}-1)}\right) \cong \mathscr{L}(q,d,m)^*$$

since Ω is an isomorphism. As a byproduct, we also have $\mathscr{T}(q,d,m)^* = \mathscr{T}(q,d,m)$. Therefore, in order to complete the proof, it is enough to show that $\mathscr{T}(q,d,p^t d) = \mathscr{L}(q,d,p^t d)^*$. The inclusion $\mathscr{L}(q,d,p^t d)^* \subseteq \mathscr{T}(q,d,p^t d)$ is obvious, in fact we already noticed in the introduction that every permutation polynomial having coefficients in a subfield is also subfield preserving for all the proper upper fields. The inclusion $\mathscr{T}(q,d,p^t d) \subseteq \mathscr{L}(q,d,p^t d)^*$ is more tricky. Consider the following commutative diagram in the category of rings:

$$\begin{array}{ccc} \mathscr{L}(q,d,p^t d) & \xrightarrow{\Delta} & \mathrm{Mat}_d\left(\frac{\mathbb{F}_q[z]}{(z-1)^{p^t}}\right) \\ \Big\downarrow \pi & & \Big\downarrow \overline{\pi} \\ \pi\mathscr{L}(q,d,p^t d) & \xrightarrow{\Delta_d} & \mathrm{Mat}_d\left(\frac{\mathbb{F}_q[z]}{(z-1)^{p^t-1}}\right) \end{array}$$

Above:

- $\pi\mathscr{L}(q,d,p^t d) \subseteq \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^m}/\mathbb{F}_{q^d})$ is the image of the morphism given by $f \mapsto \pi_W^V f$, that is consistent since any $f \in \mathscr{L}(q,d,p^t d)$ has a good reduction πf modulo $\mathbb{F}_{q^d}$, since $f(\mathbb{F}_{q^d}) \subseteq \mathbb{F}_{q^d}$.
- Δ is the isomorphism given by Theorem 75.

- $\overline{\pi}$ is the extension to the matrix ring of the projection morphism of rings

$$\pi' : \frac{\mathbb{F}_q[z]}{(z-1)^{p^t}} \longrightarrow \frac{\mathbb{F}_q[z]}{(z-1)^{p^t-1}}$$

- Δ_d is the isomorphism given by $\Delta_d(\pi f) = \overline{\pi}(\Delta(f))$, which is well defined since the minimum polynomial of ϕ_{q^d} over $\mathbb{F}_{q^d}$ is $z-1$.

For any $f \in \mathscr{L}(q,d,p^t d)$, the key observation is that:

$$\det(\Delta_d(\pi f)) = \det(\overline{\pi}(\Delta(f))) = \pi'(\det(\Delta(f))).$$

Now, if $f \in \mathscr{T}(q,d,p^t d) \subseteq \mathscr{L}(q,d,p^t d)$, then πf is invertible by Lemma 79. Therefore $z-1$ does not divide $\det(\Delta_d(\pi f))$, from which

$$z-1 \not| \, \pi'(\det(\Delta(f)))$$

Since the ring $\frac{\mathbb{F}_q[z]}{(z-1)^{p^t}}$ is local, the previous equation implies directly that

$$z-1 \not| \det(\Delta(f)).$$

Therefore f is invertible, so $\mathscr{T}(q,d,p^t d) = \mathscr{T}(q,d,p^t d)^* = \mathscr{L}(q,d,p^t d)^*$ □

Remark 82. We point out that [3, Theorem 3.1], and [3, Theorem 4.6] can be seen as corollaries of our Theorem 80. Indeed, in the non degenerate case, it holds:

$$\mathscr{L}(q,d,m)^* = \mathscr{T}(q,d,m)^* \cong \left(\mathrm{Mat}_d \left(\frac{\mathbb{F}_q[z]}{(z-1)} \right) \times \mathrm{GL}_d \left(\frac{\mathbb{F}_q[z]}{\left(\sum_{i=0}^{n-1} z^i \right)} \right) \right)^* =$$

$$\mathrm{GL}_d \left(\frac{\mathbb{F}_q[z]}{(z^n-1)} \right)$$

whereas in the degenerate case we have

$$\mathscr{T}(q,d,m) = \mathscr{T}(q,d,m)^* = \mathscr{L}(q,d,m)^* = \mathrm{GL}_d \left(\frac{\mathbb{F}_q[z]}{(z^{n'}-1)} \right).$$

6.2.2 Examples

Let us now give some examples:

Example 83. Let us consider the non degenerate case $m = 2$ and $q = 3$, let also $d = 1$, $t = 0$, $n = n' = 2$. We have that the monoid of 3-canonical, 3-linearized 2-subfield preserving polynomials consists of

$$\mathscr{T}(3, 1, 2) = \{x, 2x, x^3, 2x^3, 2x + x^3, x + 2x^3\}$$

that is isomorphic to the monoid

$$\left(\frac{\mathbb{F}_3[z]}{(z-1)} \times \left(\frac{\mathbb{F}_3[z]}{(z+1)}\right)^*, \cdot\right) = (\mathbb{F}_3 \times \mathbb{F}_3^*, \cdot)$$

Notice that, as expected in the non degenerate case, we have non invertible elements, i.e. $\{2x + x^3, x + 2x^3\}$ that correspond to $\{(0, 1), (0, 2)\}$.

Example 84. Let us consider the degenerate case $m = 4$, $q = 2$, $d = 1$, $t = 2$, and $p^t = 4$. Then we have

$$\mathscr{T}(2, 1, 4) = \{x, x^2, x^4, x + x^2 + x^4, x^8, x + x^2 + x^8, x + x^4 + x^8, x^2 + x^4 + x^8\}$$

that is isomorphic to

$$\left(\frac{\mathbb{F}_2[z]}{(z-1)^4}\right)^*.$$

Observe that in fact in this case all the elements in $\mathscr{T}(2, 1, 4)$ are invertible, as expected.

Chapter 7

Invertible Linearized Polynomials

7.1 Introduction

In this chapter we provide we provide a detailed group structure for invertible q-linearized polynomials over $\mathbb{F}_{q^m}$ having coefficients over a subfield $\mathbb{F}_{q^d}$. In what follows we use the results of Chapter 6. This is a joint work with Reto Schnyder.

7.1.1 Notation

We now fix the notation that will be used in the whole chapter. Let k be a field and d a positive integer. Let us denote by $\mathrm{Mat}_d(k)$ the algebra of d by d matrices over k. Let m be a positive integer and p be a prime number. Let $\mathbb{F}_q$ be a finite field of characteristic p and $\mathbb{F}_{q^m}$ the extension field of degree m, and take $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ to be a normal $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$. Moreover, let us denote by ϕ_q the Frobenius automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Since in this chapter we will not deal with p-adic numbers we will use the notation $\mathbb{Z}_p$ to address the additive group $(\mathbb{Z}/p\mathbb{Z}, +)$. For $d \mid m$, we denote by

$$\mathscr{L}(q, m, d) \coloneqq \mathbb{F}_{q^d}[\phi_q] = \{F \colon \mathbb{F}_{q^m} \to \mathbb{F}_{q^m} \mid F \in \mathbb{F}_{q^d}[x]\} \cap \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^m})$$

the algebra of linearized polynomials with coefficients in the subfield $\mathbb{F}_{q^d}$. If $d = 1$, we leave out the third argument: $\mathscr{L}(q, m) \coloneqq \mathscr{L}(q, m, 1)$.

7.2 Group structure for $\mathscr{L}(q,d,m)^*$

In this section we provide additional structure to the group $\mathscr{L}(q,m,d)^*$, described first in [3]. Let $n' = m/d$ and $n' = np^t$ with $\gcd(n,p) = 1$. In [3, Theorem 4.3], in order to describe $\mathrm{GL}_d(\mathbb{F}_q[z]/(z^{n'}-1))$, the ring $\mathbb{F}_q[z]/(z^{n'}-1)$ is decomposed (using the Chinese Remainder Theorem) as

$$\mathbb{F}_q[z]/(z^{n'}-1) \cong \prod_{i=1}^{\lambda} \mathbb{F}_q[z]/(h_i(z)^{e_i}).$$

Here, $\lambda, e_1, \ldots, e_\lambda \in \mathbb{N}$, and the $h_i(z)$ are distinct irreducible polynomials such that $z^{n'}-1 = \prod_{i=1}^{\lambda} h_i(z)^{e_i}$. Notice that $e_i = p^t$ for all i: Write

$$z^{n'}-1 = (z^n-1)^{p^t}$$

and note that $z^n - 1$ has no repeated irreducible factors, since

$$\gcd(z^n-1, \partial(z^n-1)) = \gcd(z^n-1, nz^{n-1}) = 1.$$

We denote the degree of $h_i(z)$ by δ_i (an interesting study of the degrees occurring in the factorization of x^n-1 is provided in [41]).

Recalling that $\mathrm{GL}(R\times S) = \mathrm{GL}(R)\times\mathrm{GL}(S)$, we have

$$\mathscr{L}(q,m,d)^* \cong \prod_{i=1}^{\lambda} \mathrm{GL}_d(\mathbb{F}_q[z]/(h_i(z)^{p^t})). \tag{7.1}$$

Our goal is now to provide a more specific structure for each component $\mathrm{GL}_d(\mathbb{F}_q[z]/h_i(z)^{p^t})$. We first need an elementary lemma from ring theory.

Lemma 85. *Let S be a (possibly noncommutative) ring, $r \in R$ be an invertible element and $e \in Z(S)$ a central and nilpotent element. Then $1-re$ is invertible.*

Proof. Let n be the smallest integer such that $e^n = 0$. A direct computation shows that the inverse of $1-re$ is

$$\sum_{i=0}^{n-1} r^i e^i.$$

□

We recall this elementary proposition from group theory (see for example []).

Proposition 86. *Let G be a group and K, N be subgroups of G. Let N be normal, $KN = G$ and $K \cap N = 1$. Then G is a semidirect product of K and N.*

Remark 87. Let t be a positive integer, $\mathbb{F}_q$ be a finite field of characteristic p and $f(z) \in \mathbb{F}_q[z]$ be an irreducible polynomial of degree D. Then the ring $\mathbb{F}_q[z]/(f(z)^{p^t})$ contains a copy of the finite field $\mathbb{F}_{q^D}$. In particular, this copy consists of $\mathbb{F}_q[z^{p^t}]/(f(z)^{p^t})$. In symbols:

$$\mathbb{F}_q[z^{p^t}]/(f(z)^{p^t}) = \left\{ \sum_{j=0}^{D-1} a_j z^{jp^t} \right\}_{a_j \in \mathbb{F}_q} \cong \mathbb{F}_{q^D}.$$

Theorem 88. *Let $d, t \in \mathbb{N}$ and $G \coloneqq \mathrm{GL}_d(\mathbb{F}_q[z]/(h(z)^{p^t}))$. Let*

$$N \coloneqq 1 + h(z)\,\mathrm{Mat}_d\,(\mathbb{F}_q[z]/(h(z)^{p^t})).$$

Then G is isomorphic to the semidirect product $N \rtimes_\zeta \mathrm{GL}_d(\mathbb{F}_{q^{\deg(h)}})$ for some morphism

$$\zeta\colon\ \mathrm{GL}_d(\mathbb{F}_{q^{\deg(h)}}) \longrightarrow \mathrm{Aut}(N)$$

Proof. We want to realize G as a semidirect product. Observe that $K \coloneqq \mathrm{GL}_d(\mathbb{F}_q[z^{p^t}]/h(z)^{p^t})$ is a subgroup of G and, by Remark 87, $K \cong \mathrm{GL}_d(\mathbb{F}_{q^{\deg(h)}})$. Indeed, we write the exact sequence

$$1 \to N \to \mathrm{GL}_d(\mathbb{F}_q[z]/(h(z)^{p^t})) \to K \to 1$$

where the last nontrivial morphism consists of raising to the power p^t each entry of a matrix in $\mathrm{GL}_d(\mathbb{F}_q[z]/(h(z)^{p^t}))$. We now verify the properties stated in Proposition 86.

