



# Mutations in Brauer Configuration Algebras and Some of Its Cryptographic Applications

Juan David Camacho Vega

Universidad Nacional de Colombia  
Facultad de Ciencias  
Departamento de Matemáticas  
Bogotá, Colombia  
2021

Mutations in Brauer Configuration Algebras and Some  
of Its Cryptographic Applications

Juan David Camacho Vega

Advisor: Professor Agustín Moreno Cañadas  
Universidad Nacional de Colombia  
TERENUFIA-UNAL  
Bogotá, Colombia

Universidad Nacional de Colombia  
Facultad de Ciencias  
Departamento de Matemáticas  
Bogotá, Colombia  
2021

**Resumen 1.** Título en español: **Mutaciones en álgebras de configuración de Brauer y algunas aplicaciones a la criptografía**

Las mutaciones de las álgebras de configuración de Brauer son exploradas y estudiadas como herramientas para obtener soluciones para algunas generalizaciones del problema de los McNuggets de pollo junto con una exposición de unos autómatas asociados a los conglomerados de configuración. Este acercamiento permite construir una descripción algebraica del itinerario de las claves AES por medio de un autómata no determinista adecuado.

*Palabras Clave* : Advanced Encryption Standard (AES), álgebras de configuración de Brauer, Problema de los McNuggets de pollo, criptografía, Números de Frobenius, Automatas finitos no deterministas, polytopos.

**Abstract 1.** Título en inglés: **Mutations in Brauer Configuration Algebras and Some of Its Cryptographic Applications**

Mutations on Brauer configurations are explored as tools to obtain a solution for some generalizations of the chicken McNugget problem, along with some associated automata to the configuration clusters. This approach allows us to give an algebraic description of the schedule of an AES key via some suitable non-deterministic automata (NFA).

*Keywords* : Advanced Encryption Standard (AES), Brauer configuration algebra, Chicken McNugget Problem (CMP), cryptography, Frobenius number, non-deterministic finite automata (NFA), polytope.

# Contents

<b>1</b>	<b>Abstract</b>	<b>5</b>
<b>2</b>	<b>Introduction</b>	<b>6</b>
2.1	Contributions . . . . .	7
<b>3</b>	<b>McNugget Type Diophantine Problems</b>	<b>8</b>
3.1	Frobenius Numbers . . . . .	8
3.2	Polytopes . . . . .	13
3.3	On Diophantine Equations of Type $\mathcal{D}(n_1, n_2, \mathcal{K}_m)$ . . . . .	16
<b>4</b>	<b>Configuration Clusters</b>	<b>19</b>
4.1	Quiver Representation . . . . .	19
4.2	The Category of Representations . . . . .	19
4.3	The Fundamentals of Path Algebras . . . . .	21
4.4	Brauer Configuration Algebras . . . . .	22
4.4.1	The Message of a Brauer Configuration . . . . .	28
4.5	Cluster Algebras . . . . .	29
4.5.1	Cluster Algebras From Quivers . . . . .	31
4.6	Cluster Configurations . . . . .	32
<b>5</b>	<b>Automata Theory</b>	<b>38</b>
5.1	Regular Languages . . . . .	40
5.2	Syntactic Monoids . . . . .	41
5.3	Descriptions of the $p$ -group Languages . . . . .	41
5.4	An Algorithm for $p$ -group Language . . . . .	44
5.5	Languages and Formations Generated by $D_4$ and $Q_8$ . . . . .	46
5.6	A Regular Language Associated with a Brauer Configuration Algebra . . . . .	48
5.7	Cluster Configurations and Diophantine Problems . . . . .	49
5.8	Criptographic applications . . . . .	52
5.9	AES Mutation . . . . .	55

## 1 Abstract

Mutations on Brauer configurations are explored as tools to obtain a solution for some generalizations of the chicken McNugget problem, along with some associated automata to the configuration clusters. This approach allows us to give an algebraic description of the schedule of an AES key via some suitable non-deterministic automata (NFA).

*Keywords* : Advanced Encryption Standard (AES), automata, Brauer configuration algebra, Chicken McNugget Problem (CMP), cryptography, diophantine equation, Frobenius number, non-deterministic finite automata (NFA), polytope.

Mathematics Subject Classification 2010 : 16G20; 16G30; 05A17; 11D45; 11E25.

## 1 Resumen

Las mutaciones de las algebras de configuración de Brauer son exploradas y estudiadas como herramientas para obtener soluciones para algunas generalizaciones del problema de los McNuggets de pollo junto con una exposición de unos autómatas asociados a los conglomerados de configuración. Este acercamiento permite construir una descripción algebraica del itinerario de las claves AES por medio de un autómata no determinista adecuado.

## Acknowledgments

I would like to thank thesis advisor, Agustín Moreno Cañadas, for his instruction and sharing of ideas. I am also thankful to all my professors; they each gave me a unique perspective of mathematics and unexpected directions of study. I want to thank my parents for supporting and encouraging me in my academic endeavors.

## 2 Introduction

Maths is filled with beautiful and surprising structures. One of such structures is the Brauer Configuration algebras introduced by E. L. Green and S. Schroll in 2017 and further explored in [31]. This generalization of Brauer graphs has excellent algebraic properties and beautiful relations between its combinatoric properties and representations. Several practical applications of these algebras have been found in different fields of science. For instance, such algebras appear almost naturally in traffic flow and mobility works. M.A.O. Angarita used Brauer configuration algebras to define visual secret sharing schemes [1](VSSS), and recently A.M. Cañadas and M.A.O. Angarita used these algebras to define systems for the security of biometric data (faces, iris, fingerprints, and others) [6].

Those applications bring forward relations between different areas of mathematics such as algebra, Diophantine problems, automata theory, Cryptography, and much more. This work will explore problems of varied mathematical areas such as number theory, representation theory, and automata theory. One of such problems is the chicken McNugget problem and some of its generalizations, especially ones related to counting lattice points inside a polytope. These problems lead to a special kind of family of Brauer configuration algebras called configuration clusters. Such configuration algebras can be used in the cryptanalysis of the Advanced Encryption Standard (AES). Taking into consideration that AES is one of the most commonly used cryptographic protocols. AES is the cornerstone for the protocol WPA2 (Wi-Fi Protected Access) used to protect wireless communications. To date, there are no known practical attacks against AES.

The work will describe an AES key schedule via suitable mutations applied to polygons of some Brauer configurations. These techniques are similar to mutations defined in cluster algebras of quiver type. Thus, the present approach connects the investigation of Brauer configuration algebras with the research of cluster algebras. Giving an algebraic interpretation of the AES keys allows us to get a novel tool for the cryptanalysis of this cryptosystem and to solve diophantine problems associated with polytopes of the form  $\{x \mid Ax = b \geq 0\}$  as well.

This work will be composed of 3 parts divided into sections 3, 4, and 5. The first one will focus on diophantine problems, specifically on the chicken McNugget problem and its generalizations. The problems of type  $\mathcal{D}(n_1, n_2, \mathcal{K}_m)$  will be introduced along with two original theorems. In section 4, there will be an introduction to representation theory, cluster algebras, path algebras, and Brauer configuration algebras to introduce the idea of cluster configurations and mutation on Brauer configuration algebras. New examples of cluster configurations will be presented. The central theme of section 5 will be automata theory; the basics of automata will be introduced, and the relationship between cluster

configurations and non-deterministic automata will be presented. The work will conclude by presenting some original findings on the relation of cluster configurations, diophantine problems, and automata leading towards applications of cluster algebras, considering that the key-schedule of an AES encryption key is nothing but a configuration cluster.

## 2.1 Contributions

The main contribution of this work is the novel notion of the mutation of a Brauer configuration and its properties. Such mutations and their specializations allow solving different types of Diophantine problems, specifically of type  $\mathcal{D}(n_1, n_2, \mathcal{K}_m)$ , which arise from the research of generalizations on denumerants in the sense of Sylvestre. As an application, we will note that the AES key schedule is nothing but the specialization of a mutation. Thus, the algebraic properties of the corresponding Brauer configuration algebra allow the description of some characteristics of an AES key.

### 3 McNugget Type Diophantine Problems

Diophantine equations are objects of study of great importance in number theory and abstract algebra. These equations consist of integer equations where only the integer solutions are of interest. The restriction to integer solutions creates different challenges and strategies to find these solutions, in many cases reducing the solutions set for any given equation. These kinds of equations are often related to transportation optimization and monoid generation.

One of such problems is the Chicken McNugget problem, noted CMP, which consists of determining what numbers of Chicken McNuggets can be ordered using only packs with 6, 9, or 20 pieces? In other words, a positive integer  $n$  is a McNugget number if and only if there is an ordered triple  $(a, b, c)$  such that:

$$6x + 9y + 20z = n \tag{3.1}$$

Positive integers satisfying the Chicken McNugget equation are now known as McNugget numbers. The sequence A065003 in the OEIS (On-Line Encyclopedia of Integer Sequences) is the list of not McNugget numbers and is finite thanks to the fact that:

**Proposition 1** ([7], Proposition 1.1). *Any positive integer  $x > 43$  is a McNugget number.*

*Proof.* Since 43 is not a McNugget number, and the following six numbers are McNugget numbers provided that:

1.  $(1, 2, 1)$  is a solution for  $6x + 9y + 20z = 44$
2.  $(0, 5, 0)$  is a solution for  $6x + 9y + 20z = 45$
3.  $(1, 0, 2)$  is a solution for  $6x + 9y + 20z = 46$
4.  $(0, 3, 1)$  is a solution for  $6x + 9y + 20z = 47$
5.  $(8, 0, 0)$  is a solution for  $6x + 9y + 20z = 48$
6.  $(0, 1, 2)$  is a solution for  $6x + 9y + 20z = 49$

Having six consecutive McNugget numbers allows every number greater than 43 to be constructed using the 6 pieces packs. This reasoning leads to a more general theorem for Frobenius numbers.  $\square$

#### 3.1 Frobenius Numbers

As a generalization of CMP, a natural question is *Given some fixed values  $a_1, a_2, \dots, a_k \in \mathbb{Z}$  where  $\mathbb{Z}$  denotes the set of integer numbers, what possible values of  $n$  can be obtained as a linear combination of these values?* This question is known as the *Knapsack Problem*. The *Knapsack Problem* originates from

its applications towards finding the possible capacity of a container. When the set of numbers for which the equation has no solution is finite, finding the largest number in the set gives origin to the concept of Frobenius numbers.

Each *Knapsack Problem* generates a numerical monoid of the form  $M = \{n : n = \sum_{i=1}^k a_i x_i\}$  where  $x_i$  is a positive integer for  $1 \leq i \leq k$ . The set  $M$  is a monoid since for all  $n_1, n_2 \in M$ , considering the solutions  $(s_{11}, \dots, s_{1k}), (s_{21}, \dots, s_{2k})$  then  $\sum_{i=1}^k a_i s_{1i} = n_1$  and  $\sum_{i=1}^k a_i s_{2i} = n_2$ . Therefore,  $\sum_{i=1}^k a_i (s_{1i} + s_{2i}) = n_1 + n_2$  showing that  $M$  is closed under sum.  $M$  can be seen as a linear combination of  $a_1, a_2, \dots, a_k$ . The notation  $\langle a_1, \dots, a_n \rangle$  will be used to denote the set generated by  $a_1, \dots, a_n$ .  $M$  is a submonoid of the natural numbers with the usual sum noted  $(\mathbb{N}, +)$ . When  $\mathbb{N} \setminus M$  is finite, it is said that  $M$  is a *numerical semigroup*.

**Theorem 1** ([25], Theorem 1.0.1). *If  $a_1, a_2, \dots, a_k$  are positive integers, then they generate a numerical semigroup if, and only if,  $\gcd(a_1, a_2, \dots, a_k) = 1$ .*

*Proof.* Since  $\gcd(a_1, \dots, a_k) = 1$ , it is possible to write  $m_1 a_1 + \dots + m_k a_k = 1$  for some integers  $m_i$ . Denote by  $P$  and  $N$  the sum of the positive and negative terms in this decomposition. So that  $P$  and  $N$  belong to the monoid  $M$  and  $P - N = 1$ . Any integer  $n \in \mathbb{N}$  can be written as  $h a_1 + r$  with  $h \geq 0$  and  $0 \leq r < a_1$ . Considering that  $h a_1 + (a_1 - 1 - r)N + rP \in M$  and  $(a_1 - 1)N + k = h a_1 + (a_1 - 1 - r)N + rP$  we can say that every  $(a_1 - 1)N \leq n$  is part of the monoid. Therefore,  $M$  is a numerical semigroup.  $\square$

When working on monoids, there are critical elements of the set known as irreducible elements of the monoid. On a monoid,  $M$ , an element  $x \in M$  is said to be irreducible if and only if  $x = z + y$  implies that either  $z = 0$  or  $y = 0$ . These elements on numerical monoids produce an interesting theorem:

**Theorem 2.** *If  $\langle n_1, n_2, \dots, n_k \rangle$  is a numerical monoid, its irreducible elements are precisely  $n_1, n_2, \dots, n_k$ .*

*Proof.* Suppose that  $x \in M$  is irreducible and that it is not in the set  $I = \{a_1, \dots, a_k\}$ . By definition  $x \in M$  only if there is a combination  $x = y_1 a_1 + \dots + y_k a_k$  with  $y_i \in \mathbb{N}$ . If  $x \notin I$  then either  $1 < y_i$  or  $y_i \neq 0$  and  $y_j \neq 0$  for  $i \neq j$ . Therefore,  $x$  is the sum of two non-zero elements of  $M$ , contradicting that  $x$  is irreducible.  $\square$

The importance of these elements is that they secure the uniqueness of the generators of  $M$  that is not generally true. In other words, for every numerical monoid  $M$ , there is a unique minimum set of generators such that  $M = \langle a_1, \dots, a_k \rangle$  that is given by its irreducible elements.

For every numerical semigroup  $M$ , the biggest  $n \in \mathbb{N}$  such that  $n \notin M$  it is known as the *Frobenius number* of  $M$  and is noted  $F_M$ . The Frobenius number

for the McNugget monoid is 43. In the general case, is not a known formula for the Frobenius number of the  $k$ -generated numerical semigroup  $S$ , but if  $k$  is fixed, there is an algorithm that computes the Frobenius number in polynomial time. J. L. Ramírez-Alfonsín proved that the Knapsack problem could be reduced to the Frobenius problem in polynomial time [24] showing that the problem is NP-hard.

At first glance, the *Frobenius Problem* consisting of calculating  $F_M$  may seem extremely specific. Nevertheless, it crops up again and again in the most unexpected places. It turns out that the knowledge of  $F_M$  has been instrumental in shining some light on a great variety of problems. Several methods from different mathematics areas have been used to find a formula giving the Frobenius number and algorithms to calculate it.

Computing the Frobenius number when  $k = 2$  is easy since there exists an explicit formula for it:

**Theorem 3** ([25], Theorem 2.1.1). *Let  $p, q$  be non-negative relatively prime integers. Then,*

$$F_{\langle p, q \rangle} = q(p - 1) - p$$

*Proof.* Since  $(p, q) = 1$ , then any integer  $n$  is representable as  $n = xp + yq$  with where  $x$  and  $y$  are integers. Note that the representation of  $n$  becomes unique if we ask for  $0 \leq x < q$ . In this case,  $n$  is representable if  $0 \leq y$ , and it is not representable if  $y < 0$ . Thus, the largest non-representable value is reached when  $x = q - 1$  and  $y = -1$ . Therefore,

$$F(p, q) = (q - 1)p + (-1)q = pq - p - q = q(p - 1) - p$$

□

For  $k = 3$ , the problem becomes significantly harder because there is not a general explicit formula. Because of these, different algorithms have been developed to compute the Frobenius number for  $2 < k$ .

