ALGEBRAIC METHODS FOR CONSTRUCTING ONE-WAY TRAPDOOR FUNCTIONS

A Dissertation

Submitted to the Graduate School
of the University of Notre Dame
in Partial Fulfillment of the Requirements
for the Degree of

Doctor of Philosophy

by

Gérard Maze, B.S., M.S.

Under the Direction of Joachim Rosenthal

Department of Mathematics
University of Notre Dame
April 2003

ALGEBRAIC METHODS FOR CONSTRUCTING ONE-WAY TRAPDOOR FUNCTIONS

A Dissertation

Submitted to the Graduate School
of the University of Notre Dame
in Partial Fulfillment of the Requirements
for the Degree of

Doctor of Philosophy

by

Gérard Maze, B.S., M.S.

Under the Direction of Joachim Rosenthal

Department of Mathematics
University of Notre Dame
April 2003

Copyright © Gérard Maze, 2003. All right reserved.

Abstract

In this dissertation, we consider an extension of the discrete logarithm problem to the case of a semigroup acting on a finite set: the Semigroup Action Problem (SAP). New protocols and one-way trapdoor functions based on the difficulty of such problems are proposed. Several instances are studied both from a conceptual and cryptographic point of view.

We discuss the application of existing generic algorithms to the resolution of an arbitrary SAP. The Pohlig-Hellman reduction leads to the notion of c-simplicity in semirings. Generic square-root attacks lead to semigroups with a negligible portion of invertible elements. After having described the situation when linear algebra over fields can be used, an application of the theory of finite c-simple semirings produces an example of SAP where no such known reduction applies.

An extension of the Elliptic Curve Discrete Logarithm Problem (ECDLP) is defined using the Frobenius homomorphism of elliptic curves over finite fields. Actions induced by the Chebyshev polynomials are studied in different algebraic structures such as $\mathbb{F}_q$, $\mathbb{Z}/n\mathbb{Z}$ and $\mathrm{Mat}_n(\mathbb{F}_q)$. Those are shown to be equivalent to known hard problems such as FACTORING and DLP in finite fields. Finally, non-associative operations lead to the study of the SAP in Paige loops, i.e., finite simple non-associative Moufang loops.

To my parents,
and to Sandrine.

Contents

List of Figures

List of Tables

List of Symbols

SAP	Semigroup Action Problem
DHAP	Diffie-Hellman semigroup action problem
DHP	Diffie-Hellman problem
DLP	discrete logarithm problem
ECDLP	elliptic curve discrete logarithm problem
$\mathbb{F}_q$	the field with q elements
gcd	greatest common divisor
lcm	least common multiple
$\mathrm{Mat}_n(R)$	the set of $n \times n$ matrices over R
$O(f(n))$	function $g(n)$ such that $\lvert g(n)\rvert < c\lvert f(n)\rvert$ for some constant $c > 0$ and all sufficiently large n
$o(f(n))$	function $g(n)$ such that $\lim_{n\to\infty} \lvert g(n)\rvert/\lvert f(n)\rvert = 0$
RSA	Rivest-Shamir-Adleman encryption scheme

Acknowledgement

I would like to thank here the people without whom these lines would not have been written. First and foremost, I am truly grateful to my advisor and friend, Joachim Rosenthal who helped me, supported me and gave me his entire trust.

I am grateful to the Department of Mathematics of the University of Notre Dame who provided me an excellent research environment as well as the opportunity to finish my dissertation abroad. I am also grateful to Professor Charles Stuart who gave me the chance to work at the Ecole Polytechnique Fédérale de Lausanne while I was in Switzerland.

I would like to thank the members of my defense committee, Karen Chandler, Claudia Polini and Andrew Sommese for their time and suggestions. I owe many thanks to Chris Monico who gave me precious advice as well as fruitful discussions.

My thanks go out to my dear friends and colleagues Hugo, Tom, Aline, Elisa, Feride, Gregory, Marc-O. and Lionel.

I would like to thank my family, maman, papa and Christine, for all their support and encouragement. Finally, Sandrine, ma douce Sandrine, merci.

Chapter 1

INTRODUCTION

This is a dissertation about public-key cryptography. One-way trapdoor functions are essential to the study of this subject. This introduction gives an overview of modern cryptography and a "cultural" background related to the study of algebraic one-way trapdoor functions. As for the last section, it will provide the reader the motivations and purposes of this work.

1.1 Overview of cryptography

Alice and Bob are old friends. Eve tries to eavesdrop on their secret conversation. Alice, Bob and Eve are the abstract protagonists of one of the oldest story of mankind: secrecy of communication. Obviously there is no assumption that Alice, Bob or Eve are human beings. They may (and probably will) be computers, some networks or an ATM machine. Cryptography, literally the science of secret writing, is an art that has developed over the ages. It has been used by many who have devised ad hoc techniques to meet the required security in their communication. The last twenty-five

years have been a period of transition as the discipline moved from an art to a science.

Modern cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, authentication, and non-repudiation. Let us now define for sake of clarity what is understood in the previous list.

1. Confidentiality is a service used to keep secret the content of information from all but those supposed to have access to it.

2. Data integrity is a service that detects data manipulation by unauthorized entities.

3. Authentication is a service related to identification such as entity authentication and data origin authentication.

4. Non-repudiation is a service which prevents an entity from denying previous commitment or actions.

In other words, modern cryptography is about the prevention and detection of cheating and other malicious activities related to secrecy. In order to reach these goals, cryptography provides basic tools, called *primitives*, such as *encryption schemes*, *digital signature schemes* and *hash functions*. These primitives can be unkeyed (mainly hash functions) or come with a symmetric-key structure or a public-key structure. We shall try in the sequel to define these notions and give examples of existing protocols. Unkeyed primitives will not appear since this dissertation is about public-key cryptography. A short section on secret-key primitives will however be presented to give an idea of the main stream related to symmetric ciphers.

1.2 Secret-key cryptography

This part of the story takes its roots in the ancient time. The interested reader will find in [2], [10], [11], and [85] all the development and details of secret-key cryptography from Egyptians to nowadays data encryption schemes. Our starting point is the notion of one-way function. This standard for "secret-key systems" arose around 1970.

Definition 1.1 A function f from a set X to a set Y is a *one-way function* if $f(x)$ is "easy" to compute for all $x \in X$ but for a random element $y \in \operatorname{Im} f$ it is "computationally infeasible" to find any $x \in X$ such that $f(x) = y$.

A rigorous definition of the terms "easy" and "computationally infeasible" is difficult to give. A possible clarification gives the term "easy" the meaning "polynomial-time computable" and "computationally infeasible" the meaning "not computable in polynomial-time". However the existence of such a function appears to be equivalent to the well-known conjecture P $\neq$ NP (see [94]). We will therefore keep the intuitive meaning and adopt the following convention: a problem will be called "easy" if there exists a polynomial-time algorithm to solve it and "computationally infeasible" or "hard" if no deterministic or probabilistic polynomial-time algorithm is known to solve it. Regarding the equivalence of computational tasks, we will say that a computational problem P_1 *reduces* to a computational problem P_2 if there exists an algorithm that produces, in polynomial-time, for each instance I_1 of P_1 an instance I_2 of P_2 to solve I_1. Two problems are equivalent if each reduces to the other.

Definition 1.2 A *symmetric-key encryption scheme* is given by

M: a message space K: a key space C: a cipher space

and two maps

$$\varphi \ : \ M \times K \longrightarrow C \quad \text{and} \quad \psi \ : \ C \times K \longrightarrow M$$

such that

- $\psi(\varphi(m,k),k) = m$,
- $\varphi(.,k) \ : \ M \longrightarrow C$ is a one-way function for all k,
- $\varphi(m,.) \ : \ K \longrightarrow C$ is a one-way function for all m.

The adjective *symmetric* of the previous definition finds its origin in the fact that the key used for encryption is the same as the one used for decryption. This private key must be communicated through a completely secure channel in order to reach security.

There exists a symmetric-key encryption scheme, the one-time pad, that is *perfectly secure*, a notion defined by Shannon in his early work on the subject [81]. Even if the system is attractive thanks to its security and ease of encryption and decryption, it nevertheless has the major disadvantage of having a key that must be communicated securely which is at least as large as the plaintext (c.f. [86] or [94]).

The historical development of cryptography has been to design cryptosystems where one key of relatively small size can be used to encrypt a relatively long string of plaintext and still remain secure. A good example would be the Data Encryption Standard (DES), a 1975 creation of IBM, that was the official standard for unclassified application until 1998. DES encrypt a plaintext bitstring of length 64 using a key which is a bitstring of length 56. The key size

being too small for current computational power, the last decade was prolific in new symmetric encryption algorithms like IDEA, SAFER, RC5, triple DES and more. However the need for an Advanced Encryption Standard (AES) remained clear. After a formal call for algorithms on September 12, 1997, the National Institute of Standards and Technology (NIST) announced on October 2, 2000, that it had selected Rijndael, out of 15 candidates, to propose for the AES (see [66] and [65]). AES is a block cipher with a flexible key size of 128, 192 or 256 bitstring. A nice algebraic description of the algorithm can be found in [77].

1.3 Public-key cryptography

As mentioned before, in a symmetric key encryption scheme, the key must remain secret at both ends. Moreover, this key has to be shared by the two entities Alice and Bob, which requires negotiation at some point. In their seminal paper [12], Diffie and Hellman solve the problem of the key distribution with what is called today the *Diffie-Hellman key exchange protocol*. This protocol is a key exchange scheme that works without *trusted authority*. See Figure 1.1 below.

The underlying hard problem behind the strength of the protocol is the Diffie-Hellman Problem (DHP) that asks to find α^{ab}, given α^a and α^b. As such, it is strongly related to the Discrete Logarithm Problem (DLP) that asks to find a given α^a. The next chapter is completely devoted to the study of this problem and we will therefore not go further into it here.

This starting point opened the world of public-key cryptography: in a public-key protocol a secrete message is exchanged without the need that a secret key has to be interchanged first.

1) A prime p and a primitive element $\gamma \in \mathbb{Z}_p^*$ are made public.

2) Alice chooses $a \in \{1, \ldots, p-1\}$, computes γ^a and sends it to Bob. Her secret key is a.

3) Bob chooses $b \in \{1, \ldots, p-1\}$, computes γ^b and sends it to Alice. His secret key is b.

4) The element $\gamma^{ab} = (\gamma^a)^b = (\gamma^b)^a$ is used as a common secret key.

Figure 1.1: Diffie-Hellman protocol

Soon after, Rivest, Shamir and Adleman created the famous RSA protocol ([74] and [75]). Before giving a list of existing public-key cryptosystems, here is the definition of a building block of public-key cryptography:

Definition 1.3 A *one-way trapdoor function* is a one-way function f from a set X to a set Y with the additional property that given some extra information, the trapdoor, it becomes feasible to find for any $y \in \mathrm{Im}f$, an $x \in X$ such that $f(x) = y$.

This notion allows *public-key transmission* and *digital signature*:

- Idea of public-key transmission : Suppose Bob wants to send Alice a message m. Alice publishes her one-way trapdoor

function $f : X \to Y$. Bob sends Alice the encrypted message $f(m)$. Alice can retrieve m using the trapdoor, but an eavesdropper will not be able to decrypt it without the secret trapdoor.

- Idea of digital signature (with message recovery): Suppose Alice wants to sign a message, i.e., she wants to be able to prove that she is the author of it. She construct a one-way trapdoor function $f : X \to Y$ and chooses the message $m \in \mathrm{Im} f$. She then sends Bob $y \in f^{-1}(m)$. Bob will be convinced that Alice is the author of the message since he will have to use her one-way trapdoor function to read the message $m = f(y)$.

1.4 Examples of one-way trapdoor functions

The following list of cryptosystems is far from exhaustive. They are based on different one-way trapdoor functions and instead of describing it for each of them, the underlying hard problem is stated. These cryptosystems appear as examples here rather than others either because of their popularity and strength or because of the underlying hard problem that will appear in the sequel. See [57, Chapter 3] for a complete description of computational problems of cryptographic relevance.

1. The *ElGamal protocol* [13] is an encryption scheme that is also based on the difficulty of the DLP in finite fields. See Figure 1.2.

2. The *RSA cryptosystem* [74] is a protocol based on the difficulty of factoring integers that are the product of large primes, see Figure 1.3. The underlying hard problem is known

1) Alice chooses publicly a prime p and a primitive element $\alpha \in \mathbb{Z}_p^*$.

2) She chooses $a \in \{1, \ldots, p-1\}$ and computes $\beta = \alpha^a$. Her public key is (α, β).

3) Bob chooses $k \in \{1, \ldots, p-1\}$ and uses the encryption function $f : m \longmapsto f(m) = (\alpha^k, m\beta^k) = (c_1, c_2)$.

4) Alice decrypts the message with $m = c_2(c_1^a)^{-1}$.

Figure 1.2: ElGamal protocol

as the RSA problem (RSAP), which precisely asks to invert the one-way trapdoor function f of the protocol. It is related to the well-known factoring problem (FACTORING) that asks to factor a given integer n into prime powers. Indeed the knowledge of n and $\varphi(n)$ is computationally equivalent to the knowledge of the factors p and q of n. However, it is not known if FACTORING is equivalent to RSAP even if the latter reduces to the former. The equivalence is strongly suspected. We will not go into the details of any factoring algorithm but rather give the expected running time of the fastest known algorithm, i.e., the Number Field Sieve Method ([8] and [93]), which is

$$O(\exp((1.923 + o(1))(\ln n)^{1/3}(\ln \ln n)^{2/3})).$$

1) Alice chooses two large primes p and q, computes $n = pq$ as well as the value $\varphi(n) = (p-1)(q-1)$

2) She chooses $e \in \{1, \ldots, n-1\}$ so that $(e, \varphi(n)) = 1$ and computes d so that $ed = 1 \mod \varphi(n)$.

Her public key is the pair (n, e).

3) Bob uses the encryption function

$$f : m \longmapsto f(m) = m^e \,(\text{mod } n).$$

4) Alice decrypts the message with the congruence

$$m = f(m)^d \,(\text{mod } n) = m^{ed} \,(\text{mod } n).$$

Figure 1.3: RSA protocol

This method belongs to the class of subexponential-time algorithms. A number n that is the product of two prime numbers for which RSAP is hard is called an *RSA number* or *RSA integer*.

3. The *Rabin cryptosystem* [73] is a protocol based on the difficulty of finding square roots modulo a RSA number, see Figure 1.4. First, the protocol described in Figure 1.4 is not complete. A square in $\mathbb{Z}_n$ possesses in general 4 square roots, i.e., Alice needs an extra information for the message recovery, although this can be done easily. Next, the underlying

1) Alice chooses two large primes $p, q = 3 \mod 4$.

She computes $n = pq$, and makes n public.

2) Bob uses the encryption function $f : m \longmapsto m^2 \mod n$.

4) Alice decrypts the message solving

$$x^2 = f(m) \mod p \quad \text{and} \quad y^2 = f(m) \mod q$$

and using the Chinese Remainder Theorem.

Figure 1.4: Rabin protocol

hard problem is the Square Root Problem modulo an RSA number (SQROOT) and it is known that SQROOT is equivalent to FACTORING (see [57]). This makes the strength of the protocol. Note that the task of finding square roots in a finite field is easy (c.f. the discussion before Proposition 6.7).

4. The *Polly Cracker cryptosystem* was created by N.Koblitz and is described in [39], see Figure 1.5. There exists many variants of it, the following description is the simplest. The construction of the polynomials Q_i is fast since it suffices to consider polynomials of type $Q_i = p(x_1, ..., x_n) - p(v_1, ..., v_n)$ for any $p \in \mathbb{F}_q[x_1, ..., x_n]$. The underlying hard problem is the Multivariate Polynomial Equation (MPE) which asks to find a root of a system of m non-linear polynomials in n variables. This problem is known to be NP-hard (even if the polynomials are required to have degree at most 2), see [17], and this

makes the system appealing. No equivalence between inverting the one-way trapdoor function and the MPE problem is yet known. See [14] and [15] for complexity issues concerning the choice of the parameters.

1) Alice chooses a finite field $\mathbb{F}_q$ and a n-vector

$v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$.

2) She builds l polynomials in n variables $Q_1, \ldots, Q_l$

such that $Q_i(v_1, \ldots, v_n) = 0$ for all $i = 1, \ldots, l$.

Her public key is $(\mathbb{F}_q, Q_1, \ldots, Q_l)$.

3) Bob chooses l polynomials in n variables $b_1, \ldots, b_m$

and use the encryption function

$$f : m \longmapsto f(m) = m + \sum_{j=1}^{l} b_j Q_j \in \mathbb{F}_q[x_1, \ldots, x_n]$$

4) Alice decrypts the message with $m = f(m)(v)$.

Figure 1.5: Polly Cracker protocol

5. We refer the interested reader to [55] for the *McEliece cryptosystem* based on algebraic coding theory and [23] for the GGH cryptosystem, the lattice version of it.

6. The quite new scheme NTRU [29] based on the difficulty of

finding an interpolating sparse polynomial of high degree and the latest version [30] NSS based on a lattice version of NTRU give an idea of the new trend in cryptography trying to use new computational hard problems to build one-way trapdoor functions.

7. The famous but yet broken Merkle-Hellman Knapsack [59] is a good example of public key cryptosystem that was revealed to be weak after some years, even though the scheme is based on an NP-hard problem.

We have one concluding remark concerning the effective utilization of the above protocols. As a matter of fact, symmetric-key ciphers need shorter keys than public-key ciphers and they are much faster in practice than any currently accepted public-key cryptosystem. But public-key ciphers offer something symmetric-key cryptosystems will never be able to give. This is why current cryptographic systems exploit the strength of each. In general, public-key encryption techniques are used to establish a key that will be utilized by the communicating entities in a symmetric-key system.

1.5 Overview and goal of this dissertation

The goal of this dissertation is to study a generalization of the Discrete Logarithm Problem (DLP) both from a cryptographic and conceptual point of view. One motivation is to find new instances on which new cryptosystems could be based, more efficient than existing protocols. Even though no such examples have been found so far, this work also defends the idea that our generalization could

ultimately lead to such a situation. Moreover, history of mathematics shows that generalizations often lead to deeper understanding: in modern cryptography, this could reveal weaknesses of cryptosystems that one wouldn't have noticed before.

In this dissertation, we present and develop this generalization, discuss its relationship with the existing DLP and explain how it can be used in building one-way trapdoor functions. Then different examples are studied and analyzed from an abstract and applied viewpoint. We prove several equivalence results and present new believed hard problem.

After describing precisely what is understood by the Discrete Logarithm Problem (DLP) and the Diffie-Hellman Problem (DHP) in cyclic groups, Chapter 2 presents existing cryptographic protocols based on the difficulty of the DLP. From this regard, the three families of existing algorithms that solve the DLP in cyclic groups are described and the key points of each of these algorithms are highlighted.

Chapter 3 presents the setting we will use in this work. Abelian semigroups acting on finite sets (G-actions) are defined leading to the analogue of the DLP for G-actions, the Semigroup Action Problem (SAP). This allows one to define the Diffie-Hellman protocol with a G-action as well as the ElGamal protocol with a G-action. The cryptographic point of view yields a study of the generic attacks in the case of semigroup actions. This leads to a discussion on the density of inverses in the semigroup and on the notion of c-simplicity.

Linear actions are the basis for Chapter 4. Theorem 4.1 gives a reduction of many SAP instances taking place over finite fields to computational problems in linear algebra. As a consequence, linear actions over semirings are considered as well as linear actions

defined via maps that do not appear as matrices. An example coming from the theory of elliptic curves over finite fields with complex multiplication is studied.

Chapter 5 is entirely devoted to the study of a class of semirings. We prove that each of these semirings are c-simple and that they possess a negligible portion of invertible elements. A study of these objects with the help of Landau's g function shows the existence of "large" commutative sub-semiring. A graph-theoretic interpretation of these semirings is given and two abelian actions are analyzed. These actions do not reduce to known problems and seem hard to solve. However, we show that the DLP over certain groups (e.g. non-singular elliptic curve) is still a more difficult problem.

Chebyshev polynomials T_n are then studied from a SAP point of view in Chapter 6. Indeed, we define the Discrete Chebyshev Problem in any finite ring R with identity and prove several equivalence results. When R is a finite field or a matrix algebra over a finite field, we prove that the Discrete Chebyshev Problem is essentially equivalent to the DLP in the finite field. A classification theorem (Theorem 6.10) on matrices $M \in \mathrm{Mat}_n(\mathbb{F})$ that possess square roots is proven in the development. When R is the ring of integers modulo an RSA number n, the problem is shown to be at least as hard as factoring n.

The Moufang loops $M(q)$ and Paige loops $M^*(q)$ are the subject of the last chapter. After having defined these objects, we prove that the DLP in $M^*(q)$ reduces to the DLP in $\mathbb{F}_q$. Adding to the exponentiation an action by conjugation, we investigate the difficulty of a new action. We manage to reduce this last action essentially to the DLP in $\mathbb{F}_q$ for almost all cases, except when a trace condition is not fulfilled. We explain why this last case seems

to be different.

Chapter 2

EXISTING CONSTRUCTIONS BASED ON THE DLP

In this chapter, we define the discrete logarithm problem in a finite commutative group. The three classes of existing algorithm that solve the DLP are presented. The notion of generic algorithm is developed. From there, the Diffie-Hellman key exchange and the ElGamal protocol are presented as well as other use of the discrete logarithm problem in cryptography.

2.1 The discrete logarithm problem

The discrete logarithm problem, commonly abbreviated DLP, is a recurrent tool in public-key cryptography. The problem takes place in any group G, but we shall always assume the group is finite and commutative.

Problem 2.1 [The Discrete Logarithm Problem - DLP] Let G be a finite commutative group. Given two group elements a (the base) and b such that $b \in \langle a \rangle$, find $0 \leqslant n < \mathrm{ord}(a)$ such that $a^n = b$. We denote such an n by $\log_a b$.

For cryptographic purposes, we will always assume that the group G is presented in such a way that multiplication is computationally easy. Note that this requirement makes exponentiation feasible as well using well-known methods of type square-and-multiply (see [57] or [93]).

The difficulty of the DLP strongly depends on the type of group that is used: it goes from easy to non-feasible. For instance the DLP in the additive group of any finite field $\mathbb{F}_q$ is trivial since division can be perfomed in polynomial-time. However, the DLP in the multiplicative group $\mathbb{F}_q^*$ is a difficult problem as well as the DLP in the group $E(\mathbb{F}_q)$ of an elliptic curve defined over a finite field. In fact the latter is much more difficult than the former and intuition tells us that the less structure the group has, the more difficult the DLP will be. This is one of the reason why we've developed the ideas of the next chapter. In the sequel, by "DLP in $\mathbb{F}_q$", we will mean that the problem takes place in the multiplicative group of the finite field.

Computing discrete logarithms is essentially computing an isomorphism between $\langle a \rangle$ and $\mathbb{Z}_{\mathrm{ord}(a)}$. It is also true that any algorithm that computes discrete logarithms in base a can be used to compute discrete logarithms in any other base $\alpha \in \langle a \rangle$.

The known algorithms to solve the DLP can be categorized as follows:

1. Algorithms that work in arbitrary groups, e.g., Shank's baby-step-giant-step algorithm, Pollard's rho algorithm, Pollard's lambda algorithm.

2. Algorithms that work in arbitrary groups but are especially efficient if the order of the group has only small prime factors, e.g., Pohlig-Hellman algorithm.

3. Algorithms that use properties of the presentation of the group, e.g., index-calculus algorithms and the number field sieve method (NFS attack).

Let us describe briefly the ideas behind each of these algorithms. Shank's algorithm (see e.g. [37]) provides a look up table built from the values a^j with $0 \leqslant j \leqslant m$ where $m = \lceil \sqrt{n} \rceil$ (the baby steps). Then one builds the sequence ba^{-mi} with $0 \leqslant i \leqslant m$ (the giant steps); as soon as an element of the sequence is detected in the look-up table, i.e., $a^{j_0} = ba^{-mi_0}$, the discrete logarithm n is found with $n = j_0 m + i_0$. This algorithm finds n with time complexity and space complexity $O(\sqrt{\text{ord } a})$. Pollard's rho and Pollard's lambda algorithms ([70], [71]) both use the same idea: finding a collision in a sequence $x_i = a^{s_i} b^{t_i}$ that behaves like a random walk in G. As soon as a collision $x_l = x_k$ is found one can compute n, with high probability, since

$$\begin{aligned} a^{s_l} b^{t_l} = a^{s_k} b^{t_k} \quad &\Longrightarrow \quad a^{s_l - s_k} = b^{t_k - t_l} \\ &\Longrightarrow \quad (t_k - t_l)n \equiv (s_l - s_k) \mod |G|. \end{aligned}$$

Note that the existence of inverses in the group is used to transform the collision into a solution. These algorithms work with expected time complexity $O(\sqrt{\text{ord } a})$ and negligible space complexity.

The Pohlig-Hellman algorithm ([69]) uses reductions into smaller quotient groups in order to find the discrete logarithm n. More precisely, for each prime power p^e that divides the order of a, one solves the problem $a^n = b$ in the quotient $\langle a \rangle / H$ with H being the unique cyclic sub-group of $\langle a \rangle$ of order p^e. These problems are solved using

one of the previous algorithms in every quotient. Then, using the Chinese Reminder Theorem, one recovers the discrete logarithm n modulo the order of a, which is clearly sufficient. The overall complexity of the Pohlig-Hellman algorithm is determined by the largest prime factor q of the order of a and the algorithm has complexity $O(\sqrt{q}\log_2 q)$.