- Observe that N is normal in G.
- $K \cap N = 1$. Let $g \in K \cap N$, then

$$g \in \mathrm{Mat}_d(\mathbb{F}_q[z^{p^t}]/(h(z)^{p^t})) \cap N.$$

Therefore, $g = 1 + h(z)A \in \mathrm{Mat}_d(\mathbb{F}_q[z^{p^t}]/(h(z)^{p^t}))$ for some matrix A in $\mathrm{Mat}_d(\mathbb{F}_q[z]/(h(z)^{p^t}))$.

Then,

$$a \coloneqq h(z)A \in \mathrm{Mat}_d(\mathbb{F}_q[z]/(h(z)^{p^t})).$$

Therefore, by considering any entry of a, say $h(z)p(z)$, we get the equation

$$h(z)p(z) = u(z^{p^t})$$

for some $u(z^{p^t}) \in \mathbb{F}_q[z^{p^t}]/(h(z)^{p^t})$. By raising the above equation to the p^t, we get

$$0 = h(z)^{p^t} p(z)^{p^t} = u(z^{p^t})^{p^t}.$$

It follows that $u(z^{p^t})$ is zero, since $\mathbb{F}_q[z^{p^t}]/(h(z)^{p^t})$ is a field. Therefore, every entry of a is zero, and so $g = 1$ as we wanted.

- $NK = G$. By looking at the exact sequence we observe that $G/N \cong K$, which implies $|K||N| = |G|$. Moreover, we have $|K||N| = |KN|$ because $K \cap N = 1$. This implies $|KN| = |G|$, which in turn implies $KN = G$.

Due to this construction, the morphism associated to the semidirect product is the conjugation by elements in K. More precisely, it is

$$\zeta_K \colon K \longrightarrow \mathrm{Aut}(N)$$

defined by

$$\zeta_K(F)(a) \coloneqq FaF^{-1}$$

for all $a \in N$ and $F \in K$. □

Remark 89. For the sake of completeness we have to describe how ζ is realized. Let $\psi \colon \mathbb{F}_q[z]/(h(z)) \to \mathbb{F}_q[z^{p^t}]/(h(z)^{p^t})$ be an isomorphism of fields and

$$\overline{\psi} \colon \mathrm{GL}_d(\mathbb{F}_{q^{\deg(h)}}) \longrightarrow \mathrm{GL}_d(\mathbb{F}_q[z^{p^t}]/(h(z)^{p^t})) = K$$

be its extension to the invertible matrix group

$$\zeta = \zeta_K \circ \overline{\psi}.$$

As stated, the conclusion of Theorem 88 may look somewhat technical. We derive some interesting consequences in what follows.

As subproduct we get

Corollary 90. *Let $l, n, d \in \mathbb{N}$, and let n be odd, $q = 2^l$ and $m = 2nd$. Then*

$$\mathscr{L}(q, m, d)^* \cong \prod_{i=1}^{\lambda} \mathbb{Z}_2^{d^2 l \delta_i} \rtimes_\Gamma \mathrm{GL}_d(\mathbb{F}_{2^{l\delta_i}})$$

for some $\Gamma\colon \mathrm{GL}_d(\mathbb{F}_{2^{l\delta_i}}) \to \mathrm{Aut}(\mathbb{Z}_2^{d^2 l \delta_i})$ suitably defined.

Proof. Observe the equivalences

$$\begin{aligned}(\mathbb{Z}_2^{d^2 l \delta_i}, +) &\cong (\mathbb{F}_{2^l}^{d^2 \delta_i}, +) \\ &\cong (\mathrm{Mat}_d(\mathbb{F}_{2^l}[z]/h_i(z)), +) \\ &\cong (1 + h_i(z)\,\mathrm{Mat}_d(\mathbb{F}_{2^l}[z]/h_i(z)^2), \cdot).\end{aligned}$$

The thesis now follows by combining formula (7.1) with Theorem 88 for $q = 2^l$ and $t = 1$. □

Remark 91. The reader should observe that the morphism Γ is determined by the equivalences in the proof of Corollary 90.

7.2.1 The commutative case

We now describe the case $d = 1$, where the coefficients of the linearized polynomials are contained in the base field $\mathbb{F}_q$. Let again $\prod_{i=1}^{\lambda} h_i(z)$ be the factorization of $z^n - 1$ into irreducible factors over $\mathbb{F}_q[z]$.

Theorem 92. *Let $n, l, t \in \mathbb{N}$ and p be a prime number not dividing n. Moreover, let $q = p^l$ and $m = p^t n$. Then*

$$\mathscr{L}(q, m, 1)^* \cong \left(\mathbb{Z}_p^{lnr_1} \times \cdots \times \mathbb{Z}_{p^t}^{lnr_t}\right) \times \prod_{i=1}^{\lambda} \mathbb{Z}_{q^{\delta_i}-1},$$

where

$$r_k = p^{t-k+1} - 2p^{t-k} + p^{t-k-1} \quad \textit{for } k = 1, \ldots, t-1$$
$$r_t = p - 1.$$

Proof. Let

$$N_i \coloneqq 1 + h_i(z)\mathrm{Mat}_1(\mathbb{F}_q[z]/(h_i(z)^{p^t})) = 1 + h_i(z)\mathbb{F}_q[z]/(h_i(z)^{p^t}),$$

$G_i \coloneqq (\mathbb{F}_q[z]/(h_i(z)^{p^t}))^*$ and $K_i \coloneqq (\mathbb{F}_q[z^{p^t}]/(h_i(z)^{p^t}))^* \cong \mathbb{Z}_{q^{\delta_i}-1}$. By Theorem 88 and formula (7.1) we have

$$\mathscr{L}(q, m, 1)^* \cong \prod_{i=1}^{\lambda} G_i \cong \prod_{i=1}^{\lambda} N_i \times K_i.$$

The reader should observe that in the previous equation the semidirect product drops, since N_i is commutative (and then the conjugation acts trivially on N_i) for every $i \in \{1, \ldots, \lambda\}$.

We will now consider each N_i for $i \in \{1, \ldots, \lambda\}$ separately. Any element $f(z) \in \mathbb{F}_q[z]/(h_i(z)^{p^t})$ can be uniquely written as

$$f(z) = \sum_{j=0}^{p^t-1} f_j(z)h_i(z)^j \tag{7.2}$$

for some $f_j(z) \in \mathbb{F}_q[z]$ of degree less than δ_i. The elements $f(z) \in N_i$ are exactly those with $f_0(z) = 1$. Clearly, any such element satisfies $f(z)^{p^t} = 1$.

Claim. Let $f(z) \in N_i$ and $k \geq 0$. Then, $f(z)^{p^k} = 1$ if and only if $f_0(z) = 1$ and $f_j(z) = 0$ for $j = 1, \ldots, p^{t-k} - 1$.

Proof. Let $g(z) = f(z) - 1$. The claim is equivalent to saying that $g(z)^{p^k} = 0$ if and only if $g_j(z) = 0$ for $j = 0, \ldots, p^{t-k} - 1$ ($g_j(z)$ as in equation (7.2)). Write

$$g(z)^{p^k} = \sum_{j=0}^{p^t-1} g_j(z)^{p^k} h(z)^{jp^k}.$$

The "if" direction is now obvious. For the "only if" direction, assume that $g(z)^{p^k} = 0$ but

$j_0 \coloneqq \min\{j \mid g_j(z) \neq 0\} < p^{t-k}$. If we lift to $\mathbb{F}_q[z]$, this means that

$$\begin{aligned} & h_i(z)^{p^t} \Big| \sum_{j=0}^{p^t-1} g_j(z)^{p^k} h(z)^{jp^k} \\ \Rightarrow\ & h_i(z)^{p^t - j_0 p^k} \Big| \sum_{j=j_0}^{p^t-1} g_j(z)^{p^k} h(z)^{jp^k - j_0 p^k} \\ \Rightarrow\ & h_i(z) \Big| \sum_{j=j_0}^{p^t-1} g_j(z)^{p^k} h(z)^{jp^k - j_0 p^k} \\ \Rightarrow\ & h_i(z) \,\big|\, g_{j_0}(z)^{p^k}. \end{aligned}$$

Since $h_i(z)$ is irreducible, we see that $h_i(z) \mid g_{j_0}(z)$. But this is impossible, since $g_{j_0}(z) \neq 0$ and $\deg g_{j_0} < \delta_i$. □

We now count the number of elements $f(z) \in N_i$ with $f(z)^{p^k} = 1$. From the claim, we see that

$$\Big|\{f(z) \in N_i \mid f(z)^{p^k} = 1\}\Big| = q^{\delta_i(p^t - p^{t-k})} = p^{l\delta_i(p^t - p^{t-k})}.$$

On the other hand, by the structure theorem of finite abelian groups, we can write

$$N_i \cong \mathbb{Z}_p^{s_1} \times \mathbb{Z}_{p^2}^{s_2} \times \cdots \times \mathbb{Z}_{p^t}^{s_t}$$

for some $s_1, \ldots, s_t \in \mathbb{N}$. Counting the elements of order dividing p^k, we have

$$\Big|\{f(z) \in N_i \mid f(z)^{p^k} = 1\}\Big| = p^{s_1} \cdot p^{2s_2} \ldots p^{ks_k} \cdot p^{ks_{k+1}} \ldots p^{ks_t}.$$

This gives the system of linear equations

$$l\delta_i(p^t - p^{t-k}) = s_1 + 2s_2 + \cdots + ks_k + ks_{k+1} + \cdots + ks_t$$

for $k = 1, \ldots, t$. We get the solution

$$\begin{aligned} s_k &= l\delta_i(p^{t-k+1} - 2p^{t-k} + p^{t-k-1}) \quad \text{for } k = 1, \ldots, t-1 \\ s_t &= l\delta_i(p-1). \end{aligned}$$

Write $s_k = l\delta_i \cdot r_k$. We then get

$$\begin{aligned}
\mathscr{L}(q,m,1)^* &\cong \prod_{i=1}^{\lambda} N_i \times K_i \\
&\cong \prod_{i=1}^{\lambda} \left(\mathbb{Z}_p^{l\delta_i r_1} \times \cdots \times \mathbb{Z}_{p^t}^{l\delta_i r_t} \right) \times \prod_{i=1}^{\lambda} C_{q^{\delta_i}-1} \\
&\cong \left(\mathbb{Z}_p^{lnr_1} \times \cdots \times \mathbb{Z}_{p^t}^{lnr_t} \right) \times \prod_{i=1}^{\lambda} C_{q^{\delta_i}-1}
\end{aligned}$$

as claimed. □

Part III

Knapsacks

Chapter 8

A general construction for multiplicative knapsack schemes

The results contained in this chapter come from a joint work with Michele Schiavina [31].