**Theorem 4** ([8], Theorem). *Let  $A = \{(a_1, a_2, a_3) \in \mathbb{N}^3 : a_1 < a_2 < a_3, a_1 \text{ and } a_2 \text{ are prime, and } a_1, a_2 \nmid a_3\}$ . Then there is no non-zero polynomial  $H \in \mathbb{C}[X_1, X_2, X_3, Y]$  such that  $H(a_1, a_2, a_3, F_{\langle a_1, a_2, a_3 \rangle}) = 0$  for all  $(a_1, a_2, a_3) \in A$ .*

To prove the theorem, the following lemmas are needed along with the concept of Farey sequence of order  $n$ , noted  $F_n$ , is the ascending series of irreducible fractions between 0 and 1 whose denominators do not exceed  $n$  [18]. Thus  $h/k$  belongs to  $F_n$  if

$$0 \leq h \leq k \leq n, \gcd(h, k) = 1 \tag{3.2}$$

the numbers 0 and 1 are included in the forms  $0/1$  and  $1/1$ . For example,  $F_6$  is:

$$0/1, 1/6, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 1/1$$

**Lemma 1** ([8], Lemma 1). *Given  $\alpha \in \mathbb{R}^+$ , where  $\mathbb{R}^+$  represents the set of positive real numbers, and  $\epsilon > 0$ . Choose a prime  $p$  and  $i, j \in \mathbb{N}$  such that  $(p, i) = (p, j) = 1$ . Then there exists  $x, y \in \mathbb{N}$  such that  $x$  is prime,  $x \equiv i \pmod{p}$ ,  $y \equiv j \pmod{p}$  and  $|\alpha - y/x| < \epsilon$ .*

*Proof.* Assuming that  $\alpha > \epsilon$ . Choose  $n > 1/\epsilon$  and let  $\frac{q}{r}, \frac{s}{t} \in (\alpha - \epsilon, \alpha + \epsilon)$  be adjacent elements in a Farey sequence  $F_n$ . By properties of the Farey sequence, it is possible to conclude that  $|qs - rt| = 1$  and therefore the following system of equations is solvable:

$$\begin{aligned} ru + tv &\equiv i \pmod{p}, \\ qu + sv &\equiv j \pmod{p} \end{aligned} \tag{3.3}$$

It is possible to assume that  $p \nmid u$ . Then, by Dirichlet prime number theorem, there exists an  $0 < a$  such that  $u' = ap + u$  is prime,  $(u', v) = 1$  and  $u' > t$ . Then  $(t, ru' + tv) = (u', ru' + tv) = 1$  since  $ru' + tv \equiv i \pmod{p}$ . So  $(ptu', ru' + tv) = 1$  and using Dirichlet theorem again there is a  $b \leq 0$  such that  $bptu' + ru' + tv$  is prime. If  $v' = bptu' + v$  then  $(u', v') = 1$  and  $x = ru' + tv'$ ,  $y = qu' + sv'$  the lemma is satisfied.  $\square$

**Lemma 2** ([8], Lemma 2). *Let  $S = \langle s_1, s_2, s_3 \rangle$ , where  $2 < s_1 < s_2 < s_3$  let  $2 \leq k \leq s_1 - 1/(2+1)$  and suppose  $s_1 - k < s_3/s_2 < s_1 - k + 1$ ,  $s_2 \equiv 1 \pmod{s_1}$  and  $s_3 \equiv s_1 - k + 1 \pmod{s_1}$ . Then  $F_S = (k - 2)s_2 + s_3 - s_1$ .*

*Proof.* Note that  $(k - 2)s_2 + s_3 \in S(s_1) = \{t \in S : t < s_1\}$ . To prove this, suppose that it does not. Then as  $(k - 2)s_2 + s_3 \equiv s_1 - 1 \pmod{s_1}$ , there are  $0 \geq a, b$  such that  $as_2 + bs_3 < (k - 2)s_2 + s_3$  and  $as_2 + bs_3 \equiv s_1 - 1 \pmod{s_1}$ . If  $b = 0$  then  $a \equiv s_1 - 1 \pmod{s_1}$  and thus  $a \geq s_1 - 1$ . Thus,  $(s_1 - 1)s_2 < as_2 < (k - 2)s_2 + s_3$  implies that  $s_1 - k + 1 < \frac{s_3}{s_2}$  is a contradiction. If  $b = 1$  then  $a \equiv k - 2 \pmod{s_1}$  so  $k - 2 \leq a$  and  $(k - 2)s_2 + s_3 \leq as_2 + bs_1$ , contradicting the assumption. For  $b \geq 2$  then  $2s_3 < (k - 2)s_2 + bs_3$ . This implies that  $s_1 - k < \frac{s_3}{s_2} < (k - 2)$  this implies that  $\frac{s_1}{2} + 1 < k$  contradicting the hypothesis of how  $k$  was chosen. So  $(k - 2)s_2 + s_3 \in S(s_1)$ .

For  $0 \leq m \leq s_1 - k$   $ms_2 \equiv m \pmod{s_1}$  and  $\frac{s_3}{s_2} > s_1 - k \geq m$ . So,  $ms_2 < s_3 < s_3 + s_2(k - 2)$ . For  $s_1 - k < m < s_1 - 1$  as  $(m - (s_1 - k + 1))s_2 + s_3 \equiv m \pmod{s_1}$ , and  $(m - (s_1 - k + 1))s_2 + s_3 < (k - 2)s_1 + s_3$ . It is now possible to conclude that  $(k - 2)s_1 + s_3$  is the largest element of  $S(s_1)$  and  $F_S = (k - 2)s_2 + s_3 - s_1$ .  $\square$

With these two lemmas, it is possible to prove Theorem 4.

*Proof.* Suppose the polynomial  $H$  exists. Then fixing a prime  $2 < p$  and,  $2 \leq k \leq \frac{p-1}{2} + 1$ . Let  $G(X_2, X_3) = H(p, X_2, X_3, (k - 2)X_2 + X_3 - p)$ . Let  $\alpha \in (p - k, p - k + 1)$  be irrational. For  $n \in \mathbb{N}$ , choose by Lemma 1,  $x_n \equiv 1 \pmod{p}$ , and  $y_n \equiv p - k + 1 \pmod{p}$ . Then  $(p, x_n, y_n) \in A$  and by Lemma 2  $g(x_n, y_n) = 0$  for all  $n \in \mathbb{N}$ . Let  $g^*(X_2, X_3, Z)$  be the homogenization of  $g$  with respect to  $Z$ , then  $g^*(x_n, y_n, 1) = 0$  which implies  $g^*(1, \frac{y_n}{x_n}, \frac{1}{x_n}) = 0$ , and thus  $g^*(1, \alpha, 0) = 0$  by continuity for every  $\alpha \in (p - k, p - k + 1)$  therefore the projective curve of

$g^*$  contains the projective curve of  $Z$ , in other words  $g(X_2, X_3) = 0$ .

Considering a fixed prime  $2 < p$  let  $G = H(X_2, X_3, Y) = H(p, X_1, X_2, Y)$  and let  $G^*(X_2, X_3, Y, Z)$  be the homogenization of  $G$  with respect to  $Z$ . Then  $G^*$  vanishes in every hyperplane  $(k-2)X_2 + X_3 - Y - pZ$  for  $1 < k \leq \frac{p-1}{2} + 1$ , so  $\frac{p-1}{2} \leq \deg G^* = \deg G \leq \deg H$ , remember that  $\deg G$  is the degree of the polynomial  $G$ . As  $p$  is arbitrary the polynomial  $H$  must be such that  $\frac{p-1}{2} \leq \deg H$  no such polynomial exist.  $\square$

**Corollary 1** ([8], Corollary). *There is no finite set of polynomials  $\{h_1, \dots, h_n\}$  such that for each choice of  $a_1, a_2, a_3$ , there is some  $i$  such that  $hi(a_1, a_2, a_3) = F_{\langle a_1, a_2, a_3 \rangle}$ .*

*Proof.*  $H = \prod_{i=1}^n (h_i - Y)$  would vanish on  $A$  contradicting the theorem 4.  $\square$

This limitations creates the need of algorithms to calculate the Frobenius number for a number of variables greater than 2. One of these algorithms is the Rødseth's method [24]. Rødseth's procedure describe as follows:

---

**Algorithm 1:** Rødseth's

---

1. **Input** three integers  $a_1, a_2, a_3$  such that  $\gcd(a_1, a_2, a_3) = 1$ .
2. **Output** the frobenius number for  $a_1, a_2, a_3$ ,  $F_{\langle a_1, a_2, a_3 \rangle}$ .
3. Let  $s_0$  be the unique integer such that  $a_2 s_0 \equiv a_3 \pmod{a_1}$ ,  $0 \leq s_0 < a_1$ .  
The continued fraction algorithm is applied to the ratio  $a_1/s_0$ :

$$\begin{aligned}
 a_1 &= q_1 s_0 - s_1, & 0 \leq s_1 < s_0, \\
 s_0 &= q_2 s_1 - s_2, & 0 \leq s_2 < s_1, \\
 s_1 &= q_3 s_2 - s_3, & 0 \leq s_3 < s_2, \\
 &\vdots \\
 s_{m-1} &= q_{m+1} s_m, \\
 s_m &= 0,
 \end{aligned} \tag{3.4}$$

where  $2 \leq q_i$ ,  $0 \leq s_i$  for all  $i$ .

Let  $p_{-1} = 0$ ,  $P_0 = 1$ ,  $p_{i+1} = q_{i+1} p_i - p_{i-1}$  and  $r_i = (s_i a_2 - p_i a_3)/a_1$ . Let  $v$  be the unique integer such that:

$$\frac{s_{v+1}}{p_{v+1}} \leq \frac{a_3}{a_2} < \frac{s_v}{p_v}.$$

then,

$$F_{\langle a_1, a_2, a_3 \rangle} = -a_1 + a_2(s_v - 1) + a_3(p_{v+1} - 1 - \min\{a_2 s_{v+1}, a_3 p_v\})$$


---

For example to compute  $F_{\langle 3,5,7 \rangle}$  using the Rødseth's method. In this case,  $s_0 = 2$  and

$$\begin{aligned} 3 &= q_1 2 - s_1, & 0 \leq s_1 < 2, & & q_1 = 1, & & s_1 = 1 \\ 2 &= q_2 - s_2, & 0 \leq s_2 < 1, & & q_2 = 2, & & s_2 = 0 \end{aligned}$$

Thus  $p_1 = 1$  and  $\frac{s_1}{p_1} = 1 < \frac{7}{5} < \frac{s_0}{p_0} = 2$ . Therefore,

$$F_{\langle 3,5,7 \rangle} = -3 + 5 + 7 \cdot 0 - \min\{5 \cdot 1, 7 \cdot 1\} = 4.$$

### 3.2 Polytopes

Another generalization of the CMP is to consider a system of equations instead of a single one. In other words, finding solutions for the following expression:

$$Ax = b$$

Where  $A$  is a  $n \times d$  integral matrix,  $b = (b_1, \dots, b_n)^T$  is a fixed  $n$ -vector of integral values, and  $x$  is a vector of the form  $x = (x_1, \dots, x_d)^T$ . That is, to find non-negative integer solutions for the following system:

$$\begin{aligned} a_{1,1}x_1 &+ \dots + a_{1,d}x_d &= b_1 \\ a_{2,1}x_1 &+ \dots + a_{2,d}x_d &= b_2 \\ \vdots & & \vdots & & \vdots \\ a_{n,1}x_1 &+ \dots + a_{n,d}x_d &= b_n \end{aligned} \tag{3.5}$$

Solutions of the diophantine equations as those mentioned above are tightly connected to the existence and enumeration of lattice points on convex polytopes (higher-dimensional analogs of a convex polygon). Convex polytopes are fundamental geometric objects. The study of polytopes is focused on optimization. For example, finding the maximum value attained by some linear objective function. This problem is central to linear programming, and algorithms to solve such problems are vital in business, economics, modeling, operations research, and related fields.

From a pure math standpoint, polytopes sometimes arise as combinatorial objects whose properties can be used to describe other objects, among them several solutions to a suitable system of polynomial equations. Polytopes are helpful to construct some algebraic objects. Such as toric varieties. Since their properties can be described in terms of combinatorial properties of polytopes, a considerable number of combinatorial structures can be counted as lattice points of polytopes. For example, matchings on graphs,  $t$ -designs, linear extensions of posets, and of course, magic squares.

In this section, we will discuss some linear algebra background and the basic definitions of polytopes and polyhedra.

A **linear subspace** of dimension  $n$  in a vector space  $\mathbb{R}^d$  is the span of  $n$  linearly independent vectors of  $\mathbb{R}^d$  [34], where  $\mathbb{R}$  is the field of real numbers. Alternatively, it is the standard zero set of  $d-n$  linearly independent elements of  $(\mathbb{R}^d)^*$ . Thus one can either think of it as:

- The set of vectors

$$L = \{\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n : \lambda_i \in \mathbb{R}\}$$

for some linearly independent set  $\{x_1, x_2, \dots, x_n\} \subset \mathbb{R}^d$ .

- The kernel of the  $(d-n) \times d$  matrix  $A$  with rows  $a_1, a_2, \dots, a_{d-n} \in \mathbb{R}^d$  linearly independent .

An affine subspace  $F$  is a translation of a linear subspace. Hence it is represented as the set of vectors of the form  $F = \{\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n + x_0 : \lambda_i \in \mathbb{R}\}$  or as the solution set to a matrix equation  $Ax = z$ .

Note that if in the first description we let  $y_0 = x_0$  and  $y_i = x_i + x_0$  for  $0 < i \leq n$ , then  $y_i \in F$  for all  $0 \leq i$ , and the condition becomes:

$$\begin{aligned} F &= \{\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n + x_0 : \lambda_i \in \mathbb{R}\} \\ &= \{\lambda_1 (y_1 - y_0) + \lambda_2 (y_2 - y_0) + \cdots + \lambda_n (y_n - y_0) + y_0 : \lambda_i \in \mathbb{R}\} \\ &= \{\lambda_0 y_0 + \lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_n y_n : \lambda_i \in \mathbb{R}, \sum_{i=0}^n \lambda_i = 1\}. \text{ Here } \lambda_0 = 1 - \sum_{i=1}^n \lambda_i. \end{aligned}$$

For any  $y_0, y_1, \dots, y_n$ , their affine span or affine hull  $F$  is obtained thanks to the construction above.

A subset  $K$  of  $\mathbb{R}^d$  is called **convex** if, for any  $x, y \in K$ , the segment with endpoints  $x$  and  $y$  is contained in  $K$ , in other words:

$$[x, y] = \{\lambda x + (1 - \lambda)y : \lambda \in [0, 1]\} \subseteq K$$

Note that the intersection of any number of convex sets is again convex.

A polytope  $P \subset \mathbb{R}^d$  is the convex hull of finitely many points. Remember that a convex hull is a set the unique minimal convex set containing  $P$ . Thus for any  $K \subset \mathbb{R}^d$ , the "smallest" convex set containing  $K$ , called the convex hull of  $K$ , can be constructed as the intersection of all convex sets that contain  $K$ :

$$\text{conv}(K) = \bigcap \{K' \subset \mathbb{R}^d : K \subseteq K', K' \text{ is convex}\} \quad (3.6)$$

When  $K$  is finite, then the convex hull is the projected simplex spanned by  $K$  and therefore:

$$\text{conv}(K) = \{\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_k x_k : \{x_1, x_2, \dots, x_k\} \subseteq K, 0 \leq \lambda_i, \sum_{i=1}^k \lambda_i = 1\} \quad (3.7)$$

The dimension of a polytope is the dimension of its affine hull. A  $d$ -polytope is a polytope of dimension  $d$  in some  $\mathbb{R}^e, e \geq d$ . Two polytopes  $P \subset \mathbb{R}^d$  and  $Q \subset \mathbb{R}^e$  are affinely isomorphic, denoted by  $P \cong Q$  if there is an affine map  $f : \mathbb{R}^d \rightarrow \mathbb{R}^e$  that is a bijection between the points of the two polytopes. It is useful to assume (without loss of generality) that the polytopes are full-dimensional so that  $d$  denotes both the dimension of the polytope and the dimension of the ambient space  $\mathbb{R}^d$ . Some examples of affinely isomorphic polytopes are zero-dimensional polytopes that are points and one-dimensional polytopes that are line segments.

One of the diophantine problems associated with polytopes arises from the question [9] *How many ways are there to give the change of 10 dollars into pennies ( $p$ ), nickels ( $n$ ), dimes ( $d$ ), quarters ( $q$ ), using exactly 100 coins?* The answer to this question is equivalent to the number of solutions of the system of linear equations  $p + 5n + 10d + 25q = 10000, p + n + d + q = 100$ . The nature and restrictions of this kind of problems generate the need for a general theory for working with volumes and lattice points.

A lattice is a set  $\Lambda = \Lambda(v_1, \dots, v_k) = \{\sum_{i=1}^k \lambda_i v_i : \lambda_i \in \mathbb{Z}\} \subseteq \mathbb{R}^n$  where  $v_1, \dots, v_k$  are linearly independent and are considered the basis of  $\Lambda$ . It is said that  $\Lambda$  is of dimension  $n$  and rank  $k$ . When  $n = k$   $\Lambda$  is said to be full rank. It is worth noting that  $\Lambda$  is a discrete additive subgroup of  $\mathbb{R}^n$ . The standard integer lattice is  $\mathbb{Z}^n$  its basis is  $\{e_1, \dots, e_n\}$ , where  $e_i$  is a vector in which the  $i$ -component is 1 and every other component is 0.