Index-calculus methods are faster than the previous algorithms. They use special properties of the representation of the elements. Indeed one needs to find a *factor base* in the group in order to apply the method. Such an object may not be possible to find depending on the group representation. For instance, there exist methods to build factor bases in any finite field, prime or not, but there is evidence that such a base will be extremely difficult to find in the case of the abelian group of an elliptic curve over a finite field (e.g. [39] and [60]). The most powerful tool to solve the DLP in a finite field is the number field sieve ([24] and [25]) which has an expected running time of

$$O(\exp((c+o(1))(\ln n)^{1/3}(\ln\ln n)^{2/3})) \tag{2.1}$$

where c depends on the finite field ($c \cong 1.92$ for a prime field). Note that this running time is essentially the same as the running time of the fastest known algorithm used to factor numbers.

Let us discuss the consequences of the running times regarding the key size N, which is the size in bits of the group: $N = \lceil \log_2(|G|) \rceil$. In a group where the best known attack is a square-root attack, then the complexity of it is $O(\sqrt{|G|}) = O(2^{N/2})$. In a finite field $\mathbb{F}_p$, Equation 2.1 gives the complexity of the best known attack as roughly $\exp(1.92(N)^{1/3}(\ln(N\ln 2))^{2/3})$ (neglecting the constant factor). In order to reach similar levels of security (c.f. [4]), if we define $N_{\mathbb{F}_p}$ to be the key size when using the group

$\mathbb{F}_p^*$ and N_{EC} when using the group $E(\mathbb{F}_q)$, they must satisfy the relation

$$N_{EC} \approx 4.91 \; N_{\mathbb{F}_p}^{1/3} \cdot \left(\log(N_{\mathbb{F}_p} \log 2)\right)^{2/3}.$$

For example when $N_{\mathbb{F}_p}$ is in the order of 4096 bits, then a comparable security is achieved when N_{EC} is in the order of 313 bits. As mentioned before, the best known algorithms to factor integers are of roughly the same asymptotic complexity as the complexity of the DLP in $\mathbb{F}_p$. Therefore the previous discussion applies to the RSA cryptosystem as well. Note that these values are approximately accurate at the time of this writing, but may change in the future if new algorithms are found.

The last few years were especially rich in new approaches to find lower bounds on the complexity of so-called *generic algorithms* for DLPs in cyclic groups ([82], [51]) and index search ([50]). Intuitively, a generic algorithm is an algorithm that does not make use of any particular property of the representation of the input elements, i.e., these algorithms may take place in any group. For instance, the index-calculus algorithm and number field sieve are not of this type. The results in this area are of prime importance since lower bounds seem to be quite rare and difficult to obtain in complexity theory ([48]) and moreover such bounds are real proofs of the difficulty of the underlying problem. The following theorem of V. Shoup [82] shows that the above bound $O(\sqrt{q}\log_2 q)$ is almost the best, in a generic sense:

Theorem 2.2 *Let G be a cyclic group and q the largest prime dividing $|G|$. Every generic algorithm that solves the DLP in G that can only input constants and add values has success probability after t steps of at most $t^2/2q$. Hence the expected running time is $O(\sqrt{q})$.*

2.2 The Diffie-Hellman protocol

As explained in the introduction, the Diffie-Hellman protocol is a key exchange protocol based on the difficulty of the DLP in finite commutative groups. The condition that the group G be finite provides a bound on the key size, the key being an element of the group. In their important paper [12], Diffie and Hellman worked in the group of invertible elements of a prime finite field $\mathbb{Z}_p$ with a primitive element as the base of the exponentiation function. However the existence of sub-exponential algorithm to solve the DLP in these groups, as explained above, led Miller [60] and Koblitz [38] to propose to work with the group $E(\mathbb{F}_q)$ of rational points of an elliptic curve where so far only a generic algorithm is known as a solution. Let us recall the protocol for a group G:

1) A group G and an element $g \in G$ are made public.

2) Alice chooses $a \in \{1, \ldots, \text{ord } g\}$, computes g^a and sends it to Bob.

3) Bob chooses $b \in \{1, \ldots, \text{ord } g\}$, computes g^b and sends it to Alice.

4) They use the element $g^{ab} = (g^a)^b = (g^b)^a$ as a common secret key.

Figure 2.1: Diffie-Hellman protocol in a group G

It is clearly sufficient to solve a DLP in G in order to find the secrete key g^{ab}. What about the necessity of solving a DLP in order to break the system? Let us consider the following problem:

Problem 2.3 [**The Diffie-Hellman Problem - DHP**] Let G be a finite commutative group and $g \in G$. Given two group elements g^a and g^b, find g^{ab}.

The DHP is the real problem to study in order to clarify the security of the Diffie-Hellman key exchange. The work of Maurer and Wolf [49] is crucial in this direction. Their results essentially show that one can construct groups for which breaking the Diffie-Hellman protocol is provably as hard as computing discrete logarithms, and this equivalence holds for any group if a plausible number-theoretic conjecture on the density of smooth integers holds. It is therefore not too risky to consider that breaking the Diffie-Hellman key exchange protocol is equivalent to solving the DLP.

2.3 The ElGamal protocol

The idea of using the difficulty of the DLP in groups for cryptographic purposes was first used by Diffie and Hellman in their key exchange. However this protocol does not provide a public key encryption scheme. ElGamal was the first to create a one-way trapdoor function using the difficulty of the DLP. The protocol is given in the introduction, therefore we will just explicit the one-way trapdoor function. Let G be a group where the DHP is hard, $\alpha \in G$, $a \in \mathbb{N}$ and $\beta = \alpha^a$. Then the following function is a one-way trapdoor function:

$$\begin{array}{ccc} G \times \mathbb{N} & \longrightarrow & G \times G \\ (m, k) & \longmapsto & (\alpha^k, m\beta^k). \end{array}$$

Note that this protocol is a *randomized encryption* since Bob is free to choose k before each encryption. In other words a message m will be encrypted in different ciphertext as long as different values of k are chosen. The protocol does not use the previous one-way trapdoor function exactly but rather the restriction of it for each parameter k chosen by Bob. The basic RSA scheme does not give this opportunity, but there is a way to modify the RSA algorithm to turn it into a randomized encryption. The main disadvantage of the ElGamal encryption is that there is message expansion by a factor of 2. Namely the ciphertext is twice as long as the corresponding plaintext.

2.4 Other use of DLP

The difficulty of the DLP in groups has been used in many different kinds of cryptographic protocol, other than the above key exchange and encryption scheme. Indeed there exists several *digital signature* schemes based on it, as well as some *group key exchange* schemes and *identification protocols* (c.f. [86] and [57]).

We already mentioned in the introduction how a one-way trapdoor function can be turned into a digital signature schemes with message recovery. However the functions usually used in RSA or ElGamal without modification yield signature lengths of the same orders as the messages, which can be avoided. In 1991 the National Institute of Standard and Technology proposed a standard, the DSA, based on the Digital Signature Standard (DSS) (c.f. [57]). The DSA is based on the difficulty of the DLP in a subgroup of the multiplicative group of a finite field $\mathbb{F}_p$. Although to break the system it would suffice to find discrete logarithms in the smaller subgroup, in practice this seems to be no easier than finding arbi-

trary discrete logarithms in $\mathbb{F}_p^*$. The signature length is 160 bits, although the DLP takes place in a finite field of size larger than 512 bits. The DSS is a modification of the ElGamal Signature Scheme [13] and the Schnorr Signature Scheme [79]. There is an elliptic curve analogue (ECDSA) of the DSA, adopted in 1998, which uses the same idea.

Regarding the group key exchange problem, E. Bresson in [6] studied cryptographic protocols that generalize Diffie-Hellman key agreement to many users. He showed how, through an insecure network, many parties can agree on a common session key, and how they can have it evolve when the group membership changes (join or removal of members).

Chapter 3

DIFFIE-HELLMAN AND ELGAMAL FROM SEMIGROUP ACTIONS

The definition of a semigroup acting on a finite set begins this chapter. Using such actions, we present generalizations of the Diffie-Hellman key exchange and of the ElGamal protocol. The semigroup action problem is then defined. The study of the security of such protocols leads to the notion of simple semigroup and to semigroups with a negligible portion of invertible elements.

3.1 Abelian semigroup action

This chapter is about a generalization of the protocols that use groups and take advantage of the difficulty of solving the discrete

logarithm problem in these groups. Our setting will use the notion of abelian semigroup acting on a set. This abstract viewpoint has been developed in collaboration with J. Rosenthal and C. Monico in [52], [54] and [53]. It is in essence the least requirement needed to extend the protocols studied in the previous chapter. The idea of using algebraic structures such as groups or semigroups acting on a set in cryptography is not new; indeed Yamamura [92] has been considering a group action of $Sl_2(\mathbb{Z})$ on the complex plane and Blackburn and Galbraith have been studying the system in [3]. However our standpoint is different and yields other protocols.

Definition 3.1 A semigroup G is a set equipped with an associative binary operation $(a, b) \longmapsto ab$. The semigroup is abelian if $ab = ba$ for all a, b in G. An identity e is an element that satisfies $ea = ae = a$ for all a in G. An element a is invertible if there exists $b \in G$ such that ab and ba are an identity.

It is interesting to note that there exist many more finite abelian semigroups than finite abelian groups. For instance there are 2 abelian groups of order 4, and 58 abelian semigroups with the same order. These numbers become 2 vs. 11,545,843 when the order is 9 (c.f. [27]). However the number of finite abelian semigroups that seem to be of any use in cryptography seems to be much smaller.

Definition 3.2 Let G be a semigroup and S be a set. The semigroup G acts on S if there exists a map

$$\begin{array}{ccc} G \times S & \longrightarrow & S \\ (g, s) & \longmapsto & g \cdot s \end{array}$$

such that the equality $(gh) \cdot s = g \cdot (h \cdot s)$ holds for all $g, h \in G$ and all $s \in S$. If the semigroup G is abelian, the action is called a G-action on S.

In the sequel, we will always assume, unless specified, that every considered action is feasible from a computational viewpoint, i.e., every operation $g \cdot s$ is easy to compute as well as any product gh in G. Note that the associativity in G allows exponentiation of an element g to the n^{th} power in $\lceil \log_2(n) \rceil$ semigroup operation. Without loss of generality, we will also always assume (unless stated) that there exists an identity e in the semigroup that satisfies $e \cdot s = s$ for all $s \in S$. Some authors (e.g. [33], [27] and [72]) call such an object a *monoid*, but we will keep on talking of semigroups as in [32].

Example 3.3 Let G be an arbitrary finite semigroup, and let C, K be two abelian subgroups of G. Then the action:

$$\begin{array}{rcl} (C \times K) \times G & \longrightarrow & G \\ ((c,k),g) & \longmapsto & cgk \end{array}$$

is a $C \times K$-action on G.

Example 3.4 Let G be an arbitrary finite group, and let C be an abelian subgroups of G and let $\mathbb{Z}$ be the integers. Then the action:

$$\begin{array}{rccl} \varphi : & (C \times \mathbb{Z}) \times G & \longrightarrow & G \\ & ((c,t),g) & \longmapsto & cg^t c^{-1} \end{array}$$

is a $C \times \mathbb{Z}$-action on G. Note that if G is abelian we simply deal with the discrete logarithm problem in a finite abelian group. In the non-abelian case things get combined with a conjugation.

Many other examples of semigroup actions will appear in this dissertation.

3.2 The cryptographic point of view

We are now ready to state the generalized version of the Diffie-Hellman protocol in the context of semigroup action:

1) A G-action on a finite set S is made public as well as an element s in S.

2) Alice chooses $a \in G$, computes $a \cdot s$ and sends it to Bob.

3) Bob chooses $b \in G$, computes $b \cdot s$ and sends it to Alice.

4) They use the element

$$a \cdot (b \cdot s) = (ab) \cdot s = (ba) \cdot s = b \cdot (a \cdot s)$$

as a common secret key.

Figure 3.1: Diffie-Hellman protocol with a G-action on S

The set S is finite in order to have a bound on the key size. Suppose the set S comes with an extra group law denoted by $\oplus$. Then there is also a generalized version of the ElGamal protocol in the context of semigroup actions, see Figure 3.2.

The security of these protocols lies of course on many aspects of the parameters. In this perspective, there is an analogue version of the DLP for semigroup action. C.Monico [62] first defined it as follows:

1) Alice chooses publicly a G-action on a finite set S

and $s \in S$.

2) She chooses $a \in G$ and computes $t = a \cdot s$.

Her public key is (s, t).

3) Bob chooses $k \in G$ and uses the encryption function

$$f : m \longmapsto f(m) = (k \cdot s, m \oplus k \cdot t) = (c_1, c_2).$$

4) Alice decrypts the message with $m = c_2 \oplus [-(a \cdot c_1)]$.

Figure 3.2: ElGamal protocol with a G-action on S

Problem 3.5 [The Semigroup Action Problem - SAP] Let G be a finite abelian semigroup, S a finite set and $\cdot$ a semigroup action of G on S. Given $x, y \in S$ with $y = g \cdot x$ for some $g \in G$, find $h \in G$ such that $y = h \cdot x$.

Any abelian semigroup G acting on a finite set S gives rise to a Diffie-Hellman protocol and an ElGamal protocol. It is clear that the main question to be answered as soon as such an action is considered is the difficulty of the SAP. Our goal is to find actions for which the SAP is hard; possibly harder than the DLP in groups. Notice that the DLP in a group H is a special instance of the SAP where the action is

$$\begin{array}{ccc} \mathbb{N} \times H & \longrightarrow & H \\ (n, h) & \longmapsto & h^n \end{array}$$

and it seems natural to expect some different kind of problems

when more general actions are considered. Of course, there is an analogue version of the Diffie-Hellman Problem stated in terms of semigroup:

Problem 3.6 [**The Diffie-Hellman Semigroup Problem**] Let G be a finite abelian semigroup, S a finite set and $\cdot$ a semigroup action of G on S. Given $x, y, z \in S$ with $y = g \cdot x$ and $z = h \cdot x$ for some $g, h \in G$, find $(gh) \cdot x \in S$.

3.3 The security

The security of the above protocols in the context of semigroup actions is of course a crucial requirement in their study. As mentioned earlier the strength of these cryptosystems strongly depends on the difficulty of the SAP. Consider the Diffie-Hellman key exchange with a G-action on S. Suppose Alice has sent Bob the set element $a \cdot s$. Eve knows the "seed" s and the public element $a \cdot s$. If she is able to solve the SAP with parameters s and $a \cdot s$, she is in possession of a semigroup element $\tilde{a}$ such that $\tilde{a} \cdot s = a \cdot s$. She can now retrieve the common secret key using Bob's public set element $b \cdot s$ since

$$\tilde{a} \cdot (b \cdot s) = (\tilde{a}b) \cdot s = (b\tilde{a}) \cdot s = b \cdot (\tilde{a} \cdot s) = b \cdot (a \cdot s) = (ab) \cdot s.$$

We have seen in Chapter 2 that there exist many different parameters to consider in choosing a "secure" group when dealing with Diffie-Hellman and ElGamal. As a matter of fact, the group order has to contain a prime factor large enough to make the Pohlig-Hellman attack useless. We have also sketched Pollard's rho algorithm that provides a generic algorithm for solving a discrete logarithm problem in expected running time of roughly $O(\sqrt{q})$, q

being the largest prime factor of the group order. These two algorithms being generic, a natural question to treat is to know if such algorithms can be extended to the case of the SAP. Another face of the problem, related to the existence of index-calculus methods and NFS attack, is simply to try to work with semigroup action problems that do not have an ad hoc attack.

3.4 Pohlig-Hellman with semigroups

Considerations on the Pohlig-Hellman attack yield the notion of *simple semigroup* (c.f. [62]). The study of semigroups and monoids shows that this notion has many faces (c.f. [32] and [72]) and we will therefore concentrate on the notion of *congruence-free* which is really what is needed in this framework. A semigroup G is congruence-free if any semigroup homomorphism $f : G \to G'$ has kernel either G or $\{e\}$. This is equivalent to ask that the only congruence relations on G, i.e., the equivalence relation $\sim$ such that

$$a \sim b \Longrightarrow \left\{ \begin{array}{l} ac \sim bc \ \ \forall c \in G \\ ca \sim cb \ \ \forall c \in G \end{array} \right. ,$$

are the trivial ones, namely $G \times G$ and $\{(g, g) \mid g \in G\}$.

The idea of the Pohlig-Hellman algorithm is to solve a family of "local" DLP in quotients of the group where the DLP takes place and then lift the local solutions to a solution of the global DLP. If all the quotients are "small" and the reverse process (the "lifting") of taking quotient brings enough information then the algorithm is useful. In the case of abelian groups (and in fact in the case of any ring with "good" ideals), the Chinese Remainder Theorem is the tool used in the process. However, when playing with semigroup actions on sets, it seems difficult to describe a general method of "lifting". Moreover, the action of G on S may not be compatible

with the quotient map from G to $G/\sim$, where $\sim$ is a congruence relation. However, in any case, congruence-free structures seem to be desirable. But it turns out that this restricted perspective is quite poor, as shown by the following theorem.

Theorem 3.7 *If G is a finite congruence-free semigroup with identity and $|G| > 2$, then G is a finite simple group.*

A proof can be found in [32]. A direct consequence is that if one wants to reduce the study of the SAP to the case of finite congruence-free abelian semigroup, then the only examples are the one with $G \cong \mathbb{Z}/p\mathbb{Z}$ for some prime p since these are the only abelian simple groups. Note that if we allow the semigroup to possess a zero, i.e., an element 0 such that $0a = a0 = 0$ for all $a \in G$, then the situation is not better. Indeed every element is either idempotent or nilpotent, a direct consequence of the next theorem due to Tamura [88].

Theorem 3.8 *Let $I = \{1, ..., m\}$ and $J = \{1, ..., n\}$ be finite sets and P a $n \times m$ matrix of 1s and 0s such that no two rows are identical, no two columns are identical and no row or column is identically 0. Let $G = I \times J \cup \{0\}$ and suppose a binary operation is defined on G by*

$$\begin{aligned} (i,j)(k,l) &= \begin{cases} (i,l) & \text{if } p_{jk} = 1 \\ 0 & \text{if } p_{jk} = 0 \end{cases} \\ (i,j)0 &= 0(i,j) = 0. \end{aligned}$$

Then G is a congruence-free semigroup of order $mn + 1$. Conversely, every finite congruence-free semigroup with zero is isomorphic to one of this kind.

Since idempotent and nilpotent elements are useless in our context, once again this restricted viewpoint is not good enough. This

digression is not in contradiction with [62] since the results presented in this thesis are related to simple semirings acting on semimodules. In that case congruence-freeness is a different issue and the previous theorems don't hold (see also Section 4.3 of Chapter 4).

3.5 Square root attack with semigroups

The known generic algorithms for DLP such as Pollard's rho, Pollard's lambda or Shank's baby-step-giant-step all need at some point the existence of inverses in the group where the DLP takes place. In the context of index search, the situation is not different. U. Maurer and S. Wolf [50] considering a Generic Index Search Problem in an indexed set S with $|S| = N$ allow the indices to be added modulo N, which is equivalent to consider the action of the additive group $\mathbb{Z}/N\mathbb{Z}$ over S and once again the complexity lower bound is $O(\sqrt{N})$.

C.Monico [62] extends a version of Pollard's rho to the context of semigroup action if the semigroup is a group. Let us consider the main idea of the algorithm. We want to solve the SAP with a group G, a set S and parameters x and y with $y = g \cdot x$ for some $g \in G$. The idea is to find a collision in a random sequence of type $\{a_1 \cdot x, b_1 \cdot y, a_2 \cdot x, b_2 \cdot y, ...\}$. With probability $1/2$ the collision will take the form $a_i \cdot x = b_j \cdot y$ and since b_j^{-1} exists, the collision can be turn into the solution $y = (b_j^{-1} a_i) \cdot x$. Invoking the Birthday paradox [57], the overall average complexity of the algorithm is $O(\sqrt{|G \cdot x|})$.

If the semigroup is not a group, the previous algorithm does not apply; indeed Pollard's square root attack described in [62] provides with high probability a collision $a_i \cdot x = b_j \cdot y$ where b_j

is non-invertible. Therefore, in the case of a general semigroup, the lower bounds of a generic algorithm may not be in the range of the square root of the input size. However, if the semigroup possesses a "large" sub-group, then a decent upper bound can still be reached. Let $G_1 = \{g \in G \mid g^{-1} \text{ exists } \}$ and $G_0 = G \setminus G_1$. In any case one may try to find a solution of the equation $y = g \cdot x$ in G_0 by exhaustive search. If no solution has been found, then one can restrict the SAP instance in G to the SAP instance in G_1, which is a group. We can therefore apply the Pollard's square root attack described earlier. Clearly this algorithm has an expected running time bounded by $|G_0| + O(\sqrt{|G_1 \cdot x|})$. This gives the next proposition.

Proposition 3.9 *Let G be a commutative semigroup acting on S and consider the SAP instance with parameters x and $y = g \cdot x$. Let $G = G_0 \sqcup G_1$ be the partition described above. If $|G_0| = O(\sqrt{|G \cdot x|})$ then there exists an algorithm to solve the SAP instance in expected running time bounded by $O(\sqrt{|G \cdot x|})$.*

In other words, if G is not "far" from being a group and the orbit of x is, as expected, relatively large, then there is still a square root attack to the SAP. Let us consider an example of such a situation:

Example 3.10 Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = q$, $A \in \mathrm{Mat}_n(\mathbb{F})$ and $\mathbb{F}[A]$ be its matrix algebra. Let G be the multiplicative abelian semigroup of this algebra and we let G act on a set S. Let $m_A(x)$ be the minimal polynomial of A and $m_A(x) = p_1(x)^{e_1} \cdot \ldots \cdot p_k(x)^{e_k}$ its decomposition into irreducible factors. Then

$$\mathbb{F}[A] = \{g(A) \mid g \in \mathbb{F}[x] \text{ and } \deg(g) < \deg(m_A)\}$$

because of Cayley-Hamilton Theorem. Using the Chinese Remain-

der Theorem and the First Isomorphism Theorem,

$$\mathbb{F}[A] \simeq \mathbb{F}[x]/\left(m_A(x)\right) \simeq \bigoplus_{i=1}^{k} \mathbb{F}[x]/\left(p_i(x)^{e_i}\right).$$

and we see that an element $g(A)$ in $\mathbb{F}[A]$ is invertible if and only if $g(x)$ is coprime to each p_i. Let ∂p be the degree of $p(x)$. We have

$$\begin{aligned} |\mathbb{F}[A]^*| &= |\bigoplus_{i=1}^{k} \left(\mathbb{F}[x]/\left(p_i(x)^{e_i}\right)\right)^*| \\ &= \prod_{i=1}^{k} |\left(\mathbb{F}[x]/\left(p_i(x)^{e_i}\right)\right)^*| \\ &= \prod_{i=1}^{k} \left(q^{e_i \partial p_i} - q^{(e_i-1)\partial p_i}\right) \end{aligned}$$

and therefore

$$\begin{aligned} \frac{|\mathbb{F}[A]^*|}{|\mathbb{F}[A]|} &= \frac{\prod_{i=1}^{k} \left(q^{e_i \partial p_i} - q^{(e_i-1)\partial p_i}\right)}{q^{\partial m_a}} \\ &= \frac{\prod_{i=1}^{k} \left(q^{e_i \partial p_i} - q^{(e_i-1)\partial p_i}\right)}{\prod_{i=1}^{k} q^{e_i \partial p_i}} \\ &= \prod_{i=1}^{k} \left(1 - q^{-\partial p_i}\right) \end{aligned}$$

Finally, since in a finite ring an element is a zero divisor if and only of it is not a unit (see Lemma 3.11 below), $G_0 = \mathbb{F}[A] \backslash \mathbb{F}[A]^*$ and

$$|G_0| = |\mathbb{F}[A]| \cdot \left(1 - \prod_{i=1}^{k} \left(1 - q^{-\partial p_i}\right)\right).$$

The product on the right-hand-side can take many different values and therefore we do not have $|G_0| = O(\sqrt{\mathbb{F}[A]})$ in general.

However, if

$$\min\{\partial p_i + \partial p_j \mid i \neq j\} \geqslant \frac{\partial m_A}{2},$$

then since

$$\prod_{i=1}^{k} \left(1 - q^{-\partial p_i}\right) = 1 + O\left(q^{-\min\{\partial p_i + \partial p_j \mid i \neq j\}}\right)$$

we have that

$$\begin{aligned} G_0 &= q^{\partial m_a} \cdot \left(1 - 1 + O\left(q^{-\min\{\partial p_i + \partial p_j \mid i \neq j\}}\right)\right) \\ &\leqslant q^{\partial m_a} \cdot O(q^{-\partial m_a/2}) = O(\sqrt{\mathbb{F}[A]}). \end{aligned}$$

Notice that the relation is always true when $n = 1, 2$ and is "often" true when $n = 3, 4$.