8.1 Introduction

Building new asymmetric encryption schemes has always been one of the main goals of cryptographers. After the idea of public key cryptography was presented in [10], only few more public key encryption schemes were developed such as the RSA [43], the El Gamal [11], the McEliece cryptosystem [28], the NTRU [18] or the HFE [39] (for an overview [16]). Some new ideas for building new cryptographic schemes based on semigroup actions can also be found in [26]. What D. Naccache and J. Stern built in [36] was a proposal for an asymmetric protocol (NSK). The NSK protocol consists of a shuffling modulo p of an easy problem over the integers, i.e. the factorization of a composite integer where the prime factors are chosen among a fixed set of small size. Given p a prime and $\mathbb{Z}/p\mathbb{Z}$ the finite field of remainder classes, the NSK protocol is based on the unique factorization property of $\mathbb{Z}$, which guarantees the uniqueness of the encryption.

This approach can be generalized to the case of multiplicative monoids (Section 8.1.1), and the NSK protocol is just a particular instance for the monoid $(\mathbb{Z}, \cdot)$ of the general framework (subsection 8.1.2). Using this new general setting we are able to construct an analogous of the NSK protocol relying on the unique factorization properties of $\mathbb{F}_q[x]$, instead of $\mathbb{Z}$, where $\mathbb{F}_q$ is

the finite field of order q (Section 8.2). The security of our particular proposal will rely on the arithmetic structure of the finite field $\mathbb{F}_q[x]/(h(x))$ for some $h(x) \in \mathbb{F}_q[x]$, irreducible of suitable degree (instead of the finite field of remainder classes $\mathbb{Z}/p\mathbb{Z}$). One of the main advantages of this kind of setting is that the security is based on an exponentiation over a finite field in such a way that it will be unfeasible for an attacker even to set up a discrete logarithm problem (DLP). Indeed, as we will show in the following, since the optimal version of the NSK protocol requires that the chosen prime be next to $\prod_i p_i$, the factorization of $p - j$ for some small j could allow for a reduction to a DLP. In our case, instead, we choose a set of irreducible polynomials and fix the degree of the reducing polynomial. By doing so there is no information leakage. Our new structural conditions will be related only to the degree of the carrier polynomials used for the encryption.

In subsection 8.6 some issues concerning the security of the protocol will be addressed, in particular to avoid *subgroup attacks*, that could possibly lead to information.

This new setting will lead to some advantages in terms of computational costs of encryption and decryption. In fact, arithmetic over finite fields $\mathbb{F}_{q^m}$ is considered to be preferable than arithmetic over $\mathbb{Z}_p$ when $p \simeq q^m$ and $q \ll p$ in terms of computations. We will analyse the key features of our protocol, such as the number of parameters involved for the setting up of the public key, and this will allow us to show a greater deal of flexibility, in comparison with the NSK protocol.

In subsection 8.5 we will analyse the asymptotics of the information rate of our protocol, showing that it is equal to that of [36]. An exact formula for the information rate will also be provided.

As a subproduct, we present in Section 8.7 a variation of the polynomial protocol where the irreducibility of $h(x)$ is dropped. The encryption is performed over a suitable direct sum of fields, and a decryption is available thanks to the Chinese Remainder Theorem.

8.1.1 The new class

In this section we will present a generalized version of the protocol presented in [36].

Let S be a monoid and $\sim$ a finite index congruence on S. We will denote the class of an element $s \in S$ with respect to $\sim$ as $[s]$.

Definition 93. A morphism ψ will be said to be $\sim$proper, if

- $\psi\colon S \longrightarrow S$ is injective;
- ψ is compatible with $\sim$ (i.e. $\psi(x) \sim \psi(y)$ iff $x \sim y$);
- the induced application $\widetilde{\psi}\colon S/\sim \longrightarrow S/\sim$ is invertible.

Definition 94. Given $L \in \mathbb{N}$ we will say that S is *L-cryptable* under $\sim$ if there exists a $\sim$proper morphism ψ and elements $s_1, \ldots, s_L \in S$ such that

$$\alpha_{\sim}^{\psi} : \mathbb{Z}_2^L \longrightarrow S/\sim$$

$$m = (m_1, \ldots, m_L) \mapsto \left[\prod_{i=1}^{L} \psi(s_i)^{m_i}\right]$$

is an injective application.

The following proposition will be useful later on

Proposition 95. *Given a monoid S that is L-cryptable under $\sim$, the following maps are also injective:*

$$\alpha^{\psi} : \mathbb{Z}_2^L \longrightarrow S$$

$$(m_1, \ldots, m_L) \mapsto \prod_{i=1}^{L} \psi(s_i)^{m_i}$$

$$\alpha_{\sim} : \mathbb{Z}_2^L \longrightarrow S/\sim$$

$$(m_1, \ldots, m_L) \mapsto \left[\prod_{i=1}^{L} s_i^{m_i}\right]$$

$$\alpha : \mathbb{Z}_2^L \longrightarrow S$$

$$(m_1, \ldots, m_L) \mapsto \prod_{i=1}^{L} s_i^{m_i}.$$

Proof. The proof follows by observing that, since ψ is $\sim$proper morphism, then also $\alpha_{\sim}$ is injective. Also $\alpha_{\sim}^{\psi}$ injective implies that α^{ψ} is injective. Again, since ψ is an injection, also α is injective. □

As we have already pointed out, this properties are necessary to keep the encryption meaningful. In the following we will see how it is possible to find non trivial examples of this construction.

Now, denote the image of any map f between sets by $\Im(f)$, and consider the following problems:

Problem 96. Given $c \in \Im(\alpha^{\psi}_{\sim})$ find m such that $\alpha^{\psi}_{\sim}(m) = c$.

Problem 97. Given $c' \in \Im(\alpha_{\sim})$ find m such that $\alpha_{\sim}(m) = c'$.

Let now S, be an L-cryptable monoid under a congruence $\sim$. Whenever a given triple $(S, \sim, \psi)$ is such that Problem 96 is difficult, Problem 97 is easy we define a cryptosystem as follows. Let

$$(S, \sim, L, \widetilde{\psi}([s_1]), \ldots, \widetilde{\psi}([s_L]))$$

be the public key and

$$(\widetilde{\psi}^{-1}, s_1, \ldots, s_L)$$

be the secret key, the main operations are given by

- *Encryption*: $E(m) := \alpha^{\psi}_{\sim}(m) = \prod_{i=1}^{L} \widetilde{\psi}([s_i])^{m_i} =: c$;
- *Decryption*: $D(c)$ is given by solving Problem 97 for $c' = \widetilde{\psi}^{-1}(c)$.

Remark 98. The reader should observe that in the definition of the protocol we did not use the injectivity of ψ nor the fact that $S/\sim$ is a quotient of a monoid S. This is nevertheless the case in all the examples of this protocol we could find, where Problem 97 is easy since a *suitable* lift to S is given. Indeed, in practical situations the problem will be solved computing $(\alpha^{-1} \circ \Gamma)(c')$ where Γ is a lift $S/\sim \longrightarrow S$ such that the following diagram

$$\begin{array}{ccc} \mathbb{Z}_2^L & \xrightarrow{\alpha} & \Im(\alpha) \\ & \searrow^{\alpha_\sim} & \uparrow \widehat{\Gamma} \\ & & \Im(\alpha_\sim) \end{array} \tag{8.1}$$

commutes when $\widehat{\Gamma} := \Gamma|_{\Im(\alpha_\sim)}$

Remark 99. Notice that the information rate is given by L/b where b is the number of bits that are needed to represent an element of $S/\sim$

In what follows we will show how the NSK protocol fits in this rather general framework, as well as brand new protocols involving polynomials over finite fields.

8.1.2 NSK as a particular instance

In this section we will show how the Naccache-Stern (NSK) protocol fits in our general framework, in the case $S = (\mathbb{Z}, \cdot)$.

Consider the prime ideal $P = \langle p \rangle$ generated by a prime number $p \in \mathbb{Z}$. Let us denote by $\sim$ the congruence induced by the ideal P. Such a congruence is obviously of finite index. Let v be a positive integer with $u = v^{-1} \mod p - 1$, and let

$$\begin{aligned} \psi \colon \mathbb{Z} &\longrightarrow \mathbb{Z} \\ a &\longmapsto a^v. \end{aligned}$$

It can be easily checked that ψ is a $\sim$proper morphism of $\mathbb{Z}$.

Now choose L distinct prime numbers p_i such that $\prod_{i=1}^{L} p_i < p$.

Proposition 100. *The map*

$$\begin{aligned} \alpha_{\sim}^{\psi} \colon \mathbb{Z}_2^L &\longrightarrow \mathbb{Z}/p\mathbb{Z} \\ (m_1, \ldots, m_L) &\longmapsto \left[\prod_{i=1}^{L} p_i^{m_i v} \right] \end{aligned} \tag{8.2}$$

is an injection and $(\mathbb{Z}, \cdot)$ is therefore L-cryptable under the relation induced by the ideal generated by p.

Proof. Assume that there exist two L-tuples $(m_1, \ldots, m_L), (n_1, \ldots, n_L)$ such that $\alpha_{\sim}^{\psi}(m_1, \ldots, m_L) = \alpha_{\sim}^{\psi}(n_1, \ldots, n_L)$, then

$$\left[\prod_{i=1}^{L} p_i^{m_i v} \right] = \left[\prod_{i=1}^{L} p_i^{n_i v} \right] \Rightarrow \left[\prod_{i=1}^{L} p_i^{m_i v} \right]^u = \left[\prod_{i=1}^{L} p_i^{n_i v} \right]^u \Leftrightarrow \left[\prod_{i=1}^{L} p_i^{m_i} \right] = \left[\prod_{i=1}^{L} p_i^{n_i} \right]$$

in $\mathbb{Z}/p\mathbb{Z}$. Since $\prod_{i=1}^{L} p_i^{m_i}$ and $\prod_{i=1}^{L} p_i^{n_i}$ are smaller than p we also have

$$\prod_{i=1}^{L} p_i^{m_i} = \prod_{i=1}^{L} p_i^{n_i} \tag{8.3}$$

in the unique factorization domain $\mathbb{Z}$, which implies $m_i = n_i \ \forall i$. □

Remark 101. Notice that we are able to express equation (8.3) because we can always consider the canonical representative $x \in \{0, \ldots, p-1\}$ in the remainder class modulo p. This represen-

tative is also the only representative in $\Im(\alpha)$ by construction, and therefore we have a canonical lift satisfying (8.1).

Remark 102. The reader should observe that when $p = t + \prod_i p_i$ for t small, than the information rate is maximal. Unfortunately in this case factoring $p - t$ is easy because $p - t$ is p_L-smooth and $p_L \ll p$, and this gives informations about the bare carriers p_i's. Indeed in this case breaking the NSK protocol is not harder than solving the DLP for the p_i's. Nevertheless the protocol remains interesting for additional features like [36, Section 3].