**Proposition 2.** *Let  $V = \{v_1, \dots, v_n\} \subseteq \mathbb{Z}^n$ .  $V$  is a basis for  $\mathbb{Z}^n$  if and only if  $|\det(V)| = 1$ , considering  $V$  as the matrix whose columns are  $v_1, \dots, v_n$ .*

*Proof.*  $V$  is a basis for  $\mathbb{Z}^n$  if and only if each  $e_i$  is an integer linear combination of  $v_i$  since the  $e_i$  are known basis of  $\mathbb{Z}^n$ . The previous statement is true if and only if  $V$  is invertible and each entry of  $V^{-1}$  is an integer. If  $|\det(V)| \neq 1$ , then either is not invertible or  $1 < |\det(V)|$ . In the latter case  $V^{-1}$  has determinant  $\frac{1}{\det(V)}$ , which cannot be an integer. Hence  $V^{-1}$  cannot have integer entries. On the other hand, if  $|\det(V)| = 1$ , then by Cramer's rule,  $V^{-1}$  has integer entries.

□

When all the points on a polytope are on a lattice, it is considered a lattice polytope. All lattices will be the standard lattice  $\mathbb{Z}^d$  unless specified otherwise. The size of a polytope is the number of lattice points inside the polytope, and its normalized volume is the Euclidean volume of the polytope multiplied by  $d!$ . These concepts are invariant modulo unimodular equivalence, considering that two lattice polytopes  $P$  and  $Q$  are unimodular equivalent if and only if there exists  $A \in \mathbb{Z}^{d \times d}$  and  $b \in \mathbb{Z}^d$  such that  $|\det(A)| = 1$  and  $Q = AP + b$ .

A natural question related to a given convex hull  $P$  is how many lattice points

are inside of  $P$  or, in other words, the size of  $P$  viewed as a lattice polytope. To answer this question it is important to define a counting function  $\Phi_A(b) = |\{x : Ax = b, 0 \leq x, x \in \mathbb{Z}^n\}|$ . This function counts the number of lattice points inside convex polytopes given in terms of a fixed matrix  $A$  and a right-hand-side vector  $b$  that is possibly changing or consists of variables.

If  $A = [3, 5, 17]$ , then the polytope  $P$  is a triangle (embedded in three-dimensional space). It generates the counting function  $\Phi_A(n) = |\{(x, y, z) : 3x + 5y + 17z = n, x \geq 0, y \geq 0, z \geq 0\}|$ . Thus, for example,  $\Phi_A(58) = 9$ ,  $\Phi_A(101) = 25$ ,  $\Phi_A(1110) = 2471$ , etc. A general formula for  $\Phi_A(b)$  could be the generating function whose terms encode the different values of  $\Phi_A$ :

$$\sum_{n=0}^{\infty} \phi_H(n)t^n = \frac{1}{(1-t^3)(1-t^5)(1-t^{17})}$$

in general it holds that:

$$\sum_{n=0}^{\infty} \phi_A(n)t^n = \frac{1}{\prod_{A_j \in A} (1-t^{A_j})}.$$

Where the  $A_i$  symbolizes the  $i$ -column of the matrix  $A$ . To reverse the function and obtain  $\phi_A(n)$ , as shown in [9], is sufficient to solve the following integral, considering  $A$  a  $m \times d$  matrix:

$$\phi_A(n) = \frac{1}{(2\pi i)^m} \int_{|t_1|=\epsilon_1} \cdots \int_{|t_m|=\epsilon_m} \frac{t^{-n_1-1} \cdots t^{-n_m-1}}{(1-t^{A_1}) \cdots (1-t^{A_m})} dt \quad (3.8)$$

Here  $\epsilon_1, \dots, \epsilon_m < 1$  are different numbers such that is possible to expand all the  $\frac{1}{1-t^{A_k}}$  into the power series around 0.

### 3.3 On Diophantine Equations of Type $\mathcal{D}(n_1, n_2, \mathcal{K}_m)$

Another family of problems related to the previously discussed structures is the diophantine problems of type  $\mathcal{D}(n_1, n_2, \mathcal{K}_m)$ . Where  $\mathcal{K}_m = (k_1, k_2, \dots, k_m) \in \mathbb{Z}^m$  and  $n_1, n_2 \in \mathbb{N}$  are defined as diophantine equations of the form:

$$\begin{aligned} \sum_{i=1}^m \lambda_i &= n_1, \\ \sum_{j=1}^m k_j \lambda_j &= n_2. \end{aligned} \quad (3.9)$$

Regarding equations of type (3.9), the following results hold:

**Theorem 5.** *If  $\lambda_1, \lambda_2, \dots, \lambda_m$  is solution of  $\mathcal{D}(n_1, n_2, \mathcal{K}_m = (1, 2, \dots, m))$  then  $(\lambda_m, \lambda_{m-1}, \dots, \lambda_1)$  is solution of the diophantine equation  $\mathcal{D}(n_1, (m+1)n_1 - n_2, \mathcal{K}_m)$ .*

*Proof.* If  $(\lambda_1, \lambda_2, \dots, \lambda_m)$  is solution of  $\mathcal{D}(n_1, n_2, \mathcal{K}_m)$  then  $\sum_{i=1}^m \lambda_i = n_1$  and  $\sum_{i=1}^m i\lambda_i = n_2$ . Thus,

$$(m+1)n_1 - n_2 = (m+1)\sum_{i=1}^m \lambda_i - \sum_{i=1}^m i\lambda_i = \sum_{i=1}^m (m+1-i)\lambda_i = \sum_{i=1}^m i\lambda_{m+1-i}. \quad (3.10)$$

Therefore  $(\lambda_m, \lambda_{m-1}, \dots, \lambda_1)$  is solution of the desired equation.

Conversely, if  $(\lambda_m, \lambda_{m-1}, \dots, \lambda_1)$  is solution of  $\mathcal{D}(n_1, (m+1)n_1 - n_2, \mathcal{K}_m)$  then the result holds provided that  $(m+1)n_1 - n'_2 = n_2$ , if  $n'_2 = (m+1)n_1 - n_2$ .  $\square$

For example consider the systems  $\mathcal{D}(11, 26, \mathcal{K}_m = (1, 2, 3, 4, 5))$  the vector  $x = (4, 2, 3, 1, 1)$  is a a solution of the sistem since:

- $4 + 2 + 3 + 1 + 1 = 11$
- $4 + 2 \cdot 2 + 3 \cdot 3 + 4 + 5 = 26$

And considering the reflection vector of  $x$ , that is  $x' = (1, 1, 3, 2, 4)$  it is a solution for  $\mathcal{D}(11, 40, \mathcal{K}_m = (1, 2, 3, 4, 5))$  because:

- $4 + 2 + 3 + 1 + 1 = 11$
- $1 + 2 + 3 \cdot 3 + 4 \cdot 2 + 5 \cdot 4 = 40 = (5 + 1) \cdot 11 - 26$

**Theorem 6.** *It is possible to solve an equation system of the type  $\mathcal{D}(n_1, n_2, \mathcal{K}_m = (1, 2, \dots, m))$  if and only if  $N_1 + \frac{m(m-1)}{2} \leq N_2 \leq mN_1 - \frac{m(m+1)}{2}$ .*

*Proof.* For  $x = (x_1, \dots, x_m) \in \mathbb{N}^m$  if  $x_i < x_j$  for  $i < j$  then for  $x' = (x'_1, \dots, x'_m)$  where  $x'_i = x_j$ ,  $x'_j = x_i$ ,  $x'_k = x_k$  for  $k \notin \{i, j\}$  then  $\sum_{i=1}^m ix_i < \sum_{i=1}^m ix'_i$ , in general  $\sum_{i=1}^m \lambda_i x_i \leq \sum_{i=1}^m \lambda_i x'_i$  if  $\lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_m$ . Therefore the minimum value for  $n_2$  for which  $\mathcal{D}(n_1, n_2, \mathcal{K}_m)$  has a solution is where  $x = (n_1 - m + 1, 1, \dots, 1)$  and the maximum value is for  $x' = (1, 1, \dots, n_1 - m + 1)$  in other words the problem has a solution only if

$$\begin{aligned} \sum_{i=1}^m ix_i &\leq n_2 \leq \sum_{i=1}^m ix'_i \\ n_1 - m + \sum_{i=1}^m i &\leq n_2 \leq \sum_{i=1}^{m-1} i + m(n_1 - m) \\ n_1 - m + \frac{(m+1)m}{2} &\leq n_2 \leq m(n_1 - m) + \frac{m(m-1)}{2} \\ n_1 + \frac{(m-1)m}{2} &\leq n_2 \leq mn_1 - \frac{m(m+1)}{2} \end{aligned} \quad (3.11)$$

$\square$

Considering the following graph where the y axis represent the number of solution for the systems  $\mathcal{D}(11, n, (1, 2, 3, 4, 5))$ . The system has solution only if  $21 \leq n \leq 45$  and has a normal distribution. The figure also shows the symmetry of the solutions given by theorem 5.



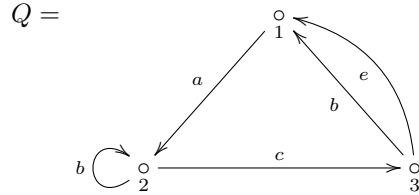
**Figure:**  $\mathcal{D}(11, n, (1, 2, 3, 4, 5))$  .

## 4 Configuration Clusters

This section aims to explore and present the concept of configuration clusters. To achieve this knowledge of representation theory, cluster algebras, and specially Brauer configuration algebras are needed. Considering the number of works and literature on each of these areas, the topics chosen in this work represent a minuscule part specifically chosen to present the ideas and concepts of each area that brought together the concept of configuration clusters.

### 4.1 Quiver Representation

A quiver  $Q$  consists of two sets  $Q_0, Q_1$  and two maps  $h, t : Q_1 \rightarrow Q_0$ . The elements of  $Q_0$  are called the vertices of  $Q$ . While those of  $Q_1$  are called the arrows as presented in [30]. The head map  $h$  and tail map  $t$  assign a head  $h_a$  and a tail  $t_a$  to every arrow  $a \in Q_1$ . Graphically,  $Q$  can be represented as a directed graph with one vertex for each element in  $Q_0$  and one arrow per element  $a \in Q_1$ . Note that there are no restrictions on the sets  $Q_0, Q_1$ , so technically, this graph is a multigraph possibly infinite.



A representation of  $Q$  over a field  $\mathbb{F}$  is a pair  $\mathbb{V} = (V_{\mathbb{F}}, v_{\mathbb{F}})$  consisting of a set of  $\mathbb{F}$ -vector spaces  $V_{\mathbb{F}} = \{V_i : i \in Q_0\}$  and a set of  $\mathbb{F}$ -linear maps  $v_{\mathbb{F}} = \{v_a : V_{t_a} \rightarrow V_{h_a} : a \in Q_1\}$ . A subrepresentation  $\mathbb{W}$  of  $\mathbb{V}$  is a representation of  $Q$  over a field  $\mathbb{F}$  such that  $W_i$  is a subspace of  $V_i$  for every  $i \in Q_0$  and the map  $w_a$  is the restriction of  $v_a$  to  $W_i$ .

Morphisms between representations  $\mathbb{V}, \mathbb{W}$  of  $Q$  is a set of  $\mathbb{F}$ -linear maps  $\Phi$  such that the following diagram commutes for every  $a \in Q_1$ :

$$\begin{array}{ccc}
 V_{t_a} & \xrightarrow{v_a} & W_{h_a} \\
 \Phi_{t_a} \downarrow & & \downarrow \Phi_{h_a} \\
 V_{t_a} & \xrightarrow{w_a} & W_{h_a}
 \end{array}$$

### 4.2 The Category of Representations

The representations of a given quiver  $Q$  over a fixed base field  $\mathbb{F}$ , together with the morphisms connecting them, form a category denoted  $Rep_{\mathbb{F}}(Q)$ . This category turns out to be abelian, so some of the nice properties of single vector spaces carry over to representations of arbitrary quivers. In particular:

- The existence of a zero item on the category.
- It is possible to form internal and external direct sums of representations.
- The kernel and cokernel exist for any morphism in the category.

It may seem that the representation of quivers has the same characteristics and difficulty as the representation of vector spaces. However, the representation category over a quiver  $Q$  not all its objects have a complement. For instance  $\mathbb{W} = 0 \xrightarrow{w_a} \mathbb{F}$  is a subrepresentation of  $\mathbb{V} = \mathbb{F} \xrightarrow{v_a} \mathbb{F}$  but there is no subrepresentation  $\mathbb{U}$  of  $\mathbb{V}$  such that  $\mathbb{V} = \mathbb{W} \oplus \mathbb{U}$ . This obstruction makes the classification of quiver representations and essentially a more challenging problem than for single vector spaces.

The classification of quiver representations tries to answer the question: given a fixed quiver  $Q$  and a fixed base field  $\mathbb{F}$ , what are the isomorphism classes of representations of  $Q$  over  $\mathbb{F}$ ?

**Theorem 7** ([22], Theorem 1.1). (*Krull, Remak, Schmidt*). *Let  $Q$  be a finite quiver, and let  $\mathbb{F}$  be a field. Then, every finite-dimensional representation  $\mathbb{V}$  of  $Q$  over  $\mathbb{F}$  decomposes as a direct sum*

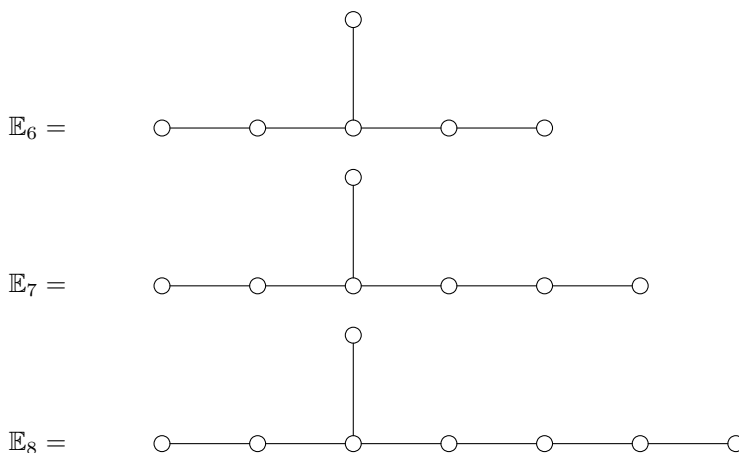
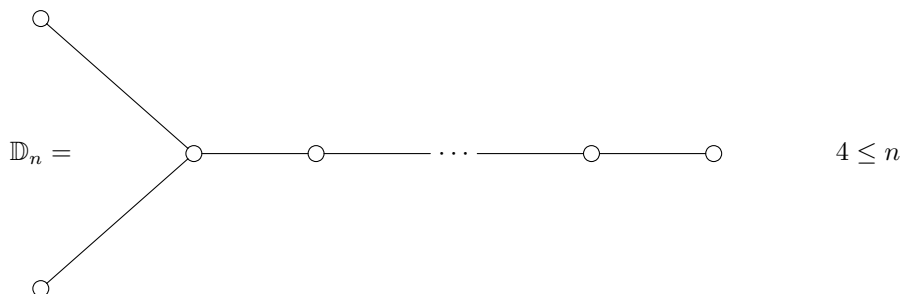
$$\mathbb{V} = \mathbb{V}^1 \oplus \dots \oplus \mathbb{V}^r \tag{4.12}$$

where each  $\mathbb{V}^i$  is itself indecomposable, meaning it cannot be further decomposed into a direct sum of at least two nonzero representations. Moreover, the decomposition is unique up to isomorphism and permutation of the terms in the direct sum.

A quiver  $Q$  is of finite representation type if the number of isomorphism classes of indecomposable representations of  $Q$  is finite. It turns out that this classification depends only on the shape of the quiver and not on the particular orientation of the arrows. Therefore the underlying graph of the quiver  $Q$  is obtained by forgetting the direction of the arrows. The underlying graph has the same vertices of  $Q$ , and each arrow in  $Q$  is an edge in the underlying graph.