Note as well that the previous example does not take into consideration any information on how the abelian semigroup acts on S. For instance when $\mathbb{F}[A]$ acts on $\mathbb{F}^n$ then simple linear algebra tools solve the problem completely (see Example 4.3). When $\mathbb{F} = \mathbb{Z}_p$ then there is an action of $\mathbb{F}[A]$ on any abelian group $H \oplus ... \oplus H$ with H of order p. This is a special case of the "matrix action on abelian groups" described in [62]; this instance always admits a square root attack. We have used the following Lemma:

Lemma 3.11 *Let R be a finite ring. Then an element is either invertible or a zero divisor.*

Proof: Let $a \in R$. Since R is finite, the sequence a^i, $i \in \mathbb{N}$, eventually repeats. There exists $n < m$ with $a^n = a^m$, i.e., $a^n \cdot (1 - a^{m-n}) = 0$. If a is not a zero divisor, then $a^{m-n} = 1$, i.e., a^{m-n-1} is the inverse of a. □

Chapter 4

LINEAR GROUP ACTIONS

This chapter is devoted to study a class of actions that behave like the multiplicative action of a set of matrices on vectors. First we consider these objects to be filled with entries in some finite field. After having proven Theorem 4.1, we present examples where the result can be used. Then we work with some more general settings leading to the notion of finite semirings acting on finite semi-modules. The last section provides a study of the action of the Frobenius homomorphism of an elliptic curve. We naturally call these kinds of actions *linear*.

4.1 Linearity over fields

This section is about linearity in the sense that there is a way to see the semigroup action as a matrix action on some vector space. We show that if the correspondence between the two approaches is computationally feasible, then the DHSP and the SAP may be

solved easily. Let us describe the situation more specifically. Let $\mathbb{F} = \mathbb{F}_q$ be the field with q elements. Suppose we are given an action $G \times S \longrightarrow S$, with G a finite abelian semigroup and S a finite set, a semigroup homomorphism $\rho : G \longrightarrow \mathrm{Mat}_n(\mathbb{F})$ (with multiplication as operation) and an embedding $\psi : S \longrightarrow \mathbb{F}^n$ such that for all $g \in G, s \in S$ one has

$$\psi(g \cdot s) = \rho(g)\psi(s).$$

So $\rho(G)$ is a commutative sub-semigroup of $\mathrm{Mat}_n(\mathbb{F})$. Let $\mathbb{F}[G]$ be the commutative subalgebra of $\mathrm{Mat}_n(\mathbb{F})$ generated by the elements of $\rho(G)$.

Suppose there exists polynomial time algorithms that compute the values of these maps and polynomial time algorithms that compute $\rho^{-1}(M)$ for each $M \in \rho(G)$ and $\psi^{-1}(v)$ for each $v \in \psi(S)$. The next theorem does not take in consideration the speed of these algorithms. It only describes what can be done at the level of the linear algebra without taking consideration of the reduction itself.

Theorem 4.1 *Let G, S, ρ and ψ be as above and let $k = \dim_{\mathbb{F}} \mathbb{F}[G]$. Then:*

1. *There exists a polynomial time reduction of the Diffie-Hellman semigroup Problem, DHSP, to a linear algebra problem over $\mathbb{F}$ that can be solved in $O(k^2n + n^3)$ field operations.*

2. *Let $N = |\mathbb{F}[G]|/|G|$. There exists a polynomial time reduction of the SAP to a linear algebra problem over $\mathbb{F}$ that can be solved in $O(N(k^2n + n^3))$ field operations.*

Proof: Let x, $y = g \cdot x$ and $z = h \cdot x$ be three elements of S with u,v and w their images in $\mathbb{F}^n$. We consider the SAP instance with parameters x and y and the DHSP instance with additional parameter z.

1. Suppose we have chosen randomly k different elements $M_1, ..., M_k$ in $\mathbb{F}[G] \subset \mathrm{Mat}_n(\mathbb{F})$. This can be done easily via the map ρ. The probability that this family is in fact a basis of the vector space $\mathbb{F}[G]$ over $\mathbb{F}$ is equal to the probability $\mathbb{P}$ that a random matrix chosen in $\mathrm{Mat}_k(\mathbb{F})$ is invertible, which satisfies

$$\begin{aligned}
\mathbb{P} &= \mathrm{Prob}\left(M_1, ..., M_k \text{ is a basis of } \mathbb{F}[G]\right) \\
&= \frac{|Gl_k(\mathbb{F})|}{|\mathrm{Mat}_k(\mathbb{F})|} \\
&= \frac{(q^k-1)(q^k-q)...(q^k-q^{k-1})}{q^{k^2}} \\
&= \left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^2}\right)...\left(1-\frac{1}{q^k}\right) \\
&> \prod_{n\geqslant 1}\left(1-\frac{1}{2^n}\right) > 0.28 > 1/4. \qquad (4.1)
\end{aligned}$$

See [43] for the cardinality of $Gl_k(\mathbb{F})$. Suppose for the moment that $\mathcal{B} = \{M_1, ..., M_k\}$ is a basis of $\mathbb{F}[G]$. If $k \geqslant n$ we extract a subfamily of cardinality n say $M_{i_1}, ..., M_{i_n}$ of $M_1, ..., M_k$ such that

$$\mathrm{Span}_{\mathbb{F}^n}\{M_{i_1}u, ..., M_{i_n}u\} = \mathrm{Span}_{\mathbb{F}^n}\{M_1u, ..., M_ku\}.$$

Note that this is always possible and can be done in $O(k^2n)$ field operations (see [8]). If $k < n$ then we may simply complete $\mathcal{B}$ with enough zero matrices to have a family of cardinality n. Let us consider the following equations with unknown $a_1, ..., a_n \in \mathbb{F}$ and $b_1, ..., b_n \in \mathbb{F}$:

$$\begin{aligned}
(a_1M_{i_1} + ... + a_nM_{i_n})\,u &= v \\
\text{and} \quad (b_1M_{i_1} + ... + b_nM_{i_n})\,u &= w. \qquad (4.2)
\end{aligned}$$

If $\mathcal{B}$ is a basis, then both possess at least one solution because of the property of the family $M_{i_1}, ...M_{1_n}$. If $a = [a_1, ..., a_n]^t$

and $b = [b_1, ..., b_n]^t$ then Equations 4.2 are equivalent to the following :

$$\begin{aligned} [M_{i_1} u \,|\, ... \,|\, M_{i_n} u]\, a &= v \\ \text{and} \quad [M_{i_1} u \,|\, ... \,|\, M_{i_n} u]\, b &= w, \end{aligned}$$

and therefore both possess a solution that can be found by solving a $n \times n$ system of linear equations in $\mathbb{F}$. If the previous systems do not each have a solution, then we choose another family $M_1, ..., M_k$ and restart the process; the number of trials is expected to be less than 4 by Inequality 4.1. Therefore we can find the vectors a and b in $O(n^3)$ field operations.

The matrices

$$\begin{aligned} M_g &= (a_1 M_{i_1} + ... + a_n M_{i_n}) \\ \text{and} \quad M_h &= (b_1 M_{i_1} + ... + b_n M_{i_n}) \end{aligned}$$

satisfy

$$M_g M_h = M_h M_g \ , \quad M_g u = v \quad \text{and} \quad M_h u = w.$$

Let $\sigma = M_g M_h u = M_h M_g u$. Since $M_g u = \rho(g)u$ and $M_h u = \rho(h)u$, we have

$$\sigma = M_g M_h u = \rho(g)\rho(h)u = \psi((gh) \cdot x) \Longrightarrow \psi^{-1}(\sigma) = (gh) \cdot x$$

which shows that the DHSP instance can be solved after a resolution of a family of problems that take $O(k^2 n + n^3)$ operations over $\mathbb{F}$.

2. The matrix M_g above belongs to $\rho(G)$ with probability $1/N$. Therefore the number of trials before reaching this state is $O(N)$. If $M_g \in \rho(G)$, then $\tilde{g} = \rho^{-1}(M_g)$ is a solution to the semigroup action problem since $\psi(y) = M_g \psi(x) = \psi(\tilde{g} \cdot x)$.

□

Remark 4.2 The dimension $k = \dim_{\mathbb{F}} \mathbb{F}[G]$ can take many different values. We can have $k \leqslant n$, see Example 4.3 below. However the rich literature on commuting matrices, e.g. [90], [34] and [87], shows that there are many cases where $k > n$. Indeed one has Schur's Theorem that gives the bound $k \leqslant \lfloor n^2/4 \rfloor + 1$ and this bound is reached in any finite field for some semigroup G.

4.2 Examples

Here are some examples where the previous theorem holds or can be used:

Example 4.3 Let M be a $n \times n$ matrix with entries in $\mathbb{F} = \mathbb{F}_q$ and $G = \mathbb{F}[M]$ acting on $\mathbb{F}^n$. If the minimal polynomial of M is $m(x)$ then Cayley-Hamilton Theorem shows that $\mathbb{F}[M] \cong \mathbb{F}[x]/(m(x))$ and the latter is a vector space of dimension $k = \deg m \leqslant n$. In such a situation, both the SAP and DHSP are trivial.

Example 4.4 Here is an example that takes its origin in the action of $PSL_2(\mathbb{F})$ on the projective space $\mathbb{P}^2_{\mathbb{F}}$, $\mathbb{F} = \mathbb{F}_q$.If G is a commutative subgroup of $PSL_2(\mathbb{F})$, we consider the action

$$\begin{array}{ccc} G \times (\,\mathbb{F} \cup \{\infty\}\,) & \longrightarrow & \mathbb{F} \cup \{\infty\} \\ \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z\right) & \longmapsto & \dfrac{az+b}{cz+d} \quad \text{, if } z \neq \infty, -d/c \\ \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \infty\right) & \longmapsto & \dfrac{a}{c} \end{array}$$

and

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, -d/c\right) \longmapsto \infty.$$

Let ρ be the canonical embedding of $PSL_2(\mathbb{F})$ into $\mathrm{Mat}_2(\mathbb{F})$ and $\psi : \mathbb{F} \cup \{\infty\} \longrightarrow \mathbb{F}^2$ with

$$\psi(z) = \begin{pmatrix} z \\ 1 \end{pmatrix} \ , \ \psi(\infty) = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \ \text{ and } \ \psi^{-1}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{cases} a/b & \text{if } b \neq 0 \\ \infty & \text{if } b = 0 \end{cases}$$

Note that $\psi^{-1}(\psi(s)) = s$. We do not have $\psi(M \cdot s) = \rho(M) \cdot \psi(s)$ but rather $M \cdot s = \psi^{-1}(\rho(M) \cdot \psi(s))$ which is enough to apply the previous theorem. Note that since $n = 2$, $k \leqslant 3$ and both the SAP and DHSP are easy to solve.

Example 4.5 This example comes from invariant theory over finite fields, as an application of the contragradient matrix action on polynomials. Here is the setting: we fix a finite field $\mathbb{F} = \mathbb{F}_q$, a degree d, and an abelian sub-semigroup G of $\mathrm{Mat}_n(\mathbb{F})$. Let V_d be the vector space over $\mathbb{F}$ of polynomials in $\mathbb{F}[x_1, ..., x_n]$ of total degree less or equal to d. The considered action is

$$\begin{array}{ccc} G \times V_d & \longrightarrow & V_d \\ (A, f(x)) & \longmapsto & A \cdot f = f((Ax)^t) \end{array}$$

where $x = [x_1, ...x_n]^t$ and Ax is the usual matrix multiplication. This action is linear since $A \cdot (f + g) = A \cdot f + A \cdot g$. If $N = \dim_{\mathbb{F}} V_d$ then we can naturally imbed V_d in $\mathbb{F}^N$ after having chosen the basis $\mathcal{B} = \{x_1^{e_1}...x_n^{e_n} \mid \sum e_i \leqslant d\}$ of V_d. This makes the map ψ easy to compute and to invert. For sake of clarity, we suppose that $\mathcal{B} = \{v_1 = x_1, ..., v_n = x_n, v_{n+1}, ..., v_N\}$. We define the map $\rho : G \longrightarrow \mathrm{Mat}_N(\mathbb{F})$ as follows:

$$\rho(A)_{ij} = (A \cdot v_j)_i = \left(\prod_{k=1}^{N} \left(\sum_{l=1}^{n} a_{kl} x_l \right)^{e_k} \right)_i$$

where $v_j = x_1^{e_1}...x_n^{e_n}$. So ρ gives the matrix representation of the linear map induced by the action since the j^{th} column of $\rho(A)$ is

the image of the j^{th} basis vector v_j. Since all the polynomials have degree less or equal to d, the right-hand-side can be computed in $O(Nnd \log d)$ field operations (see [83, Chapter 1]). Note that if $M \in \rho(G)$, then we can easily find A such that $\rho(A) = M$ since the i^{th} row of A is contained in the n first components of the i^{th} column of M. Indeed, if $1 \leqslant i \leqslant n$ then

$$i^{th} \text{ column of M} = A \cdot v_i = \sum_{j=1}^{n} a_{ij} x_j = \sum_{j=1}^{n} a_{ij} v_j.$$

Once again the previous theorem holds and makes the DHSP as hard as the linear algebra problem in $\mathbb{F}^N$. However note that in that case the SAP problem may still be difficult since the ratio $|G|/|\mathbb{F}[G]|$ may take very small values because of the big dimension expansion from n to N.

Example 4.6 The idea of the following group action is based on the theory of differential operators. In the sequel consider C^2-functions $u(x_1, x_2)$ and $v(x_1, x_2)$, these are functions which can be differentiated twice. One has

$$\begin{aligned} \frac{\partial}{\partial x_i}\left(ue^v\right) &= \frac{\partial u}{\partial x_i} e^v + u \frac{\partial v}{\partial x_i} e^v, \\ \frac{\partial^2}{\partial x_1 \partial x_2}\left(ue^v\right) &= \frac{\partial^2}{\partial x_2 \partial x_1}\left(ue^v\right). \end{aligned}$$

Fix a finite field $\mathbb{F}_q$, $q = p^n$, a number $k \in \mathbb{N}$ and an element $v \in \mathbb{F}[x_1, \ldots, x_k]$. We define the linear operators ∂_i, $i = 1, \ldots, k$ as follows:

$$\begin{array}{ccccc} \partial_i & : & \mathbb{F}[x_1, \ldots, x_k] & \longrightarrow & \mathbb{F}[x_1, \ldots, x_k] \\ & & u & \longmapsto & \partial_i u = \frac{\partial u}{\partial x_i} + u \frac{\partial v}{\partial x_i} \end{array}$$

Their continuous analogues are commutative and one can easily check that it is still true for the discrete version: the family of linear

operators $\{\partial_i\}_{i=1,\dots,k}$ is commutative. With this, it is apparent that $\mathbb{F}[x_1,\dots,x_k]$ has the structure of a $\mathbb{F}[\partial_1,\dots,\partial_k]$-module as well as the structure of a $\mathbb{F}$-vector space. The ring $\mathbb{F}[x_1,\dots,x_k]$ is infinite but the following lemma shows how a finite version can be built:

Lemma 4.7 *Consider the ideal $I_m \subset \mathbb{F}[x_1,\dots,x_k]$ generated by $x_i^{p^m} - a_i$ for $i = 1,\dots,k$ and $a_i \in \mathbb{F}$, i.e.*

$$I_m = \left(x_1^{p^m} - a_1, \dots, x_k^{p^m} - a_k\right) \subset \mathbb{F}[x_1,\dots,x_k].$$

Then $\partial_j\ I_m \subset I_m$ for all $j = 1,\dots,k$.

Proof: Let $p(x) = \sum_{i=1}^{k} f_i \cdot (x_i^{p^m} - a_i) \in I_m$. Then

$$\begin{aligned}
\partial_j\ (p(x)) &= \sum_{i=1}^{k} \partial_j\ (f_i \cdot (x_i^{p^m} - a_i)) \\
&= \sum_{i=}^{k} \frac{\partial f_i}{\partial x_j} \cdot (x_i^{p^m} - a_i) + \underbrace{f_i \cdot p^m \cdot x_i^{p^m-1}}_{0} \\
&\quad + f_i \cdot (x_i^{p^m} - a_i)\frac{\partial v}{\partial x_j} \\
&= \sum_{i=1}^{k} \left(\frac{\partial f_i}{\partial x_j} + f_i \cdot \frac{\partial v}{\partial x_j}\right) \cdot (x_i^{p^m} - a_i) \quad \in \quad I_m
\end{aligned}$$

□

Clearly, by the previous lemma, the algebra $\mathbb{F}[\partial_1,\cdots,\partial_k]$ acts on the quotient $\mathbb{F}[x_1,\cdots,x_k]/I_m$ which is finite. We can now define the parameters of the semigroup action. We take a polynomial v in $\mathbb{F}[x_1,\dots,x_k]$ and consider

- $G = \mathbb{F}[\partial_1, \ldots, \partial_k]$
- $S = \mathbb{F}[x_1, \ldots, x_k]/I_m$
- $s = f(x_1, \ldots, x_k) \neq 0$

The group action defined in this example is once more $\mathbb{F}$-linear. It differs from the previous examples mainly because it is not clear if one could write the semigroup $\mathbb{F}[\partial_1, \ldots, \partial_k]$ in the form $\mathbb{F}[M]$ for one single operator. The details are similar to the previous example.

4.3 Semirings acting on semi-modules

This part of the chapter takes its roots in Chapter 3 of [62] as a study of finite c-simple semirings. It is also motivated by the consequences of Theorem 4.1 that basically shows that linear algebra makes the DHSP easy to solve, when linear algebra can be used. We develop here the ideas leading to the action of a semiring on a semi-module and why simplicity is important in this context. After having described the notion of semirings, we will study them from a semigroup action problem point of view.

The definitions appearing in this section also fix a terminology for the next chapter.

Definition 4.8 A semiring R is a non-empty set together with two associative operations $+$ and $\cdot$ where the following distributive laws hold:

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad (a + b) \cdot c = a \cdot c + b \cdot c.$$

We will always assume that the addition is commutative and possesses a zero, i.e, an element 0 with $a+0 = a$ and $a \cdot 0 = 0 \cdot a = 0$

for all $a \in R$; this element is then unique. We write ab for $a \cdot b$. If R has a multiplicative identity, it is unique and we denote it by $1_R = 1$.

Definition 4.9 A semiring R is zero-sum free if

$$a + b = 0 \Longrightarrow a = b = 0 \; \forall \; a, \, b.$$

A zero-sum free semiring possesses no elements that are opposites except 0.

Definition 4.10 A congruence relation on a semiring R is an equivalence relation $\sim$ such that

$$a \sim b \Longrightarrow \begin{cases} ac \sim bc \\ ca \sim cb \\ a + c \sim b + c \\ c + a \sim c + b \end{cases}$$

for all possible choice of a, b and c. A semiring R is congruence-free, or *c-simple*, if the only congruence relations are $R \times R$ and $\{(a, a) \mid a \in R\}$.

Any congruence relation gives the set $R/\!\sim$ a natural structure of semiring and the quotient map $R \longrightarrow R/\!\sim$ becomes a semiring homomorphism. The next lemma gives a way to build new semirings from existing ones. We omit the proof.

Lemma 4.11 *Let R be a semiring with 1 and $n \in \mathbb{N}$. Then $\mathrm{Mat}_n(R)$, the set of $n \times n$ matrices with entries in R is a semiring with 1.*

Definition 4.12 Let R be a semiring and $(M, +)$ be a commutative semigroup with identity 0_M. M is a semi-module over R if there is a (left) action $\cdot$ of R on M such that

$$(a+b)\cdot m = a\cdot m + b\cdot m \;\; , \;\; a\cdot(m+n) = a\cdot n + a\cdot m \;\text{ and }\; a\cdot 0_m = 0_m,$$

for all $a, b \in R$ and $m, n \in M$.

The most important examples in this discussion are the following: first a semiring R is a semi-module over itself. Next let R be a semiring, $M = R^n = R \oplus ... \oplus R$ and we let $\mathrm{Mat}_n(R)$ act on R^n by left matrix multiplication. Then M is a semi-module over $\mathrm{Mat}_n(R)$. In this context a congruence relation on $\mathrm{Mat}_n(R)$ gives M a congruence relation of a commutative semigroup. We can indeed see M as a sub-semigroup of $(\mathrm{Mat}_n(R), +)$ via the map

$$\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \longmapsto \begin{pmatrix} m_1 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ m_n & 0 & \dots & 0 \end{pmatrix}$$

and the congruence relation on M is then induced by the one on $\mathrm{Mat}_n(R)$. This congruence relation $\sim$ on M makes the quotient map $f : \mathrm{Mat}_n(R) \longrightarrow \mathrm{Mat}_n(R/\sim)$ compatible with the actions in the sense that

$$f(A \cdot v) = f(A) \cdot f(v).$$

This phenomenon yield a situation completely different than the one explained in Section 3.4 since now the notion of c-simplicity has a direct consequence: the non-simplicity of the semiring $\mathrm{Mat}_n(R)$ would give a way to mimic the Pohlig-Hellman attack.

The next theorem gives a strong relationship between the congruence relations in R and congruence relations in $\mathrm{Mat}_n(R)$. But first we need the following statement:

Lemma 4.13 *Let R be an additively commutative semiring with 1 and 0 and $M \in \mathrm{Mat}_n(R)$. If M' is obtained from M by a permutation of rows and columns, there exist two invertible matrices $S, P \in \mathrm{Mat}_n(R)$ such that $M' = SMP$.*

Proof: The statement is true if one consider matrices with entries in $\mathbb{Z}$ and the usual multiplication, i.e. there exist two permutation matrices (therefore with entries in $\{0,1\}$) such that $M' = S \cdot M \cdot P$ with $\cdot$ being the usual matrix multiplication. It is then straightforward to verify that the same is true with the operation in R because of the properties of 0 and 1. □

Theorem 4.14 *Let R be an additively commutative semiring with 1 and 0 and let $\sim$ be a congruence relation on $\mathrm{Mat}_n(R)$. Then there exists a congruence relation $\sim_0$ on R such that*

$$A \sim B \in \mathrm{Mat}_n R \Longleftrightarrow a_{ij} \sim_0 b_{ij} \ , \ \forall\, 0 \leqslant i,j \leqslant n.$$

Proof: Clearly the theorem is true if $n = 1$. Suppose $n > 1$. Let $f : R \longrightarrow \mathrm{Mat}_n(R)$ be the map that sends $a \in R$ to the diagonal matrix with first diagonal element a and zeros everywhere else. The map f is a semiring homomorphism. Let $\sim_0$ be the relation on R defined by $a \sim_0 b$ in R if and only if $f(a) \sim f(b)$ in $\mathrm{Mat}_n(R)$. Observe that $\sim_0$ is a congruence relation on R (see also [62]). We prove now that the statement of the theorem is true for $\sim_0$. Let $A, B \in \mathrm{Mat}_n(R)$ and $J = f(1)$. Let $0 \leqslant i,j \leqslant n$ and $S_{ij}, P_{ij} \in \mathrm{Mat}_n(R)$ be permutation matrices such that

$$(S_{ij}AP_{ij})_{11} = a_{ij} \quad \text{and} \quad (S_{ij}BP_{ij})_{11} = b_{ij}.$$

Note that the matrices S_{ij} and P_{ij} exists in $\mathrm{Mat}_n(R)$ by the previous Lemma. Therefore $JS_{ij}AP_{ij}J = f(a_{ij})$ and $JS_{ij}BP_{ij}J = f(b_{ij})$.
Proof of $\Rightarrow$: If $A \sim B$ then $JS_{ij}AP_{ij}J \sim JS_{ij}BP_{ij}J$ and therefore $a_{ij} \sim_0 b_{ij}$.
Proof of $\Leftarrow$: Clearly

$$A = \sum_{i,j} S_{ij}^{-1} f(a_{ij}) P_{ij}^{-1} \text{ and } B = \sum_{i,j} S_{ij}^{-1} f(b_{ij}) P_{ij}^{-1}$$

and since $f(a_{ij}) \sim f(b_{ij})$, $A \sim B$. □

Hence we obtain the following:

Corollary 4.15 *Let R be an additively commutative semiring with 1 and 0 and let $n \in \mathbb{N}$. Then R is c-simple if and only if* $\mathrm{Mat}_n(R)$ *is c-simple.*

This result is well-known in the case where the semiring has the structure of a division ring, as a consequence of the Wedderburn-Artin Theorem [33]. In that case, since the notion of ideal is deeply connected to the notion of congruence relation, the result gives a classification of ideals in $\mathrm{Mat}_n(R)$. Note as well that Theorem 4.14 can give a classification of congruence relations of many non-usual algebraic objects such as max-min algebras (see Proposition 5.2 and Remark 5.3) and max-plus algebras. The latter will not be of any need in this work, we therefore avoid their study.

4.4 Endomorphism actions on the abelian groups $E(\mathbb{F}_q)$

Any abelian group H is equipped with its ring of endomorphisms $\mathrm{End}\, H$ where addition is defined pointwise and multiplication via composition of maps. Such a ring is unitary and may not be commutative. There is a natural action of $\mathrm{End}\, H$ on H as follows :

$$\begin{array}{ccc} \mathrm{End}\, H \times H & \longrightarrow & H \\ (\varphi, h) & \longmapsto & \varphi(h) \end{array}$$

Note that this action is linear, i.e., $\varphi(h+h') = \varphi(h) + \varphi(h')$. For a given $\varphi \in \mathrm{End}\, H$, the sub-ring $\mathbb{Z}[\varphi]$ of polynomial in φ inside $\mathrm{End}\, H$ is commutative. In the case where the group is cyclic we are dealing

with the usual action of $\mathbb{Z}$ since in that case any endomorphism of H is obtain as a multiplication by a constant. Another trivial case appears when one chooses the identity as endomorphism.