8.2 A polynomial version

In this section we give a version of the protocol that works over $\mathbb{F}_{q^d}$ instead of $\mathbb{Z}/p\mathbb{Z}$ in such a way that q^d will be of the same order of magnitude than the size p of the field $\mathbb{Z}/p\mathbb{Z}$ in the NSK but $q \ll p$. In this case the specific difficult problem we want to rely on is the following

Problem 103. Let $\mathbb{F}$ be a finite field and $L \in \mathbb{N}$.Given $y_1, \ldots, y_L \in \mathbb{F}$,

$$\alpha : \mathbb{Z}_2^L \longrightarrow \mathbb{F}$$

$$\alpha(m) = \prod_i y_i^{m_i}$$

and $c \in \Im(\alpha)$, find m such that $\alpha(m) = c$.

Let now $k = \mathbb{F}_q$ and $k[x]$ the polynomial ring in one variable over k. Let $h(x)$ be an irreducible element in $k[x]$ of degree d. Set $\sim$ to be the congruence associated to the ideal $H = \langle h(x) \rangle$ generated by the irreducible polynomial $h(x)$. Set

$$S = (k[x], \cdot)$$

and

$$S' := S/\sim = ((k[x]/H)^*, \cdot)$$

where $(k[x]/H)^* = (k[x]/H) \setminus \{0\}$. Fix $v, u \in \mathbb{N}$ such that $\gcd(v, |S'|) = \gcd(v, q^d - 1) = 1$ and

$uv \equiv 1 \mod |S'|$. Set

$$\widetilde{\psi}\colon S' \longrightarrow S'$$
$$[s] \longmapsto [s^v].$$

Remark 104.

- $\widetilde{\psi}^{-1}\colon [z] \longmapsto [z]^u$;
- $k[x]/H \cong \mathbb{F}_{q^d}$ is again a finite field.

Let now $L \in \mathbb{N}$ such that there exist L distinct irreducible monic polynomials $p_1, \ldots, p_L \in \mathbb{F}_q[x]$ with the property

$$\sum_{i=1}^{L} \deg p_i < d. \tag{8.4}$$

Notice that in the present description of the protocol there are several different strategies to choose the polynomials; we will analyse the properties of some interesting choices in the following sections.

Again, we have the encryption map.

Proposition 105. *$(k[x], \cdot)$ is an L cryptable monoid with the map*

$$\begin{aligned} \alpha_{\sim}^{\psi} &: \mathbb{Z}_2^L \longrightarrow S' \\ m = (m_1, \ldots, m_L) &\longmapsto \left[\prod_{i=1}^{L} p_i^{vm_i}\right]. \end{aligned} \tag{8.5}$$

Proof. Definition 94 requires that the map $\alpha_{\sim}^{\psi}$ be an injection. Assume

$$\alpha_{\sim}^{\psi}(m_1, \ldots, m_L) = \alpha_{\sim}^{\psi}(n_1, \ldots, n_L)$$
$$\left[\prod_{i=1}^{L} p_i^{vm_i}\right] = \left[\prod_{i=1}^{L} p_i^{vn_i}\right].$$

It follows

$$\left[\prod_{i=1}^{L} p_i^{vm_i}\right]^u = \left[\prod_{i=1}^{L} p_i^{vn_i}\right]^u$$
$$\left[\prod_{i=1}^{L} p_i^{m_i}\right] = \left[\prod_{i=1}^{L} p_i^{n_i}\right]$$

where, in the last equation, we can assume no reduction has happened, since property (8.4)

holds. Indeed

$$\prod_{i=1}^{L} p_i^{m_i} = \prod_{i=1}^{L} p_i^{n_i}. \tag{8.6}$$

Recalling that $k[x]$ is a unique factorization domain we have $m_i = n_i \ \forall i$. □

So our ciphered text is given by $c(x) = \alpha_{\sim}^{\psi}(m_1, \ldots, m_L)$. The explicit decryption for this protocol is simply given by the polynomial division of the deciphered code $(c(x))^u$, that is to say

$$m_i = 1 \Longleftrightarrow (c(x))^u = 0 \mod p_i(x). \tag{8.7}$$

Remark 106. We stress once again the fact that in obtaining equation (8.6) we used the canonical lift

$$\begin{aligned} \Gamma \colon S/\sim &\longrightarrow S \\ [f(x)] &\longmapsto g(x) \end{aligned}$$

where, for any representative $l(x) \in [f(x)]$, $g(x)$ is the remainder of the division of $l(x)$ by $h(x)$ in $k[x]$, and it is obviously independent of the choice of $l(x)$. The decryption is effectively performed in $\Im(\alpha)$ and the solution to Problem 97 is then given by $(\alpha^{-1} \circ \Gamma)(c(x)^u)$.

The information rate $\mathcal{I} = L/\deg(h)\log_2(q)$ depends on the choice of the carrier polynomials. We will explain later how to maximise this value.

Remark 107. Once the p_i's are fixed the top information rate for this protocol is obtained when we choose $h(x)$ such that

$$\sum_{i=1}^{L} \deg p_i = \deg h - 1. \tag{8.8}$$

Indeed the information rate can always be maximised since it is always possible to choose $h(x)$ in $k[x]$ such that (8.8) is satisfied (cf. Remark 102) without allowing for a straightforward reduction to a DLP. This case will be analysed in detail in 8.4.

Remark 108. The reader should notice that the encryption in this protocol together with the generic problem the attacker has to solve are similar to the ones in Lenstra's Powerline system [22, (2.5)]. We want now to point out the main differences between Lenstra's approach and ours.

1. The form of the carriers for the powerline is quite special [22, (2.1) System Generation, (g)]: the v_i's are in fact chosen to be all powers of linear polynomials over the base field multiplied by a fixed element u

$$v_i = u^k \cdot (t - c_i)^k$$

for c_i in $\mathbb{F}_q$, t generator for $\mathbb{F}^*_{q^h}$ and $u \in \mathbb{F}_{q^h}$. This leads to a structural weakness as explained in [22, Section 5].

2. In order to avoid exhaustive search attacks on the messages, both the base field $\mathbb{F}_q$ and the weight of the message h (which is also the degree of the extension field) must be chosen quite large. In our version the base field can be chosen to be small, since the number of carriers is the only parameter on which the degree of the irreducible polynomial we select depends on.

3. The randomness given by the multiplication by u of each carrier is paid with the condition $\sum_i m_i = h$, which is a restriction we do not have.

4. It is straightforward to observe that the decryption of our variant is cheaper compared to [22, (2.6)] in terms of computations.

5. Our approach is based on a principle that can be easily generalized to function fields using properties of Riemann-Roch spaces as section 8.8 shows.

8.2.1 A simple example

We now give an example in which $k[x] = \mathbb{F}_2[x]$ and the space of messages has size 2^9. In order to reach a message size of 9 bits, we need exactly 9 keys, that is to say monic irreducible polynomials in $\mathbb{F}_2[x]$. From finite field theory, we know that there are exactly q monic polynomials of degree 1, and

$$\frac{q^d - q}{d}$$

irreducible monic polynomials of prime degree d. So, for $q = 2$ we have two polynomials of degree 1, one polynomial of degree 2, two polynomials of degree 3 and six polynomials of degree 5. For the sake of simplicity, even if the example is non optimal as we will explain, let us choose

all the irreducible monic polynomials of degree 1,2 and 5, summing up to exactly 9 keys, namely:

$$p_1 = x \tag{8.9}$$

$$p_2 = 1 + x \tag{8.10}$$

$$p_3 = 1 + x + x^2 \tag{8.11}$$

$$p_4 = 1 + x^2 + x^5 \tag{8.12}$$

$$p_5 = 1 + x^3 + x^5 \tag{8.13}$$

$$p_6 = 1 + x + x^2 + x^3 + x^5 \tag{8.14}$$

$$p_7 = 1 + x + x^2 + x^4 + x^5 \tag{8.15}$$

$$p_8 = 1 + x + x^3 + x^4 + x^5 \tag{8.16}$$

$$p_9 = 1 + x^2 + x^3 + x^4 + x^5. \tag{8.17}$$

Then, the public key $h(x)$ must be of degree

$$d = \deg(h(x)) = \sum_{i=1}^{9} \deg(p_i(x)) + 1 = 35$$

and irreducible. For instance we may take

$$h(x) = 1 + x^2 + x^{35} \tag{8.18}$$

and set our protocol onto $\mathbb{F}_{2^{35}} \cong (\mathbb{F}_2[x]/H)^*$, whose order is $2^{35}-1$ when $H = \langle h(x) \rangle$. We choose the secret key and the decryption exponent, accordingly, to be $v = 3821$ and $u = 25169564954$,

so that $uv = 1 \bmod (2^{35} - 1)$. Then we may publish the 9 carrier keys $p_i^v \mod (h(x), 2)$:

$$\begin{aligned} p_1^v =& 1 + x^2 + x^4 + x^{10} + x^{12} + x^{18} + x^{22} \\ &+ x^{23} + x^{24} + x^{26} + x^{27} + x^{29} + x^{32} \end{aligned} \tag{8.19}$$

$$\begin{aligned} p_2^v =& x + x^3 + x^5 + x^6 + x^7 + x^{10} + x^{12} + x^{13} \\ &+ x^{17} + x^{20} + x^{21} + x^{22} + x^{24} + x^{28} + x^{30} + x^{32} \end{aligned} \tag{8.20}$$

$$\begin{aligned} p_3^v =& x + x^4 + x^5 + x^7 + x^{13} + x^{20} + x^{22} \\ &+ x^{28} + x^{29} + x^{30} + x^{31} + x^{32} + x^{33} + x^{34} \end{aligned} \tag{8.21}$$

$$\begin{aligned} p_4^v =& 1 + x^2 + x^3 + x^4 + x^{11} + x^{14} + x^{15} + x^{17} + x^{18} \\ &+ x^{19} + x^{20} + x^{21} + x^{24} + x^{28} + x^{30} + x^{34} \end{aligned} \tag{8.22}$$

$$\begin{aligned} p_5^v =& 1 + x + x^2 + x^3 + x^4 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{15} \\ &+ x^{18} + x^{20} + x^{21} + x^{22} + x^{24} + x^{26} + x^{29} + x^{32} + x^{33} \end{aligned} \tag{8.23}$$

$$\begin{aligned} p_6^v =& 1 + x + x^2 + x^4 + x^7 + x^{12} + x^{13} + x^{15} + x^{16} + \\ &x^{18} + x^{21} + x^{22} + x^{23} + x^{24} + x^{30} + x^{34} \end{aligned} \tag{8.24}$$

$$p_7^v = 1 + x^4 + x^8 + x^9 + x^{10} + x^{15} + x^{19} + x^{28} + x^{30} + x^{32} + x^{33} \tag{8.25}$$

$$\begin{aligned} p_8^v =& x + x^3 + x^4 + x^5 + x^8 + x^{10} + x^{12} + x^{13} + x^{15} + x^{16} \\ &+ x^{17} + x^{25} + x^{26} + x^{27} + x^{28} + x^{30} \end{aligned} \tag{8.26}$$

$$\begin{aligned} p_9^v =& x + x^4 + x^6 + x^7 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{15} + x^{16} \\ &+ x^{17} + x^{18} + x^{20} + x^{23} + x^{24} + x^{30} + x^{31} + x^{32} + x^{33}. \end{aligned} \tag{8.27}$$

Suppose we want to send the message $m = 111000111 \in \mathbb{Z}_2^9$, we encode it into

$$\begin{aligned} c =& \prod_{i=1}^{9} p_i^{vm_i} \mod (h(x), 2) \\ =& x^2 + x^3 + x^6 + x^{10} + x^{15} + x^{16} + x^{17} + x^{18} \\ &+ x^{20} + x^{21} + x^{23} + x^{26} + x^{27} + x^{30} + x^{31} + x^{33} + x^{34}. \end{aligned} \tag{8.28}$$

Once the message has been received, it is sufficient to take the u-th power, and the result is

as follows:

$$\begin{aligned} c^u &= \prod_{i=1}^{9} p_i^{vum_i} \mod (h(x), 2) = \prod_{i=1}^{9} p_i^{m_i} \\ &= x + x^3 + x^4 + x^6 + x^{11} + x^{12} + x^{14} + x^{15} + x^{16} + x^{19} \end{aligned} \tag{8.29}$$

whose factorization yields:

$$\begin{aligned} \mathsf{Factor}_2(c^u) =& x(1+x)(1+x+x^2)(1+x+x^2+x^3+x^5) \\ & (1+x+x^3+x^4+x^5)(1+x^2+x^3+x^4+x^5). \end{aligned} \tag{8.30}$$

We used the factorization algorithm in this simple example because we are working with small messages. The decryption algorithm presented in (8.7) is to be considered preferential.