**Theorem 8** ([30], Theorem 3.1). (*Gabriel Part I*). *A connected quiver is of finite representation type if and only if its underlying graph is one of the Dynkin diagrams of type  $\mathbb{A}$ ,  $\mathbb{D}$ , or  $\mathbb{E}$  presented as:*

$$\mathbb{A}_n = \bigcirc \text{---} \bigcirc \text{---} \bigcirc \text{---} \dots \text{---} \bigcirc \text{---} \bigcirc \qquad 1 \leq n$$



### 4.3 The Fundamentals of Path Algebras

Path algebras, and their ideals based on the work of I. Assem et al. in [2]. The following definition is given by R. Shiffler in [30]. Let  $K$  be an algebraically closed field then, a  $K$ -algebra  $A$  is a ring with a unit such that  $A$  has also a  $K$ -vector space structure such that:

1. the addition in the vector space  $A$  is the same as in the ring  $A$ ,
2. for all  $\lambda \in K$  and  $a, b \in A$ , it is true that

$$\lambda(ab) = (\lambda a)b = a(\lambda b) = (ab)\lambda$$

The dimension of algebra  $A$  is its dimension as a vector space.

For a quiver  $Q$  a sequence of directed edges  $a_1, \dots, a_m$  defines a directed path  $p$  in  $Q$  if for each  $1 \leq i \leq m$   $t(a_i) = h(a_{i+1})$ . Then  $p$  has head  $h(p) = h(a_1)$  and tail  $t(p) = t(a_m)$ . The concatenation  $pq$  is defined in the natural way if  $t(p) = h(q)$  and as 0 otherwise. Where  $Q$  is a directed graph, and  $k$  a field

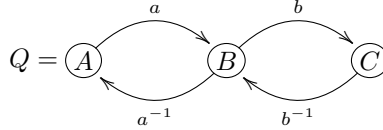
(assumed algebraically closed), the path algebra  $kQ$  is defined to be the  $k$ -algebra spanned by the directed paths in  $Q$ , with the product of paths defined as before and the addition in  $kQ$  is the usual  $k$ -vector space addition.

Let  $Q$  be the quiver:

$$\begin{array}{c} \alpha \\ \curvearrowright \\ 1 \end{array} \quad (4.13)$$

The paths in  $Q$  are  $e_1, \alpha^1, \alpha^2, \alpha^3, \dots$ . Thus, the algebra  $kQ$  has basis  $\{\alpha^t : t \in \mathbb{N}\}$ , and the multiplication is given by  $\alpha^s \alpha^t = \alpha^{s+t}$ . It follows that  $kQ$  is isomorphic to the algebra of polynomials  $k[x]$ .

Suppose that  $P$  is a set of paths, each of length at least 2. Then the monomial algebra  $KQ/P$  is defined to be the quotient of  $KQ$  defined by setting every path in  $P$  to be zero. The path algebra is a monomial algebra determined by taking  $P$  to be the empty set. If additionally, every vertex in  $Q$  is the head of at most two arrows and also the tail of at most two arrows and given any arrow  $b$ , there is at most one arrow  $a$  with  $t(a) = h(b)$  and  $ab$  outside  $P$ , and also at most one arrow  $c$  with  $h(c) = t(b)$  and  $bc$  outside  $P$ , then  $kQ/P$  is called a string algebra [26].



For the quiver presented above the path algebra,  $kQ$  is a string algebra.

#### 4.4 Brauer Configuration Algebras

S. Schroll and E. Green introduced Brauer configuration algebras in [17]. Configuration algebras are a generalization of Brauer graphs algebras, showing that in the same way that for each Brauer graph, there is an underlying Brauer graph algebra, every Brauer configuration has a Brauer configuration algebra associated with it. With the definition of Brauer configuration algebras, Brauer graphs algebras result in a particular case where each polygon is a set with only two vertices. That is why only the definition and some properties of Brauer configuration algebras will be presented in this work.

A *Brauer configuration*  $\Gamma$  is a quadruple of the form  $\Gamma = (\Gamma_0, \Gamma_1, \mu, \mathcal{O})$  where:

- (B1)  $\Gamma_0$  is a finite set whose elements are called *vertices*,
- (B2)  $\Gamma_1$  is a finite collection of multisets called *polygons*. In this case, if  $V \in \Gamma_1$  then the elements of  $V$  are vertices possibly with repetitions,  $\text{occ}(\alpha, V)$  denotes the frequency of the vertex  $\alpha$  in the polygon  $V$  and the *valency* of  $\alpha$  denoted  $\text{val}(\alpha)$  is defined such as:

$$val(\alpha) = \sum_{V \in \Gamma_1} occ(\alpha, V), \quad (4.14)$$

(B3)  $\mu$  is an integer valued function such that  $\mu : \Gamma_0 \rightarrow \mathbb{N}$  where  $\mathbb{N}$  denotes the set of positive integers, it is called the *multiplicity function*,

(B4)  $\mathcal{O}$  denotes an orientation defined on  $\Gamma_1$  which is a choice, for each vertex  $\alpha \in \Gamma_0$ , of a cyclic ordering of the polygons in which  $\alpha$  occurs as a vertex, including repetitions, we denote  $S_\alpha$  such collection of polygons. More specifically, if  $S_\alpha = \{V_1^{(\alpha_1)}, V_2^{(\alpha_2)}, \dots, V_t^{(\alpha_t)}\}$  is the collection of polygons where the vertex  $\alpha$  occurs with  $\alpha_i = occ(\alpha, V_i)$ , meaning that  $S_\alpha$  has  $\alpha_i$  copies of  $V_i$  then an orientation  $\mathcal{O}$  is obtained by endowing a linear order  $<$  to  $S_\alpha$  and adding a relation  $V_t < V_1$ , if  $V_1 = \min S_\alpha$  and  $V_t = \max S_\alpha$ . According to this order the  $\alpha_i$  copies of  $V_i$  can be ordered as  $V_{1,i} < V_{2,i} < \dots < V_{(\alpha_i-1),i} < V_{\alpha_i,i}$  and  $S_\alpha$  can be ordered in the form  $V_1^{(\alpha_1)} < V_2^{(\alpha_2)} < \dots < V_{(t-1)}^{(\alpha_{(t-1)})} < V_t^{\alpha_t}$ ,

(B5) Every vertex in  $\Gamma_0$  is a vertex in at least one polygon in  $\Gamma_1$ ,

(B6) Every polygon has at least two vertices,

(B7) Every polygon in  $\Gamma_1$  has at least one vertex  $\alpha$  such that  $\mu(\alpha)val(\alpha) > 1$ .

The set  $(S_\alpha, <)$  is called the *successor sequence* at the vertex  $\alpha$ .

A vertex  $\alpha \in \Gamma_0$  is said to be *truncated* if  $val(\alpha)\mu(\alpha) = 1$ , that is,  $\alpha$  is truncated if it occurs exactly once in exactly one  $V \in \Gamma_1$  and  $\mu(\alpha) = 1$ . A vertex is *nontruncated* if it is not truncated.

### The Quiver of a Brauer Configuration Algebra

The quiver  $Q_\Gamma = ((Q_\Gamma)_0, (Q_\Gamma)_1)$  of a Brauer configuration algebra is defined in such a way that the vertex set  $(Q_\Gamma)_0 = \{v_1, v_2, \dots, v_m\}$  of  $Q_\Gamma$  is in correspondence with the set of polygons  $\{V_1, V_2, \dots, V_m\}$  in  $\Gamma_1$ , noting that there is one vertex in  $(Q_\Gamma)_0$  for every polygon in  $\Gamma_1$ .

The successor sequences define arrows in  $Q_\Gamma$ . That is, there is an arrow  $v_i \xrightarrow{s_i} v_{i+1} \in (Q_\Gamma)_1$  provided that  $V_i < V_{i+1}$  in  $(S_\alpha, <) \cup \{V_t < V_1\}$  for some non-truncated vertex  $\alpha \in \Gamma_0$ . In other words, for each non-truncated vertex  $\alpha \in \Gamma_0$  and each successor  $V'$  of  $V$  at  $\alpha$ , there is an arrow from  $v$  to  $v'$  in  $Q_\Gamma$  where  $v$  and  $v'$  are the vertices in  $Q_\Gamma$  associated to the polygons  $V$  and  $V'$  in  $\Gamma_1$ , respectively.

### The Ideal of Relations and Definition of Brauer Configuration Algebra

Fix a polygon  $V \in \Gamma_1$  and suppose that  $\text{occ}(\alpha, V) = t \geq 1$  then there are  $t$  indices  $i_1, \dots, i_t$  such that  $V = V_{i_j}$ . Then the *special  $\alpha$ -cycles* at  $v$  are the cycles  $C_{i_1}, C_{i_2}, \dots, C_{i_t}$  where  $v$  is the vertex in the quiver of  $Q_\Gamma$  associated to the polygon  $V$ . If  $\alpha$  occurs only once in  $V$  and  $\mu(\alpha) = 1$  then there is only one special  $\alpha$ -cycle at  $v$ .

Let  $k$  be a field and  $\Gamma$  a Brauer configuration. The *Brauer configuration algebra associated to  $\Gamma$*  is defined to be the bounded path algebra  $\Lambda_\Gamma = kQ_\Gamma/I_\Gamma$ , where  $Q_\Gamma$  is the quiver associated to  $\Gamma$  and  $I_\Gamma$  is the *ideal* in  $kQ_\Gamma$  generated by the following set of relations  $\rho_\Gamma$  of type I, II and III.

1. **Relations of type I.** For each polygon  $V = \{\alpha_1, \dots, \alpha_m\} \in \Gamma_1$  and each pair of non-truncated vertices  $\alpha_i$  and  $\alpha_j$  in  $V$ , the set of relations  $\rho_\Gamma$  contains all relations of the form  $C^{\mu(\alpha_i)} - C'^{\mu(\alpha_j)}$  where  $C$  is a special  $\alpha_i$ -cycle and  $C'$  is a special  $\alpha_j$ -cycle.
2. **Relations of type II.** Relations of type II are all paths of the form  $C^{\mu(\alpha)}a$  where  $C$  is a special  $\alpha$ -cycle and  $a$  is the first arrow in  $C$ .
3. **Relations of type III.** These relations are quadratic monomial relations of the form  $ab$  in  $kQ_\Gamma$  where  $ab$  is not a subpath of any special cycle unless  $a = b$  and  $a$  is a loop associated to a vertex of valency 1 and  $\mu(\alpha) > 1$ .

As an example consider a configuration  $\Gamma = (\Gamma_0, \Gamma_1, \mu, \mathcal{O})$  such that:

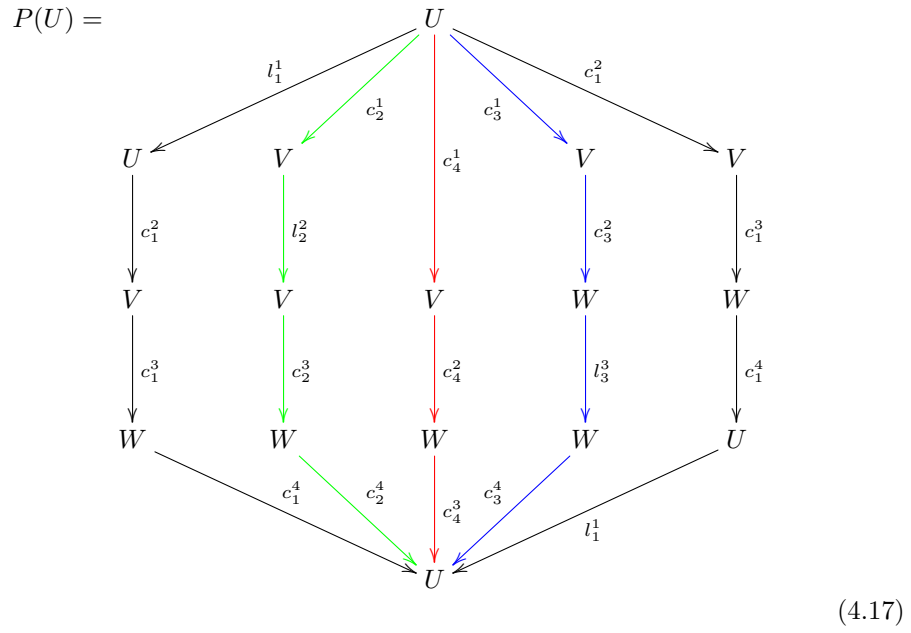
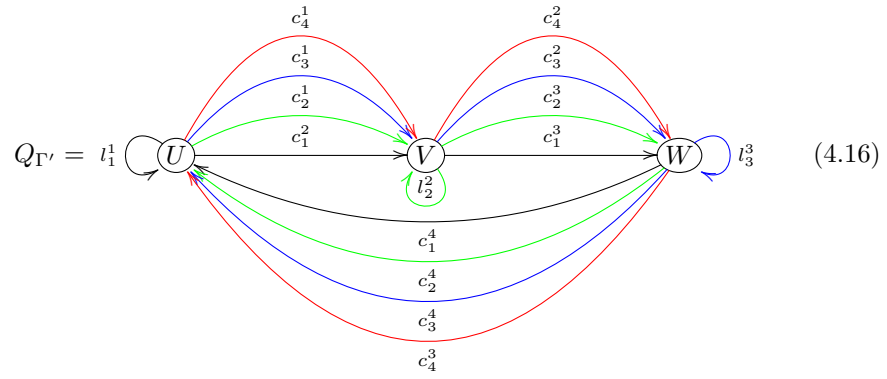
1.  $\Gamma_0 = \{1, 2, 3, 4\}$ ,
2.  $\Gamma_1 = \{U = \{1, 1, 2, 3, 4\}, V = \{1, 2, 2, 3, 4\}, W = \{1, 2, 3, 3, 4\}\}$ ,
3.  $\mu(\alpha) = 1$  for any vertex  $\alpha$ ,
4.  $\mathcal{O}$  we have that  $A < B < C < A$ ,
5. At vertex 1, it holds that;  $S_1 = \{U^{(2)}V^{(1)}W^{(1)}\}$ ,  $X < X < Y < Z$ ,  $\text{val}(1) = 4$ ,
6. At vertex 2, it holds that;  $S_2 = \{U^{(1)}V^{(2)}W^{(1)}\}$ ,  $X < Y < Y < Z$ ,  $\text{val}(2) = 4$ ,
7. At vertex 3, it holds that;  $S_3 = \{U^{(1)}V^{(1)}W^{(2)}\}$ ,  $X < Y < Z < Z$ ,  $\text{val}(3) = 3$ ,
8. At vertex 4, it holds that;  $S_4 = \{U^{(1)}V^{(1)}W^{(1)}\}$ ,  $X < Y < Z$ ,  $\text{val}(4) = 3$ .

The ideal  $I$  of the corresponding Brauer configuration algebra  $\Lambda_\Gamma$  is generated by the following relations (see Figure 4.16), for which it is assumed the following notation for the special cycles:

$$\begin{aligned}
P_1^{u,1} &= l_1^1 c_1^2 c_1^3 c_1^4, \\
P_2^{u,1} &= c_1^2 c_1^3 c_1^4 l_1^1, \\
P_3^{u,2} &= c_2^1 l_2^2 c_2^3 c_2^4, \\
P_4^{u,3} &= c_3^1 c_3^2 l_3^3 c_3^4, \\
P_5^{u,4} &= c_4^1 c_4^2 c_4^3, \\
P_1^{v,1} &= c_1^3 c_1^4 l_1^1 c_1^2, \\
P_2^{v,2} &= c_2^3 c_2^4 c_2^1 l_2^2, \\
P_3^{v,2} &= l_2^2 c_2^3 c_2^4 c_2^1, \\
P_4^{v,3} &= c_3^2 l_3^3 c_3^4 c_3^1, \\
P_5^{v,4} &= c_4^2 c_4^3 c_4^1, \\
P_1^{w,1} &= c_1^4 l_1^1 c_1^2 c_1^3, \\
P_2^{w,2} &= c_2^4 c_2^1 l_2^2 c_2^3, \\
P_3^{w,3} &= l_3^3 c_3^4 c_3^1 c_3^2, \\
P_4^{w,3} &= c_3^4 c_3^1 c_3^2 l_3^3, \\
P_5^{w,4} &= c_4^3 c_4^1 c_4^2,
\end{aligned} \tag{4.15}$$

1.  $c_h^i c_s^r$ , if  $h \neq s$ , for all possible values of  $i$  and  $r$ ,
2.  $(l_1^1)^2$ ;  $(l_2^2)^2$ ;  $(l_3^3)^2$ ;  $c_4^1 c_4^2 c_4^3$ ;  $c_3^1 c_3^2 c_3^4$ ;  $c_2^1 c_2^3 c_2^4$ ;  $c_1^2 c_1^3 c_1^4$ ,
3.  $P_j^{u,i} - P_l^{u,k}$ , for all possible values of  $i, j, k$  and  $l$ ,
4.  $P_j^{v,i} - P_l^{v,k}$ , for all possible values of  $i, j, k$  and  $l$ ,
5.  $P_i^{u,j} a (P_i^{v,j} a')$ , with  $a$  ( $a'$ ) being the first arrow of  $P_i^{u,j}$  ( $P_i^{v,j}$ ) for all  $i, j$ .