This setting is conceptually no different from the matrix action of the previous section. However there are cases of algebraic groups where endomorphisms do not appear as matrices. Examples are groups of elliptic curves over finite fields or more generally the Jacobians of abelian varieties. This section is devoted to bring evidence that the situation with elliptic curves is non-trivial and interesting, although competitive examples seem to be hard to find. Note that Theorem 4.1 cannot be used since the maps ρ and ψ are hard to compute.

Let $\mathbb{F}_q$ be the finite field with q elements and E an elliptic curve over $\mathbb{F}_q$ defined by its Weierstrass normal form

$$0 = F(x,y) = \begin{cases} y^2 + xy + x^3 + ax^2 + b & \text{if } \operatorname{char}\mathbb{F} = 2, \\ y^2 - x^3 - ax - b & \text{otherwise,} \end{cases}$$

where $a, b \in \mathbb{F}_q$ have to satisfy some discriminant conditions. Recall that the sets

$$E(\mathbb{F}_{q^k}) = \{(x,y) \in \mathbb{F}_{q^k} | F(x,y) = 0\} \cup \mathcal{O}$$

are finite commutative groups (c.f. [4], [56] and more generally [84]). All the groups $E(\mathbb{F}_{q^k})$ and their rings of endomorphisms are well defined. The ring of endomorphisms $\operatorname{End} E$ of E, i.e. the set of all isogenies from E to itself together with the zero map, contains $\operatorname{End} E(\mathbb{F}_{q^k})$ for all k and has one of the following forms [4, Chapter III]:

- $\operatorname{End} E$ is the maximal order in a quaternion algebra,
- $\operatorname{End} E \cong \mathbb{Z} \oplus \mathbb{Z}\tau$ where τ is a complex algebraic number of degree two lying in the upper half of the complex plane. Such curves are said to have complex multiplication.

The point is that there exists curves over finite fields, namely the curves with complex multiplication, whose endomorphism rings are strictly bigger than $\mathbb{Z}$. In such a situation the previous action does not reduce to the usual action by $\mathbb{Z}$. We will call these actions *complex actions* over E. Moreover, any curve over a finite field has its Frobenius endomorphism :

$$\begin{aligned} \varphi : E(\mathbb{F}_{q^k}) &\longrightarrow E(\mathbb{F}_{q^k}) \\ (x, y) &\longrightarrow (x^q, y^q) \end{aligned}$$

We will see that there exist situations where this endomorphism does not reduce to a multiplication by a constant. Even so, this endomorphism can be used to speed up point multiplication on a curve (c.f. [4]) since the computation of $\varphi(P)$ is often more efficient than the usual binary (doubling and addition) method.
Let l_k be the cardinality of $E(\mathbb{F}_{q^k})$. Clearly, we can restrict the action of $\mathbb{Z}[\varphi]$ on $E(\mathbb{F}_{q^k})$ to the action of $\mathbb{Z}_{l_k}[\varphi]$ on the same group. The endomorphism φ satisfies the functional equation $\varphi^2 - [t]\varphi + [q^k] = [0]$ which implies that we can once again restrict our attention to the action of $\mathbb{Z}_{l_k} \oplus \mathbb{Z}_{l_k}\varphi$ on $E(\mathbb{F}_{q^k})$. The action becomes then

$$\begin{aligned} \mathbb{Z}_{l_k} \oplus \mathbb{Z}_{l_k}\varphi \times E(\mathbb{F}_{q^k}) &\longrightarrow E(\mathbb{F}_{q^k}) \\ (a + b\varphi, P) &\longmapsto [a]P + [b]\varphi(P) \end{aligned}$$

For a given $P \in E(\mathbb{F}_{q^k})$, a necessary and sufficient condition for this action to be complex is that $\varphi(P) \neq [s]P\,,\ \forall s \in \mathbb{Z}_{l_k}$. A necessary condition is that $E(\mathbb{F}_{q^k})$ is not cyclic. The next lemma gives enlightenment on this phenomenon.

Lemma 4.16 *1.* $E(\mathbb{F}_{q^k}) \cong \mathbb{Z}/u\mathbb{Z} \oplus Z/uv\mathbb{Z}$ *where* $u, v \in \mathbb{N}$ *and* $u|q^k - 1$.

2. If $\operatorname{ord} P = d$ *then*

$$\varphi(P) = [s]P \Longleftrightarrow s^k - 1 \equiv 0 \mod d$$

Proof: 1. c.f. [4, Section III.3.].

2. If $\varphi(P) = [s]P$, then since $\varphi^k = [1]$ over $\mathbb{F}_{q^k}$, we have $0 = [s]^k P - [1]P = [s^k - 1]P$ and then $s^k - 1 \equiv 0 \mod \operatorname{ord} P$. Clearly the converse is true.

□

The previous Lemma has the following consequences:

1. Since $|E(\mathbb{F}_{q^k})| = u^2 v$, l_k must be divisible by a square in order to have a complex action. From a cryptographic point of view, this square cannot be negligible with respect to l_k. Indeed a reduction in the spirit of Pohlig-Hellman would lead to the resolution of the SAP in two steps: first modulo u^2, i.e., a usual DLP in a cyclic group and then modulo v, which in order to be difficult forces u to be rather large.

2. The integer $\operatorname{ord} P$ divides uv.

3. To build complex actions, one could try to find examples of curves where l_k is divisible by a square and then test for different points P if $\varphi(P) \neq [s]P\,,\ \forall s \in D$ where $D = \{s \mid s^k - 1 \equiv 0 \mod |P|\}$.

Here is an example of such a complex action.

Example 4.17 We choose the elliptic curve and prime :

$$E: \ Y^2 = X^3 + 86X + 61\,,\ p = 101.$$

$\mathbb{F}_{p^2}$ is identified with $\mathbb{F}_p(\xi)$ where ξ is a root of the following irreducible polynomial modulo 101 : $p(x) = x^2 + 6x + 55$. The number of $\mathbb{F}_{p^2}$-rational points is $l_2 = 17^2 \cdot 7 \cdot 5$, i.e. $|E(\mathbb{F}_{p^2})| = 10115$.

On $E(\mathbb{F}_{p^2})$ we choose the point $P = (64 + 4\xi, 55 + 91\xi)$ whose order is $d = 17 \cdot 35 = 595$. Now

$$s^2 - 1 = 0 \mod d \iff s \in D = \{1, 69, 169, 239, 356, 426, 526, 594\}$$

Since $\varphi(P) = (10 + 97\xi, 89 + 10\xi)$, we check that $\varphi(P) \neq [s]P$, and then

$$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/17\mathbb{Z} \oplus \mathbb{Z}/(17 \cdot 35)\mathbb{Z}$$

with $\varphi(P) \notin [\mathbb{Z}]P$.

The following result shows that there exists many instances where the previous method applies:

Proposition 4.18 *Let $q = p^n$ and $N = q + 1 - t$, $0 \neq t \leqslant 4q$. If a_l, b_l are integers which satisfy $a_l \geqslant b_l$, $a_l + b_l = v_l(N)$ (where $v_l(N)$ is the largest integer with $l^{v_l(N)} | N$) and $b_l \leqslant (q-1)$ for each prime $l \neq p$, then there exists an elliptic curve E defined over $\mathbb{F}_q$ such that $E(\mathbb{F}_q)$ has the structure*

$$\mathbb{Z}/p^{v_p(N)}\mathbb{Z} \oplus \bigoplus_{l \neq p} \left(\mathbb{Z}/l^{a_l}\mathbb{Z} \oplus \mathbb{Z}/l^{b_l}\mathbb{Z}\right).$$

See [78] for a proof. However there exists no known polynomial-time algorithm that output the equation of such an elliptic curve, given a finite field $\mathbb{F}_q$ and integers N, a_l and b_l that satisfy the previous proposition. The best one can do with current knowledge is to randomly test curves until one is found with the desired properties, i.e., a random search [80]. This cannot be implemented in a systematic way. Indeed, it has been shown [42] that the cardinality of elliptic curves over the finite field $\mathbb{F}_q$ is roughly uniformly

distributed in the interval $[q+1-\sqrt{q}, q+1+\sqrt{q}]$. On the other hand the integer l_k has to be divisible by a rather large square (c.f. consequence 2. above). If we fix a lower bound B^2 for the largest square dividing l_k, following Section 18.6 of [28], the number of integers less or equal to x whose least square factor is larger than B^2 is given by

$$r(x,B) = x - \sum_{d \leqslant B} Q(x/d^2) = \frac{6x}{\pi^2 B} + O(\sqrt{x}) \ , \quad x \gg B,$$

where $Q(y)$ counts the number of square free integers not exceeding y. Therefore, the probability that a random integer in the interval $[q+1-\sqrt{q}, q+1+\sqrt{q}]$ is divisible by a square larger that B^2 is

$$\frac{r(q+1+\sqrt{q},B) - r(q+1-\sqrt{q},B)}{2\sqrt{q}} \approx \frac{6}{\pi^2 B}.$$

This makes the random search of such an number in the interval non-feasible for large B, since the expected number of trial before finding a candidate is linear in B.

4.5 Conclusion

In this chapter, we proved Theorem 4.1 which gives a basis for all linear actions over finite fields from a semigroup action point of view. Examples have been presented to expose its utility. As a consequences, a theory of actions induced by semiring acting on semi-modules is presented. The next chapter is entirely devoted to it. An extension of ECDLP was defined using the Frobenius homomorphism of elliptic curves over finite fields. Evidence that such actions are difficult to find in a random manner was given.

Chapter 5

A CLASS OF C-SIMPLE SEMIRINGS

This chapter presents a study of a family of semirings, as descibed in Section 4.3. We first define them and study their congruence relations as well as the proportion of invertible elements. Large commutative sub-semirings are built. From there, two actions are defined and studied from a semigroup action problem point of view.

5.1 The semirings R_n

We introduce now an infinite family of finite semirings that fulfill many nice properties in this context. These properties will appear in the sequel. Let $R = \{0, 1\}$ with the following addition and multiplication tables:

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

It is not difficult to check that it is a commutative c-simple semiring with 1 and 0 which is zero-sum free. The operations satisfy the following:

$$a + b = \max\{a, b\} \qquad a \cdot b = \min\{a, b\},$$

i.e. $(R, +, \cdot) = (\{0, 1\}, \max, \min)$. These operations can also be defined as OR/AND.

Remark 5.1 The set $R = \{0, 1, ..., m\}$ with the same max-min operations is also a zero-sum free, commutative semiring with $1_R = m$ and $0_R = 0$. This family of semirings is sometimes called *max-min algebras*. The next discussion shows that as long as $m > 1$, they are not c-simple. Indeed the following equivalence relations on R are non-trivial congruence relations. Let

$$\{0, 1, ..., m\} = \bigsqcup_i [a_i, b_i]$$

be a non-trivial partition of $\{0, 1, ..., m\}$ in segments $[a_i, b_i] = \{x \mid a_i \leqslant x \leqslant b_i\}$. By non-trivial we mean that the partition is not reduced to only one segment and at least one segment contains more than one element. We define $\sim$ in R with

$$x \sim y \iff \exists i \text{ such that } a_i \leqslant \min(x, y) \leqslant \max(x, y) \leqslant b_i. \quad (5.1)$$

Then the equivalence relations described above give the following classification of congruence relations in such a semiring:

Proposition 5.2 *The equivalence relation $\sim$ given in 5.1 is a non-trivial congruence relation in $R = (\{0, 1, ..., m\}, \max, \min)$. Moreover any non-trivial congruence relation in R is of this form.*

Proof: Let $x \sim y$ and i such that $a_i \leqslant \min(x,y) \leqslant \max(x,y) \leqslant b_i$. Then for all $c \in \{0,1,...,m\}$ we have the following cases:

i) If $c \leqslant a_i$, then $\min\{x,c\} = c \sim c = \min\{y,c\}$ and $\max\{x,c\} = x \sim y = \max\{y,c\}$.

ii) If $a_i < c < b_i$, then $\min\{x,c\} \sim \min\{y,c\}$ since

$$a_i \leqslant \min\{x,c\}, \min\{y,c\} \leqslant b_i$$

and $\max\{x,c\} \sim \max\{y,c\}$ since

$$a_i \leqslant \max\{x,c\}, \max\{y,c\} \leqslant b_i.$$

iii) If $b_i \leqslant c$, then $\max\{x,c\} = c \sim c = \max\{y,c\}$ and $\min\{x,c\} = x \sim y = \min\{y,c\}$.

This proves that $\sim$ is a congruence relation. Let us now check that any non-trivial congruence relation in R is of this form. If $x \sim y$ then $\forall c \in [x,y]$, $x \sim c$ since $\min(x,c) \sim \min(y,c)$. In other words, the equivalence classes of $\sim$ are segments. Therefore, the partition leading to $\sim$ via 5.1 is the partition given by its equivalence classes. Clearly the equivalence relation is non-trivial if and only if there is more than one segment in the partition. □

Remark 5.3 The previous proposition combined with Theorem 4.14 gives a complete classification of congruence relations in the max-min matrix algebras
$\mathrm{Mat}_n(\{0,1,...,m\}, \max, \min)$.

Let us now come back to the study of the case where $R = \{0,1\}$.

Definition 5.4 $R_n = \mathrm{Mat}_n((\{0,1\}, \max, \min))$

The semirings R_n have been studied in different contexts. Several computational aspects have been developed by M. Gavalec in [19], [20], [21] and [22]. These papers study the question of computing orbit periods in R_n and orbit periods in R_1^n via the action of R_n (see Definition 5.11 and Section 5.3). These questions will be useful in the following discussion.

The semirings R_n possess a characterization using oriented graph theory. Let $\mathcal{G}_n$ be the set of oriented graphs with n vertices and at most one oriented edge from a vertex to another. Each vertex is numbered once and for all. We can define two operations $\oplus$ and $\otimes$ in $\mathcal{G}_n$ as follows: Let G_1 and G_2 be two graphs in $\mathcal{G}_n$. Then $G_1 \oplus G_2$ is the oriented graph in $\mathcal{G}_n$ such that there exists an oriented edge from vertex i to vertex j if and only if such an oriented edge exists either in G_1 or in G_2. The oriented graph $G_1 \otimes G_2$ possess an oriented edge from vertex i to vertex j if and only if there exists a vertex k with an oriented edge from i to k in G_1 and an oriented edge from k to j in G_2.

It is not difficult to see that there is a bijection between $\mathcal{G}_n$ and R_n given by the incidence matrix of each graph. More precisely, we define the incidence matrix map as follows:

$$\begin{array}{rccc} F & : & \mathcal{G}_n & \longrightarrow & R_n \\ & & G & \longmapsto & M = F(G) \end{array}$$

with

$$M_{ij} = \begin{cases} 1 & \text{if there exists an oriented edge from } i \text{ to } j \text{ in } G, \\ 0 & \text{otherwise.} \end{cases}$$

Note that the transpose of a matrix M in R_n is the incidence matrix of the the graph obtained by inverting all the arrows of the graph associated to M. In fact, the operations $\oplus$ and $\otimes$ behave nicely with respect to this bijection, as shown in the next proposition:

Proposition 5.5 *The bijection F satisfies*

$$\begin{aligned} F(G_1 \oplus G_2) &= F(G_1) + F(G_2), \\ F(G_1 \otimes G_2) &= F(G_1) \cdot F(G_2)\ ,\ \forall\, G_1, G_2 \in \mathcal{G}_n. \end{aligned}$$

moreover, if $G_i^t = F^{-1}(M_i^t)$ then $G_1^t \otimes G_2^t = (G_2 \otimes G_1)^t$.

Proof: The identity $F(G_1 \oplus G_2) = F(G_1) + F(G_2)$ comes directly from the definition. For the product, we have

$$\begin{aligned} [F(G_1) \cdot F(G_2)]_{ij} &= \max_k(\min(F(G_1)_{ik}, F(G_2)_{kj}) \\ &= \begin{cases} 1 & \text{if } \exists\, k \text{ s.t. } F(G_1)_{ik} = F(G_2)_{kj} = 1, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

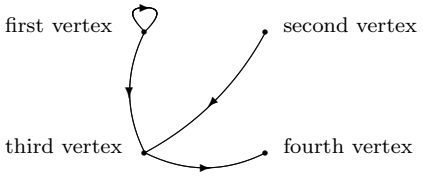
and this last expression is exactly $F(G_1 \otimes G_2)_{ij}$. The last equality comes from

$$F(G_1^t \otimes G_2^t) = F(G_1^t) \otimes F(G_2^t) = M_1^t \cdot M_2^t = (M_2 \cdot M_1)^t = F(G_2 \otimes G_1)^t.$$

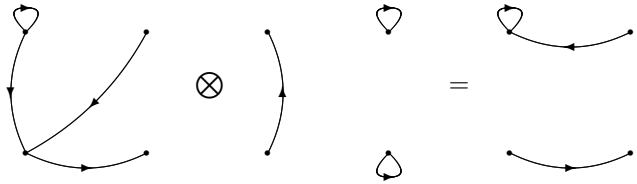
□

Example 5.6 In this example, we consider the case $n = 4$ with the following labeling:

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \longleftrightarrow$$



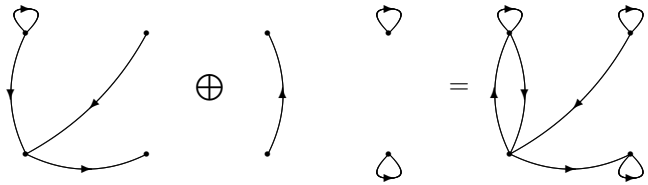
Here are the actions of the addition and the multiplication on two oriented graphs:



correspond to

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

and



correspond to

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Corollary 5.7 *The triple* $(\mathcal{G}_n, \oplus, \otimes)$ *is a zero-sum free semiring with identity and zero.*

This graph theoretic interpretation allows one to think more geometrically. For instance suppose a graph G possesses a left inverse G' with respect to $\otimes$, i.e., $G \otimes G' = 1_{\mathcal{G}_n}$. Let us fix a vertex i. Since there is a path that starts at i in G and ends at i in G' (by definition of the product of two graphs), there exists a vertex j such that an edge from i to j exists in G and for any other vertex $i' \neq i$ there is no edge in G from i' to j because otherwise $G \otimes G'$ would contain an edge from i' to i. Let j_i be such a vertex. The map $i \longmapsto j_i$ is a bijection since it is injective. This means that each vertex j is the end point of exactly one oriented edge in G, i.e., there is exactly one oriented edge that starts at the vertex i. Note that if G had a right inverse, G^t would have had a left inverse. This gives the next corollary:

Corollary 5.8 *Let* $M \in R_n$*. The following are equivalent:*

1. *the matrix* M *has a left inverse in* R_n*,*
2. *the matrix* M *has a right inverse in* R_n*,*
3. *the matrix* M *is invertible in* R_n*,*
4. *the matrix* $M \in R_n$ *is a permutation matrix.*

A consequence of this second corollary is that the number of invertible elements in R_n is $n!$. Since $|R_n| = 2^{n^2}$, for a randomly chosen element M in R_n, the probability that this element possesses an inverse is

$$\text{Prob}(M \text{ is invertible}) = \frac{n!}{2^{n^2}} = \begin{cases} 0.125 & \text{if } n = 2, \\ \cong 0.0117 & \text{if } n = 3, \\ \cong 0.00037 & \text{if } n = 4, \\ < 0.36 \cdot 10^{-5} & \text{if } n \geqslant 5, \end{cases}$$

and in general,

$$\text{Prob}(M \text{ is invertible}) \ll n^{-1/2}.$$

The next corollary gives a graph theoretic interpretation of the entries of the powers of an element in R_n. Recall that the length of a path in a directed graph is the number of edges (counted with multiplicity) contained in the path:

Corollary 5.9 *Let $M \in R_n$ with associated graph $G \in \mathcal{G}_n$ and $k \in \mathbb{N}$. Then*

$$(M^k)_{ij} = \begin{cases} 1 & \text{if there exists an oriented path of length } k \\ & \text{from } i \text{ to } j \text{ in } G, \\ 0 & \text{otherwise.} \end{cases}$$

Here is another key property of the family of semirings R_n:

Theorem 5.10 *The semirings R_n are c-simple.*

Proof: Since R_1 is c-simple, the result is a consequence of Corollary 4.15. □

5.2 Elements with large orders

In this section we study the "sizes" of the orbit of powers of elements in R_n. Note that since the semiring R_n is finite any sequence $\{M^k\}_{k\in\mathbb{N}}$ will eventually repeat, i.e., create a collision of the form $M^k = M^{k'}$ such that $M^{k+t} = M^{k'+t}$ for all $t \in \mathbb{N}$.

Definition 5.11 Let a be a sequence in a finite set such that $a_n = a_m \implies a_{n+1} = a_{m+1}$. The *order* $\text{ord}\,(a)$ of a is the least positive integer m such that there exists $k \leqslant m$ with $a_k = a_m$. The *preperiod* $p_r(a)$ of a is the largest non-negative integer m such

that for all $k > m$ we have $a_k \neq a_m$. The *period* $p(a)$ of a is the least positive integer m such that there exists an integer N with $a_{m+k} = a_k$ for all $k > N$. If G is a finite semigroup and $g \in G$, then we set $\mathrm{ord}\,(g) = \mathrm{ord}\,(\{g^n\}_{n\in\mathbb{N}})$, $p(g) = p(\{g^n\}_{n\in\mathbb{N}})$ and $p_r(g) = p_r(\{g^n\}_{n\in\mathbb{N}})$.

Clearly $\mathrm{ord}\,(a) = p(a)+p_r(a)$. Returning to the situation of the multiplicative semigroup of R_n, we study the question "How large can the order of $M \in R_n$ be?". There already exist some results in this direction. To describe them, we recall that for a given oriented graph G, a *strongly connected component* (written SCC) of G is a sub-graph H of G inside which any two vertices i and j belong to a same oriented cycle and H is a maximal sub-graph with this property. Such a SCC is written $H \subseteq_{SCC} G$. The period of a strongly connected component is the maximum between the gcd of the length of its cycles and 1. We refer the reader to [45] for the details.

Proposition 5.12 *Let $M \in R_n$ and $G = F^{-1}(M)$, where F is the incidence matrix map. Then*

1. $p(M) = \mathrm{lcm}\,\{\textit{period of } H \mid H \textit{ is a SCC of } G\}$,
2. *The numbers $p(M), p_r(M)$ and $\mathrm{ord}\,(M)$ can be computed in $O(n^3)$ time.*

This proposition is essentially in [18]. The algorithm given there computes $p(M)$ in $O(n^3)$ time and an easy modification of it allows to computes $p_r(M)$ and therefore $\mathrm{ord}\,(M)$.

We introduce now a function that play a crucial role: Landau's function g. It is defined by

$$\begin{aligned} g(n) &= \max\{\mathrm{ord}\,\sigma \mid \sigma \in S_n\} \\ &= \max\{\mathrm{lcm}\,\{a_1, ..., a_m\} \mid a_i > 0,\ a_1 + ... + a_m = n\}. \end{aligned}$$

It was first studied by Landau [40] in 1903 who proved that

$$\ln(g(n)) \sim \sqrt{n \ln(n)} \quad \text{as} \quad n \longrightarrow \infty. \tag{5.2}$$

In 1984, Massias [46] showed that for sufficiently large n,

$$\sqrt{n \ln(n)} \leqslant \ln(g(n)) \leqslant \sqrt{n \ln(n)} \left(1 + \frac{\ln \ln(n)}{2 \ln(n)}\right), \tag{5.3}$$

the second inequality in 5.3 being true for all n. Clearly, the function g is increasing. It also satisfies an equality related to the maximal degree of the field extension needed to factorize a polynomial over a finite field. Indeed, if $\mathbb{F}_q$ is any finite field and $\mathbb{K}_p$ is the splitting field of a polynomial $p(x)$ then

$$\begin{aligned} g(n) &= \max\{[\mathbb{K}_p : \mathbb{F}_q] \mid p \in \mathbb{F}_q[x] \ , \ p \text{ of degree } n\} \\ &= \min\{[\mathbb{K} : \mathbb{F}_q] \mid \text{any } n \times n \text{ matrix in } \mathbb{F}_q \text{ is} \\ &\quad \text{diagonalisable in } \mathbb{K}\}. \end{aligned}$$

We will not need these results and therefore we will not prove them, but it is worth mentioning that the result of Menezes and Wu in [58] on the DLP in $Gl_n(\mathbb{F}_q)$ is not trivial mainly because of the exponential growth of $g(n)$.

In any case, we have

$$\max\{\text{lcm}\,\{a_1, .., a_m\}, |a_1| + ... + |a_m| = n\} = \exp\left((1 + o(1))\sqrt{n \ln n}\right).$$

On the other hand, the period of any SCC $H \subset G = F^{-1}(M)$ is less or equal to $|H|$ and

$$\sum_{H \subseteq_{SCC} G} |H| \leqslant n.$$

Since the function g is increasing, Proposition 5.12 and equation 5.2 give

$$p(M) \leqslant g\left(\sum_{H \subseteq_{SCC} G} |H|\right) \leqslant g(n) = \exp\left((1+o(1))n^{1/2}\ln^{1/2} n\right).$$

Further, it is not difficult to see that there always exists an oriented graph $G \in \mathcal{G}_n$ with period $g(n)$. Indeed if $g(n)$ is reached by a partition $a_1 + ... + a_m = n$, then a graph G built out of cyclic SCCs of order a_i satisfies $p(M) = g(n)$ (see Example 5.14 for an example of such a situation). In other words we have:

Proposition 5.13 *Let $n \in \mathbb{N}$. Then*

$$\max\{p(M) \mid M \in R_n\} = g(n) = \exp\left((1+o(1))n^{1/2}\ln^{1/2} n\right).$$

The exact computation of $g(n)$, or more precisely, of the partition $a_1 + ... + a_m = n$ that yield the maximum $g(n)$, is necessary in order to build explicitly a matrix $M \in R_n$ such that $p(M) = g(n)$. Indeed, the integer $g(n)$ is always a product of primes less or equal to $2.86\sqrt{n\ln(n)}$, c.f. [47]. Therefore the factorization of $g(n)$ can be found in polynomial time in n. It is also known that the partition of n that gives the maximum lcm has parts that are all prime powers, c.f. [26], and therefore the factorization of $g(n)$ gives the expected partition directly. The algorithm given in [64] allows one to compute $g(n)$ for large integers n, up to $n = 32,000$, so the exact determination of the matrix M is not a problem. See Table 5.1 for a list of values of $g(n)$ with the associated partition.