The information rate associated to this encryption protocol is

$$\mathcal{I} = \frac{L}{\deg(h)} = \frac{9}{35} \cong 25,7\% \tag{8.31}$$

with the size of the space of messages being 2^9.

Remark 109. A similar example is presented in [36], with 2^8 messages. In the cited example the information rate is slightly higher than ours, yet comparable, but the space of messages is smaller.

If we wanted to match the size of space of messages it would be sufficient to remove one polynomial of degree 5, obtaining an information rate of $\mathcal{I} = 8/30 \sim 26,7\%$.

Remarkably enough, as in the NSK-protocol there is apparently no key leakage, our protocol preserves the security of the carrier keys. As a matter of fact, factoring the ciphertext c, one gets no information whatsoever on the cleartext, as it can be seen in the given example:

$$\begin{aligned} \mathsf{Factor}_2(c) = x^2 \left(x^4 + x^3 + 1\right) (& x^{28} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{18} + \\ & x^{17} + x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^4 + x^3 + x + 1) \end{aligned}$$

Remark 110. More generally, let $g(x)$ be the public modulus and

$$p_1^{vm_1} p_2^{vm_2} \cdots p_L^{vm_L} \equiv c(x) \mod g(x)$$

a ciphertext. Observe that over $\mathbb{F}_q[x]$ we have

$$P(x) = p_1^{vm_1} p_2^{vm_2} \dots p_L^{vm_L} = t(x)g(x) + c(x)$$

for some $t(x) \in \mathbb{F}_q[x]$. Now notice that inferring on the factorization of $P(x)$ from the data of $c(x)$ in terms of the factor basis

$$\{p_1^{vm_1}, \dots, p_L^{vm_L}\}$$

is the difficult problem on which the protocol relies, since the factorization of polynomials behaves badly with respect to reductions modulo irreducible polynomials. As a matter of fact, we base the security of our protocol on the randomness of the factorization of elements in the image of the map

$$\begin{aligned} \Gamma_{g,c} : \mathbb{F}_q[x] &\longrightarrow \mathbb{F}_q[x] \\ \Gamma_{g,c}(t(x)) &= t(x)g(x) + c(x). \end{aligned}$$

In general, the usual security one expects using prime numbers as carriers (NSK) can be extended to monic irreducible polynomials.

As we already pointed out, we are using here a non-optimal setting for our example, in that we skipped the polynomials of degree 3 and 4, and used all those of degree 5 instead. If we decided to optimize the information rate, we could take the two polynomials of degree 1, the single polynomial of degree 2, two of degree 3 and three of degree 4, for an overall encoding power of 2^8 messages. Notice that the space of messages is again equal to the example given in [36].

Choosing polynomials of degree 3 and 4 instead of 5 allows us to reduce the degree of $h(x)$, that is to say the number of bits that are needed to encrypt a message. So, if we compute the information rate in this case we obtain a much better result:

$$\mathcal{I} = \frac{\log_2 m}{\log_2 c} = \frac{8}{23} \cong 34,78\% \tag{8.32}$$

which is slightly higher than the information rate presented in [36] for the same message size.

The procedure works exactly the same when we change the ground field from $p = 2$ to $p = 3$.

This time we may choose three polynomials of degree 1, three of degree 2 and two of degree 3, all monic and irreducible, allowing us to reduce the overall degree of $h(x)$ to $\deg(h(x)) = 16$. In this case, for the same message size, we get an information rate of

$$\mathcal{I} = \frac{8}{16 \log_2 3} \cong 31,55\% \tag{8.33}$$

which is not better than the information rate in [36], for a space of messages of the same size, yet comparable.

8.3 Flexibility of the protocol

We have already pointed out in the previous sections that the important condition (8.4) can be fulfilled in several different ways according to the strategy we use in choosing the carrier polynomials p_i's. In what follows we will present a strategy that optimises the information rate and one that, to our analysis, improves security.

We will give a detailed analysis of the asymptotics of the information rate of our protocol and of NSK, showing that they have the same behaviour. In what follows our finite field k will be $\mathbb{F}_q$ for some prime power q.

8.4 Optimization of the information rate

The optimization of the information rate is ensured by the following:

Proposition 111. *There exists a strategy that maximises the information rate $\mathcal{I}$ for any choice of q and L. Moreover, in this strategy the information rate is determined by the closed formula*

$$\mathcal{I}(q, N) = \frac{\sum_{n=1}^{N} \frac{1}{n} \sum_{k|n} \mu\left(\frac{n}{k}\right) q^k}{\left(\sum_{n=1}^{N} \sum_{k|n} \mu\left(\frac{n}{k}\right) q^k + 1 \right) \log_2 q} \tag{8.34}$$

where $\mu(x)$ is the Möbius function.

Proof. We defined the information rate to be $\mathcal{I} = L/(\deg h \log_2 q)$ and we know that the degree of h depends on the particular choice of carrier polynomials. The strategy we will consider

is simply given by choosing *all* irreducible polynomials of all degrees up to a given degree N. Denote the number of degree-n irreducible polynomials in $\mathbb{F}_q[x]$ by D_n^q, we have the formula

$$D_n^q = \frac{1}{n} \sum_{k|n} \mu\left(\frac{n}{k}\right) q^k$$

where $\mu(x)$ is the Möbius function. The overall number of chosen polynomials, that is the number of bits that the plain text is composed by, as well as the sum of the degrees of the p_i's are given by a closed formula, namely:

$$L = \sum_{n=1}^{N} D_n^q = \sum_{n=1}^{N} \sum_{k|n} \mu\left(\frac{n}{k}\right) \frac{q^k}{n} \tag{8.35}$$

$$\deg(h(x)) = \sum_{n=1}^{N} n D_n^q + 1 = \sum_{n=1}^{N} \sum_{k|n} \mu\left(\frac{n}{k}\right) q^k + 1 \tag{8.36}$$

for some maximal degree N (which is dependent on L if we consider L to be the fundamental parameter). Then, the information rate $\mathcal{I}$ as a function of the prime power q and (implicitly) the parameter L has the desired closed expression.

It is easy to gather that such a choice of the polynomials guarantees maximal information rate, in that we are lowering as much as possible the degree of $h(x)$ and as a result the number of bits of the encrypted message. □

Remark 112. The obvious disadvantage of the strategy above is that one can always assume that the bare carrier polynomials are known, for we take all of them progressively up to degree N. As a matter of fact, the strategy above gives us a clear upper bound for the information rate, for all different combinations of L and q. Notice, however, by comparison with the tables of [36], that this is the same strategy adopted by Naccache and Stern, where the chosen prime p has the same size of $\mathsf{NextPrime}(\prod p_i)$.

Within this strategy it is important to notice that all the variations proposed in [36, Section 2.3] are importable in the present context. For example, it is possible to express the message m in a basis different from 2, and this would lead to some modification to the suitable degrees for our carriers. Moreover, it is possible to restrict the space of messages to constant-weight strings. This last choice increases the information rate since it allows to lower the degree of $h(x)$. In

L (bits)	$\deg h$ (bits)	$\mathcal{I}$
131	1024	12,8 %
233	2048	11,4%
418	4096	11,2%

Table 8.1: Information rate matching with [36, Section 2.2]

L (bits)	$\mathcal{M}$ (bits)	Size of p & $\deg h$ (bits)	$\mathcal{I}$
759	758	8192	11,4%

Table 8.2: Extension to next block and matching of the information rate

fact, if w is the constant weight, the bound on the degree of h is:

$$\deg h > wN$$

where N is the highest degree of the chosen carriers.

Apart from these extensions, the standard NSK protocol is summarized in the table presented in [36, Section 2.2], where the information rate for 512, 1024 and 2048 bits-sized p's is given. The strategy we have just outlined to reach the maximal information rate, allows us to obtain the exact values presented in [36] matching the degree of our polynomial h with the size of their prime p and L with the size $\mathcal{M}$ of the message. So we are able to obtain the same information rate.

The matching procedure works as follows: compute the degree of h obtained by choosing all polynomials up to a given degree, say 9 to obtain $\deg h = 977$. Then, top it to the next block, in this case 1024 bits, choosing *some* polynomials of one degree higher, in this case 11. This leads to an increase in the number L of carrier polynomials from 127 to 131, and the information rate is then given by the ratio $L/\deg h$.

In Table 8.1 we show how to match the examples presented in [36], and the last row is obtained by extending their calculations to 4096 bits. If we go further and compute the relevant figures in the case of 8192 bits we find almost perfect agreement also in this case (cf. Table 8.2). It will be clear in what follows why this happens.

8.5 Asymptotics comparison with previous works

We will prove in this section that our protocol has the same asymptotic information rate of [36]. A naive explanation of this fact is given by arguing that the number of primes below a certain

number of bits has the same behaviour as the number of irreducible polynomials in $\mathbb{F}_q[x]$ below a certain degree.

Let us fix the notation

$$a_N \sim b_N \iff \lim_{N\to\infty} \frac{a_N}{b_N} = 1.$$

We will make use of the following

Lemma 113.

$$\sum_{n=1}^{N} D_n^q \sim \frac{q}{q-1} D_N^q \tag{8.37}$$

Proof. First recall that [44, Theorem 2.2] $D_n^q \sim \frac{q^n}{n}$ and therefore the sums behave asymptotically as $\sum_{n=1}^{N} D_n^q \sim \sum_{n=1}^{N} \frac{q^n}{n}$. Then we have (8.37) if and only if

$$\lim_{N\to\infty} \frac{\sum_{n=1}^{N} \frac{q^n}{n}}{\frac{q^N}{N}} = \frac{q}{q-1}. \tag{8.38}$$

Now, denote by $S_N := \sum_{n=1}^{N} \frac{N}{n} q^{n-N}$ and observe that it might be expressed in terms of the recursive sequence

$$S_{N+1} = \frac{1}{q} \frac{N+1}{N} S_N + 1. \tag{8.39}$$

for the initial value $S_1 = 1$. Consider $S_- = \liminf_{N\to\infty} S_N$ and $S_+ = \limsup_{N\to\infty} S_N$. Passing to the lim sup and lim inf in (8.39) we get the same equation for $S_\pm$:

$$S_\pm = \frac{S_\pm}{q} + 1$$

provided that they are both finite. Assuming that they are, we conclude that

$$\lim_{N\to\infty} S_N = S_\pm = \frac{q}{q-1} \tag{8.40}$$

This assumption is legitimate since $S_N \geq 0$ for all $N \in \mathbb{N}$, thus $S_- \geq 0$, and for S_+ we observe that

- When $x \in \mathbb{R}^+$ we have that $\frac{q^x}{x}$ is increasing for $x \geq \frac{1}{\log q} \geq 2$, since $q \geq 2$, and in particular this is true for $x \in \mathbb{N}^*$;

- $\limsup_{N\to\infty} \frac{N}{q^N} \sum_{n=1}^{N} \frac{q^n}{n} = \limsup_{N\to\infty} \frac{N}{q^N} \sum_{n=2}^{N} \frac{q^n}{n}$.