The following diagrams (4.16-4.19) show the quiver  $Q_\Gamma$  associated with this configuration, the indecomposable projective modules  $P_U$  and  $P_V$ , and the corresponding heart and radical square of these modules.





$\{\bar{p} \mid p \text{ is a proper prefix of some } C^{\mu(\alpha)} \text{ where } C \text{ is a special } \alpha\text{-cycle}\} \cup \{\overline{C^{\mu(\alpha)}} \mid V \in \Gamma_1\}$  is a  $k$ -basis of  $\Lambda$ .

**Proposition 6** ([17], Proposition 3.13.). *Let  $\Lambda$  be a Brauer configuration algebra associated to the Brauer configuration  $\Lambda$  and let  $\mathcal{C} = \{C_1, \dots, C_t\}$  be a full set of equivalence class representatives of special cycles. Assume that for  $i = 1, \dots, t$ ,  $C_i$  is a special  $\alpha_i$ -cycle where  $\alpha_i$  is a non-truncated vertex in  $\Gamma$ . Then*

$$\dim_k \Lambda = 2|Q_0| + \sum_{C_i \in \mathcal{C}} |C_i|(n_i|C_i| - 1), \quad (4.20)$$

where  $|Q_0|$  denotes the number of vertices of  $Q$ ,  $|C_i|$  denotes the number of arrows in the  $\alpha_i$ -cycle  $C_i$  and  $n_i = \mu(\alpha_i)$ .

A. Sierra [32] proved the following result regarding the center of a Brauer configuration algebra.

**Theorem 12** ([32], Proposition 3.13). *Let  $\Gamma$  be a reduced (i.e., without truncated vertices) and connected Brauer configuration and let  $Q$  be its induced quiver and let  $\Lambda$  be the induced Brauer configuration algebra such that  $\text{rad}^2 \Lambda \neq 0$  then the dimension of the center of  $\Lambda$  denoted  $\dim_k Z(\Lambda)$  is given by the formula:*

$$\dim_k Z(\Lambda) = 1 + \sum_{\alpha \in \Gamma_0} \mu(\alpha) + |\Gamma_1| - |\Gamma_0| + \#(\text{Loops } Q) - |\mathcal{C}_\Gamma|. \quad (4.21)$$

where  $\mathcal{C}_\Gamma = \{\alpha \in \Gamma_0 \mid \text{val}(\alpha) = 1, \text{ and } \mu(\alpha) > 1\}$ .

Dimensions of some Brauer configuration algebras and its centers allow to give an algebraic description of the structure of the AES keys.

#### 4.4.1 The Message of a Brauer Configuration

The notion of labeled Brauer configurations and the message of a Brauer configuration was introduced by P. F. Fernández et al. to define suitable specializations of some Brauer configuration algebras [11]. According to them, since polygons in a Brauer configuration  $\Gamma = (\Gamma_0, \Gamma_1, \mu, \mathcal{O})$  are multisets, it is possible to assume that any polygon  $U \in \Gamma_1$  is given by a word  $w(U)$  of the form

$$w(U) = x_1^{s_1} x_2^{s_2} \dots x_{t-1}^{s_{t-1}} x_t^{s_t} \quad (4.22)$$

where for each  $i$ ,  $1 \leq i \leq t$ ,  $s_i$  is the number of times that the vertex  $x_i$  occurs in the polygon. In particular, if vertices  $x_i$  in a polygon  $U$  of a Brauer configuration are integer numbers then the corresponding word  $w(U)$  is interpreted as a partition of an integer number  $n_U$  associated to the polygon  $U$  where it is assumed that each vertex  $x_i$  is a part of the partition and  $s_i$  is the number of times that the part  $x_i$  occurs in the partition and  $n_U = \sum_{i=1}^t s_i x_i$ .

The message is in fact an element of an algebra of words  $\mathscr{W}_\Gamma$  associated to a fixed Brauer configuration such that for a given field  $\mathbb{F}$  the word algebra  $\mathscr{W}_\Gamma$  consists of formal sums of words with the form

$$\sum_{\substack{\alpha_i \in \mathbb{F} \\ U \in \Gamma_1}} \alpha_i w(U)$$

where  $0w(U) = \varepsilon$  is the empty word, and  $1w(U) = w(U)$  for any  $U \in \Gamma_1$ . The product in this case is given by the usual word concatenation. The formal product (or word product)

$$M(\Gamma) = \prod_{U \in \Gamma_1} w(U) \quad (4.23)$$

is said to be the *message of the Brauer configuration*  $\Gamma$ .

An *integer specialization* of a Brauer configuration  $\Gamma = \{\Gamma_0, \Gamma_1, \mu, \mathcal{O}\}$  is a Brauer configuration  $\Gamma^e = (\Gamma_0^e, \Gamma_1^e, \mu^e, \mathcal{O}^e)$  endowed with a preserving orientation map  $e : \Gamma_0 \rightarrow \mathbb{N}$ , such that

$$\begin{aligned} \Gamma_0^e &= \text{Img } e \subset \mathbb{N}, \\ \Gamma_1^e &= e(\Gamma_1), \quad \text{if } H \in \Gamma_1 \text{ then } e(H) = \{e(\alpha_i) \mid \alpha_i \in H\} \in e(\Gamma_1), \\ \mu^e(e(\alpha)) &= \mu(\alpha), \text{ for any } \alpha \in \Gamma_0. \end{aligned} \quad (4.24)$$

Orientation  $\mathcal{O}^e$  is given by defining a linear order  $\triangleleft$  such that  $e(U) \triangleleft e(V)$  in  $\Gamma_1^e$  provided that  $U < V$  in  $\Gamma_1$ .

We let  $w^e(U) = (e(\alpha_1))^{f_1} (e(\alpha_2))^{f_2} \dots (e(\alpha_n))^{f_n}$  denote the specialization under  $e$  of a word  $w(U)$ . In such a case,  $M(\Gamma^e) = \prod_{U \in \Gamma_1^e} w^e(U)$  is the *specialized message*

of the Brauer configuration  $\Gamma$  with the usual integer sum and product (in general with the sum and product associated to  $\text{Img } e$ ).

## 4.5 Cluster Algebras

S. Fomin and A. Zelevinsky introduced the term cluster algebra [13], as a sub-algebra of a field of rational functions generated by a set of  $n$  cluster variables [12, 14, 15]. The cluster algebras are related to different topics in mathematics, as algebraic combinatorics, Lie theory, discrete dynamical systems, tropical geometry, and others [4, 12, 21].

Let  $\mathbb{T}_n$  be the  $n$ -regular tree whose edges are labeled by the numbers  $1, \dots, n$ , so that the  $n$ -edges incident to each vertex receive different labels. The symbol  $t \overset{k}{-} t'$  is used to denote that vertices  $t, t' \in \mathbb{T}_n$  are joined by an edge labeled by  $k$ .

If  $\mathcal{F}$  is a field isomorphic to the field of rational functions over  $\mathbb{C}$  (alternatively over  $\mathbb{Q}$ ) in  $m$  independent variables, then a *labeled seed of geometric type* over  $\mathcal{F}$  is a pair  $(\tilde{x}, \tilde{B})$  where:

1.  $\tilde{x} = (x_1, x_2, \dots, x_m)$  is an  $m$ -tuple of elements of  $\mathcal{F}$  forming a free generating set, that is,  $x_1, x_2, \dots, x_m$  are algebraically independent, and  $\mathcal{F} = \mathbb{C}(x_1, \dots, x_m)$ ,
2.  $\tilde{B} = (b_{ij})$  is an  $m \times n$  extended skew-symmetrizable integer matrix.  $\tilde{B}$  is said to be the extended exchange matrix of the seed. Its top  $n \times n$  submatrix  $B$  is the exchange matrix.

Let  $(\tilde{X}, \tilde{B})$  be a labeled seed as above. Take an index  $k \in \{1, 2, \dots, n\}$ . The *seed mutation in direction  $k$*  transforms  $(\tilde{x}, \tilde{B})$  into the new labeled seed  $\mu_k(\tilde{x}, \tilde{B}) = (\tilde{x}', \tilde{B}')$  defined as follows;

$$\tilde{B}' = \mu_k(\tilde{B}) = (b'_{ij}) \tag{4.25}$$

where

$$b'_{ij} = \begin{cases} -b_{ij}, & \text{if } i = k \text{ or } j = k, \\ b_{ij} + b_{ik}b_{kj}, & \text{if } b_{ik} > 0 \text{ and } b_{kj} > 0, \\ b_{ij} - b_{ik}b_{kj}, & \text{if } b_{ik} < 0 \text{ and } b_{kj} < 0, \\ b_{ij}, & \text{otherwise.} \end{cases}$$

The *extended cluster*  $\tilde{x}' = (x'_1, \dots, x'_m)$  is given by the identifications  $x'_j = x_j$  for  $j \neq k$ , whereas  $x'_k \in \mathcal{F}$  is determined by the exchange rule.

$$x_k x'_k = \prod_{b_{ik} > 0} x_i^{b_{ik}} + \prod_{b_{ik} < 0} x_i^{-b_{ik}}. \tag{4.26}$$

A *seed pattern* is defined by assigning a labeled seed  $(\tilde{x}(t), \tilde{B}(t))$  to every vertex,  $t \in \mathbb{T}_n$ , so that the seeds assigned to the end points of any edge  $t \overset{k}{-} t'$  are obtained from each other by the seed mutation in direction  $k$ . A seed pattern is uniquely determined by one of its seeds.

Let  $(\tilde{x}(t), \tilde{B}(t))_{t \in \mathbb{T}_n}$  be a seed pattern as above, and let  $\mathcal{X} = \bigcup_{t \in \mathbb{T}_n} x(t)$  be the set of all cluster variables appearing in its seeds. We let the ground ring be  $R = \mathbb{C}[x_{n+1}, \dots, x_m]$  the polynomial ring generated by the *frozen variables*.

The *cluster algebra*  $\mathcal{A}$  (of geometric type over  $R$ ) associated with the given seed pattern is the  $R$ -subalgebra of the ambient field  $\mathcal{F}$  generated by all cluster variables  $\mathcal{A} = R[\mathcal{X}]$ . This definition of cluster algebras was given by S. Fomin et al. [14].

### 4.5.1 Cluster Algebras From Quivers

Cluster algebras associated with quivers are defined as follows [20]:

Fix an integer  $n \geq 1$ . In this case, a seed  $(Q, u)$  consists of a finite quiver  $Q$  without loops or 2-cycles with vertex set  $\{1, \dots, n\}$ , whereas  $u$  is a free-generating set  $\{u_1, \dots, u_n\}$  of the field  $\mathbb{Q}(x_1, \dots, x_n)$ .

Let  $(Q, u)$  be a seed and  $k$  a vertex of  $Q$ . The mutation  $\mu_k(Q, u)$  of  $(Q, u)$  at  $k$  is the seed  $(Q', u')$ , where:

(a)  $Q'$  is obtained from  $Q$  as follows:

- (1) reverse all arrows incident with  $k$ ,
- (2) for all vertices  $i \neq j$  distinct from  $k$ , modify the number of arrows between  $i$  and  $j$ , in such a way that a system of arrows of the form  $(i \xrightarrow{r} j, i \xrightarrow{s} k, k \xrightarrow{t} j)$  is transformed into the system  $(i \xrightarrow{r+st} j, k \xrightarrow{s} i, j \xrightarrow{t} k)$ . And the system  $(i \xrightarrow{r} j, j \xrightarrow{t} k, k \xrightarrow{s} i)$  is transformed into the system  $(i \xrightarrow{r-st} j, i \xrightarrow{s} k, k \xrightarrow{t} j)$ . Where,  $r, s$  and  $t$  are non-negative integers, an arrow  $i \xrightarrow{l} j$ , with  $l \geq 0$  means that  $l$  arrows go from  $i$  to  $j$  and an arrow  $i \xrightarrow{l} j$ , with  $l \leq 0$  means that  $-l$  arrows go from  $j$  to  $i$ .

(b)  $u'$  is obtained from  $u$  by replacing the element  $u_k$  with

$$u_k = \frac{1}{u_k} \left( \prod_{\text{arrows } i \rightarrow k} u_i + \prod_{\text{arrows } k \rightarrow j} u_j \right). \quad (4.27)$$

If there are no arrows from  $i$  with target  $k$ , the product is taken over the empty set and equals 1. It is not hard to see that  $\mu_k(\mu_k(Q, u)) = (Q, u)$ . In this case, the matrix mutation  $B'$  has the form

$$b'_{ij} = \begin{cases} -b_{ij}, & \text{if } i = k \text{ or } j = k, \\ b_{ij} + \text{sgn}(b_{ik})[b_{ik}b_{kj}]_+, & \text{else,} \end{cases}$$

where  $[x]_+ = \max(x, 0)$ . Thus, if  $Q$  is a finite quiver without loops or 2-cycles with vertex set  $\{1, \dots, n\}$ , the following interpretations take place:

1. the clusters with respect to  $Q$  are the sets  $u$  appearing in seeds,  $(Q, u)$  obtained from an initial seed  $(Q, x)$  by iterated mutation,
2. the cluster variables for  $Q$  are the elements of all clusters,
3. the cluster algebra  $\mathcal{A}(Q)$  is the  $\mathbb{Q}$ -subalgebra of the field  $\mathbb{Q}(x_1, \dots, x_n)$  generated by all the cluster variables.

As an example, the cluster variables associated to the quiver  $Q = 1 \rightarrow 2$  are:

$$\left\{x_1, x_2, \frac{1+x_2}{x_1}, \frac{1+x_1+x_2}{x_1x_2}, \frac{1+x_1}{x_2}\right\}.$$

In this work, Brauer configuration algebras and cluster algebras will be merged to describe an algebraic structure for the AES keys.

## 4.6 Cluster Configurations

The concept of mutating Brauer configuration algebras was introduced in [5] by A.M Cañadas, I.D. Marin, and J.D. Camacho. For the mutation of configuration algebras is needed the definition of a seed  $(\Gamma, \mathcal{X})$ , where  $\mathcal{X} = (x_0, x_1, \dots, x_{l-1})$  with  $x_i = (y_{i,0}, \dots, y_{i,s-1}) \in \mathbb{F}^s$  where  $\mathbb{F} = \mathbb{A}[x]/\langle p(x) \rangle$  for a suitable irreducible polynomial  $p(x)$  of degree  $n \geq 1$  and an integral domain  $\mathbb{A}$ .

$\Gamma = \{\Gamma_0, \Gamma_1, \mu, \mathcal{O}\}$  is a Brauer configuration for which:

$$\begin{aligned} \Gamma_0 &= \mathbb{A}, \\ \Gamma_1 &= \{w(0), w(1), \dots, w(l-1) : \text{as vector } w(i) \in \mathbb{A}^{sn}\}, \\ w(i) &= (w_{i,0}, \dots, w_{i,s-1}), w_{i,j} \text{ is the binary expansion of } y_{i,j} \\ \mu(0) &= \mu(1) = 1. \end{aligned} \tag{4.28}$$

For the orientation  $\mathcal{O}$  in successor sequences, it is considered the order  $w(0) < w(1) < \dots < w(l-1)$ .

A *mutation*  $\mathcal{M}(\Gamma, \mathcal{X}) = (\Gamma', \mathcal{X}')$  is given by a Brauer configuration  $\mathcal{M}(\Gamma) = \Gamma' = (\Gamma'_0, \Gamma'_1, \mu', \mathcal{O}')$  and a vector  $\mathcal{X}' = (x'_0, x'_1, \dots, x'_{l-1})$  with  $x'_i \in \mathbb{F}^s$ ,  $0 \leq i \leq l-1$  such that:

$$\begin{aligned} \Gamma'_0 &= \mathbb{A}, \\ \Gamma'_1 &= \{w'(0), w'(1), \dots, w'(l-1) \mid w'(i) \in \mathbb{A}^n\}, \\ x'_i &= (y'_{i,0}, \dots, y'_{i,s-1}), \\ y'_{0,j} &= y_{0,j} + \mathcal{H}(y_{s-1,j}), 0 \leq j \leq s-1 \\ y'_{i,j} &= y_{i,j} + y'_{i-1,j}, i \neq 0, \\ \mu(0) &= \mu(1) = 1. \end{aligned} \tag{4.29}$$

Where  $\mathcal{H}(y_{i,j}) = \lambda y_{i,j} + v$  for some suitable,  $\lambda, v \in \mathbb{F}$ .