Example 5.14 Let $n = 19$ and $g(n) = 420$ reached by the partition $4 + 3 + 5 + 7 = 19$. Then any matrix with the following form

Table 5.1: Some values of Landau's function g

n	$g(n)$	Associated partition
256	4243057729190280	8, 9, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 43
512	70373028815644182 \ 5899620	1, 1, 1, 4, 9, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61
1024	855674708268439827 \ 7434193536488991600	1, 1, 1, 16, 27, 25, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89

has period 420 in R_{19}.

$$\begin{pmatrix}
0 & 1 & 0 & 0 & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * \\
0 & 0 & 1 & 0 & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * \\
0 & 0 & 0 & 1 & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * \\
1 & 0 & 0 & 0 & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & * & * & * & * & * & * & * & * & * & * & * & * \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & * & * & * & * & * & * & * & * & * & * & * & * \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & * & * & * & * & * & * & * & * & * & * & * & * \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & * & * & * & * & * & * & * \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & * & * & * & * & * & * & * \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & * & * & * & * & * & * & * \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & * & * & * & * & * & * \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & * & * & * & * & * & * & * \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

For a given matrix $M \in R_n$, we define

$$R[M] = \left\{ \sum_{i \in I} M^i \mid I \subset \mathbb{N}\,,\ |I| < \infty \right\},$$

the commutative semiring generated by M. Since $R[M] \supset \{M^k\}_{k \in \mathbb{N}}$, we have

$$|R[M]| \geqslant \mathrm{ord}\,(M) \geqslant p(M),$$

and the last inequality can give $|R[M]| \geqslant g(n)$ for a wisely chosen M.

Here is what we have so far: a collection of finite zero-sum free c-simple semirings R_n inside which one can easily build commutative sub-semirings of size sub-exponential in n. These semirings possess a negligible portion of invertible elements.

5.3 An action related to a flow problem

In this section, we define and study a first action built out of the semirings R_n studied so far. Let $M \in R_n$ acting by multiplication on vectors as follows:

$$\begin{array}{ccc} R_n[M] \times R_1^n & \longrightarrow & R_1^n \\ (\sum_{i \in I} M^i, v) & \longmapsto & \sum_{i \in I} M^i v. \end{array}$$

Although this action looks like the usual matrix action on the associated vector space, it does not yield the same problem mainly because of the non-existence of the Cayley-Hamilton theorem in R_n, i.e., an element $\sum_{i \in I} M^i$ may not be expressible in terms of a polynomial $p(M)$ with low degree. In this situation, for two given vectors v and w in R_1^n, the semigroup action problem asks to find a set of indices I with the property that $\sum_{i \in I} M^i v = w$.

The size $\operatorname{ord}(M^i v)$ of the orbit sequence $M^i v$ is crucial since Algorithm 5.15 solves the SAP of the previous action with parameter M, v and w in essentially $O(\operatorname{ord}(M^i v))$ semiring operation. First a notation: For any rectangular matrices M and N of same dimension with entries in R_1, $M \leqslant N$ means that $\min(m_{ij}, n_{ij}) = m_{ij} \cdot n_{ij} = m_{ij}$ for all i and j.

Algorithm 5.15 Given $M \in R_n$, $v \in R_1^n$ and $w = \sum_{i \in J} M^i v$ for some finite $J \subset \mathbb{N}$, this algorithm finds a set I with $w = \sum_{i \in I} M^i v$.

1. Set $I = \emptyset$ and $t = 1$.

2. If $\sum_{i \in I} M^i v + M^t v \leqslant w$ and $M^t v \not\leqslant \sum_{i \in I} M^i v$ then set $I \longleftarrow I \cup \{t\}$.

3. If $\sum_{i \in I} M^i v \geqslant w$ then output I and stop.

4. Set $t \longleftarrow t + 1$ and go to step 2.

Remark 5.16 The condition $M^t v \not\leqslant \sum_{i \in I} M^i v$ in step 2. is not necessary in order to make the algorithm work. However it gives the insurance that the index set I does not contain too many indices that are useless.

After k loops, the algorithm has built a set of indices I_k with the property $\sum_{i \in I_k} M^i v \leqslant w$. Loop $k+1$ strictly increases I_k if and only if the vector $M^{k+1} v + \sum_{i \in I_k} M^i v$ has changed from $\sum_{i \in I_k} M^i v$ and has the property $M^{k+1} v + \sum_{i \in I_k} M^i v \leqslant w$. The algorithm essentially tests combinations of type $\sum_{i \in I} M^i v$ and combines those for which $\sum_{i \in I} M^i v \leqslant w$. The search being exhaustive, the algorithm must stop before $\operatorname{ord}(M^i v) + 1$ loops. Let us state once again the result:

Proposition 5.17 *Algorithm 5.15 solves the SAP instance with parameter* $M \in R_n$, $v \in R_1^n$ *and* $w = \sum_{i \in J} M^i v$, *for some finite* $J \subset \mathbb{N}$, *in* $O(\mathrm{ord}\,(M^i v))$.

Using Corollary 5.9, it is not difficult to see that the problem has the following graph theoretic interpretation:

Problem 5.18 [The Flow Problem] Given an oriented graph G, two sets S and T of source vertices and sink vertices, find a set L of positive integers with the following properties:

i) For each $s \in S$ and each path γ in G starting at s of length $l \in L$, the end point of γ is in T.

ii) For each $t \in T$, there exists a path γ ending at t with starting point in S and of length $l \in L$.

This problem does not seem to be known in the theory of *flow problems*. Clearly any set L that fulfills the conditions of the Flow Problem is appropriate to solve the SAP instance. By asking the set L to be *minimal*, we strengthen the search problem, but even with this requirement, the problem is not known to be NP-hard [35]. Note that flow problems are known to be quite difficult in general (c.f. [17] and [36]). However this action does not seem to be appropriate for building a cryptosystem on it. Here are the reasons why:

i) Even if the commutative semigroup $R_n[M]$ is large (by choosing M with large order), the sequence $M^i v$ may have a small order. Computational search even showed that for a general vector v it is almost always the case, leading to a sequence $M^i v$ whose order is far below the order of M.

ii) One could try to find a vector v leading to a sequence $M^i v$ with large order, say the same order as M. But it turns out that this search problem is NP-hard. Indeed deciding if the order of $M \in R_n$ can be reached by the order of some sequence $M^i v$ is a NP-complete decision problem [19].

5.4 A two-sided matrix multiplication action

Let R be an additively commutative semiring with 0 and 1. As usual if $M \in \mathrm{Mat}_n(R)$, then $R[M]$ is the multiplicatively commutative semiring generated by M in $\mathrm{Mat}_n(R)$, i.e., the set of all polynomial $p(M)$ in M with coefficients in R. Let $M_1, M_2 \in \mathrm{Mat}_n(R)$ and consider the following action:

$$\begin{array}{ccc} (R[M_1] \times R[M_2]) \times \mathrm{Mat}_n(R) & \longrightarrow & \mathrm{Mat}_n(R) \\ ((p(M_1), q(M_2)), A) & \longmapsto & p(M_1) \cdot A \cdot q(M_2). \end{array}$$

This action is linear since

$$p(M_1) \cdot (A + B) \cdot q(M_2) = p(M_1) \cdot A \cdot q(M_2) + p(M_1) \cdot B \cdot q(M_2).$$

Because of this linearity, we avoid the case when R a finite field (see Theorem 4.1) even if the initial SAP instance related to this semigroup action looks difficult. Indeed, a naive approach would lead to the resolution of a family of quadratic equations over a finite field. As mentioned in the introduction, this problem is NP-hard in general.

In the sequel, we choose to work with the c-simple semirings R_n. In particular, by polynomial in R_1 we mean any expression of type $\sum_{i \in I} x^i$ for some finite $I \subset \mathbb{N}$. Once again the orders of the matrices M_1 and M_2 chosen to act on the matrix A on the left

and on the right are of prime importance. At first sight, a brute force search that would solve a SAP instance where the matrices M_1 and M_2 act on a matrix A would take $O(|R_1[M_1]| \cdot |R_1[M_2]|)$ trials. This is obviously not feasible as soon as one chooses wisely the matrices M_1 and M_2 and the integer n, even a fairly small one. Let us consider the following equality:

$$B = \left(\sum_{i\in I} M_1^i\right) \cdot A \cdot \left(\sum_{j\in J} M_2^j\right) = \sum_{(i,j)\in I\times J} M_1^i \cdot A \cdot M_2^j.$$

It follows that each couple (i,j) in $I \times J$ satisfies $M_1^i \cdot A \cdot M_2^j \leqslant B$ and therefore

$$\begin{aligned} I \times J \quad \subset \quad & \{(i,j) \,|\, 0 \leqslant i \leqslant \operatorname{ord}(M_1),\ 0 \leqslant j \leqslant \operatorname{ord}(M_2) \\ & \text{and } M_1^i \cdot A \cdot M_2^j \leqslant B\} = S. \end{aligned}$$

Although the index sets I and J may not be easy to find from the knowledge of the set S above, we make the following assumption:

Assumption 5.19 There exists an algorithm $\mathcal{A}$ that finds two index sets I' and J' from S in expected running time bounded by $O(|S|^k)$ $(k \geqslant 1)$ such that

$$B = \left(\sum_{i\in I'} M_1^i\right) \cdot A \cdot \left(\sum_{j\in J'} M_2^j\right).$$

This assumption yields the following consequence: there exists an algorithm that solves the SAP instance in time polynomial in $\operatorname{ord}(M_1) \cdot \operatorname{ord}(M_2)$, say in

$$O\left((\operatorname{ord}(M_1) \cdot \operatorname{ord}(M_2))^d\right). \tag{5.4}$$

Indeed, one can find S in $\operatorname{ord}(M_1) \cdot \operatorname{ord}(M_2)$ step, and use the algorithm $\mathcal{A}$ to find I' and J'. Since $|S| \leqslant \operatorname{ord}(M_1) \cdot \operatorname{ord}(M_2)$, the conclusion follows.

This assumption is reasonable. First, computational search showed that the set S tends to be quite small in comparison to $\mathrm{ord}\,(M_1) \cdot \mathrm{ord}\,(M_2)$. Second, C. Monico [61] has developed an algorithm that seems to verify the assumption.

5.5 The choice of the parameters

The previous action led to an interesting semigroup action problem. Indeed, a simplification of the problem in the spirit of Pohlig-Hellman attack is avoided by the fact that the problem takes place in a c-simple semiring: no congruence relation exists in the set we are working in that could be used to simplify the resolution of the SAP. On the other hand, we have seen that the negligible proportion of inverses in R_n makes the known square-root attacks non-reproducible in this context, even conceptually.

We discuss now the complexity of solving the semigroup action problem of the last section with respect to the size of the input and taking in consideration the assumption that there exists an algorithm that solves the SAP, with parameter M_1, M_2 and A as above, in expected running time $O((\mathrm{ord}\,(M_1) \cdot \mathrm{ord}\,(M_2))^d)$ as in Equation 5.4. Moreover, we will assume that the matrices M_1 and M_2 have been chosen with large orders using Proposition 5.13, i.e.,

$$\mathrm{ord}\,(M_1) = \mathrm{ord}\,(M_2) = \exp\left((1 + o(1))\sqrt{n \ln(n)}\right)$$

For fixed matrices M_1, M_2 and A, the input size of B is clearly n^2 if no assumption is made regarding the proportion of 0's and 1's in B. Therefore, building a cryptosystem on this SAP would lead us to consider keys with size of $N = n^2$ bits. Using the previous assumptions we are to consider an algorithm that solves the SAP

in expected time

$$\begin{aligned} T &= O\left(\left(\exp\left((1+o(1))\sqrt{n\ln(n)}\right)\right)^{2d}\right) \\ &= O\left(\exp\left((2d+o(1))\sqrt{n\ln(n)}\right)\right). \end{aligned}$$

Let us rephrase this in terms of key sizes:

Proposition 5.20 *Consider the semigroup action problem induced by the matrices M_1, M_2 and A as above and a matrix B of bit-size N. Under Assumption 5.19, there exists an algorithm that solves the problem in expected time bounded by*

$$O\left(\exp\left((\sqrt{2}d+o(1))N^{1/4}\sqrt{\ln(N)}\right)\right)$$

for some $d \in \mathbb{N}$.

This result shows that, compared with the usual DLP in groups, this setting is not competitive. Recall for instance that the running time of the fastest known algorithm for solving the DLP in a prime finite field is

$$O\left(\exp\left((1.92+o(1))N_{\mathbb{F}_p}^{1/3}(\ln(N_{\mathbb{F}_p}))^{2/3}\right)\right)$$

and this is always faster than the bound given by Proposition 5.20, mainly because of the fourth root of N. Table 5.2 shows different values of $N_{\mathbb{F}_p}$ associated to values of the key N in order to reach similar levels of security, in the case $d = 1$.

We now consider conditions under which one can reduce substantially the key size of the cryptosystem based on the semigroup action problem of the two-sided matrix action studied so far. The goal is to restrict the class of matrices used during the action in order to decrease the bit-size N of B. The general idea is to work

Table 5.2: $N_{\mathbb{F}_p}$ and N

$N_{\mathbb{F}_p}$	N
256	6892
512	19111
1024	52475

with sparse matrices instead of full ones. Suppose that we choose the matrices M_1, M_2 and A as sparse matrices. We have seen that even with this restriction, the matrices M_1 and M_2 can still have the desired orders. Then if one chooses sparse polynomial p and q we certainly get a matrix B which is sparse as well. Here is a possible choice: take A any permutation matrix in R_n, choose M_1 and M_2 two permutation matrices in R_n with large orders and restrict the choice of the polynomials p and q to polynomials with exactly k monomials each. Since any matrix of the type $M_1^s \cdot A \cdot M_2^t$ is also a permutation matrix, the matrix

$$B = p(M_1) \cdot A \cdot q(M_2) = \sum_{i,j=1\ldots k} M_1^{s_i} \cdot A \cdot M_2^{t_j}$$

will have at most k^2 ones in each row, i.e., the matrix B contains at most $k^2 n$ ones. As long as $k = o(\sqrt{n})$, the matrix B is sparse. Now comes the question of the number of bits needed to "describe" such an object. A first way is simply to use the set of couples (i, j) such that $B_{ij} = 1$. This method is simple and one can easily encode such a matrix using $k^2 n$ pairs, each of them being a pair of numbers of $\log_2(n)$ bit-length. The overall bit-length needed to completely describe B using this method is $N_s = O(k^2 n \log_2(n))$. In fact more can be said. We can see B as a random variable of words made out of the symbols 0 and 1, where the symbol 1 appears independently

with probability $\pi = k^2 n/n^2 = k^2/n$. The entropy of this random variable is then $H = n^2 \cdot (-\pi \log_2(\pi) - (1-\pi)\log_2(1-\pi)$. The noiseless coding theorem for memoryless sources (c.f. [91]) states that there exists a way to encode B with roughly $1 + H \cong H$ bits and one cannot do better. In other words, another way to encode B would be the use of the Huffman coding algorithm [91]. Here we will need roughly

$$n^2 \cdot \left(-k^2/n \log_2(k^2/n) - (1-k^2/n)\log_2(1-k^2/n)\right)$$

bits to encode the matrix B. For a fixed k, as n goes to infinity, we have

$$\begin{aligned} H &\cong n^2 \cdot \left(-k^2/n \log_2(k^2/n) - (1-k^2/n)(-k^2/n)\right) \\ &= nk^2 \log_2(n) - \left[nk^2\left(2\log_2(k) - 1\right) + k^2\right] \\ &= nk^2 \log_2(n) - O(n). \end{aligned}$$

Therefore, the naive way to encode B by indexing the entries 1 is not far from optimal when n goes to infinity. However, in the range of interesting values for our purpose, i.e. $n \ll 10^5$, the latter method still yields advantageous key-length. For instance, when $n = 512$, the naive method would use 73 Kb to code B and the optimal Huffman algorithm would need 50 Kb. Regarding the key size, this method provides a decrease from $N = n^2$ to $N_s = nk^2 \log_2(n) - O(n) = nk^2 \log_2(n) - o(n \log(n))$. Note that we have

$$n \ln(n) = \frac{\ln(2)}{k^2} N_s + o(n \log(n)) = \frac{\ln(2)}{k^2} N_s + o(N_s).$$

We can therefore state the following:

Proposition 5.21 *Consider the semigroup action problem induced by the permutation matrices M_1, M_2 and A as above. Suppose that*

the polynomial p and q used in the action possess each k monomials. Then any matrix $B = p(M_1) \cdot A \cdot q(M_2)$ *can be encoded with* $N_s = nk^2 \log_2(n)$ *bits and under Assumption 5.19, there exists an algorithm that solves the problem in expected time bounded by*

$$O\left(\exp\left((\nu + o(1))\sqrt{N_s}\right)\right)$$

where $\nu = \dfrac{\sqrt{2}d}{\sqrt{\ln(2)}k}$ *and* $d \in \mathbb{N}$.

Let us discuss the consequences of the bound given by the previous proposition. Suppose that Assumption 5.19 yields an algorithm that solve the SAP in time linear in $\operatorname{ord}(M_1) \cdot \operatorname{ord}(M_2)$, i.e., $d = 1$ in the previous proposition. Once again this supposition put us on a safe side regarding the power of an adversary willing to break a cryptosystem based on the difficulty of the semigroup action problem. So if $d = 1$ then $\nu \cong 1.69 \cdot k^{-1}$. The bound of Proposition 5.21 behaves now more like the running time of the fastest known algorithm that solves DLPs in finite field than the bound of Proposition 5.20, and even provides a bigger upper bound asymptotically. In other words, for large n, the new situation seems to be competitive with cryptosystems based on the difficulty of the DLP in finite fields and RSA.

At this point, we must make clear that this discussion is valid only if no faster algorithm that solves the SAP is known. Prudence tells us that such a supposition may not be true.

Moreover, even for small values of k, the same level of security for cryptosytems based on the DLP over $\mathbb{F}_p$ and based on the difficulty of the previous semigroup action problem is not reached for the usual values of the key size. Note that a similar level of security is obtained (neglecting the constant factor) when

$$N_s \cong 1.27 \cdot k^2 \cdot N_{\mathbb{F}_p}^{2/3} \cdot \ln(N_{\mathbb{F}_p})^{4/3}.$$

Even for $k = 4$, $N_{\mathbb{F}_p} < N$ as long as $N_{\mathbb{F}_p} < 1.7 \cdot 10^9$, and the situation is worse for larger k. Table 5.3 shows how big should be N_s for a given $N_{\mathbb{F}_p}$ in order to have equivalent problems from a computational viewpoint.

Table 5.3: k, $N_{\mathbb{F}_p}$ and N_s

k	$N_{\mathbb{F}_p}$	N_s
4	256	8089
4	512	15024
4	1024	27446
6	256	18200
6	512	33804
8	256	32356

5.6 Conclusion

In this chapter, we have studied the family of semirings R_n of matrices over the max-min algebra $(\{0,1\}, \max, \min)$, $n \in \mathbb{N}$. We have shown that these semirings are c-simple and possess a negligible portion of invertible elements. Commutative sub-semiring with orders subexponential in n have been constructed inside R_n. Two different semigroup actions have been studied using these semirings, both of them leading to non-competitive cryptosystems. However, we have produced an example of a semiring action on a semi-module where no Pohlig-Hellman type of attack and no square root attack is known and even reproducible from a conceptual point of view.

Chapter 6

ACTIONS INDUCED BY CHEBYSHEV POLYNOMIALS

In this chapter, we study the action of Chebyshev polynomials on commutative finite rings R. The rings $\mathbb{F}_q$, $\mathbb{Z}/n\mathbb{Z}$ where n is an RSA integer and commutative subrings of $\mathrm{Mat}_n(\mathbb{F}_q)$ are the main examples. We study the difficulty of the discrete Chebyshev problem in these rings and prove several equivalence results.

6.1 Chebyshev polynomials

The Chebyshev polynomials T_n defined below are named after the Russian mathematician P.L. Chebyshev (1821-1894). The T comes from the French spelling Tchebychef. A wealth of information on these polynomials can be found in [5] and [76]. Here is a way to

define them. First, using de Moivre's formula

$$\cos(n\theta) + i\sin(n\theta) = (\cos\theta + i\sin\theta)^n = \sum_{k=0}^{n} \binom{n}{k} i^k \cos^{n-k}\theta \sin^k\theta$$

and collecting the real parts, we have

$$\cos(n\theta) = \sum_{l=0}^{\lfloor n/2 \rfloor} \binom{n}{2l} (-1)^l \cos^{2l}\theta \cdot (1 - cos^2\theta)^l.$$

Definition 6.1 For all non-negative integers n, the n^{th} Chebyshev polynomial T_n is

$$T_n(x) = \sum_{l=0}^{\lfloor n/2 \rfloor} \binom{n}{2l} (-1)^l x^{2l} \cdot (1 - x^2)^l.$$

The first Chebyshev polynomials are

$$\begin{aligned} T_0(x) &= 1 \\ T_1(x) &= x \\ T_2(x) &= 2x^2 - 1 \\ T_3(x) &= 4x^3 - 3x \\ T_4(x) &= 8x^4 - 8x^2 + 1 \end{aligned}$$

Clearly the polynomials T_n have integer coefficients, and satisfy the equation

$$T_n(\cos(\theta)) = \cos(n\theta)$$

which will give Property 1. below. They also satisfy $T_n(1) = 1$ and $T_n(-1) = (-1)^n$. Given a ring R with unity 1_R, one can always see $T_n(x)$ as a polynomial with coefficient in R by using the well defined ring homomorphism from $\mathbb{Z}[x]$ to $R[x]$ induced by the homomorphism defined via the canonical homomorphism from

$\mathbb{Z}$ to R with $1 \longmapsto 1_R$. Here are collected the properties of the Chebyshev polynomials that will be needed in the sequel. All the proofs can be found either in [5] or in [76]:

Properties 6.2 The Chebyshev polynomials satisfy the following:

1. $T_{nm}(x) = T_n(T_m(x))$ in $\mathbb{Z}[x]$.
2. $T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$ for all $n = 2, 3, \ldots$.
3. $T_n(\frac{1}{2}(x + x^{-1})) = \frac{1}{2}(x^n + x^{-n})$.

Properties 1. and 2. naturally extend to the case where the polynomials are considered as elements of $R[x]$ where R is a ring with unity. Property 3. is also valid in any field of characteristic different from 2. Property 1. comes from the fact that $T_{nm}(\cos\theta) = \cos(mn\theta)) = T_n(\cos(m\theta)) = T_n(T_m(\cos(\theta)))$ and the polynomial functions T_{nm} and $T_n \circ T_m$ being equal on $[-1, 1]$ are equal as polynomial. This property also implies that for all positive integers n and m, $T_n \circ T_m = T_m \circ T_n$, i.e., the sequence $(T_n)_{n=1}^{\infty}$ is a sequence of commuting polynomials in the semigroup $(\mathbb{Z}[x], \circ)$. Note that the sequence $(x^n)_{n=1}^{\infty}$ is also a family of commuting polynomials, polynomials that were used originally by Diffie and Hellman in there key exchange (c.f. Figure 1.1.). From our viewpoint such families are clearly important and therefore the following proposition is rich in consequences:

Proposition 6.3 *Let $\mathbb{F}$ be a field. Suppose $(p_n)_{n=0}^{\infty}$ is a sequence of polynomials of degree n in $\mathbb{F}$ and for all positive integers n and m*

$$p_n \circ p_m = p_{nm}.$$

Then there exists a linear transformation $w(x) = ax + b$, $a \neq 0$, so that

$$w \circ p_n \circ w^{-1} = x^n\,,\ n \in \mathbb{N}^* \quad or \quad w \circ p_n \circ w^{-1} = T_n(x)\,,\ n \in \mathbb{N}^*$$

A proof can be found in [41]. Property 2. gives the following proposition that characterize the computational complexity of the evaluation of $T_n(a)$:

Proposition 6.4 *Let R be a ring with unity, a be an element in R and n be an integer. The computation of $T_n(a)$ can be reduced to $O(\log_2(n))$ arithmetical operations in R.*

Proof: Property 2. gives

$$\begin{pmatrix} 0 & 1 \\ -1 & 2a \end{pmatrix} \cdot \begin{pmatrix} T_{n-2}(a) \\ T_{n-1}(a) \end{pmatrix} = \begin{pmatrix} T_{n-1}(a) \\ T_n(a) \end{pmatrix},$$

and by induction,

$$\begin{pmatrix} 0 & 1 \\ -1 & 2a \end{pmatrix}^{n-1} \cdot \begin{pmatrix} 1 \\ a \end{pmatrix} = \begin{pmatrix} T_{n-1}(a) \\ T_n(a) \end{pmatrix}.$$

By repeating square-and-multiply method, $O(\log_2(n))$ matrix multiplications suffice to compute the left-hand-side and therefore $T_n(a)$. In dimension 2, a matrix multiplication costs 8 multiplications and 4 additions, which keeps the complexity to $O(\log_2(n))$ arithmetical operations in R. □

Let us now define the semigroup action induced by the Chebyshev polynomials. Let R be a finite ring with unity. The *Chebyshev action on R* is the map

$$\begin{array}{ccc} \mathbb{N} \times R & \longrightarrow & R \\ (n, a) & \longmapsto & T_n(a) \end{array}$$

This map is a semigroup action by $(\mathbb{N}, \cdot)$ on R because of Property 1. above. The previous proposition shows that this action is computationally feasible if arithmetic is feasible in R. Namely there exists a polynomial time reduction of computing the value of $T_n(a)$

to the usual arithmetic in R. This fact is at the heart of the following problem: One could naively try to consider any polynomial p of degree $d > 1$ (the case d=1 being trivial) with integer coefficients and work with the family of polynomials $p^{(n)} = p \circ \cdots \circ p$, where the product of composition contains n factors. The action would then be

$$\begin{array}{ccc} \mathbb{N} \times R & \longrightarrow & R \\ (n, a) & \longmapsto & p^{(n)}(a) \end{array}$$

In order to compute the value of $p^{(n)}(a)$, one can still use square-and-multiply methods which is polynomial in $\log_2 n$ but if no special property is known, in the chain $(p^{(k_i)})_{i=1}^{N}$, $N = O(\log_2 n)$, of polynomials used in the computation, one has to store every polynomials $p^{(k_i)}$ to compute $p^{(k_{i+1})}$ which requires to store polynomials of degree up to roughly d^n. Even for small degree, n being in the range of the key size, the storage of such a polynomial is not feasible. Such an action is therefore of no practical value.