It follows that

$$\limsup_{N\to\infty} \frac{N}{q^N} \sum_{n=1}^{N} \frac{q^n}{n} = \limsup_{N\to\infty} \frac{N}{q^N} \sum_{n=2}^{N} \frac{q^n}{n} \leq \limsup_{N\to\infty} \frac{N}{q^N} \int_2^{N+1} \frac{q^x}{x} dx$$

where the last inequality comes from the fact that $\sum_{n=2}^{N} \frac{q^n}{n}$ are the lower sums of $\int_2^{N+1} \frac{q^x}{x} dx$, since $\frac{q^x}{x}$ is increasing for $x \geq 2$. Moreover

$$\lim_{N\to\infty} \frac{\int_2^{N+1} \frac{q^x}{x} dx}{\frac{q^N}{N}} = \lim_{t\to\infty} \frac{\int_2^{t+1} \frac{q^x}{x} dx}{\frac{q^t}{t}} = \lim_{t\to\infty} \frac{\frac{q^{t+1}}{t+1}}{\frac{q^t}{t}(\log q - \frac{1}{t})} = \frac{q}{\log q}$$

where the second equality follows from the De L'Hôpital rule. This proves that

$$0 \leq \liminf_{N\to\infty} S_N \leq \limsup_{N\to\infty} S_N \leq \frac{q}{\log q}$$

and yields the claim. □

We are now ready to prove

Proposition 114.

$$\mathcal{I}(q, N) \sim \frac{1}{\log_2 q} \frac{1}{N} \tag{8.41}$$

Proof. Observe that $nD_n^q \sim q^n$ and therefore, from (8.34)

$$\mathcal{I}(q, N) \sim \left(\sum_{n=1}^{N} \frac{q^n}{n} \right) \Big/ \left(\log_2 q \sum_{n=1}^{N} q^n \right)$$

Now, it is easy to gather that

$$\sum_{n=1}^{N} q^n \sim \frac{q}{q-1} q^N \tag{8.42}$$

then, plugging the results of (8.42) and of Lemma 113 into (8.34), we obtain

$$\mathcal{I}(q, N) \sim \frac{1}{\log_2 q} \frac{\frac{q}{q-1} \frac{q^N}{N}}{\frac{q}{q-1} q^N} = \frac{1}{\log_2 q} \frac{1}{N}. \tag{8.43}$$

□

We would like to compare this result with the information rate of the NSK protocol. Notice

that in order to make a consistent comparison we must understand the role of our parameter N in the NSK.

Once q is fixed, bounding the degree of the carrier polynomials by N is the same as bounding the number of bits required to represent any of them by the quantity $M = \lfloor N \log_2(q) \rfloor$.

The analogous bound for the NSK is then given by bounding the number of bits of the prime carriers by M. This is the same as bounding the prime carriers themselves by $2^M \simeq q^N$. In the following proposition the comparison is made explicit.

Proposition 115. *Let N be the bound on the degree of the carrier polynomials and $M = \lfloor N \log_2(q) \rfloor$ the analogous bound for the bits of the prime carriers in the NSK. The information rate for the NSK protocol is asymptotically given by*

$$I_{NSK} \sim \frac{1}{\log_2 q} \frac{1}{N}. \tag{8.44}$$

Proof. It is known that for large $m \in \mathbb{N}$

$$\prod_{p<m} p \sim e^m.$$

Let us consider $m = 2^M \simeq q^N$, then $\prod_{p<q^N} p \sim \exp q^N$. Now, the number of prime numbers up to q^N asymptotically goes, by the prime number theorem, as

$$\pi(q^N) \sim \frac{q^N}{N \ln q}.$$

In our case this will be the number of carrier prime numbers up to q^N. On the other hand $\exp q^N$, which is the size of the prime modulus of [36], has $\lfloor q^N \log_2 e \rfloor$ digits, and therefore the information rate is computed as

$$I_{NSK} \sim \frac{\frac{q^N}{N \ln q}}{q^N \log_2 e} = \frac{1}{\log_2 q} \frac{1}{N}. \tag{8.45}$$

□

By comparing Propositions 114 and 115 it is now clear that the two information rates have the same behaviour. This explains that the matching procedure we perform at the end of the previous section will attain the information rate of NSK also in the asymptotic limit. Moreover it justifies the claim on the large-N behaviour of irreducible polynomials with respect to prime

numbers.

8.6 Some precautions to avoid subgroup-like attacks

The security of this protocol is strictly related to the size of the degree of h and, as a consequence, to the range of degrees that the carriers can have. Indeed, when the carriers are chosen within a large set, the attacker will not have chances (in terms of a brute force attack) to find the p_i's to set up a discrete logarithm problem for the pair (p_i, p_i^s) for any i.

As a matter of fact, the knowledge of h will only lead to the following information on the degrees:

$$\deg(h) = \sum_i \deg(p_i) + 1.$$

This is not the case when working with integers and primes in $\mathbb{Z}/p\mathbb{Z}$, where we can always assume that the prime factors are known when $p \simeq \prod_i p_i$.

We first sketch a subgroup like attack in the most *unsafe* case. Let G be an abelian group and $p_1^v, \ldots, p_L^v$ be carriers, as in Section 8.2. Let the order of p_i^v in G be n_i and suppose $\gcd(n_i, n_j) = 1$ for $i \neq j$. Let now

$$M_j = n_1 \cdots n_{j-1} \cdot n_{j+1} \cdots n_L.$$

It is easy to observe that, for a generic ciphertext c, $m_j = 1$ if and only if $c^{M_j} \neq 1$. As it is elementary to observe, this leads to decryption in L steps. Moreover, it can also be adapted to work when the condition $\gcd(n_i, n_j) = 1$ is just partially fulfilled. In this case, indeed, only partial information on the text can be extracted.

Consider now the decomposition in cyclic subgroups of the multiplicative group of the finite field $(\mathbb{F}_{q^d})^*$. In order to avoid subgroup-like attacks on the ciphertext we will require all the p_i's to be generators of the same subgroup of large order. This will lead to certain requirements on $q^d - 1$.

The most natural choice to solve this problem is asking that the degree d of the reducing polynomial $h(x)$ be constrained by the following:

$$r := \frac{q^d - 1}{q - 1} \text{ is prime.} \tag{8.46}$$

Now one could choose the p_i's such that

$$p_i(x)^r \neq 1 \mod h(x) \quad \forall i \in \{1, \ldots, L\}. \tag{8.47}$$

8.7 "Chinese remainder" version

In what follows we will present another example of a protocol that fits the general picture, which stems on the well known chinese remainder theorem. To do this, let us introduce a large prime power q and a natural number $L \in \mathbb{N}$. Consider now the monoid $S = (\mathbb{F}_q^{L+1})^*$, with the multiplication defined componentwise, and the set $R = \{r_1, \ldots, r_{L+1}\} \subseteq \mathbb{F}_q$.

Let $\alpha_i \in \mathbb{F}_q \backslash R \quad \forall i \in \{1, \ldots, L\}$ and choose two large integers u, v such that $uv = 1 \mod (q-1)$. Compute the following list of vectors $p_i \in (\mathbb{F}_q^{L+1})^*$ as

$$(g_i)_j := (r_j - \alpha_i)$$
$$(p_i)_j := (g_i)^v.$$

Let

$$((\mathbb{F}_q^{L+1})^*, \{p_1, \ldots, p_L\})$$

be the public key and

$$(\{g_1, \ldots, g_L\}, \{r_1 \ldots r_L\})$$

be the secret key. Let

$$\begin{aligned} F: \quad \mathbb{Z}_2^L \quad &\longrightarrow \quad S \\ (m_1, \ldots, m_L) \quad &\mapsto \quad \prod_{i=1}^{L} p_i^{m_i} \end{aligned}$$

be the encryption map.

Remark 116. Observe that the information rate is

$$\frac{L}{(L+1)\log_2(q)}.$$

Proposition 117. *F is an injection.*

Proof. We define a polynomial on $\mathbb{F}_q[x]$ by

$$h_R(x) := \prod_{i=1}^{L+1}(x - r_i)$$

whose set of zeros coincide with R. We will prove the proposition by showing how to compute the inverse over the image of F using $h(x)$, i.e. we will show how to uniquely decrypt any ciphertext $c \in \Im(F)$ using the secret key. Let

$$\begin{aligned} \psi : S &\longrightarrow S \\ x &\mapsto x^v, \end{aligned}$$

$$\begin{aligned} G : \mathbb{F}_q[x]/h_R(x) &\xrightarrow{\text{CRT}} \mathbb{F}_q^L \\ k(x) &\mapsto (k(r_1), \ldots, k(r_L)), \end{aligned}$$

and

$$\Gamma : \mathbb{F}_q[x]/h_R(x) \longrightarrow \mathbb{F}_q[x]$$

be the canonical lift. The decryption map D is given by checking $\Gamma(G^{-1}(\psi^{-1}(x)))$ modulo $g_i(x) = (x - \alpha_i)$: whenever it is zero it means $m_i = 1$, where $\psi^{-1}(x) = x^u$. Observe that the decryption is well defined: the map

$$\alpha_{\sim}^{\psi} : \mathbb{Z}_2^L \longrightarrow \mathbb{F}_q[x]/(h_R(x))$$

is clearly injective (and then $\alpha_{\sim}$ is, by Proposition 95) since the product of all the $g_i(x)$ has degree $L < L + 1$. Observe that $\sim$ is as usual the relation induced by the ideal of $h_R(x)$. □

8.8 Function Field Knapsack Scheme

In this section we show a more theoretical version of the scheme that uses the context of function fields of curves. For the notation and definitions we refer to [49]. Let F be a function field over a finite field $\mathbb{F}_q$. We denote by $\mathcal{O}_P$ the valuation ring associated to the place P. Moreover, if

$f \in \mathcal{O}_P$, then we denote by $f(P)$ its image in the residue field $\mathcal{O}_P/P$. Let $\{P_1, \ldots, P_L\}$ distinct places of F. Let x_i be a uniformizer of the place P_i invertible in the valuation ring $\mathcal{O}_{P_j}$ for $j \neq i$ (this can be done thanks to the *Approximation Theorem* for valuations).