For successor sequences, the orientation  $\mathcal{O}'$  is defined in such a way that,

$$w'(0) < w'(1) < \dots < w'(l-1)$$

It turns out that according to the indices assumed for the original seed, the  $i$ th mutation  $\mathcal{M}^i$  has the form:

$$\mathcal{M}^i = \{w(i(l-1)+1), w(i(l-1)+2), \dots, w(i(l-1)+l) \mid w(i) \in \mathbb{A}^n\}.$$

Brauer configurations obtained from mutations are said to be *Brauer clusters*. Polygons are called *cluster polygons*.

For a fixed positive integer  $m_0$ , the  $m_0$ -Brauer cluster,  $\Phi^{m_0}$  is a Brauer configuration,

$$\Phi^{m_0} = (\Phi_0^{m_0}, \Phi_1^{m_0}, \mu, \mathcal{O}) \quad (4.30)$$

such that:

1.  $\Phi_0^{m_0} = \mathbb{A}$ ,
2.  $\Phi_1^{m_0}$  consists of messages of the Brauer clusters  $\mathcal{M}^i$ ,  $i \geq 0$ ,
3.  $\mu(0) = \mu(1) = 1$ ,
4. If  $M(i)$  denotes the message associated to the  $i$ th Brauer cluster then for successor sequences, it is assumed the order  $M(0) < M(1) < \dots < M(m_0)$ .

As an example, consider the mutations of the following seed  $(\Gamma, \mathcal{X} = \{x+1, x\})$ , where  $\mathbb{F} = \mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$ .

$$\begin{aligned} \Gamma &= (\Gamma_0, \Gamma_1, \mu, \mathcal{O}), \\ \Gamma_0 &= \{0, 1\}, \\ \Gamma_1 &= \{w(0) = 11, w(1) = 10\}, \\ \mu(0) &= \mu(1) = 1, \\ v &= 1, \quad \lambda = x, \end{aligned} \quad (4.31)$$

In this case the only non truncated vertex is 1 and sequence at 1 is defined as follows:

$$1 : w(0) < w(0) < w(1). \quad (4.32)$$

The first mutation  $\mathcal{M}(\Gamma) = (\Gamma^1, \mathcal{X}^1 = \{1, x+1\})$  is defined as follows:

$$\begin{aligned} \Gamma^1 &= (\Gamma_0^1, \Gamma_1^1, \mu^1, \mathcal{O}'), \\ \Gamma_0^1 &= \{0, 1\}, \\ \Gamma_1^1 &= \{w^1(0) = 01, w^1(1) = 11\}, \\ \mu^1(0) &= \mu^1(1) = 1, \\ v_{2,0} &= 1, \quad \lambda_2 = x. \end{aligned} \quad (4.33)$$

In this case the only non truncated vetrex is 1 and sequence at 1 is defined as follows:

$$1 : w^1(0) < w^1(1) < w^1(1). \quad (4.34)$$

The second mutation  $\mathcal{M}^2 = (\Gamma^2, \mathcal{X}^2 = \{1, x\})$  is described as follows:

$$\begin{aligned} \Gamma^2 &= (\Gamma_0^2, \Gamma_1^2, \mu^2, \mathcal{O}^2), \\ \Gamma_0^2 &= \{0, 1\}, \\ \Gamma_1^2 &= \{w^2(0) = 01, w^2(1) = 10\}, \\ \mu^2(0) &= \mu^2(1) = 1. \end{aligned} \quad (4.35)$$

In this case successor sequences at 0 and 1 are defined as follows:

$$\begin{aligned} 0 : w^2(0) < w^2(1), \\ 1 : w^2(0) < w^2(1). \end{aligned} \quad (4.36)$$

The third mutation  $\mathcal{M}^3 = (\Gamma^3, \mathcal{X}^3 = \{x + 1, 1\})$  is described as follows:

$$\begin{aligned} \Gamma^3 &= (\Gamma_0^3, \Gamma_1^3, \mu^3, \mathcal{O}^3), \\ \Gamma_0^3 &= \{0, 1\}, \\ \Gamma_1^3 &= \{w^3(0) = 11, w^3(1) = 01\}, \\ \mu^3(0) &= \mu^3(1) = 1. \end{aligned} \quad (4.37)$$

In this case the only non truncated vetrex is 1 and sequence at 1 is defined as follows:

$$1 : w^3(0) < w^3(1) < w^3(1). \quad (4.38)$$

The fourth mutation  $\mathcal{M}^4 = (\Gamma^4, \mathcal{X}^4 = \{0, 1\})$  is described as follows:

$$\begin{aligned} \Gamma^4 &= (\Gamma_0^4, \Gamma_1^4, \mu^4, \mathcal{O}^4), \\ \Gamma_0^4 &= \{0, 1\}, \\ \Gamma_1^4 &= \{w^4(0) = 00, w^4(1) = 01\}, \\ \mu^4(0) &= \mu^4(1) = 1. \end{aligned} \quad (4.39)$$

In this case the only non truncated vetrex is 0 and sequence at 1 is defined as follows:

$$0 : w^4(0) < w^4(1) < w^4(1). \quad (4.40)$$

The fifth mutation  $\mathcal{M}^5 = (\Gamma^5, \mathcal{X}^5 = \{x + 1, x\})$  coincides with the initial seed.

The 5-Brauer cluster  $\Phi^5 = (\Phi_0^5, \Phi_1^5, \mu, \mathcal{O})$  has the following form:

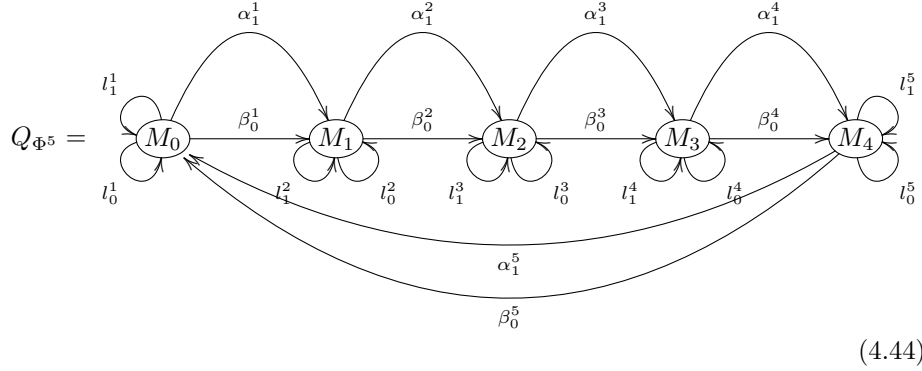
$$\begin{aligned}
\Phi_0^5 &= \{0, 1\}, \\
\Phi_1^5 &= \{M(5) = M(0) = 0111, M(1) = 0111, M(2) = 0110, \\
&\quad M(3) = 1101, M(3) = 0001, M(4) = 0111\}, \\
\mu(0) &= \mu(1) = 1,
\end{aligned} \tag{4.41}$$

For successor sequences, it holds that:

$$M(0) < M(1) < M(2) < M(3) < M(4) < M(5). \tag{4.42}$$

The following  $Q_\Gamma, Q_{\Gamma'}, Q_{\Gamma''}$  and  $Q_{\Phi^2}$  are the Brauer quivers of all these mutations and of the 2-Brauer cluster  $\Phi^2$ .

$$\begin{aligned}
Q_\Gamma &= \begin{array}{ccc} & \beta_1^1 & \\ & \curvearrowright & \\ l_1^1 & \circ_{x+1} & \circ_x \\ & \curvearrowleft & \\ & \beta_1^2 & \end{array} \\
Q_{\Gamma^1} &= \begin{array}{ccc} & \beta_1^1 & \\ & \curvearrowright & \\ \circ_1 & \circ_{x+1} & l_1^1 \\ & \curvearrowleft & \\ & \beta_1^2 & \end{array} \\
Q_{\Gamma^2} &= \begin{array}{ccc} & \alpha_0^2 & \\ & \curvearrowright & \\ \circ_1 & \circ_x & \\ & \alpha_0^1 & \\ & \curvearrowleft & \\ & \beta_1^1 & \\ & \beta_1^2 & \end{array} \\
Q_{\Gamma^3} &= \begin{array}{ccc} & \beta_1^1 & \\ & \curvearrowright & \\ l_1^1 & \circ_{x+1} & \circ_1 \\ & \curvearrowleft & \\ & \beta_1^2 & \end{array} \\
Q_{\Gamma^4} &= \begin{array}{ccc} & \beta_1^1 & \\ & \curvearrowright & \\ l_1^1 & \circ_0 & \circ_1 \\ & \curvearrowleft & \\ & \beta_1^2 & \end{array}
\end{aligned} \tag{4.43}$$



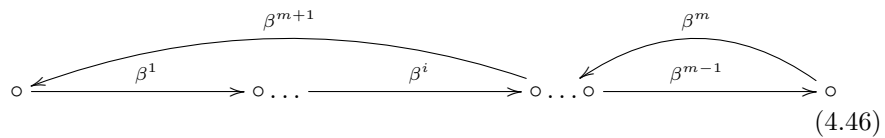
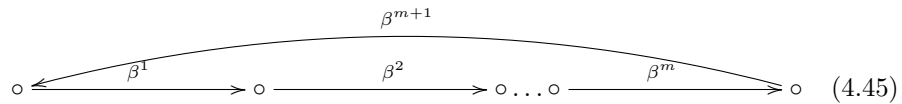
The admissible ideal  $I$  in the Brauer configuration algebra  $\Lambda_{(\Phi^n, \mathcal{X})}$  is generated by the following relations:

1.  $(l_j^i)^2$ ,  $l_0^i l_1^j$ , for all possible values of  $i$  and  $j$ ,
2.  $\alpha_1^i \beta_0^r$ ,  $\alpha_1^i l_0^r$ ,  $l_1^r \alpha_1^i$ , for all possible values of  $i$  and  $r$ ,
3.  $\beta_0^r \alpha_1^i$ ,  $\beta_0^r l_1^s$ ,  $l_j^s \beta_0^r$ , for all possible values of  $i, r$  and  $s$ .

**Theorem 13.** For  $m_0 > 1$ , the Brauer configuration algebra  $\Lambda_{\Phi^{m_0}}$  induced by the Brauer configuration  $\Phi^{m_0}$  (see (4.30)) is connected and reduced.

*Proof.* Since each polygon  $M(i) \in \Phi_1^{m_0}$  contains at least one 0 and at least one 1, it is possible to conclude that  $\Phi^{m_0}$  does not contain truncated vertices. The result follows, provided that  $\bigcap_{i=0}^{m_0} M(i) \neq \emptyset$ .  $\square$

**Theorem 14.** If  $\mathbb{F}$  is a finite field, then the set  $M_\Phi$  of  $m_0$ -Brauer clusters obtained by mutation is finite, and the special cycle of maximal length has one of the two shapes (4.45) or (4.46). Moreover, if  $\Phi^i \neq \Phi^j$  whenever  $i \neq j$  then there exists  $m \in \mathbb{N}$  such that  $(\Gamma, \mathcal{X}) = (\Gamma^{m+1}, \mathcal{X}^{m+1})$  for a given initial seed  $(\Gamma, \mathcal{X})$ .



where  $\beta^m \beta^{m+1} \neq 0$ .

*Proof.* Every mutation  $(\Gamma^i, \mathcal{X}^i)$  is uniquely determined by  $\mathcal{X}^i$ . Since,  $\mathcal{X}^i \in \mathbb{F}^l$  for any  $i \in \mathbb{N}$  then  $|M_\Phi| \leq |\mathbb{F}^l|$ . Note that, since the set  $M$  of mutations is finite, there exist integers  $m$  and  $n$  such that  $M_m(\Gamma, \mathcal{X}) = M_{m+n}(\Gamma, \mathcal{X})$ . If  $\mathcal{M} = \{m \in \mathbb{N} : M_m(\Gamma, \mathcal{X}) = M_{m+n}(\Gamma, \mathcal{X})\}$  and  $\min(\mathcal{M}) = 0$  then the maximal special cycle of the quiver  $Q\Gamma$  obtained after the mutations has the form 4.45, otherwise the special cycle of the quiver  $Q\Gamma$  after the mutations has the form 4.46.  $\square$

## 5 Automata Theory

Computer Science aims to give an abstract representation of problems and processes, understanding that the solutions and techniques developed need to be mechanizable. These problems must be representable and manipulated inside a computer. For this purpose, as exposed in [19] automata are an incredible tool with unbelievable expressiveness.

Automata can be represented as a graph in which an alphabet labels arcs and each vertex is considered a state. There are two special types of states known as starting and accepting states. A basic implementation of an automaton is: getting a sequence of symbols of an alphabet, a word, and follow from the starting state-changing state according to the labeled arcs and the inputted symbol. In this application, an automaton accepts or rejects a word generating a language subset of all possible words known as the recognized language.

The applications of the abstract concept of automata are important and varied kinds of software and hardware such as vending machines, logical processors, and pattern and phrases recognition software. Such a concept has applications to other areas of mathematics as well. Some examples are the creation of language-based fractals and solution of some diophantine problems [28].

The development of automata presented the problem of giving a compatible abstract description of the data obtained by the automata. The first approach was algebraic, and its starting point is considered to be Kleene's theorem for finite deterministic automata showing that the class of recognizable languages for this automaton coincides with rational languages. Regular expressions were defined using three operators union, concatenation, and iterate. Later, J. Brzozowski expanded the definition, including the notion of derivative of a rational expression, which allowed him to prove Kleene's theorem without the need for non-deterministic automata this is further explored in [29].

This algebraic interpretation leads to the definition of the syntactic monoid, a monoid constructed accordingly to each language, an important construct for the algebraic study of these objects. Pressing the fundamental question: what information about a language, or an automaton accepting this language, is encoded in its syntactic monoid? For example, it was shown that a language is recognizable if and only if its syntactic monoid is finite. Even more, M. Schützenberger proved that a rational language is star-free if and only if its syntactic monoid is aperiodic.

However, this algebraic treatment could not describe most of the inherent dynamical structures used in Computer Science. Coalgebras are useful for the representation of infinite data and behavior based on observations instead of construction. Coalgebra theory offers a unifying mathematical framework for state-based behavioral systems and programming paradigms. Most of these new

techniques rely on the description of the final coalgebra.

An alphabet  $A$  is a set whose elements are called letters. A word over an alphabet  $A$  is a finite sequence  $a_1a_2\cdots a_m$  of letters of  $A$ . The empty word that is a word with no letters is denoted as  $\varepsilon$ . The set of all words over  $A$  is denoted by  $A^*$ . Note that  $A^*$  can be regarded as the free monoid over the set  $A$ . Where the multiplication in  $A^*$  is defined as the concatenation of words.

A language  $L$  over  $A$  is a subset  $L \subseteq A^*$ , and the set of all languages over  $A$  is denoted by

$$2^{A^*} = \{L : L \subseteq A^*\}$$

If  $L$  and  $L'$  are languages, some useful operations are ([19], p. 14):

1.  $L + L' = L \cup L'$
2.  $LL' = \{ww' : w \in L, w' \in L'\}$
3. The complement of  $L$  is  $A^* \setminus L$
4. The Kleen star of  $L$ , denoted by  $L^*$ , is  $\cup_{n \in \mathbb{N}} L^n$  with  $L^0 = \{\varepsilon\}$  and  $L^{n+1} = L^n L$ .

The set of all regular languages  $R$  is the smallest set of languages containing all finite languages and closed under taking sums, products, and Kleene stars.

The  $w$ -derivative of  $L$  for some  $w \in A^*$ , as state in [19], is

$$L_w = \{v \in A^* : wv \in L\}$$

This derivative is also called right derivatives of  $L$ , in contrast, the left derivative of  $L$  is

$${}_w L = \{v \in A^* : vw \in L\}$$

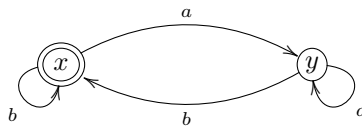
Given an alphabet  $A$ , a *deterministic automaton* is a pair  $(X, \alpha)$  consisting of a (possibly infinite) set  $X$  of states and a transition function  $\alpha : X \rightarrow X^A$  ([19], Definition 2.14.). The following is an illustration of this kind of transition, where  $\alpha(x)(a) = y = x_a$ .

$$\textcircled{x} \xrightarrow{a} \textcircled{y} \tag{5.47}$$

If  $\varepsilon$  denotes the empty word, then  $x_\varepsilon = x$ , for any  $x \in X$  and  $x_{wa} = \alpha(x_w)(a)$  with  $w \in A^*$ .