The Chebyshev action is bound to the following semigroup action problem:

Problem 6.5 [The discrete Chebyshev problem] Let R be a finite ring with unity. Given a and b such that $b = T_l(a)$ for some $l \in \mathbb{N}$, find a $n \geqslant 0$ such that $b = T_n(a)$.

This action is in essence different from the action induced by the sequence of powers, i.e., the sequence $(x^n)_{n=1}^{\infty}$. Indeed, the powers of an element stay in the multiplicative semigroup generated by this element, but the values $T_n(a)$ live in the whole sub-ring $R[a]$. There is however a strong connection between these two actions. The next section is a study of it in the case of a finite field.

6.2 The discrete Chebyshev problem in finite fields

In this section we consider the case where $R = \mathbb{F}_q$, the finite field with $q = p^d$ elements. The issue is to determine if Chebyshev polynomials behave in finite fields in a manner that fulfills cryptographic requirements such as mixing property and difficulty of the underlying mathematical problem.

A first thing to note is that characteristic 2 has to be avoided. Indeed, using Property 2. of 6.2, we see that

$$T_n(x) \mod 2 = \begin{cases} 1 & \text{if } n \text{ is even} \\ \text{x} & \text{if } n \text{ is odd} \end{cases}$$

Therefore, we will always assume that $p \neq 2$. Next, most of Chebyshev polynomials have a nice mixing property in such algebraic structure. More precisely, we have:

Proposition 6.6 *Let n be an integer and $q = p^d$. Then $(n, q^2 - 1) = 1$ if and only if $T_n \in \mathbb{F}_q[x]$ is a permutation polynomial, i.e., the function induced by T_n on $\mathbb{F}_q$ is a permutation.*

A proof can be found in [41] as a special case of Theorem 9.43. Now come the question of determining the difficulty of the discrete Chebyshev problem in a finite field. It turns out that the problem is computationally equivalent to the DLP in $\mathbb{F}_q^*$, as long as $p \neq 2$ (Corollary 6.8 below). Therefore this action does not yield some more secure system, but rather gives another point of view of the long standing DLP in finite fields of odd characteristic. A key point in the equivalence is the fact that SQROOT is an easy problem in any finite field. Indeed there exists a randomized algorithm to solve SQROOT in $\mathbb{F}_q$ that has an expected running time of $O((\log_2 q)^4)$ bit operations. The idea of it goes back to A.Tonelli in an 1891

paper. There are algorithms even faster if one works over $\mathbb{F}_{2^d}$ or $\mathbb{Z}_p$. A detailed description of both the algorithms and the complexities can be found in [57].

Here is the main result of this section. It provides a strong connection between the discrete Chebyshev problem and the DLP in $\mathbb{F}_q$.

Proposition 6.7 *Let $\mathbb{F}_q$ be a finite field of odd characteristic.*

1. *The discrete Chebyshev problem with parameters $b = T_n(a)$ reduces to at most two DLPs in the field $\mathbb{F}_q(\sqrt{a^2-1})$. Here $\sqrt{a^2-1}$ is any square root of a^2-1.*
2. *The DLP in $\mathbb{F}_q$ reduces to the discrete Chebyshev problem in $\mathbb{F}_q$.*

Proof: Let us prove the first point. Suppose one wants to find n such that $T_n(a) = b$, with a an element of $\mathbb{F}_q$ and b in the orbit of a. Let $x \in \mathbb{F}_q(\sqrt{a^2-1})$ such that $\frac{1}{2}(x+x^{-1}) = a$. Such an x exists, it suffices to take $x = a+\sqrt{a^2-1}$. The element x can be computed in expected polynomial time as explained above. Because of Property 3. of 6.2, we have

$$\begin{aligned} T_n(a) &= T_n(\tfrac{1}{2}(x+x^{-1})) \\ &= \tfrac{1}{2}(x^n+x^{-n}) \\ &= b \end{aligned}$$

and therefore $x^n = b \pm \sqrt{b^2-1}$. The discrete Chebyshev problem reduces in finding n such that one of the equalities $x^n = b+\sqrt{b^2-1}$ or $x^n = b-\sqrt{b^2-1}$ holds. This requires at most two DLPs in $\mathbb{F}_q(\sqrt{a^2-1})$.

We now prove the second point. Suppose one wants to find n such that $a^n = b$, with a an element in $\mathbb{F}_q^*$ and b in the cyclic

sub-group generated by a. Let us define the elements x and y as follows:

$$x = \tfrac{1}{2}(a + a^{-1}) \quad \text{and} \quad y = \tfrac{1}{2}(b + b^{-1}).$$

Because of Property 3. of 6.2, $y = T_n(x)$ is equivalent to

$$\tfrac{1}{2}(b + b^{-1}) = \tfrac{1}{2}(a^n + a^{-n}),$$

i.e.,

$$b - a^n = \frac{1}{a^n} - \frac{1}{b} = \frac{b - a^n}{ba^n},$$

which is equivalent to

$$(b - a^n) \cdot \left(1 - \frac{1}{ba^n}\right) = 0.$$

The equality is fulfilled if and only if either $a^n = b$ or $a^{q-1-n} = b$. After having solved the discrete Chebyshev problem with parameters x and y, we have an integer n' that fulfilled one of the previous equalities. If $a^{n'} = b$ then we define $n = n'$ and if $a^{q-1-n'} = b$ then we define $n = q - 1 - n'$. In both cases the DLP is reduced to the discrete Chebyshev problem with parameters x and y. □

Corollary 6.8 *Let $\mathbb{F}_q$ be as above. The discrete Chebyshev problem and the DLP in $\mathbb{F}_q$ are computationally equivalent.*

Proof: There remains only one reduction to study. The previous proposition shows that the discrete Chebyshev problems in $\mathbb{F}_q$ is at most as hard as the DLP in $\mathbb{F}_{q^2}$. We have seen that the Pohlig-Hellman reduction solves the DLP in $\mathbb{F}_{q^2}^*$ by solving a family of DLPs in quotients of $\mathbb{F}_{q^2}^*$ and the overall complexity is determined by the largest prime dividing $q^2 - 1 = (q - 1)(q + 1)$. This largest prime is less than $(q + 1)/2$, i.e., the problem is no more difficult that the DLP in F_q, computationally speaking. □

The proof of the proposition shows that if SQROOT is feasible in some extension ring S of the ring R, then the same argument holds and therefore the discrete Chebyshev problem in R will always reduce to the DLP in S. In the search of new hard problems related to our study, a natural idea is to find rings where SQROOT is a non-trivial problem, computationally speaking. On the other hand, the reduction of the DLP to the discrete Chebyshev problem in the previous proof has been done using the fact that there is no zero divisors in a field. In a finite ring R which is not a field, the situation is different since R must possess zero divisors, see Lemma 3.11. In such a situation, a reduction of this type does not seem to be evident.

6.3 The discrete Chebyshev problem in $\mathrm{Mat}_n(\mathbb{F}_q)$

The next natural step after having looked at the case of a finite field is the study of the problem in $\mathrm{Mat}_n(\mathbb{F}_q)$. As mentioned earlier, there exists a probabilistic polynomial-time reduction of the DLP in $Gl_n(\mathbb{F}_q)$ to the DLP in some small extension field of $\mathbb{F}_q$ [58]. Note that using Jordan decomposition technics, the DLP in $\mathrm{Mat}_n(\mathbb{F}_q)$ also reduces to the DLP in $Gl_n(\mathbb{F}_q)$. What about the discrete Chebyshev problem in $\mathrm{Mat}_n(\mathbb{F}_q)$? As explain above, the non-feasibility of SQROOT in some extension of the considered ring is essential in order to face a problem that does not reduce to a DLP in that ring. As a matter of fact, there exists matrices over fields that do not admit any square root in any extension field. A toy example is the matrix

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

that does not have a square root in *any* field. Let us recall the notion needed to state and prove the theorem of classification of matrices that are squares. This theorem is not fundamentally useful in our context since we will see that in fact the discrete Chebyshev problem in $\mathrm{Mat}_n(\mathbb{F}_q)$ is no more difficult than the DLP in some small extension field of $\mathbb{F}_q$, but the result has an intrinsic mathematical value and deserves as such to figure in these pages.

A *Jordan block* of order d corresponding to λ, $J(\lambda, d)$, is an upper-triangular square matrix of dimension d with λs in the main diagonal, 1's in the first upper-diagonal and 0's everywhere else. Two matrices A and B with entries in a field $\mathbb{F}$ are *equivalent*, written $A \sim B$, if there exists an invertible matrix S with entries in $\mathbb{F}$ such that $A = SBS^{-1}$. In addition, Jordan's theorem says that if the characteristic polynomial of a matrix A split in $\mathbb{F}$ then A is equivalent (as a matrix in $\mathrm{Mat}_n(\mathbb{F})$) to a matrix of the form

$$\mathrm{Diag}(J(\lambda_1, d_1), \ldots, J(\lambda_k, d_k)) = \begin{pmatrix} J(\lambda_1, d_1) & & 0 \\ & \ddots & \\ 0 & & J(\lambda_k, d_k) \end{pmatrix} \quad (6.1)$$

where $\lambda_1, \ldots, \lambda_k$ are the eigenvalues of A (not necessarily distinct) and $\sum_{i=1}^{k} d_i = n$. This matrix, *the Jordan canonical form*, is unique up to a permutation of the component Jordan blocks (see e.g. [9] or [31]).

Lemma 6.9 *Let $\mathbb{F}$ be a field and $Z \in \mathrm{Mat}_n(\mathbb{F})$ having all its eigenvalues in $\mathbb{F}$. Then for each eigenvalue λ of Z and all integer $k \geqslant 1$, the number of Jordan blocks $J(\lambda, d)$ with $d \geqslant k$ is*

$$\mathrm{rank}\,(Z - \lambda I)^{k-1} - \mathrm{rank}\,(Z - \lambda I)^{k}.$$

Hence the number of Jordan blocks of size exactly k is

$$\mathrm{rank}\,(Z - \lambda I)^{k+1} - 2\mathrm{rank}\,(Z - \lambda I)^{k} + \mathrm{rank}\,(Z - \lambda I)^{k-1}$$

The first part of the lemma is Theorem 5.14 of [9]. The second part is a direct consequence of it.

Theorem 6.10 *Let $\mathbb{F}$ be a field (finite or not) and $N \in \mathrm{Mat}_n(\mathbb{F})$. There exists $M \in \mathrm{Mat}_n\left(\overline{\mathbb{F}}\right)$ such that $M^2 = N$ if and only if*

- $\mathrm{char}\,\mathbb{F} \neq 2$ *and the Jordan blocks associated to N corresponding to 0 are either non-existent or of type $J(0,1)$ or come in pair of type $(J(0,d), J(0,d))$ or of type $(J(0,d), J(0,d-1))$.*
- $\mathrm{char}\,\mathbb{F} = 2$ *and for each eigenvalue λ of N the Jordan blocks corresponding to it associated to N are either of type $J(\lambda,1)$ or come in pair either of type $(J(\lambda,d), J(\lambda,d))$ or of type $(J(\lambda,d), J(\lambda,d-1))$.*

Proof: The proof is divided into the following claims:

1. In characteristic different from 2, any Jordan block $J(\lambda,d)$ with $\lambda \neq 0$ is a square.
2. The Jordan canonical form of the square $J(0,l)^2$, $l > 1$, is either $\mathrm{Diag}(J(0,l/2), J(0,l/2))$ if l is even or $\mathrm{Diag}(J(0,(l+1)/2), J(0,(l-1)/2))$ if l is odd. These Jordan decomposition matrices are themselves squares.
3. In characteristic 2, the Jordan canonical form of $J(\mu,l)^2$, $l > 1$, is either $\mathrm{Diag}(J(\mu^2,l/2), J(\mu^2,l/2))$ if l is even or $\mathrm{Diag}(J(\mu^2,(l+1)/2), J(\mu^2,(l-1)/2))$ if l is odd. These Jordan decomposition matrices are themselves squares.

Proof of 1): The proof is constructive. Let

$$M := \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_d \\ & a_1 & a_2 & & a_{d-1} \\ & & \ddots & \ddots & \vdots \\ & 0 & & a_1 & a_2 \\ & & & & a_1 \end{pmatrix}.$$

Clearly $M^2 = J(\lambda, d)$ if and only if $(M^2)_{1j} = (J(\lambda, d))_{1,j}$. This equality holds if and only if

$$(M^2)_{11} = a_1^2 = \lambda \ , \quad (M^2)_{12} = 2a_1a_2 = 1$$

and for all $j \geqslant 3$

$$(M^2)_{1j} = \sum_{i=1}^{j} a_i a_{j-i+1} = 0. \tag{6.2}$$

Let μ in $\overline{\mathbb{F}}$ with $\mu^2 = \lambda$. If $a_1 = \mu$ then in order to satisfy the above equations, $a_2 = (2a_1)^{-1}$ and one can define by induction each a_j, $j > 2$, using the knowledge of the previous $a_1, \ldots, a_{j-1}$ since using Equations 6.2,

$$a_j = \frac{1}{2a_1} \sum_{i=2}^{j-1} a_i a_{j-i+1}.$$

Hence, the matrix M can be built and $J(\lambda, d)$ is a square.
Proof of 2): First, we define Z as

$$Z = J(0, l)^2 = \begin{pmatrix} 0 & 0 & 1 & \ldots & 0 \\ & 0 & 0 & & \vdots \\ & & \ddots & \ddots & 1 \\ & 0 & & & 0 \\ & & & & 0 \end{pmatrix}.$$

The goal is to find the Jordan canonical form of Z. Clearly all its eigenvalues are 0. It suffices to determine the size of its Jordan blocks. For all $1 \leqslant k \leqslant \lfloor l/2 \rfloor$, Z^k is a matrix with 1s in the $2k^{th}$

upper-diagonal and 0s everywhere else, i.e.,

$$Z^k = \begin{pmatrix} \overbrace{0\dots0}^{2k} & 1 & 0 & \dots & 0 \\ & & \ddots & \ddots & \vdots \\ & & & 1 & 0 \\ & 0 & & & 1 \\ & & & & \end{pmatrix}$$

and $\operatorname{rank}(Z-0I)^k = \operatorname{rank} Z^k = \max(l-2k,0)$. Using the formula of Lemma 6.9, the number of Jordan blocks of Z of size d is

$$\max(l-2(d+1),0) - 2\max(l-2d,0) + \max(l-2(d-1),0).$$

If l is even then

$$\text{Number of Jordan blocks of } Z \text{ of size } d = \begin{cases} 2 & \text{if } d = l/2 \\ 0 & \text{otherwise.} \end{cases}$$

If l is odd then

$$\text{Number of Jordan blocks of } Z \text{ of size } d = \begin{cases} 1 & \text{if } d = (l-1)/2 \\ 1 & \text{if } d = (l+1)/2 \\ 0 & \text{otherwise.} \end{cases}$$

The last statement of 2) comes from the fact that if $A \sim B^2$, i.e., $A = SB^2S^{-1}$, then $A = C^2$ for $C = SBS^{-1}$. This finishes the proof of 2).

Proof of 3): In characteristic 2, we have

$$J(\mu,l)^2 = \begin{pmatrix} \mu^2 & 2\mu & 1 & \dots & 0 \\ & \mu^2 & 2\mu & \ddots & \vdots \\ & & \ddots & \ddots & 1 \\ & 0 & & & 2\mu \\ & & & & \mu^2 \end{pmatrix} = \begin{pmatrix} \mu^2 & 0 & 1 & \dots & 0 \\ & \mu^2 & 0 & \ddots & \vdots \\ & & \ddots & \ddots & 1 \\ & 0 & & & 0 \\ & & & & \mu^2 \end{pmatrix}.$$

All the eigenvalues of this matrix are μ^2 and as before, let us find the size of the Jordan blocks associated to it. If $W = J(\mu, l)^2 - \mu^2 \cdot I$, then $W = Z$ (c.f. 2)) and the same result is still true. This proves 3).

Let M be a matrix with $N = M^2$, i.e.,

$$\begin{aligned} M &\sim \mathrm{Diag}(J(\mu_1, d_1), \ldots, J(\mu_k, d_k)) \ , \\ N &\sim \mathrm{Diag}(J(\mu_1, d_1)^2, \ldots, J(\mu_k, d_k)^2). \end{aligned}$$

If $\mathrm{char}\,\mathbb{F} = 2$ then we apply 3) to each Jordan block with $d_i > 1$ and if $\mathrm{char}\,\mathbb{F} \neq 2$ then we apply 2) to each Jordan block associated to 0 with $d_i > 0$. In each case we see that the conditions stated in the theorem are necessary. To see that they are also sufficient, suppose that the Jordan canonical form of N satisfies them. Without loss of generality, we can assume that

$$N \sim \mathrm{Diag}(J_1, J_2, J_3)$$

where: J_1 is a block that contains all the Jordan blocks with non-zero eigenvalues (if any) placed such that the elements of every couple $(J(\lambda, d), J(\lambda, d))$ or $(J(\lambda, d), J(\lambda, d-1))$ are consecutive, J_2 contains all the Jordan blocks with eigenvalues zero placed (if any) such that the elements of every couple $(J(0, d), J(0, d))$ or $(J(0, d), J(0, d-1))$ are consecutive, and finally where J_3 is a diagonal matrix.

If $\mathrm{char}\,\mathbb{F} \neq 2$: Because of 1), there exists a block M_1, built from matrices whose square are the Jordan blocks of J_1 such that $M_1^2 = J_1$. Because of 2), there exists a block M_2, built from matrices whose square are the Jordan blocks of J_2 such that $M_2^2 = J_2$. J_3 being diagonal, the diagonal matrix M_3 whose diagonal elements are square roots of the diagonal elements of J_3 satisfies $M_3^2 = J_3$. Therefore $\mathrm{Diag}(M_1, M_2, M_3)^2 = \mathrm{Diag}(J_1, J_2, J_3)$ and N is equivalent to the

square of a matrix, i.e., N is a square of a matrix.
If $\mathrm{char}\,\mathbb{F} = 2$: Because of 3), there exists two blocks M_1 and M_2, built from matrices whose square are the Jordan blocks of J_1 and J_2 such that $M_i^2 = J_i$, $i = 1, 2$. J_3 being diagonal, the diagonal matrix M_3 whose diagonal elements are square roots of the diagonal elements of J_3 satisfies $M_3^2 = J_3$. Therefore $\mathrm{Diag}(M_1, M_2, M_3)^2 = \mathrm{Diag}(J_1, J_2, J_3)$ and the same remark above applies.
This completes the proof of the theorem. □

Remark 6.11 There exists an expected polynomial-time algorithm that produces the Jordan canonical form of a matrix over a finite field (c.f. [58]). It is not difficult to deduce from the proof of the previous theorem an expected polynomial-time algorithm that will produce a square root of a matrix as long as it possesses one.

Example 6.12 A matrix N with Jordan blocks

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

is a square if and only if the characteristic of the field is different from 2.

Let us now build an example where the reduction used in the proof of Proposition 6.7 is useless. First, the matrix a should be chosen such that $a^2 - 1$ is not a square. Let

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad a^2 - 1 = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Theorem 6.10 shows that $a^2 - 1$ is not a square. It is also not difficult to see (e.g. [16]) that

$$T_n(a) = \begin{pmatrix} T_n(1) & T_n'(1) \\ 0 & T_n(1) \end{pmatrix} = \begin{pmatrix} 1 & T_n'(1) \\ 0 & 1 \end{pmatrix} = b$$

and the problem of finding n such that $T_n(a) = b$ simply reduces to find n such that $T'_n(1) = b_{22}$.

Lemma 6.13 *For all* $n \geqslant 1$, $T_n(1)' = n^2$ *and* $T_n(-1)' = (-1)^n n^2$.

Proof: The proof is an induction on n. First, the statement is true for $n = 1, 2$; suppose it is true for all $k \leqslant n$. Then using Property 2. of 6.2 and the induction hypothesis, we have

$$T'_{n+1}(1) = 2T_n(1)+2T'_n(1)-T'_{n-1}(1) = 2+2n^2-(n-1)^2 = (n+1)^2.$$

The proof is the same with -1. □

Now, it is clear that the discrete Chebyshev problem in any finite field with this particular a is an easy problem, since it suffices to solve $n^2 = b_{22}$ in order to solve this instance of discrete Chebyshev problem.

This particular example also gives the idea that any discrete Chebyshev problem in $\mathrm{Mat}_n(\mathbb{F}_q)$ will always boil down to either a square root problem in $\mathbb{F}_q$ or several DLP in some small extension field. Indeed, if the matrix a possesses a square root, then the proof of Proposition 6.7 shows that it suffices to solve a DLP in $\mathrm{Mat}_n(\mathbb{F})$ where $\mathbb{F}$ is a small extension fields of $\mathbb{F}_q$. On the other hand, if the matrix a does not possess a square root in any field extension then because of Theorem 6.10, it has at least one Jordan block of dimension at least 2 associated to the eigenvalue ± 1. Using Jordan decomposition techniques and the fact that (e.g. [16])

$$T_n(J(\pm 1, d)) = \begin{pmatrix} T_n(\pm 1) & T'_n(\pm 1) & & * \\ & T_n(\pm 1) & T'_n(\pm 1) & \\ & & \ddots & \\ & 0 & \ddots & T'_n(\pm 1) \\ & & & T_n(\pm 1) \end{pmatrix},$$

the same phenomenon appearing in the previous example can be used to reduce the problem, via Lemma 6.13, to a square root problem in $\mathbb{F}_q$. We have proven the following proposition:

Proposition 6.14 *Let $\mathbb{F}_q$ be a finite field of odd characteristic.*

1. *The discrete Chebyshev problem in $\mathrm{Mat}_n(\mathbb{F}_q)$ with parameters a and $b = T_l(a)$ reduces the DLP in some small extension field of $\mathbb{F}_q$ when $a^2 - 1$ is a square in $\mathrm{Mat}_n(\overline{\mathbb{F}_q})$.*

2. *The discrete Chebyshev problem in $\mathrm{Mat}_n(\mathbb{F}_q)$ with parameters $a \in \mathrm{Mat}_n(\mathbb{F}_q)$ and $b = T_l(a)$ reduces to SQROOT in $\mathbb{F}_q$ when $a^2 - 1$ is not a square in $\mathrm{Mat}_n(\overline{\mathbb{F}_q})$.*

The consequence of the theorem is that the discrete Chebyshev problem in $\mathrm{Mat}_n(\mathbb{F}_q)$ is not appropriate for cryptographic purpose. Indeed the key size is much larger in that case compared to the key size of the usual cryptosystems based on the DLP in $\mathbb{F}_q$ for the same level of security. The next section describes a choice of ring R that will produce a hard problem not directly connecting to a DLP in R^*.

6.4 The discrete Chebyshev problem and RSA integers

The difficulty of finding square roots modulo an RSA number has already been used in the conception of the Rabin cryptosystem as shown in the Introduction. In this section we consider $R = \mathbb{Z}_n$, with $n = pq$ an RSA number and study the relationship between the discrete Chebyshev problem in R and FACTORING. First, the reduction of the discrete Chebyshev problem to the DLP in

the proof of Proposition 6.7 is clearly not computationally feasible because of the difficulty of SQROOT. Therefore the discrete Chebyshev problem in R seems to be different than the DLP in R.

For an integer b, any integer $e \neq 0$ with the property that

$$b^e \equiv 1 \mod n$$

is called an *exponent* for b modulo n. Here is a key point of this study based on the relationship of computation of exponents and DLP:

Lemma 6.15 *Let n be an RSA number. If there exists a polynomial time algorithm that provides for each $b \in \mathbb{Z}_n^*$ an exponent for b modulo n, then one can factor n in expected polynomial time.*

The Lemma is an extension of a result of [1] and is in essence Theorem 6.6 of [56]. This result is usually used in the reduction of the factoring problem to the DLP in $\mathbb{Z}_n^*$.