Fix P a place of the holomorphy ring $\mathcal{O}$ containing the subring generated by $x_1, \ldots x_L$. Choose P satisfying

$$\deg(P) > \sum_{i=1}^{L} \deg((x_i)_\infty)$$

and let $D = \sum_{i=1}^{L} (x_i)_\infty$ Let $l(D) := \dim_{\mathbb{F}_q}(\mathcal{L}(D))$.

Remark 118. Notice that, for any $(m_1, \ldots, m_L) \in \{0,1\}^L$, we have

$$\prod_{i=1}^{L} x_i^{m_i} \in \mathcal{L}(D).$$

Now observe that $\mathcal{L}(D)$ evaluates at P into the finite field $\mathbb{F}_{q^{\deg(P)}}$. In addition $\mathcal{L}(D)$ embeds into $\mathbb{F}_{q^{\deg(P)}}$ since an element in the kernel of the evaluation would live in $\mathcal{L}(D-P)$ but $D-P$ is a divisor of negative degree, so $\mathcal{L}(D-P) = 0$.

Remark 119. Call ψ the embedding of $\mathcal{L}(D)$ into $\mathbb{F}_{q^{\deg(P)}}$. Observe that, given an $\mathbb{F}_q$-basis $\{e_1, \ldots, e_{l(D)}\}$ of $\mathcal{L}(D)$, $\psi^{-1}(c)$ is computable for any c in the image of ψ. In fact it is enough to write down $c = \sum_{i=1}^{L} a_i \psi(e_i)$ for some $a_i \in \mathbb{F}_q$; then $\psi^{-1}(c) = \sum_i^L a_i e_i$.

Let $\mathcal{M} = \{0,1\}^L$ be the space of messages and $\mathcal{C} := \mathbb{F}_{q^{\deg(P)}}$ be the space of ciphertexts. Let $e, d \in \mathbb{Z}$ for which $ed \equiv 1 \mod q^{\deg(P)} - 1$. Now we are able to set up public and private key:

- **Public key:** $(\mathbb{F}_{q^{\deg(P)}}, \{x_1(P)^e, \ldots, x_L(P)^e\})$
- **Private key:** $(F, d, \{x_1, \ldots, x_L\}, \psi)$

Encryption and decryption are defined as

- **Encryption:** let $m = (m_1, \ldots, m_L) \in \mathcal{M}$. The encryption map is defined by $E(m) := \prod_{i=1}^{L} (x_i(P)^e)^{m_i}$.
- **Decryption:** Let $c \in \mathcal{C}$. Compute c^d and invert ψ, getting $\overline{c} = \prod_{i=1}^{L} x_i^{m_i}$.

Remark 120. The reader should notice that in this case hiding the residue field is not necessary, since the attack does not have available the function field used for decryption, but only the residue field.

Chapter 9

Tuning the information rate for the PNSK cryptosystem

The results in this chapter come from a joint work with Joachim Rosenthal and Reto Schnyder, which is to appear on the book series *Lecture notes in Electrical Engineering*.

9.1 Prime Packing

In what follows our goal is to show that a direct adaptation of the NSK packing presented in [7] is also possible in the case of the polynomial variant described in Chapter 8, Section 8.2. We pack the irreducible polynomials up to degree d as follows: Let $b, t \in \mathbb{N}$ be positive integers for which $bt \leq \overline{\pi}(d)$, where $\overline{\pi}(d)$ is the number of irreducible polynomials up to degree d. Partition the first (according to any ordering respecting the degree) bt polynomials in t sets $\{S_i\}$ each of size b satisfying that for all $i, j \in \{1, \ldots, t\}$, if $f \in S_i$ and $h \in S_j$ we have

$$i \leq j \Rightarrow \deg(f) \leq \deg(h).$$

More informally, we pack the polynomials up to degree d into t packs, each of them containing the b polynomials of the lowest possible degree. Let us denote by $p_{j,i}$ the i-th polynomial living in the j-th box S_j, again ordered by degree. The protocol will then be modified as follows. The space of messages becomes $\{1, \ldots, b\}^t$, we require now only $\sum_{j=1}^{L} \deg p_{j,b} < \deg g = N$. Again,

let $es \equiv 1 \mod q^N - 1$.

The public key is set up as $\big(\{v_{j,i}\}_{i,j}, \mathbb{F}_q[x]/(g(x))\big)$, where again $v_{j,i} = p_{j,i}^e$. The secret key is analogously $\big(\{p_{j,i}\}_{i,j}, s\big)$. The encryption of a message $m = (m_1, \ldots, m_t) \in \{1, \ldots, b\}^t$ is performed as

$$m \mapsto \prod_{j=1}^{t} v_{j,m_j} = c \in \mathbb{F}_q[x]/(g(x)).$$

Alice can then decrypt by computing $c^s \in \mathbb{F}_q[x]/(g(x))$ and reducing the result modulo $p_{j,i}$ for each i, j, as before.

It is now easy to compute the information rate and public key size: The information rate is $\frac{t \log b}{N \log q}$, and the public key has size $btN \log q$.

9.1.1 Example Parameters

As an example, consider the medium prime case $q = 6287$. We compare the information rate and public key size of our scheme in the case $\deg g = 131$ for various values of the box size b in Table 9.1. Computations were done using Sage [47]. The first row corresponds to the original pNSK (which is not quite the same as setting $b = 1$). Note that for small box sizes b, we always get $t = 130$ boxes. This is because it is possible to use only degree 1 polynomials for the $p_{j,i}$. As b becomes larger, this is no longer possible, and the information rate suffers.

b	t	information rate	public key size
pNSK	130	7.9%	215 kbit
5	130	18.3%	1074 kbit
10	130	26.1%	2149 kbit
30	130	38.6%	6447 kbit
50	127	43.4%	10496 kbit
70	109	40.4%	12612 kbit

Table 9.1: Information rate and public key size of prime packing for $q = 6287$, $\deg g = 131$ and various box sizes.

Evidently, the information rate can be greatly improved at the cost of a much larger public key size. This cost can be somewhat reduced by applying the "powers of primes" technique of [7], and we will do so in Section 9.2.

9.1.2 Asymptotic Information Rate

As in [7], we can obtain linear bandwidth by setting the number of packs equal to their size. Indeed, we show that if we set $n := b = t$, then the information rate of pNSK using prime

packing is asymptotically equal to $\frac{1}{2}$.

To analyze the information rate, we first need to find the degree of the n-th irreducible polynomial p_n, according to any order respecting the degree. In [31, Section 3.2.2], it was shown that the number of irreducible polynomials in $\mathbb{F}_q[x]$ of degree at most d is asymptotically equal to $\frac{q}{q-1}\frac{q^d}{d}$. Hence, the polynomials with a given degree d should be numbered roughly between $\frac{q}{q-1}\frac{q^{d-1}}{d-1}$ and $\frac{q}{q-1}\frac{q^d}{d}$. Thus, if the polynomial p_n has degree d_n, we have

$$\frac{q}{q-1}\frac{q^{d_n-1}}{d_n-1} \lesssim n \lesssim \frac{q}{q-1}\frac{q^{d_n}}{d_n},$$

where $a_n \lesssim b_n$ means that $\limsup_{n\to\infty} a_n/b_n \leq 1$. Taking logarithms gives

$$(d_n-1) - \log_q(d_n-1) \lesssim \log_q n - \log_q \frac{q-1}{q} \lesssim d_n - \log_q d_n,$$

which asymptotically is the same as

$$d_n - 1 \lesssim \log_q n \lesssim d_n.$$

We hence see that $d_n = \deg p_n \sim \log_q n$.

Now we can approximate the degree of g:

$$\begin{aligned} N = \deg g &= 1 + \sum_{i=1}^{n} \deg p_{in} \\ &\sim \sum_{i=1}^{n} \log_q(in) \sim \sum_{i=1}^{n} \log_q(n^2) \sim 2n \log_q n. \end{aligned}$$

For the first $\sim$, note that the indices of p_{in} in the sum are all at least n, and so only the asymptotic behaviour of $\deg p_{in}$ is relevant. Finally, we get for the information rate

$$\frac{t \log_2 b}{N \log_2 q} \sim \frac{n \log_2 n}{2n \log_q n \log_2 q} = \frac{n \log_2 n}{2n \log_2 n} = \frac{1}{2}.$$

9.2 Powers of Primes

In [7, Section 4], prime packing was applied to a variant of NSK using a base larger than 2 in order to further improve information rate and reduce public key size. This method can also be

applied to the polynomial NSK variant.

As in Section 9.1, we again choose a degree d and integers b and t satisfying $bt \leq \overline{\pi}(d)$, and we partition the first bt irreducible polynomials into t sets S_i of size b. We further choose an integer parameter $\ell \geq 1$. We again denote by $p_{j,i}$ the i-th polynomial in the j-th box. As before, we need an irreducible polynomial $g \in \mathbb{F}_q[x]$ of large degree as our modulus, but this time, we require that $\sum_{j=1}^{L} \ell \deg p_{j,b} < \deg g = N$. Again, we choose integers e and s with $es \equiv 1 \mod q^N - 1$ and set $v_{j,i} = p_{j,i}^e$. The public key is $\big(\{v_{j,i}\}_{i,j}, \ell, \mathbb{F}_q[x]/(g(x))\big)$ and the private key is $\big(\{p_{j,i}\}_{i,j}, s\big)$.

For each box S_i, we now have more options available for encryption than simply choosing one element of S_i: we can choose up to ℓ elements, allowing repetitions, and multiply those. Each of these possibilities corresponds to a b-tuple in $T = \{(k_1, \ldots, k_b) \in \mathbb{N}^b \mid k_1 + \cdots + k_b \leq \ell\}$. As shown in [7, Appendix A], there are $\binom{b+\ell}{\ell} = B$ such tuples, and there is a bijection $\phi\colon \{1, \ldots, B\} \to T$ that can be computed efficiently [46]. Hence, we use the message space $\{1, \ldots, B\}^t$, and we encrypt a message $m = (m_1, \ldots, m_t)$ as

$$m \mapsto \prod_{j=1}^{t} \prod_{i=1}^{b} v_{j,i}^{k_{j,i}} = c \in \mathbb{F}_q[x]/(g(x)),$$

where $\phi(m_j) = (k_{j,1}, \ldots, k_{j,b}) \in T$.

Decryption is again done by lifting and factoring c^s and inverting ϕ.

We can again give a formula for information rate and public key size. The information rate is $\frac{t \log B}{N \log q}$, and the public key still has size $btN \log q$.