A deterministic automaton can be decorated through a coloring function  $c : X \rightarrow 2 = \{0, 1\}$  such that  $c(x) = 1$  if and only if  $x$  is an *accepting (or final)* state. A triple  $(X, c, \alpha)$  is a deterministic colored automaton. In the following

diagram, an accepting state is denoted with a double circle,  $x$  is an accepting state, whereas  $y$  is a non-accepting state.



Given a deterministic colored automaton  $(X, c, \alpha)$  and a state  $x \in X$ , the set

$$O_c(x) = \{w \in A^* \mid c(x_w) = 1\}$$

is the *language accepted* or recognized by the automaton  $(X, c, \alpha)$  starting from the state  $x$ . A deterministic automaton also has an *initial state*  $x : 1 = \{0\} \rightarrow X$ . The triple  $(X, x, \alpha)$  is said to be a *deterministic pointed automaton*. For instance, the language accepted by the automaton previously presented is the set of words on the alphabet  $A = \{a, b\}$  where:

- the letter  $b$  can only be followed by the letter  $b$ ,
- the word can not end in a  $a$ .

A *non-deterministic automaton* is a pair  $(X, \alpha)$  consisting of a set  $X$  (possibly infinite) of states and a transition function  $\alpha : X \rightarrow P_w(X)^A$  that assigns to each letter and to each state a finite set of states ([27], Definition 2.17.). If each state is assigned a single new state, the definition of a deterministic automaton is recovered. As in the deterministic case, a state  $x$  in a non-deterministic automaton can be either accepting ( $c(x) = 1$ ) or non-accepting ( $c(x) = 0$ ). And  $x_\varepsilon = \{x\}$ ,  $x_{w_a} = \bigcup \{y_a \mid y \in x_w\}$ . A triple  $(X, c, \alpha)$  is called a *colored non-deterministic automaton*.

## 5.1 Regular Languages

A language is *regular* if it is representable by a regular expression. According to Kleene's theorem, a language is regular if and only if some finite automaton recognizes it.

There is an equivalent definition in terms of monoids. A language  $L$  of  $A^*$  is recognized by a monoid morphism  $\Phi : A^* \rightarrow M$  if there exists a subset  $P$  of the monoid  $M$  such that  $L = \Phi^{-1}(P)$ . By extension,  $L$  is said to be recognized by a monoid  $M$  if a monoid morphism  $\Phi : A^* \rightarrow M$  that recognizes  $L$  exists. In other words, saying a language is recognizable is equivalent to saying that a finite monoid recognizes it ([23], p. 3).

The Nerode automaton of  $L$  is the deterministic automaton  $A(L) = (Q, A, \cdot, L, F)$  where  $Q = \{ {}_u L : u \in A^* \}$ ,  $F = \{ {}_u L : u \in L \}$  and the transition function is defined, for each  $a \in A$ , by the formula

$$({}_u L) \cdot a = {}_{ua} L$$

Each state of  $A(L)$  is a left derivative of  $L$ , and hence is a language of  $A^*$ . The initial state is the language  $L$ , and the set of final states is the set of all left derivatives of  $L$  by a word of  $L$ .

## 5.2 Syntactic Monoids

Let  $L$  be a language over an alphabet  $A$ , and let  $x$  and  $y$  be words. The derivative  ${}_x L^y$  of  $L$  by  $x$  and  $y$  is defined as before:

$${}_x L^y = \{ u \in A^* : xuy \in L \}$$

The syntactic monoid of a language  $L \subseteq A^*$ , as stated in ([23], Section 2.3), is the monoid obtained as the quotient of  $A^*$  by the syntactic congruence of  $L$ , defined on  $A^*$  as follows:

$$u \sim_L v \text{ if and only if, for every } x, y \in A^*, xuy \in L \Leftrightarrow xvy \in L.$$

The natural morphism  $\eta : A^* \rightarrow A^* / \sim_L$  is the syntactic morphism of  $L$ . The syntactic monoid is the smallest monoid recognizing a language. In particular, a language is regular if and only if its syntactic monoid is finite. When the syntactic monoid is isomorphic to a  $p$ -group, a group whose order is a power of a prime  $p$ , it is known as  $p$ -group language [23].

## 5.3 Descriptions of the $p$ -group Languages

Describing the  $p$ -group languages and languages, in general, is usually really difficult. That is why a varied array of tools has been implemented and developed. One such tool is the **binomial coefficients on words** ([23], Definition 3.1).

A word  $u = u_1 u_2 \cdots u_n$ , with  $u_i \in A$ , is a subword of a word  $v$  if  $v$  can be factored as  $v = v_0 u_1 v_1 \cdots u_n v_n$  with  $v_i \in A^*$ . For instance,  $ab$  is a subword of  $cacbc$ . Given two words  $u$  and  $v$ :

$$\binom{v}{u} = \text{denotes the number of distinct ways to write } u \text{ as a subword of } v$$

Formally, if  $u = u_1 u_2 \cdots u_n$ , then

$$\binom{v}{u} = | \{ (v_0, v_1, \dots, v_n) : v_0 u_1 v_1 \cdots u_n v_n = v \} |$$

Observe that if  $u$  is a letter  $a$ , then  $\binom{v}{u}$  is simply the number of occurrences of the letter  $a$  in  $v$ . These binomial coefficients satisfy the following recursive formula, where  $u, v \in A^*$  and  $a, b \in A$ :

$$\left\{ \begin{array}{l} \binom{u}{\epsilon} = 1 \\ \binom{\epsilon}{u} = 0 \quad \text{if } u \neq \epsilon \\ \binom{va}{ub} = \binom{v}{ub} \quad \text{with } a \neq b \\ \binom{vb}{ub} = \binom{v}{ub} + \binom{b}{u} \end{array} \right. \quad (5.48)$$

For instance considering the words  $ababba$  and  $ab$  the binomial coefficients  $\binom{ababba}{ab} = 5$ , because the distinct ways of writing  $ab$  a subword of  $ababba$  are:

$ababba, ababba, ababba, ababba$  and  $ababba$ .

**Proposition 7** ([23], Proposition 3.1.). *Let  $u \in \{a, b\}^*$ . Then the following formula holds*

$$\binom{u}{a} \binom{u}{b} + \binom{u}{ab} + \binom{u}{ba} \equiv 0 \pmod{2} \quad (5.49)$$

*Proof.* Reasoning by induction if  $|u| = 0$  the result is trivial. For the induction step, it suffices to prove the result for  $ua$ . The case  $ub$  is analogs.

$$\begin{aligned} \binom{ua}{a} \binom{ua}{b} + \binom{ua}{ab} + \binom{ua}{ba} &= \left( \binom{u}{a} + \binom{u}{\epsilon} \right) \binom{u}{b} + \binom{u}{ab} + \binom{u}{ba} + \binom{u}{b} \\ &= \binom{u}{a} \binom{u}{b} + \binom{u}{b} + \binom{u}{ab} + \binom{u}{ba} + \binom{u}{b} \\ &= \binom{u}{a} \binom{u}{b} + 2 \binom{u}{b} + \binom{u}{ab} + \binom{u}{ba} \\ &\equiv \binom{u}{a} \binom{u}{b} + \binom{u}{ab} + \binom{u}{ba} \pmod{2} \\ &\equiv 0 \pmod{2} \end{aligned}$$

□

Some characterizations of  $p$ -group languages are given in [10] and [23].

**Proposition 8** ([23], Proposition 4.1.). *A language of  $A^*$  is a  $p$ -group language if and only if it is a Boolean combination of languages of the form*

$$L(x, r, p) = \{u \in A^* : \binom{u}{x} \equiv r \pmod{p}\} \quad (5.50)$$

where  $0 \leq r < p$  and  $x \in A^*$

A function  $f : A^* \rightarrow \mathbb{Z}$  is said to be a **linear combination of binomial coefficients** if there exist  $c_1, \dots, c_n \in \mathbb{Z}$  and  $x_1, \dots, x_n \in A^*$  such that

$$f(u) = c_1 \binom{u}{x_1} + \dots + c_n \binom{u}{x_n}, \text{ for all } u \in A^*. \quad (5.51)$$

Note that since  $f(u) = c \binom{u}{\epsilon} = c$ , for every  $u \in A^*$ , every constant function is a linear combination of binomial coefficients.

**Proposition 9** ([23], Proposition 4.2.). *A language  $A^*$  is a  $p$ -group language if and only if it is a finite union of languages of the form:*

$$L(f_1, \dots, f_r, p) = \{u \in A^* : f_1(u) \equiv \dots \equiv f_r(u) \equiv 0 \pmod{p}\} \quad (5.52)$$

where  $f_1, \dots, f_r$  are linear combinations of binomial coefficients.

*Proof.* Consider the Boolean algebra  $\mathcal{G}_p$  generated by the languages of the form  $L(x, r, p)$  and let  $\mathcal{S}_p$  be the set of languages that are finite unions of languages from  $L(x, r, p)$ .

$\mathcal{S}_p$  is closed under union by definitions. It is also closed under intersection since

$$L(f_1, \dots, f_r, p) \cap L(g_1, \dots, g_s, p) = L(f_1, \dots, f_r, g_1, \dots, g_s, p).$$

In particular,

$$L(f_1, \dots, f_r, p) = L(f_1, p) \cap \dots \cap L(f_r, p).$$

Since  $\mathcal{S}_p$  is closed under union and intersection, it suffices to prove that the complement of each language of the form  $L(f, p)$ , where  $f$  is a linear combination of binomial coefficients, belongs in  $\mathcal{S}_p$ , to show that it is closed under complementation.

$$\begin{aligned} L(f, p)^c &= \{u \in A^* : f(u) \not\equiv 0 \pmod{p}\} \\ &= \bigcup_{c \in \mathbb{F}_p \setminus \{0\}} \{u \in A^* : f(u) \equiv c \pmod{p}\} \\ &= \bigcup_{c \in \mathbb{F}_p \setminus \{0\}} \{u \in A^* : (f - c)(u) \equiv 0 \pmod{p}\} \end{aligned}$$

Where  $c(u)$  is the constant function in  $c$ . As  $f$  and  $c$  are a linear combination of binomial coefficients, the sum of them is also one, and therefore,  $\mathcal{S}_p$  is a boolean algebra.

Note that  $\mathcal{S}_p$  is a subalgebra of  $\mathcal{G}_p$ . For a language  $L(f, p)$ , if  $f$  is given by 5.51 then:

$$L(f, p) = \bigcup_{\{r_1, \dots, r_n : c_1 r_1 + \dots + c_n r_n \equiv 0 \pmod{p}\}} (L(x_1, r_1, p) \cap \dots \cap L(x_n, r_n, p))$$

thus  $L(f, p) \in \mathcal{G}_p$  and by properties of Boolean algebras is possible to conclude that  $\mathcal{S}_p \subseteq \mathcal{G}_p$ .

$\mathcal{G}_p \subseteq \mathcal{S}_p$  immediately follows from the formula  $L(x, r, p) = L(f, p)$  where  $f(u) = -r \binom{u}{\epsilon} + \binom{u}{x}$ . Therefore  $\mathcal{G}_p = \mathcal{S}_p$  and by the characterization in proposition 8 given in [10] is sufficient to conclude the proof.  $\square$

## 5.4 An Algorithm for $p$ -group Language

Let  $p$  be a prime and  $U_m(\mathbb{F}_p)$  be the group of unitriangular  $m \times m$  matrices with coefficients in  $\mathbb{F}_p$ , the finite field of order  $p$ .  $U_m(\mathbb{F}_p)$  is a  $p$ -group and is a known fact that every  $p$ -group is isomorphic to a subgroup of some  $U_m(\mathbb{F}_n)$  for a suitable choice of  $m$ .

Consider the map  $\pi : A \rightarrow U_{n+1}(\mathbb{F}_p)$  and  $G$  the subgroup generated by  $\pi(A)$ . The  $\pi$  can be extended to a surjective monoid morphism  $\pi : A^* \rightarrow G$  which maps every word  $a_1 a_2 \cdots a_k \in A^*$  to the matrix  $\pi(a_1) \pi(a_2) \cdots \pi(a_k)$ . For  $1 \leq i < j \leq n+1$ , define  $\pi_{i,j} : A^* \rightarrow \mathbb{F}_p$  for all  $u \in A^*$  as:

$$\pi_{i,j}(u) = (\pi(u))_{i,j}.$$

A language  $K$  is recognized by  $\pi$  if a subset  $S$  of  $G$  such that  $K = \pi^{-1}(S)$ . According to the second characterization of  $p$ -languages,  $K$  is a finite union of languages of the form  $L(f_1, \dots, f_r, p)$ .

Setting  $K_s = \pi^{-1}(s)$ , for each  $s \in S$ , then:

$$K = \cup_{s \in S} K_s \text{ and}$$

$$K - s = \{u \in A^* : \text{for } 1 \leq i < j \leq n+1, \pi_{i,j}(u) = s_{i,j}\}$$

It just remains to verify that the languages  $K_s$  are of the form  $L(f_1, \dots, f_r, p)$ . The previous statement is a consequence of the following result:

**Theorem 15** ([23], Proposition 4.3.). *Each function  $\pi_{i,j}$  is a linear combination of binomial coefficients.*

To prove this is necessary to introduce a new binomial identity that relies on the properties of the Magnus automorphism. Let  $\mathbb{Z} \langle A \rangle$  be the ring of noncommutative polynomials with coefficients in  $\mathbb{Z}$  and variables in  $A$ . The Magnus automorphism of the ring  $\mathbb{Z} \langle A \rangle$  known as  $\mu_A$  is defined, for each letter  $a \in A$ , by  $\mu_A(a) = 1 + a$ , note that  $\mu_A^{-1}(a) = a - 1$ . Generally for all  $u \in A^*$ :

$$\mu_A(u) = \sum_{x \in A^*} \binom{u}{x} x.$$

**Lemma 3** ([23], Proposition 3.2.). *Let  $\varphi : A^* \rightarrow B^*$  be a morphism with  $u \in A^*$  and  $x \in B^*$ . Then*

$$\binom{\varphi(u)}{x} = \sum_{|s| \leq |x|} \binom{u}{s} \langle \gamma(s), x \rangle.$$

Where  $\gamma : \mathbb{Z}\langle A \rangle \rightarrow \mathbb{Z}\langle B \rangle$  is the ring morphism defined by  $\gamma = \mu_B \circ \varphi \circ \mu_A^{-1}$  and  $\langle \gamma(s), x \rangle$  denotes the coefficient of  $x$  in  $\gamma(s)$ .

*Proof.* Considering that  $\mu_A^{-1}(a) = a - 1$  for all  $a \in A$ , then

$$\gamma(a) = \mu_B(\varphi(a - 1)) = \mu_B(\varphi(a)) - 1 = \sum_{x \in B^*} \binom{\varphi(a)}{x} x - 1 = \sum_{x \in B^+} \binom{\varphi(a)}{x} x.$$

Note that  $B^+ = B^* \setminus \{\epsilon\}$  and thus  $\langle \gamma(a), 1 \rangle = 0$ . It follows that  $\langle \gamma(s), x \rangle = 0$  if  $|x| < |s|$ . Furthermore, for each  $u \in A^*$ :

$$\mu_B(\varphi(u)) = \sum_{x \in B^*} \binom{\varphi(u)}{x} x.$$

On the other hand:

$$\gamma(\mu_A(u)) = \gamma\left(\sum_{s \in A^*} \binom{u}{s} s\right) = \sum_{s \in A^*} \binom{u}{s} \gamma(s) = \sum_{s \in A^*} \sum_{x \in B^*} \binom{u}{s} \langle \gamma(s), x \rangle x$$

Since  $\gamma \circ \mu_A = \mu_B \circ \varphi$ , the polynomials  $\mu_B(\varphi(u))$  and  $\gamma(\mu_A(u))$  have the same coefficients and, therefore,

$$\binom{\varphi(a)}{x} = \sum_{s \in B^*} \binom{u}{s} \langle \gamma(s), x \rangle = \sum_{|s| \leq |x|} \binom{u}{s} \langle \gamma(s), x \rangle$$

□

With this lemma, it is now possible to prove the Theorem 15.

*Proof.* Let  $\theta : A \rightarrow U_{n+1}(\mathbb{F}_p)$  be the map defined by  $\theta(a) = \pi(a) - 1$ .  $\theta$  can be extended to a ring morphism  $\theta : \mathbb{Z}\langle A \rangle \rightarrow U_{n+1}(\mathbb{F}_p)$ , and the maps  $\theta_{i,j} : A^* \rightarrow \mathbb{F}_p$  are defined as  $\theta_{i,j}(u) = (\theta(u))_{i,j}$  for  $1 \leq i < j \leq n+1$ .  $\theta(a)$  is a strictly triangular matrix for all  $a \in A$ , it follows that  $\theta(x) = 0$  for all words with length greater than  $n$ .