Theorem 6.16 *Let n be an RSA number. Then*

1. *If one can factor n and solve the DLP modulo each prime factor of n in polynomial time, then one can solve the discrete Chebyshev problem in $\mathbb{Z}_n$ in polynomial time.*

2. *If one can solve the discrete Chebyshev problem in $\mathbb{Z}_n$ in polynomial time, one can factor n in expected polynomial time.*

Proof: The proof of 1. comes from the feasibility of the reduction of the discrete Chebyshev problem to the DLP used in the proof of Proposition 6.7 (Note that since n is an RSA number, n is odd and $\frac{1}{2}$ has a meaning). Let us now prove the second point by showing that if one can solve the discrete Chebyshev problem in polynomial time then one can find either exponents modulo n or a factorization

of n in polynomial time. Let $b \in \mathbb{Z}_n^*$ and p be a prime such that p does not divide $\varphi(n)$. First, note that such a p exists amongst the first $\lfloor \log_2 n \rfloor + 1$ primes since otherwise if

$$d := 2 \cdot 3 \cdot \ldots \cdot p_{\lfloor \log_2 n \rfloor + 1}$$

then

$$d > 2^{\lfloor \log_2 n \rfloor + 1} > 2^{\log_2 n} = n > \varphi(n) \quad \text{and} \quad d | \varphi(n)$$

which is a contradiction. Therefore such a prime p can be found in polynomial time. If $a \equiv b^p \mod n$ then $a \in \mathbb{Z}_n^*$. The reduction of the DLP to the discrete Chebyshev problem used in the proof of Proposition 6.7 shows that if $x = \frac{1}{2}(a + a^{-1})$ and $y = \frac{1}{2}(b + b^{-1})$ then

$$\begin{aligned} T_k(x) = y \text{ in } R &\iff (a^k - b) \cdot \left(a^k - \frac{1}{b} \right) = 0 \text{ in } R \\ &\iff (a^k - b) \cdot \left(a^k - \frac{1}{b} \right) \equiv 0 \mod n. \end{aligned}$$

Then if $T_k(x) = y$, either

$$a^k = b \text{ in } R \quad \text{or} \quad a^k = b^{-1} \text{ in } R \quad \text{or} \quad \gcd(a^k - b\,,\, n) \neq 1,$$

i.e.,

either $pk - 1$ is an exponent of b modulo n,

or $pk + 1$ is an exponent of b modulo n,

or $\gcd(a^k - b\,,\, n)$ is a non-trivial divisor of n.

In any case, by solving the discrete Chebyshev problem $T_k(x) = y$, we have found in polynomial time either an exponent of b modulo n or the factorization of n. Using Lemma 6.15, the result is then clear. □

6.5 Conclusion

In this chapter, we have studied the action of Chebyshev polynomials on different finite rings R. We have studied the difficulty of the discrete Chebyshev problem in these rings.

1. When $R = \mathbb{F}_q$, we have shown that the discrete Chebyshev problem is computationally equivalent to the DLP in $\mathbb{F}_q^*$.

2. When $R = \mathrm{Mat}_n(\mathbb{F}_q)$, We have shown that the discrete Chebyshev problem is no more difficult than the DLP in some small extension field of $\mathbb{F}_q$.

3. When $R = \mathbb{Z}_n$, with n an RSA integer, we have shown that if one can solve the discrete Chebyshev problem in polynomial time, on can factor n in expected polynomial time.

Chapter 7

PAIGE LOOPS AND SEMIGROUP ACTION PROBLEMS

In this chapter, the stucture of Moufang loops and Paige loops is presented. We study the DLP in the Paige loop $M^*(q)$ and a semigroup action problem based on exponentiation and conjugation in the Moufang loop $M(q)$ is analyzed.

7.1 Loops, Moufang loops and Paige loops

Definition 7.1 Let L be a set with a binary operation $(a, b) \longmapsto ab$. Then L is a *loop* if:

i) For $a, b, c \in L$, the knowledge of any two elements in the equation $ab = c$ uniquely specifies the third.

ii) There exists a neutral element e such that $ea = ae = a$ for all $a \in L$.

It can be shown by a standard argument that the neutral element is unique. The important point in the previous definition is the absence of rules concerning the associativity of the binary operation. A loop is associative when it is specified that the associative law applies to the operation. Even without this requirement, loop theory is very close to group theory. The next concepts are examples of such a similarity. A loop homomorphism is defined in the same way as in group theory. A *sub-loop* P of a loop L is a subset of L that is closed under the operation and such that the restriction of the operation gives P the structure of a loop. A sub-loop P is normal if

$$aP = Pa \ , \ (aP)b = a(Pb) \ , \ a(bP) = (ab)P$$

for all a, b in L. A congruence relation in a loop L is an equivalence relation $\sim$ such that

$$a \sim b \Longrightarrow \begin{cases} ac \sim bc \ \ \forall c \in L, \\ ca \sim cb \ \ \forall c \in L. \end{cases}$$

This notion is closer to the notion of congruence relation in groups than in semigroups. Indeed, the following proposition shows that both are equivalent, contrary to the case of semigroups where the notion of c-simplicity had to be created to capture the essence we were looking for.

Proposition 7.2 *Let L be a loop. If P is a normal sub-loop of L then the relation $\sim$ such that $a \sim b \iff a \in bP$ is a congruence relation in L. Reciprocally, if $\sim$ is a congruence relation in L, then $P = \{a \in L \mid a \sim e\}$ is a normal sub-loop of L.*

Since no proof of this result has been found in the literature and because of its importance from our point of view, we give here a proof of it:

Proof: Suppose P is a normal sub-loop of L. The proof that $\sim$ is an equivalence relation is the same as in group theory, so we skip it. Now if $a \sim b$ then $a = bp$ for some p in P. Therefore $ac = (bp)c$ and since P is normal we can write $(bp)c = b(p'c) = b(cp'') = (bc)p'''$ for some p', p'', p''' in P. Thus $ac \sim bc$ for all c in L. The proof that $ca \sim cb$ is similar.

Suppose $\sim$ is a congruence relation and let us check that the set P defined in the statement is a normal sub-loop. The fact that $a \sim e$ and $b \sim e$ implies $ab \sim eb \sim ee = e$ shows that P is stable under the operation. Clearly $e \in P$. The properties of a loop are inherited from L. Moreover, since $ap \sim ae = a = ea \sim p'a$, $(ap)b \sim (ae)b = ab = a(eb) \sim a(p'b)$ and $a(bp) \sim a(be) = ab = a(be) \sim a(bp')$ for all $p, p' \in P$, the sub-loop P is normal. □

Definition 7.3 A loop L is simple if it has no proper normal sub-loop or equivalently if it has no non-trivial congruence relation.

In order to understand the vast variety of loops, one habitually studies loops satisfying some weak form of associativity:

Definition 7.4 A loop M is called a Moufang loop if the Moufang identities

$$\begin{aligned} (ab)(ca) &= a((bc)a) \\ a(b(ac)) &= ((ab)a)c \\ a(b(cb)) &= (a(bc))b \end{aligned}$$

are satisfies for every a, b, c in M.

Ruth Moufang first studied these objects in 1935 [63]. The next proposition states the most remarquable results concerning Moufang loops. We refer the reader to [68] for the proofs.

Proposition 7.5 *Let M be a Moufang loop. Then*

1. *Any two of the three Moufang identities imply the third.*

2. *Every element in M has a unique both-sided inverse.*

3. *(Moufang Theorem [63]) Let a, b, c be elements in M. The smallest sub-loop containing a, b, c, $\langle a, b, c\rangle$, is associative if and only if $(ab)c = a(bc)$.*

4. *Any sub-loop that is two-generated, i.e., of type $\langle a, b\rangle$, is associative. Thus, it is a group.*

Statement 4. of the proposition shows that the order $\operatorname{ord} x$ of an element x in a Moufang loop is well-defined. We are now ready to define the main subject of this chapter:

Definition 7.6 A Moufang loop M is a Paige loop if it is non-associative, finite and simple.

Statement 2. of Proposition 7.5 shows that Paige loops can be considered as simple groups, without the associative law. Note that because of Theorems 3.7 and 3.8, studying simple non-associative objects is "a last chance" to discover interesting actions from conceptually new objects.

Paige loops have been discovered by L. Paige in 1956 [67] who constructed such a loop based on every finite field $\mathbb{F}_q$. Thirty years later, M. Liebeck [44] proved that there are no other Paige loops. We will denote the unique Paige loop constructed over $\mathbb{F}_q$ by $M^*(q)$, as in [89]. The following constructive description of $M^*(q)$ is due to M. Zorn.

Let $\mathbb{F}_q$ be a fixed finite field. For $\alpha, \beta \in \mathbb{F}_q^3$, let $\alpha \cdot \beta$ denote the standard dot product and $\alpha \times \beta$ the standard vector product:

$$\begin{aligned} \alpha \cdot \beta &= \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3, \\ \alpha \times \beta &= (\alpha_2\beta_3 - \alpha_3\beta_2, \alpha_3\beta_1 - \alpha_1\beta_3, \alpha_1\beta_2 - \alpha_2\beta_1). \end{aligned}$$

The *Zorn algebra* $Z(q)$ is the set of 2×2 matrices

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \text{ where } a, b \in \mathbb{F} \text{ and } \alpha, \beta \in \mathbb{F}_q^3,$$

with the following multiplication:

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \cdot \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha \cdot \delta & a\gamma + d\alpha - \beta \times \delta \\ c\beta + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{pmatrix}. \quad (7.1)$$

We do not discuss here the properties of the Zorn algebra such as the existence of a non-degenerate quadratic form that makes $Z(q)$ a split composition algebra [89]. The notions of determinant and trace will however be needed in the sequel. Let us define these objects:

The determinant of an element in the Zorn algebra is defined by

$$\det \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} = ab - \alpha \cdot \beta.$$

Surprisingly enough, the determinant is still multiplicative, i.e., the identity

$$\det(x \cdot y) = \det x \cdot \det y$$

is fulfilled for all elements x, y in $Z(q)$. An element of $Z(q)$ has a multiplicative inverse if and only if its determinant is nonzero. In such a case,

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}^{-1} = \frac{1}{ab - \alpha \cdot \beta} \begin{pmatrix} b & -\alpha \\ -\beta & a \end{pmatrix}.$$

An easy argument shows that if an element x possesses an inverse in $Z(q)$, then $x^{-1} = x^{\operatorname{ord} x - 1}$. All the elements in $Z(q)$ with nonzero determinant form a Moufang loop, as well as all elements with determinant 1. Let us denote this latter loop by $M(q)$. The neutral element is clearly

$$e = \begin{pmatrix} 1 & (0,0,0) \\ (0,0,0) & 1 \end{pmatrix}$$

and the set $\{e, -e\}$ is the unique normal sub-loop of $M(q)$, which is also the biggest commutative and associative sub-loop of $M(q)$ [89].

Definition 7.7 For each finite field $\mathbb{F}_q$, the Paige loop $M^*(q)$ is defined as the quotient loop $M(q)/\!\sim$, where $\sim$ is the congruence relation induced by the normal sub-loop $\{e, -e\}$ given by Proposition 7.2.

It will be convenient to work with $M(q)$ instead of $M^*(q)$, keeping in mind that the operations are to be considered modulo $\sim$. From a computational point of view, working either in $M(q)$ or in $M^*(q)$ is equivalent. Indeed, for each class in $M^*(q)$, there is at most two possible elements in it in $M(q)$ and each computation in $M^*(q)$ can be lifted to at most two computations in $M(q)$.

L. Paige gave the cardinality of $M^*(q)$ [67] with

$$|M^*(q)| = \begin{cases} q^3(q^4-1) & \text{if } q \text{ is even,} \\ \frac{q^3(q^4-1)}{2} & \text{if } q \text{ is odd.} \end{cases}$$

P. Vojtěchovský showed that any Paige loop is three-generated, i.e., is of type $\langle a, b, c \rangle$, and gave different families of generators [89].

The trace of an element in the Zorn algebra is defined by

$$\operatorname{tr} \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} = a + b.$$

Clearly the trace is $\mathbb{F}_q$-linear. It also satisfies the equality

$$\mathrm{tr}\,(x \cdot y) = \mathrm{tr}\,(y \cdot x)$$

because of the similarity of the diagonal elements of $x \cdot y$ with the usual matrix multiplication. The determinant together with the trace satisfy the following analogue to Cayley-Hamilton Theorem:

Proposition 7.8 *Any element x of the Zorn algebra $Z(q)$ satisfies the equation*

$$x^2 - \mathrm{tr}\,(x)x + \det(x)e = 0.$$

The proof is a straightforward computation. One can also notice that the algebraic expression of x^2 is the same when we consider α and β as element in $\mathbb{F}_q$. Cayley-Hamilton theorem being true in $\mathrm{Mat}_2(\mathbb{F}_q)$, the result is valid as well in $Z(q)$.

7.2 The DLP in $M^*(q)$

This section presents the study of the discrete logarithm problem in the Paige loop $M^*(q)$. It will be shown that the problem completely reduces to the discrete logarithm problem in a quotient of $SL_2(\mathbb{F}_q)$, namely in

$$L_2(q) = SL_2(\mathbb{F}_q)/\{\pm I\} = \{M \in GL_2(\mathbb{F}_q) \mid \det M = 1\}/\{\pm I\}.$$

This reduction is possible due to a group isomorphism ω that maps a 1-generated sub-loop $\langle x \rangle$ of $M^*(q)$ into a sub-group of $L_2(q)$. This group homomorphism already exists in essence in Proposition 3.6 of [89]. However, we believe that the proof of the injectivity is false, which is a crucial point in the development of the theory. Therefore, we present here a complete proof of the statement. We need first a nice representation of elements in $\langle x \rangle$ given by the next lemma.

Lemma 7.9 *Let x be in $M^*(q)$ and $y \in \langle x \rangle$. Then*

$$x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \Longrightarrow y = \begin{pmatrix} c & s\alpha \\ s\beta & d \end{pmatrix}$$

for some $c, d, s \in \mathbb{F}_q$. If $\alpha = \beta = 0$, then by setting $s = 0$, every element $y \in \langle x \rangle$ has a unique representation as above.

Proof: Using the Zorn multiplication formula (7.1) and the fact that $\alpha \times \alpha = \beta \times \beta = 0$, it is easy to check by induction on n that

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}^n = \begin{pmatrix} c_n & s_n\alpha \\ t_n\beta & d_n \end{pmatrix} \tag{7.2}$$

with $c_n, d_n \in \mathbb{F}_q[a, b, \alpha \cdot \beta]$ and $s_n, t_n \in \mathbb{F}_q[a, b]$. In particular, the coefficients s_n and t_n do not depend on the parameters α and β. Thus we may replace α, β by any other variables and the values of s_n and t_n will not change in (7.2). Therefore

$$\begin{pmatrix} * & s_n \\ t_n & * \end{pmatrix} = \begin{pmatrix} a & 1 \\ 1 & b \end{pmatrix}^n$$

and the right-hand-side being a symmetric matrix, $s_n = t_n$ for all n. The last part of the statement is clear. □

Proposition 7.10 *Let x and y be as in Lemma 7.9 and define $\omega : \langle x \rangle \longrightarrow L_2(q)$ by*

$$\omega(y) = \omega \begin{pmatrix} c & s\alpha \\ s\beta & d \end{pmatrix} = \begin{pmatrix} c & s\alpha \cdot \beta \\ s & d \end{pmatrix}.$$

Then ω is an injective group homomorphism.

Proof: First, ω is well defined by Lemma 7.9. A straightforward computation shows that ω is a group homomorphism. It is also injective since the representation of y in Lemma 7.9 implies that

$$\omega(y) = 1_{L_2(q)} \Longrightarrow y = e.$$

This proves the proposition. □

A polynomial-time reduction from the DLP in $M^*(q)$ to the DLP in $\mathbb{F}_q$ can easily be deduced from this proposition. Here it is:

Algorithm 7.11 Given q a power of a prime number, $x \in M^*(q)$ and $y \in \langle x \rangle$, this algorithm finds an integer n such that $x^n = y$ using a call to an oracle that solve the DLP in $SL_2(\mathbb{F}_q)$.

1. Set $M = \omega(x)$ and $N = \omega(y)$. Consider both M and N as elements of $SL_2(\mathbb{F}_q)$.
2. Solve the DLP $M^n = N$ in $SL_2(\mathbb{F}_q)$ using the known reduction [58] to the DLP in $\mathbb{F}_q$.
3. Output n.

Proposition 7.12 *Algorithm 7.11 finds an integer n that solves the DLP in $M^*(q)$.*

Proof: Since $\omega(x^n) = \omega(x)^n = M^n = N = \omega(y)$, the result follows from the injectivity of ω. □

Remark 7.13 The algorithm presented in the next section will also solve, as a special case, the DLP in $M^*(q)$ using another method. However the previous algorithm uses the strong connection between a one-generated sub-loop of $M^*(q)$ and group theory, which enlightens the situation.

7.3 Exponentiation and conjugation in $M(q)$

The next action tries to take advantage of the absence of eigenvalues in $M(q)$. Indeed, the heart of the (yet hidden) reduction

presented in the previous section lies in the resolution of the DLP in $SL_2(\mathbb{F}_q)$ that can be accomplished using the eigenvalues of the matrices in this linear group. Here, using conjugation, we avoid the possible use of the homomorphism ω. The use of $M(q)$ instead of $M^*(q)$ is justified mainly because of the absence of choice of class elements. Since every class possesses at most 2 elements, the use of $M(q)$ has no computational consequences: $M(q)$ is not simple, but it is up to a quotient by $\{\pm I\}$.

Let C be a commutative and associative sub-loop of $Z(q)$. For example

$$C = \langle z \rangle \text{ or } C = \{az + be | a, b \in \mathbb{F}_q\,,\ \det(az + be) \neq 0\}.$$

Then the current action will be the following (c.f. Example 3.4):

$$\begin{array}{rcl} (C \times \mathbb{Z}) \times M(q) & \longrightarrow & M(q) \\ (c, n), g & \longmapsto & cg^n c^{-1} \end{array} \tag{7.3}$$

Note that the conjugation uses the full power of the Zorn multiplication, i.e., the product $cg^n c^{-1}$ makes appear the "twist" of the vector product in 7.1. Note as well that the conjugation is well defined according to Moufang's theorem. Indeed the sub-loop $\langle c, g \rangle$ is two-generated, and the operation is associative inside it.

We want here to point out that the situation is different than when the actual objects are matrices over fields. The possibility to transform a matrix into a triangular one via conjugation can be used over $Gl_2(\mathbb{F})$ in order to solve the analogue semigroup action problem of 7.3 in this algebraic group solving at most two DLPs in $\mathbb{F}$. Indeed, if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^n = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \text{ and } \begin{pmatrix} a & b \\ c & d \end{pmatrix} = M \begin{pmatrix} \lambda & w \\ 0 & \mu \end{pmatrix} M^{-1}$$

then

$$\begin{pmatrix} \lambda^n & w' \\ 0 & \mu^n \end{pmatrix} = M^{-1} \begin{pmatrix} r & s \\ t & u \end{pmatrix} M = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix},$$

and this last equation yield the resolution of the DLPs in $\mathbb{F}$. However, playing with Moufang loops makes the situation completely different. Given a element g in $M(q)$, even if one can transform it using conjugation into an element $\widetilde{g}$ which is "upper-triangular", say $\widetilde{g} = vgv^{-1}$ for some $v \in M(q)$ (which is moreover not possible in general), one may not be able to find an element in $u \in \langle c, g \rangle$ in order to have $\widetilde{g} = ugu^{-1}$. The associativity being not a general rule in $M(q)$, any expression of type $\widetilde{g} = vgv^{-1}$ will not help in the resolution of the SAP.

Under some conditions, the linearity of the trace together with the equation of Proposition 7.8 will however allow a reduction of the associated semigroup action problem to the DLP in $\mathbb{F}_q$ via Chebyshev polynomials, when q is odd. When q is even, i.e., $q = 2^d$, the reduction can be realized using specific properties of finite field of characteristic 2.

First note that because of the property of the trace, one has

$$\operatorname{tr}(cg^n c^{-1}) = \operatorname{tr}(g^n cc^{-1}) = \operatorname{tr}(g^n). \tag{7.4}$$

This shows that the trace is invariant under conjugation. The invariance can be used as follows:

Proposition 7.14 *Let $c, g \in M(q)$. If $u_n = \operatorname{tr}(cg^n c^{-1})$ then:*

1. *The sequence $\{u_n\}_{n \in \mathbb{N}}$ satisfies the second order linear recurrence relation*

$$u_{n+2} - \tau u_{n+1} + u_n = 0$$

where $\tau = \operatorname{tr}(g) = u_1$.

2. If q is odd, then the sequence $\{u_n\}_{n\in\mathbb{N}}$ satisfies

$$u_n/2 = T_n(\tau/2)$$

where T_n is the n^{th} Chebyshev polynomial and τ is as above.

Proof: 1. By Proposition 7.8 and Equation 7.4, we have

$$\begin{aligned} 0 &= \operatorname{tr}(g^n(\underbrace{g^2 - \operatorname{tr}(g)g + 1}_{=0})) \\ &= \operatorname{tr}(g^{n+2} - \operatorname{tr}(g)g^{n+1} + g^n) \\ &= \operatorname{tr}(g^{n+2}) - \tau\operatorname{tr}(g^{n+1}) + \operatorname{tr}(g^n) \\ &= \operatorname{tr}(cg^{n+2}c^{-1}) - \tau\operatorname{tr}(cg^{n+1}c^{-1}) + \operatorname{tr}(cg^nc^{-1}) \\ &= u_{n+2} - \tau u_{n+1} + u_n. \end{aligned}$$

2. The sequence $T_n(\tau/2)$ satisfies the second order linear recurrence relation stated in 1. (see Proposition 6.2). It suffices therefore to check that $T_i(\tau/2) = u_i/2$, $i = 0, 1$. This is done with

$$T_0(\tau/2) = 1 = u_0/2 \text{ and } T_1(\tau/2) = \tau/2 = u_1/2.$$

□

Proposition 7.15 *For fixed $g \in M(q)$ with $\operatorname{tr} g \neq \pm 2$ and $\tau \in \mathbb{F}_q$, there is at most two solutions of the equation $\operatorname{tr}(g^n) = \tau$ with $0 \leqslant n < \operatorname{ord} g$.*

Proof: Suppose the equation possesses at least one solution. Using Proposition 7.8 and the condition $\operatorname{tr}(g) \neq \pm 2$, we see that each element in $\langle g\rangle$ has a unique representation in $\mathbb{F}_q g + \mathbb{F}_q e$. If we write $g^n = ag + be$ with $a, b \in \mathbb{F}_q$, the proof would follow from the

existence of at most two solutions of the equation $\mathrm{tr}\,(ag+be)=\tau$ with unknown a, b. A direct computation shows that

$$1 = \det g^n = \det(ag+be) = a^2 + ab\mathrm{tr}\,(g) + b^2$$

and

$$\tau = \mathrm{tr}\,(g^n) = a\mathrm{tr}\,(g) + 2b.$$

It follows from these two equations that $a^2 \cdot (\mathrm{tr}\,(g)^2 - 4) = \tau^2 - 4$. So if $\mathrm{tr}\,(g) \neq \pm 2$, the field element a is determined up to a sign as

$$a = \pm\sqrt{\frac{\tau^2-4}{\mathrm{tr}\,(g)^2-4}}$$

and then b is determined by the first of the above equations (the second equation could be useless when $\mathrm{char}\,\mathbb{F} = 2$). This proves the statement. □

Proposition 7.16 *The semigroup action problem induced by the action 7.3 in* $M(q)$ *with parameter* $g \in M(q)$ *satisfying* $\mathrm{tr}\,(g) \neq \pm 2$ *reduces to the DLP in* $\mathbb{F}_q(\lambda)$ *where* λ *is any root of the equation* $x^2 - \mathrm{tr}\,(g)x + 1 = 0$.

Proof: For given g, y and C, the SAP asks to find n and $c \in C$ such that $y = cg^n c^{-1}$ in $M(q)$. The first point of Proposition 7.14 being true in any characteristic, the integer n can be found by solving the equation

$$u_n = \mathrm{tr}\,(y) \tag{7.5}$$

where

$$u_{n+2} - \tau u_{n+1} + u_n = 0 \quad \text{and} \quad u_1 = \tau = \mathrm{tr}\,(g)\ ,\ u_0 = \mathrm{tr}\,(g^0) = 2.$$

Let λ be a root of $x^2 - \tau x + 1 = 0$. One can easily check that $u_n = \lambda^n + \lambda^{-n}$. Indeed the right-hand-side satisfies the recurrence

relation and is equal to u_0 and u_1 when n is 0 and 1. Therefore, combining Equation 7.5 we have

$$\lambda^{2n} - \mathrm{tr}\,(y)\lambda^n + 1 = 0.$$

In other words, λ^n is one of the roots of the quadratic equation $x^2 - \mathrm{tr}\,(y)x + 1 = 0$. We see by the way that the roots of the previous equation are in $\mathbb{F}_q(\lambda)$. Let n_1 and n_2 be the solutions of these two DLPs in λ. Note that $n_2 = |\mathbb{F}_q(\lambda)|^* - n_1$ and therefore only one DLP has to be solved in order to compute both n_1 and n_2. Using Proposition 7.15, we see that one of the n_i gives the desired n. The element c is then found by solving the linear system of equations in the entries of c in $\mathbb{F}_q$ that is equivalent to the equation $yc = cg^n$ with known n, g and y. □

Remark 7.17 When q is odd, the proof of the previous proposition could have been based on the resolution of a Discrete Chebyshev Problem using the second point of Proposition 7.14.