9.2.1 Toy Example

We present a small example to clarify the "powers of primes" method. Let $q = 2$, and we consider a system with $t = 2$ packs of $b = 3$ irreducible polynomials each. Let furthermore $\ell = 2$. The first six irreducible polynomials are

$$p_{1,1} = x \qquad p_{2,1} = x^3 + x + 1$$
$$p_{1,2} = x + 1 \qquad p_{2,2} = x^3 + x^2 + 1$$
$$p_{1,3} = x^2 + x + 1 \qquad p_{2,3} = x^4 + x^3 + 1.$$

We need $\ell \deg p_{1,3} + \ell \deg p_{2,3} = 12 < \deg g = N$, so we choose

$$g = x^{13} + x^4 + x^3 + x + 1.$$

We randomly choose secret exponents $e = 6020$ and $s = 6380 \equiv e^{-1} \mod 2^{13} - 1$. The public elements are now given by $v_{j,i} \equiv p_{j,i}^e \mod g$:

$$\begin{aligned}
v_{1,1} &= x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 & v_{2,1} &= x^8 + x^7 + x^6 + x^5 + x^4 + 1 \\
v_{1,2} &= x^{11} + x^{10} + x^9 + x^8 + x^6 + x & v_{2,2} &= x^{12} + x^{11} + x^6 + x^5 + x^3 \\
v_{1,3} &= x^{12} + x^{11} + x^{10} + x^9 + x^5 + x^3 + x^2 + 1 & v_{2,3} &= x^{12} + x^{11} + x^{10} + x^6 + x^5 + x^2.
\end{aligned}$$

Note that $B = \binom{3+2}{2} = 10$, so we can represent a message in base 10. We choose the following encoding from integers 0 to 9 to 3-tuples (k_1, k_2, k_3) satisfying $k_1 + k_2 + k_3 \leq 2$.

$$\begin{aligned}
&0 \mapsto (0,0,0) \quad 1 \mapsto (1,0,0) \quad 2 \mapsto (2,0,0) \quad 3 \mapsto (0,1,0) \quad 4 \mapsto (1,1,0) \\
&5 \mapsto (0,2,0) \quad 6 \mapsto (0,0,1) \quad 7 \mapsto (1,0,1) \quad 8 \mapsto (0,1,1) \quad 9 \mapsto (0,0,2).
\end{aligned}$$

To encrypt the message $m = 94$, we hence compute

$$v_{1,1}^0 v_{1,2}^0 v_{1,3}^2 \cdot v_{2,1}^1 v_{2,2}^1 v_{2,3}^0 \equiv x^{12} + x^9 + x^8 + x^3 + x^2 + 1 = c \mod g.$$

To decrypt, raise the ciphertext to s and factor:

$$\begin{aligned}
m^s &\equiv x^{10} + x^9 + x^6 + x^5 + x^4 + x + 1 \mod g \\
&= (x^2 + x + 1)^2 \cdot (x^3 + x + 1) \cdot (x^3 + x^2 + 1) \\
&= p_{1,1}^0 p_{1,2}^0 p_{1,3}^2 \cdot p_{2,1}^1 p_{2,2}^1 p_{2,3}^0,
\end{aligned}$$

from which the message is recovered.

9.2.2 Example Parameters

We again consider the case $q = 6287$ and compare the information rate and public key size of the "powers of primes" variant in the case $\deg g = 131$ for different values for b and ℓ in Table 9.2.

The first row corresponds to the original pNSK, which is obtained by setting $b = 1$ and $\ell = 1$.

b	ℓ	t	information rate	public key size
1	1	130	7.9%	215 kbit
2	2	65	10.1%	215 kbit
10	10	13	13.8%	215 kbit
30	1	130	39.0%	6447 kbit
42	2	65	38.9%	4513 kbit
310	26	5	38.8%	2562 kbit
83	26	5	25.1%	686 kbit

Table 9.2: Information rate and public key size of the "powers of primes" variant for $q = 6287$, $\deg g = 131$ and various box sizes and bases.

As we can see, the "powers of primes" method allows, to an extent, for larger information rates at the same key size, or for smaller keys for a given information rate.

Bibliography

[1] R. Alvarez, F. Martinez, J. Vicent, and A. Zamora. A new public key cryptosystem based on matrices. *6th WSEAS International Conference on Information Security and Privacy, Tenerife, Spain*, 2007.

[2] F. Barroero, C. Frei, and R. Tichy. Additive unit representations in rings over global fields - a survey. *Publ. Math. Debrecen*, 79(3):291–307, 2011.

[3] J. Brawley, L. Carlitz, and T. Vaughan. Linear permutation polynomials with coefficients in a subfield. *Acta Arithmetica*, 24(2):193–199, 1973.

[4] L. Carlitz and D. Hayes. Permutations with coefficients in a subfield. *Acta Arithmetica*, 21 (1):131–135, 1972. URL `http://eudml.org/doc/205098`.

[5] F. Cellarosi and I. Vinogradov. Ergodic properties of k-free integers in number fields. *Journal of Modern Dynamics*, 7(3):461–488, 2013. ISSN 1930-5311. doi: 10.3934/jmd.2013.7.461.

[6] Mei-Chu Chang. On a matrix product question in cryptography. 439(7):1742–1748, 2013. doi: 10.1016/j.laa.2013.05.013.

[7] B. Chevallier-Mames, D. Naccache, and J. Stern. Linear bandwidth naccache-stern encryption. In *Security and Cryptography for Networks*, volume 5229 of *Lecture Notes in Computer Science*, pages 327–339. Springer Berlin Heidelberg, 2008.

[8] P. M. Cohn. *Algebra, Volume 3*. John Wiley & Sons, Chichester, 2nd edition, 1991.

[9] N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In Bart Preneel, editor, *Advances in Cryptology EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer*

Science, pages 392–407. Springer Berlin Heidelberg, 2000. ISBN 978-3-540-67517-4. doi: 10.1007/3-540-45539-6_27. URL http://dx.doi.org/10.1007/3-540-45539-6_27.

[10] W. Diffie and M. E Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644–654, 1976.

[11] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in Cryptology*, pages 10–18. Springer, 1985.

[12] J. Faugre. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139:61–88, 1999.

[13] A. Ferraguti and G. Micheli. On Cesaro Theorem for number fields. 2014. URL http://arxiv.org/abs/1409.6527.

[14] X. Guo and G. Yang. The probability of rectangular unimodular matrices over $\mathbb{F}_q[x]$. *Linear Algebra and its Applications*, 438(6):2675–2682, 2013.

[15] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Clarendon Press Oxford, 1960.

[16] M. E Hellman. An overview of public key cryptography. *IEEE Communications Magazine*, 40(5):42–49, 2002.

[17] R. Heyman and I. E. Shparlinski. On the number of eisenstein polynomials of bounded height. *Applicable Algebra in Engineering, Communication and Computing*, 24(2):149–156, 2013.

[18] J. Hoffstein, J. Pipher, and J. H. Silverman. Ntru: A ring-based public key cryptosystem. In *Algorithmic number theory*, pages 267–288. Springer, 1998.

[19] T. J. Laffey. Simultaneous reduction of sets of matrices under similarity. 84(0):123–138, 1986. doi: 10.1016/0024-3795(86)90311-3.

[20] J. L. Kelley. *General topology*. New York: Van Nostrand, 1955.

[21] Peter Lancaster and Miron Tismenetsky. *The theory of matrices : with applications*. Computer science and applied mathematics. Academic Press, Orlando, 1985.

[22] Jr. Lenstra, H.W. On the chorrivest knapsack cryptosystem. *Journal of Cryptology*, 3(3): 149–155, 1991. ISSN 0933-2790. doi: 10.1007/BF00196908. URL `http://dx.doi.org/10.1007/BF00196908`.

[23] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2nd edition, 1997.

[24] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20. Cambridge University Press, 1997.

[25] D. Masser and J.D. Vaaler. Counting algebraic numbers with large height ii. *Trans. of American Math. Soc.*, 359(1):427 – 445, 2007.

[26] G. Maze, C. Monico, and J. Rosenthal. Public key cryptography based on semigroup actions. *Advances in Mathematics of Communications*, 1(4):489–507, 2007.

[27] G. Maze, J. Rosenthal, and U. Wagner. Natural density of rectangular unimodular integer matrices. *Linear Algebra and its Applications*, 434(5):1319 – 1324, 2011. doi: http://dx.doi.org/10.1016/j.laa.2010.11.015.

[28] R. J McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN progress report*, 42(44):114–116, 1978.

[29] M.F.Atiyah and I.G. MacDonald. *Introduction to Commutative Algebra*. Westview Press, 1969.

[30] G. Micheli. On coefficient constraints and evaluation restrictions for linearized polynomials. *Finite Fields and Their Applications*, 34, 2015. doi: 10.1016/j.ffa.2015.02.001.

[31] G. Micheli and M. Schiavina. A general construction for monoid-based knapsack protocols. *Advances in Mathematics of Communications*, 8(3):343–358, August 2014. URL `http://dx.doi.org/10.5167/uzh-98258`.

[32] G. Micheli and D. Schipani. On canonical subfield preserving polynomials. *Acta Arithmetica*, 166:23–32, 2014. doi: 10.4064/aa166-1-3.

[33] G. Micheli and R. Schnyder. On the density of coprime m-tuples over holomorphy rings. *arXiv:1411.6876 [math.NT] (To appear in International journal of number theory)*.

[34] G. Micheli, J. Rosenthal, and P. Vettori. Linear spanning sets for matrix spaces. *http://arxiv.org/abs/1409.3020, (To appear in Linear algebra and its applications)*, 2014.

[35] C. Moreno. *Algebraic Curves over Finite Fields*. Cambridge University Press, 1991. ISBN 9780511608766. Cambridge Books Online.

[36] D. Naccache and J. Stern. A new public key cryptosystem. In *Advances in Cryptology*, pages 27–36. EUROCRYPT, 1997.

[37] J.E Nymann. On the probability that k positive integers are relatively prime. *Journal of Number Theory*, 4(5):469 – 473, 1972. doi: http://dx.doi.org/10.1016/0022-314X(72)90038-8.

[38] F. Özbudak. On maximal curves and linearized permutation polynomials over finite fields. *Journal of Pure and Applied Algebra*, 162(1):87–102, 2001.

[39] J. Patarin. Hidden fields equations (hfe) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms. In U. Maurer, editor, *Advances in Cryptology EUROCRYPT 96*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer Berlin Heidelberg, 1996. ISBN 978-3-540-61186-8. doi: 10.1007/3-540-68339-9_4. URL `http://dx.doi.org/10.1007/3-540-68339-9_4`.

[40] H.K. Pathak and M. Sanghi. Public key cryptosystem and a key exchange protocol using tools of non-abelian groups. *(IJCSE) International Journal on Computer Science an Engineering*, pages Vol 02, No 04, 1029–1033, 2010.

[41] G. Pollack and L. Thompson. On the degree of divisors of $t^n - 1$. *New York J. Math*, (19): 91–116, 2013.

[42] B. Poonen and M. Stoll. The cassels-tate pairing on polarized abelian varieties. *Ann. of Math*, 2:15–0, 1998.

[43] R. L Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[44] M. Rosen. *Number theory in function fields*, volume 210. Springer Science & Business Media, 2002.

[45] B. D. Sittinger. The probability that random algebraic integers are relatively r-prime. *Journal of Number Theory*, 130(1):164 – 171, 2010. ISSN 0022-314X. doi: http://dx.doi.org/10.1016/j.jnt.2009.06.008.

[46] Dennis Stanton and Dennis White. *Constructive combinatorics*. Springer-Verlag New York, Inc., 1986.

[47] W. A. Stein et al. *Sage Mathematics Software (Version 6.1.1)*. The Sage Development Team, 2014. URL `http://www.sagemath.org`.

[48] R. Steinwandt and A. S. Corona. Cryptanalysis of a 2-party key establishment based on a semigroup action problem. *Adv. in Math. of Comm.*, 5(1):87–92, 2011.

[49] H. Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer, 2009.

[50] H. Sugita and S. Takanobu. The probability of two $\mathbb{F}_q[x]$-polynomials to be coprime. *Probability and number theory, Advanced Studies in Pure Mathematics*, 49:455–478, 2007.