On the way of the proof, we had to solve quadratic equations in $\mathbb{F}_{2^d}$ when n is even. Since the usual school formula does not hold when the characteristic is even, let us explain how this can be done. We follow [4] and [7]. Recall that the *trace* of an element β in $\mathbb{F}_{2^d}$ is the element in $\mathbb{F}_2$ defined by

$$\mathrm{Tr}_{2^d|2}\,(\beta) = \beta^2 + \beta^4 + ... + \beta^{2^{d-1}} = \sum_{j=1}^{d-1} \beta^{2^j}.$$

Lemma 7.18 *Consider the following quadratic equation over* $\mathbb{F}_{2^d}$*:*

$$x^2 + x + \beta = 0. \tag{7.6}$$

Then 7.6 possesses solutions in $\mathbb{F}_{2^d}$ *if and only if* $\mathrm{Tr}_{2^d|2}\,(\beta) = 0$*. In this case the solutions* x_0 *and* $x_0 + 1$ *are given by*

1. $x_0 = \sum_{j=0}^{(d-1)/2} \beta^{2^{2j}}$ *if* d *is odd,*
2. $x_0 = \sum_{i=0}^{d-2} \left(\sum_{j=i+1}^{d-1} \delta^{2^j} \right) \beta^{2^j}$ *if* d *is even, where* $\delta \in \mathbb{F}_{2^d}$ *is any element such that* $\mathrm{Tr}_{2^d|2}(\delta) = 1$.

The proof is a straightforward computation. The lemma also shows how one would explicitly find the roots of a second degree polynomial. Note that an element δ appearing when n is even in the lemma is easily found by choosing random elements in the field: the probability of selecting such an element is $1/2$. Since any quadratic equations over $\mathbb{F}_{2^d}$ can be reduced to the form of Equation 7.6 after a suitable linear change of variable, the problem of solving such polynomial equations is settled.

When $\mathrm{tr}(g) \neq \pm 2$, a polynomial time reduction from the SAP (7.3) in $M(q)$ to the DLP in a small extension of $\mathbb{F}_q$ can easily be deduced from Proposition 7.16. Here it is:

Algorithm 7.19 Given q a power of a prime number, $g \in M(q)$ with $\mathrm{tr}(g) \neq \pm 2$, $C = \langle z \rangle$ and $y = c' g^{n'} (c')^{-1}$ with $c' \in C$, this algorithm finds an integer n and an element $c \in C$ such that $cg^n c^{-1} = y$ using a call to an oracle that solve the DLP in $\mathbb{F}_q(\lambda)$.

1. Solve over $\mathbb{F}_q$ the equation $x^2 - \mathrm{tr}(g)x + 1 = 0$. Let λ be one of the roots.
2. Solve over $\mathbb{F}_q(\lambda)$ the equation $x^2 - \mathrm{tr}(y)x + 1 = 0$. Let μ be one of the roots.
3. Find n such that $\lambda^n = \mu$.
4. Using linear algebra, find $c \in C$ such that $yc = g^n c$. If no such c exists, set $n \longleftarrow |F_q(\lambda)^*| - n$ and find $c \in C$ such that $yc = g^n c$.
5. Output n and c.

7.4 The case $\mathrm{tr}\,(g) = \pm 2$

Let us come back to the family of SAP instances in (7.3) with $\mathrm{tr}\,(g) = \pm 2$. We have seen that the reduction used in Proposition 7.16 leading to Algorithm 7.19 via Proposition 7.15 strongly used the fact that the square of the trace of g is not 4. There are still some cases where the problem can be solved.

Lemma 7.20 *If* $\mathrm{tr}\,(g) = -2$ *and* q *is odd, then*

$$y = cg^n c^{-1} \Longrightarrow n = \frac{2 - \mathrm{tr}\,(y)}{4}.$$

Therefore, the SAP induced by the action (7.3) is trivial with these parameters.

Proof: The result comes from the fact that $u_n = -4n + 2$ is the solution of the recurrence relation of Proposition 7.14 with $u_0 = 2$ and $u_1 = \mathrm{tr}\,(g) = -2$. In view of the end of the proof of Proposition 7.16, the statement is clear. □

This settles the case $\mathrm{tr}\,(g) = -2$, q odd. When the trace of g is 2 and q is odd, the recurrence relation of Proposition 7.14 becomes

$$u_{n+2} - 2u_{n+1} + u_n = 0 \ , \ \ u_0 = 2 \ , \ u_1 = 2$$

which gives $u_n = 2$ for all n. In the same spirit, when q is even and $\mathrm{tr}\,(g) = \pm 2 = 0$ then $u_n = 0$ is the solution of the recurrence relation and the recurrence relation is not helpful anymore. However the strong condition on both the determinant and the trace can be used in a different manner when q is even:

Lemma 7.21 *If* $\mathrm{tr}\,(g) = 0$ *and* q *is even, then* $\mathrm{ord}\, g \in \{1, 2\}$. *Therefore the SAP induced by the action (7.3) is trivial with these parameters .*

Proof: The conditions $\mathrm{tr}\,(g) = 0$ and $\det g = 1$ imply that g has the following form:

$$g = \begin{pmatrix} 1 + \sqrt{\alpha \cdot \beta} & \alpha \\ \beta & 1 + \sqrt{\alpha \cdot \beta} \end{pmatrix}.$$

From this, the equality $g^2 = e$ is straightforward. This ends the proof. □

It remains to consider the case q odd with $\mathrm{tr}\,(g) = 2$. Let us consider the analogue case with $SL_2(\mathbb{F}_q)$ instead of $M(q)$ and let us try to figure out what are the consequences of the trace condition in $SL_2(\mathbb{F}_q)$. Let G be a matrix in $SL_2(\mathbb{F}_q)$ that plays the role of the loop element g. The condition $\mathrm{tr}\,(g) = 2$ translates into $\mathrm{tr}\,(G) = 2$. In other words,

$$G \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

where $*$ is zero or 1 whether the minimal polynomial of G is $x - 1$ or $x^2 - 2x + 1$. When $* = 0$, then $G = Id$ and the SAP is trivial. When $* = 1$ then

$$G^n \sim \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

and the SAP in $SL_2(\mathbb{F}_q)$ can be solved via Jordan decomposition techniques. As explained in the beginning of Section 7.3, such a tool does not help in $M(q)$. The following proposition shows that the trace condition restricts the order of the elements.

Proposition 7.22 *Let $q = p^d$ be odd and $g \in M(q)$ with $\mathrm{tr}\,(g) = 2$. Then either $g = e$ or $\mathrm{ord}\, g = p$.*

Proof: Suppose $g \neq e$. Consider the commutative and associative sub-algebra $\mathbb{F}[g]$ of $Z(q)$. Classical ring theory shows that up to

isomorphism, $\mathbb{F}[g]$ is the quotient ring $\mathbb{F}[t]/((t-1)^2)$. Indeed the kernel of the ring epimorphism

$$\begin{array}{ccc} \mathbb{F}[t] & \longrightarrow & \mathbb{F}[g] \\ p(t) & \longmapsto & p(g) \end{array}$$

is the ideal generated by $(t-1)^2$ by Proposition 7.8. Moreover the order of g in $M(q)$ is the order of g in $\mathbb{F}[g]$. Thus

$$\operatorname{ord}(g) = \min\{e \in \mathbb{N}\backslash\{0\} \mid t^e \equiv 1 \bmod (t-1)^2 \text{ in } \mathbb{F}_q\}.$$

But since $t^p - 1 = (t-1)^p \equiv 0 \mod (t-1)^2$ in characteristic $p > 2$, we have $\operatorname{ord} g | p$. However $\operatorname{ord} g \neq 1$ since $g \neq e$ and therefore $\operatorname{ord} g = p$. □

Corollary 7.23 *Let $q = p^d$ be odd and $g \in M(q)$ with $\operatorname{tr}(g) = 2$ and $g \neq e$. Consider the semigroup action problem induced by 7.3 where C is a commutative and associative sub-loop of $Z(q)$. If $H = \{c \in C \mid cgc^{-1} = g\}$ then the cardinality of the orbit of g is given by*

$$|(C \times \mathbb{Z}) \cdot g| = \frac{p \cdot |C|}{|H|}.$$

Proof: According to the previous proposition, it is enough to consider the action of $C \times C_p$ on g where C_p is the multiplicative cyclic group of order p. The loop C being a group, we know from classical group action theory that

$$|(C \times C_p) \cdot g| = \frac{|C \times C_p|}{|H'|} = \frac{|C| \cdot p}{|H'|}$$

where $H' = \{(c, m) \mid cg^m c^{-1} = g\} < C \times C_p$. However since C_p is simple and $g \neq e$, we have $H' = \{c \in C \mid cgc^{-1} = g\} \times \{1 \in C_p\}$. This last group is isomorphic to H and the statement is proven. □

Example 7.24 Here is an example based on the action 7.3 with artificially small parameters. Let $p = 11$, with g, z and C as follows:

$$g = \begin{pmatrix} 3 & (2,3,4) \\ (1,4,1) & 10 \end{pmatrix}, \quad z = \begin{pmatrix} 3 & (3,4,10) \\ (2,4,1) & 4 \end{pmatrix}$$

and $C = \langle z \rangle$. Note that $\operatorname{tr}(g) = 2$. One can check that $|C| = p^2 - 1 = 120$ since $x^2 - \operatorname{tr}(z)x + \det(z) = x^2 - 7x + 2$ is primitive in $\mathbb{F}_{11}$ and that $|H| = |\{c \in C \mid cgc^{-1} = g\}| = 10$. Therefore the orbit of g possesses $11 \cdot 12 = 132$ elements.

Remark 7.25 Any element g in $M(p)$ with $\operatorname{tr}(g) = 2$ can be uniquely written as

$$g = \begin{pmatrix} 1 + \sqrt{-\alpha \cdot \beta} & \alpha \\ \beta & 1 - \sqrt{-\alpha \cdot \beta} \end{pmatrix}.$$

Therefore g needs roughly $6 \cdot \log_2 p$ bits to be described.

We end this chapter and work with the following question:

Question 7.26 Let g in $M(q)$, C a commutative and associative sub-loop of $Z(q)$ and h an element obtained by conjugation of an element in $\langle g \rangle$ by an element in C. Given that $\operatorname{tr}(g) = 2$ and q is odd, is there a reduction of the problem

"Find $0 \leqslant n < \operatorname{ord} g$ and $c \in C$ such that $cg^n c^{-1} = h$"

to the DLP in $\mathbb{F}_q$?

7.5 Conclusion

In this chapter, the stucture of Moufang loops and Paige loops has been developed. We have studied the DLP in the Paige loop $M^*(q)$ and a semigroup action problem based on exponentiation and conjugation in the Moufang loop $M(q)$. The DLP in $M^*(q)$ has been

shown to reduce to the usual DLP in $\mathbb{F}_q$ using the group monomorphism ω of Proposition 7.10. The semigroup action problem in $M(q)$ has been reduced to the DLP in an extension field of $\mathbb{F}_q$ of degree at most 2 when a trace condition is fulfilled. The reduction used the theory of linear recurrence relation. When the trace condition is not satisfied, the SAP is either easy to solve or presents difficulties whose relation to the DLP in finite fields is unclear.

Bibliography

[1] E. Bach. Discrete logarithms and factoring. *Report No. UCB/CSD 84/186, Computer Science Division (EECS), Univ. of California, Berkeley*, 1984.

[2] Friedrich L. Bauer. *Decrypted secrets*. Springer-Verlag, Berlin, updated edition, 2002. Methods and maxims of cryptology.

[3] S.R. Blackburn and S.D. Galbraith. Cryptanalysis of two cryptosystems based on group actions. In *Advances in Cryptology – ASIACRYPT '99*, volume 1716 of *Lecture Notes in Computer Science*, pages 52–61. Springer Verlag, Berlin, 1999.

[4] I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography*. Lecture Note Series 265. London Mathematical Society, 1999.

[5] Peter Borwein and Tamás Erdélyi. *Polynomials and polynomial inequalities*, volume 161 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[6] E. Bresson. *Protocoles Cryptographiques pour l'Authentification et l'Anonymat dans les Groupes*. Phd thesis, École polytechnique, October 2002.

[7] Chin Long Chen. Formulas for the solutions of quadratic equations over GF(2^m). *IEEE Trans. Inform. Theory*, 28(5):792–794, 1982.

[8] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[9] Charles G. Cullen. *Matrices and linear transformations*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., second edition, 1972.

[10] Cipher Deavours, David Kahn, Louis Kruh, Greg Mellen, and Brian Winkel, editors. *Cryptology: machines, history & methods*. Artech House Inc., Boston, MA, 1989.

[11] Cipher A. Deavours, David Kahn, Louis Kruh, Greg Mellen, and Brian Winkel, editors. *Cryptology*. Artech House Inc., Boston, MA, 1987. Yesterday, today, and tomorrow.

[12] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT-22(6):644–654, 1976.

[13] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory*, 31(4):469–472, 1985.

[14] J. D. Emerald and K. G. Subramanian. A note on Polly Cracker public-key cryptosystems. In *Graph theory and its applications (Tirunelveli, 1996)*, pages 63–69. Tata McGraw-Hill, New Delhi, 1997.

[15] Michael Fellows and Neal Koblitz. Combinatorial cryptosystems galore! In *Finite fields: theory, applications, and algo-*

rithms (Las Vegas, NV, 1993), volume 168 of *Contemp. Math.*, pages 51–61. Amer. Math. Soc., Providence, RI, 1994.

[16] F. R. Gantmacher. *The Theory of Matrices*, volume 1 and 2. Chelsea, New York, 1959.

[17] Michael R. Garey and David S. Johnson. *Computers and intractability.* W. H. Freeman and Co., San Francisco, Calif., 1979. A guide to the theory of NP-completeness, A Series of Books in the Mathematical Sciences.

[18] Martin Gavalec. Computing matrix period in max-min algebra. *Discrete Appl. Math.*, 75(1):63–70, 1997.

[19] Martin Gavalec. Reaching matrix period is NP-complete. *Tatra Mt. Math. Publ.*, 12:81–88, 1997. Fuzzy sets (Liptovský Ján, 1996).

[20] Martin Gavalec. Computing orbit period in max-min algebra. *Discrete Appl. Math.*, 100(1-2):49–65, 2000.

[21] Martin Gavalec. Solvability and unique solvability of max-min fuzzy equations. *Fuzzy Sets and Systems*, 124(3):385–393, 2001. Fuzzy logic (Palma, 1999/Liptovský Ján, 2000).

[22] Martin Gavalec and Günter Rote. Reachability of fuzzy matrix periods. *Tatra Mt. Math. Publ.*, 16(, part I):61–79, 1999. Fuzzy sets, Part I (Liptovský Ján, 1998).

[23] O. Goldreich, S. Goldwasser, and S. Halevi. Public-key cryptosystems from lattice reduction problems. *CRYPTO'97*, 1997.

[24] Daniel M. Gordon. Discrete logarithms in GF(p^n) using the number field sieve. Preprint, 1991.

[25] Daniel M. Gordon. Discrete logarithms in GF(p) using the number field sieve. *SIAM J. Discrete Math.*, 6(1):124–138, 1993.

[26] Jon Grantham. The largest prime dividing the maximal order of an element of S_n. *Math. Comp.*, 64(209):407–410, 1995.

[27] P.A. Grillet. *Commuative Semigroups*. Advances in Mathematics. Kluwer Academic Publishers, Dordrecht, 2001.

[28] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

[29] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: a ring-based public key cryptosystem. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 267–288. Springer, Berlin, 1998.

[30] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NSS: an NTRU lattice-based signature scheme. In *Advances in cryptology—EUROCRYPT 2001 (Innsbruck)*, volume 2045 of *Lecture Notes in Comput. Sci.*, pages 211–228. Springer, Berlin, 2001.

[31] R. A. Horn and Ch. R. Johnson. *Matrix Analysis*. Cambridge University Press, Cambridge, 1985.

[32] John M. Howie. *Fundamentals of semigroup theory*, volume 12 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, New York, 1995. Oxford Science Publications.

[33] T. W. Hungerford. *Algebra*. Graduate Texts in Mathematics. Springer, New York, 1980.

[34] N. Jacobson. Schur's theorems on commutative matrices. *Bull. Amer. Math. Soc.*, 50:431–436, 1944.

[35] V. Kann. personal communication, 2002.

[36] V. Kann and P. Crescenzi. A compendium of NP optimization problems, 2002. Available at http://www.nada.kth.se/∼viggo/problemlist/.

[37] Donald E. Knuth. *The art of computer programming. Volume 3.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1973. Sorting and searching, Addison-Wesley Series in Computer Science and Information Processing.

[38] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.

[39] N. Koblitz. *Algebraic Aspects of Cryptography.* Springer-Verlag, Berlin, 1998. With an appendix by A. J. Menezes, Y.-H. Wu and R. J. Zuccherato.

[40] E. Landau. über die maximalordnung der permutationene gegebenen grades. *Archiv der Math. und Phys.*, pages 92–103, 1903.

[41] Hans Lausch and Wilfried Nöbauer. *Algebra of polynomials.* North-Holland Publishing Co., Amsterdam, 1973. North-Holland Mathematical Library, Vol. 5.

[42] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math. (2)*, 126(3):649–673, 1987.

[43] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and their Applications.* Cambridge University Press, Cambridge, London, 1986.

[44] Martin W. Liebeck. The classification of finite simple Moufang loops. *Math. Proc. Cambridge Philos. Soc.*, 102(1):33–47, 1987.

[45] D. Lind and B. Marcus. *An Introduction to Symbolic Dynamics and Coding*. Cambridge University Press, 1995.

[46] Jean-Pierre Massias. Majoration explicite de l'ordre maximum d'un élément du groupe symétrique. *Ann. Fac. Sci. Toulouse Math. (5)*, 6(3-4):269–281 (1985), 1984.

[47] Jean-Pierre Massias, Jean-Louis Nicolas, and Guy Robin. Effective bounds for the maximal order of an element in the symmetric group. *Math. Comp.*, 53(188):665–678, 1989.

[48] Ueli Maurer. *Cryptography* 2000 ± 10, volume 2000 of *Lecture Notes in Computer Science*, pages 63–85. Springer-Verlag, 2001.

[49] Ueli Maurer and Stefan Wolf. On the complexity of breaking the Diffie-Hellman protocol. Technical Report 244, Institute for Theoretical Computer Science, ETH Zurich, 1996.

[50] Ueli Maurer and Stefan Wolf. Lower bounds on generic algorithms in groups. In *Advances in cryptology—EUROCRYPT '98 (Espoo)*, volume 1403 of *Lecture Notes in Comput. Sci.*, pages 72–84. Springer, Berlin, 1998.

[51] Ueli M. Maurer and Stefan Wolf. Diffie-Hellman oracles. In *Advances in cryptology—CRYPTO '96 (Santa Barbara, CA)*, volume 1109 of *Lecture Notes in Comput. Sci.*, pages 268–282. Springer, Berlin, 1996.

[52] G. Maze, C. Monico, and J. Rosenthal. A public key cryptosystem based on group actions. Preprint, October 2001.

[53] G. Maze, C. Monico, and J. Rosenthal. Public key cryptography based on simple modules over simple rings. In *Proceedings of the 2002 Mathematical Theory of Networks and System*, South Bend, USA, 2002.

[54] G. Maze, C. Monico, and J. Rosenthal. A public key cryptosystem based on actions by semigroups. In *Proceedings of the 2002 IEEE International Symposium on Information Theory*, page XY, Lausanne, Switzerland, 2002.

[55] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. Technical report, DSN Progress report # 42-44, Jet Propulsion Laboratory, Pasadena, Californila, 1978.

[56] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian. *Applications of Finite Fields*. The Kluwer International Series in Engineering and Computer Science. Kluwer Academic Publishers, 1993.

[57] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.

[58] A. J. Menezes and Y.-H. Wu. The discrete logarithm problem in $\mathrm{Gl}(n, q)$. *Ars Combin.*, 47:23–32, 1997.

[59] Ralph C. Merkle and Martin E. Hellman. Hiding information and signatures in trapdoor knapsacks. In *Secure communications and asymmetric cryptosystems*, volume 69 of *AAAS Sel. Sympos. Ser.*, pages 197–215. Westview, Boulder, CO, 1982.

[60] V. S. Miller. Use of elliptic curves in cryptography. In *Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985)*, pages 417–426. Springer, Berlin, 1986.

[61] C. Monico. personal communication, 2002.

[62] C. Monico. *Semirings and Semigroup Actions in Public-Key Cryptography*. PhD thesis, University of Notre Dame, May 2002. Available at http://www.nd.edu/~rosen/preprints.html.

[63] R. Moufang. Zur Struktur von Alternativkörpern. *Math. Ann.*, 110:416–430, 1935.

[64] Jean-Louis Nicolas. Calcul de l'ordre maximum d'un élément du groupe symétrique S_n. *Rev. Francaise Informat. Recherche Opérationnelle*, 3(Ser. R-2):43–50, 1969.

[65] NIST. Advanced encryption standard (aes) development effort, 2001. Available at http://csrc.nist.gov/encryption/aes/index2.html#overview.

[66] NIST. Federal information processing standards publication 197, aes, 2001. Available at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[67] L. J. Paige. A class of simple Moufang loops. *Proc. Amer. Math. Soc.*, 7:471–482, 1956.

[68] Hala O. Pflugfelder. *Quasigroups and loops: introduction*, volume 7 of *Sigma Series in Pure Mathematics*. Heldermann Verlag, Berlin, 1990.

[69] Stephen C. Pohlig and Martin E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryp-

tographic significance. *IEEE Trans. Information Theory*, IT-24(1):106–110, 1978.

[70] J. M. Pollard. Monte Carlo methods for index computation (mod p). *Math. Comp.*, 32(143):918–924, 1978.

[71] J. M. Pollard. On not storing the path of a random walk. *BIT*, 19(4):545–548, 1979.

[72] Mohan S. Putcha. *Linear algebraic monoids*, volume 133 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1988.

[73] M.O. Rabin. Digitalized signatures and public-key function as intractable as factorization. *MIT/LCS/TR-212, MIT Laboratory for Computer Science*, 1979. Available at http://ncstrl.mit.edu/Dienst/UI/2.0/Print/ncstrl.mit_lcs%2fMIT%2fLCS%2fTR-212.

[74] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2):120–126, 1978.

[75] R. L. Rivest, A. Shamir, and L. Adleman. Cryptographic communications system and method. 1983. US Patent No 4405829.

[76] Theodore J. Rivlin. *Chebyshev polynomials*. Pure and Applied Mathematics. John Wiley & Sons Inc., New York, second edition, 1990. From approximation theory to algebra and number theory.

[77] J. Rosenthal. A polynomial description of the rijndael advanced encryption standard. *To appear in Journal of Algebra and its Application*, 2003.

[78] Hans-Georg Rück. A note on elliptic curves over finite fields. *Math. Comp.*, 49(179):301–304, 1987.

[79] C.-P. Schnorr. Efficient identification and signatures for smart cards. In *Advances in cryptology—CRYPTO '89 (Santa Barbara, CA, 1989)*, volume 435 of *Lecture Notes in Comput. Sci.*, pages 239–252. Springer, New York, 1990.

[80] R. Schoof. personal communication, 2002.

[81] C. E. Shannon. Communication theory of secrecy systems. *Bell System Tech. J.*, 28:656–715, 1949.

[82] Victor Shoup. Lower bounds for discrete logarithms and related problems. In *Advances in cryptology—EUROCRYPT '97 (Konstanz)*, volume 1233 of *Lecture Notes in Comput. Sci.*, pages 256–266. Springer, Berlin, 1997.

[83] Igor E. Shparlinski. *Computational and algorithmic problems in finite fields*, volume 88 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1992.

[84] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. Corrected reprint of the 1986 original.

[85] Simon Singh. *The Code Book : The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography*. Doubleday Books, 1999.

[86] D. Stinson. *Cryptography, Theory and Practice*. CRC Press, 1996.

[87] D. A. Suprunenko. On maximal commutative matrix algebras and maximal commutative matrix groups. *Dokl. Akad. Nauk BSSR*, 8:425–428, 1964.

[88] Takayuki Tamura. Indecomposable completely simple semigroups except groups. *Osaka Math. J.*, 8:35–42, 1956.

[89] P. Vojtěchovský. *Finit simple Moufang loops.* PhD thesis, Iowa State University, 2001. Available at http://www.public.iastate.edu/˜petr.

[90] Zhe-xian Wan and Gen-dao Li. The two theorems of Schur on commutative matrices. *Chinese Math.*, 5:156–164, 1964.

[91] Dominic Welsh. *Codes and cryptography.* Oxford Science Publications. The Clarendon Press Oxford University Press, New York, 1988.

[92] A. Yamamura. Public-key cryptosystems using the modular group. In *Public Key Cryptography*, volume 1431 of *Lecture Notes in Computer Science*, pages 203–216. Springer, Berlin, 1998.

[93] Song Y. Yan. *Number theory for computing.* Springer-Verlag, Berlin, 2000.

[94] G. Zémor. *Cours de Cryptographie.* Cassini, Paris, 2002.