Considering the Magnus automorphism in  $A^*$ , the following  $\theta(\mu_A(a)) = \theta(a + 1) = \theta(a) + 1 = \pi(a) - 1 + 1 = \pi(a)$  holds for all  $a \in A$  and  $\pi = \theta \circ \mu_A$ . It follows by the definition of the Magnus morphism that:

$$\pi(u) = \theta(\mu(u)) = \theta\left(\sum_{x \in A^*} \binom{u}{x} x\right) = \sum_{x \in A^*} \binom{u}{x} \theta(x) = \sum_{|x| \leq n} \binom{u}{x} \theta(x)$$

and hence

$$\pi_{i,j}(u) = \sum_{|x| \leq n} \theta(x)_{i,j} \binom{u}{x}.$$

Which shows that  $\pi_{i,j}(u)$  is a linear combination of binomial coefficients. □

An interesting particular case occurs if the language is defined by constraints on the first row of the matrix, for instance, for a language of the form

$$L = \{u \in A^* : \pi_{1,2} = \dots = \pi_{1,n} = 0\}$$

Observing that  $L$  can also be written as

$$L = \{u \in A^* : (1, 0, \dots, 0)\pi(u) = (1, 0, \dots, 0)\},$$

it is possible to directly obtain a deterministic automaton for  $L$  by taking  $\mathbb{F}_p^n$  as set of states. Where the initial and unique final state is  $(0, \dots, 0)$ , and the transitions for each  $(z_1, \dots, z_n) \in \mathbb{F}_p^n$  and each letter  $a$  are defined by setting  $(z_1, \dots, z_n) \cdot a = (z'_1, \dots, z'_n)$  where  $(1, z_1, \dots, z_n)\pi(a) = (1, z'_1, \dots, z'_n)$  that is:

$$\begin{aligned} z'_1 &= \pi_{1,2}(a) + z_1, \\ z'_2 &= \pi_{1,3}(a) + \pi_{2,3}(a)z_1 + z_2, \\ z'_3 &= \pi_{1,4}(a) + \pi_{2,4}(a)z_1 + \pi_{3,4}(a)z_2 + z_3, \text{ etc.} \end{aligned} \tag{5.53}$$

## 5.5 Languages and Formations Generated by $D_4$ and $Q_8$

The following results were given by J.E. Pin and X. Soler-Escrivà in ([23], Example 4.2. and Example 4.3.). The group  $D_4$  is generated by matrices:

$$a = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \text{ and } b = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The group consists of the matrices:

$$\begin{aligned} a &= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad b = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad a^2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad b^2 = 1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ ab &= \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad ba = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad a^3 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad a^2b = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{aligned}$$

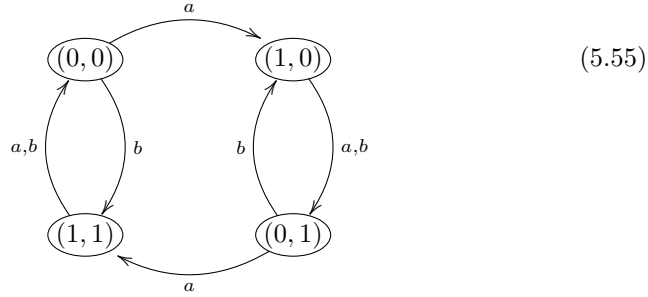
Let  $\pi : A^* \rightarrow D_4$  be the natural morphism and let:

$$L = \{u \in A^* : \pi_{1,2}(u) = \pi_{1,3}(u) = 0\}$$

To obtain a deterministic automaton for  $L_2$ , take  $\mathbb{F}_2^2$  as the set of states and define the transitions, for all  $(z_1, z_2) \in \mathbb{F}_2^2$ , by setting:

The resulting automaton, which turns out to be minimal, is the following:

$$\begin{cases} (z_1, z_2, z_3) \cdot a = (1 + z_1, z_1 + z_2) \\ (z_1, z_2, z_3) \cdot b = (1 + z_1, 1 + z_2) \end{cases} \tag{5.54}$$



The syntactic monoid of  $L$  is the group  $D_4$ .

The subgroup of  $U_4(\mathbb{F}_2)$  generated by the two matrices:

$$a = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, b = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

is isomorphic to  $Q_8$ . The group consists of the matrices of the following form, where  $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \mathbb{F}_2$ .

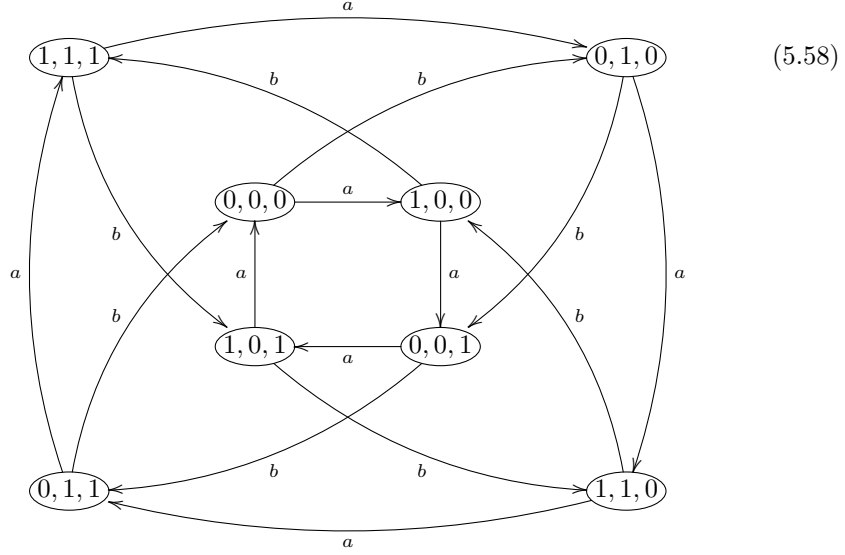
$$a = \begin{bmatrix} 1 & \varepsilon_1 & \varepsilon_2 & \varepsilon_3 \\ 0 & 1 & 0 & \varepsilon_1 + \varepsilon_2 \\ 0 & 0 & 1 & \varepsilon_2 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \quad (5.56)$$

Let  $\pi : A^* \rightarrow Q$  be the natural morphism and let

$$L_2 = \{u \in A^* : \pi_{1,i}(u) = 0, 2 \leq i \leq 4\}.$$

To obtain a deterministic automaton of  $L_2$  take the states as  $\mathbb{F}_2^3$  and define the transitions by setting:

$$\begin{cases} (z_1, z_2) \cdot a = (1 + z_1, z_2, z_1 + z_3) \\ (z_1, z_2) \cdot b = (z_1, 1 + z_2, z_1 + z_2 + z_3) \end{cases} \quad (5.57)$$



## 5.6 A Regular Language Associated with a Brauer Configuration Algebra

Automata associated with path algebras have been studied by S. Rees [26], who introduced some automata associated with some string algebras. Such automata were used to describe indecomposable representations over these types of algebras. She points out that the set of strings defining representations of string algebras and many other bounded path algebras constitute a regular set. In this section, we follow the ideas of S. Rees to describe an automaton associated with a Brauer configuration algebra.

Values of the map  $c : Q_1 \rightarrow 2$  can be obtained by endowing to the successor sequences a length-lexicographic order. In this case, both  $\Gamma_0$  and  $\Gamma_1$  are well-ordered sets with partial orders  $\prec$  and  $<$ , respectively. In such a way that initial states in the corresponding automaton are given by minimal successor sequences. Note that if  $S_{a,U}$  denotes a successor sequence starting in a polygon  $U$  with  $a \in U$  and if  $|S_{\alpha,V_1}| = |S_{\alpha',V_1}| = |S_{\alpha,V_2}| = |S_{\alpha',V_2}|$ ,  $\alpha, \alpha' \in V_1 \cap V_2$ , and  $\alpha \prec \alpha'$  then  $c(S_{\alpha,V_1}) = 1$  and  $c(S_{\alpha',V_1}) = c(S_{\alpha,V_2}) = c(S_{\alpha',V_2}) = 0$ .

A Brauer configuration algebra  $\Lambda_\Gamma$  induced by a Brauer configuration  $\Gamma = (\Gamma_0, \Gamma_1, \mu, \mathcal{O})$  has associated a regular language  $L_\Gamma = A_\Gamma^* / \sim$ , where the alphabet  $A_\Gamma = \{x_\alpha^i \mid \alpha \in \Gamma_0, 1 \leq i \leq \text{val}(\alpha)\}$ , each letter  $x_\alpha^i$  corresponds to a unique arrow in  $(Q_\Gamma)_1$ . Each path  $P \in Q_\Gamma$  corresponds to a word  $w \in L_\Gamma$ .

Two words  $w, w' \in L_\Gamma$  are equivalent (in other words,  $w \sim w'$ ) if their corresponding paths are equivalent as elements of the Brauer configuration algebra. In this case, if  $S_\alpha$  is a successor sequence associated with the vertex  $\alpha \in \Gamma_0$ ,

then  $w_{S_\alpha}$  denotes the word associated with the corresponding special cycle up to equivalence. If  $\min S_\alpha = U \in \Gamma_1$ , then  $w_{S_\alpha} \in O_c(U)$  (final vertices of special cycles are final states up to equivalence).

In the associated automaton of a Brauer configuration algebra, polygons are states. All states we represent are accepted states. The order  $<$  gives the transition between states. In other words, if  $x_i^\alpha$  is the letter associated with an arrow  $U_i < U_{i+1}$ , that is,  $U_i \xrightarrow{x_i^\alpha} U_{i+1} \in (Q_\Gamma)_1$ , then  $x_i^\alpha$  is a transition from  $U_i$  to  $U_{i+1}$ . Note that, if  $x_\alpha^i x_{\alpha'}^j$  belongs to the admissible ideal  $I$ , with  $\Lambda_\Gamma = kQ_\Gamma/I$  then it is not accepted as word in  $L_\Gamma$  if  $\alpha \neq \alpha'$ .

$$\begin{aligned} c(C_{i,V_j}^k) &= 0, \quad \text{if } , i \neq 0, j \neq 1, k \neq 1. \\ c(C_{i,V_j}^k a) &= 0, \quad \text{if } a \text{ is the first arrow of } C_{i,V_j}^k \text{ for all possible values of } i, j \text{ and } k. \\ c(\alpha_j^i \beta_{j'}^{i'}) &= c(\beta_j^i \alpha_{j'}^{i'}) = 0, \text{ for all the possible values of } i, j, i', j'. \end{aligned}$$

## 5.7 Cluster Configurations and Diophantine Problems

Given a seed  $(\Gamma, \mathcal{X})$  there is a system of diophantine equations associated with a cluster configuration:

$$\begin{aligned} \sum_{i=0}^{\infty} x_i &= |\Gamma_0| \\ \sum_{i=0}^{\infty} i x_i &= n |\Gamma_1| \end{aligned} \tag{5.59}$$

Where  $\Gamma_0$  and  $\Gamma_1$  are the set of vertices and polynomials of the Brauer configuration algebra, respectively,  $n$  is the degree of the polynomial  $p(x)$ . Considering  $C_i = \{v \in \Gamma_0 : \text{val}(v) = i\}$ , then a solution for the equation system is obtained as  $x_i = |C_i|$ . Note that for each mutation of the seed, the number of vertices, polynomials, and the degree of  $p$  is constant, and therefore the mutation obtains solutions for the equation system, and there is only a finite number of  $C_i \neq \Phi$ .

### On Diophantine Equations of Type $\mathcal{D}(n_1, n_2, \mathcal{K}_m)$

**Theorem 16.** *For a fixed integer positive  $m_0$ ,  $n \geq 2$ , and a fixed seed  $(\Gamma, \mathcal{X})$  (see (4.28) and (4.29)), the Brauer configuration algebra  $\Lambda_{\Phi^{m_0}}$  induced by the Brauer configuration*

$$\Phi^{m_0} = (\Phi_0^{m_0}, \Phi_1^{m_0}, \mu, \mathcal{O}) \quad (\text{see (4.30)})$$

*has associated a finite non-deterministic automaton whose states are given by solutions of a problem of type  $\mathcal{D}(n_1, l^2 2^{n-2}, \mathcal{K}_{m_i})$  with  $n_1 \leq 16$ , and*

$$\mathcal{K}_{m_i} = \{\text{occ}(T(\alpha), T(\mathcal{M}^i)) \mid T(\alpha) \in T(\Phi_0^{m_0}), T(\mathcal{M}^i) \in T(\Phi_1^{m_0}), \alpha \in \Phi_0^{m_0}, \mathcal{M}^i \in \Phi_1^{m_0}\},$$

*where  $T(\Phi^{m_0}) = ((T(\Phi_0^{m_0}), T(\Phi_1^{m_0}), T(\mu), T(\mathcal{O}))$  is a suitable transformation between Brauer configurations.*

*Proof.* Since the length of the message  $|M(\Phi^{m_0})| = l^2 2^n$  then it consists of  $l^2 2^{n-2}$  lists of four bits. We let  $\mathcal{A} = \{\alpha_1, \alpha_2, \dots, \alpha_{l^2 2^{n-2}}\}$  denote this set of lists. Define a map  $T : \mathcal{A} \rightarrow Hex$  such that  $T(\alpha_i) = \alpha'_i \in Hex$ , where  $Hex$  is a notation for the hexadecimal numbering system  $Hex = \{0, 1, 2, \dots, 9, A, B, C, \dots, F\}$ . In this case,  $T(\alpha_i \alpha_{i+1}) = \alpha'_i \alpha'_{i+1} \in Hex^*$  if  $\alpha_i, \alpha_{i+1} \in \mathcal{A}$ .

The map  $T$  defines a new Brauer configuration  $T(\Phi^{m_0}) = (\text{Img } T, T(\Phi_1^{m_0}), \mu', \mathcal{O}'$ ) which we assume reduced without loss of generality. Each polygon  $T(\mathcal{M}^i)$  consists of elements of the form  $\alpha'_j$  with  $\alpha_j \in \mathcal{M}^i$ . If  $M(\mathcal{M}^i) = \alpha_1 \alpha_2 \dots \alpha_{r_i}$  is the message of  $\mathcal{M}^i$ , then  $\alpha'_1 \alpha'_2 \dots \alpha'_{r_i} \in \mathcal{A}^*$  is the message of  $T(\mathcal{M}^i)$ . Besides if  $\mathcal{M}_i < \mathcal{M}_{i+1}$  in  $\Phi^{m_0}$  then  $T(\mathcal{M}_i) < T(\mathcal{M}_{i+1})$  in  $T(\Phi^{m_0})$ . And  $\mu'(\alpha'_i) = 1$  for any  $\alpha'_i \in \text{Img } T$ . So, the message  $M(T(\Phi^{m_0})) \in \mathcal{A}^*$  is a word length  $l^2 2^{n-2}$  whose letters  $\alpha'_j$  can be grouped according to its valency. Thus,  $M(T(\Phi^{m_0}))$  has the form:

$$M(T(\Phi^{m_0})) = \mathcal{A}_{i_1} \mathcal{A}_{i_2} \dots \mathcal{A}_{i_m}, \quad (5.60)$$

where  $\mathcal{A}_{i_s}$  is a multiset with  $|\mathcal{A}_{i_s}| = L_{i_s}$  and  $\mathcal{A}_{i_x} \cap \mathcal{A}_{i_y} = \emptyset$ . Note that  $\mathcal{A}_{i_s}$  consists of all letters  $\alpha'_i$  such that  $val(\alpha'_i) = v_{i_s}$ , in other words, the message  $M(\mathcal{A}_{i_s})$  associated to  $\mathcal{A}_{i_s}$  can be written as

$$M(\mathcal{A}_{i_s}) = (\alpha'_{i_{s1}} \alpha'_{i_{s2}} \dots \alpha'_{L_{i_s}})^{v_{i_s}}. \quad (5.61)$$

Therefore,

$$\begin{aligned} \sum_{h=1}^m L_{i_h} &= n_1 \leq 16, \\ \sum_{g=1}^m L_{i_g} v_{i_g} &= l^2 2^{n-2}. \end{aligned} \quad (5.62)$$

Then terms  $L_{i_h}$  give a solution of a diophantine equation of type

$$\mathcal{D}(n_1, l^2 2^{n-2}, \mathcal{K}_m = \{v_{i_1}, \dots, v_{i_m}\}). \quad (5.63)$$

Since any Brauer configuration algebra defines a regular language, whose associated automaton uses arrows of the Brauer quiver as transitions between states given by polygons, obtained by mutation. Thus, it is impossible to precisely determine what kind of message or diophantine equation is obtained after applying a mutation; therefore, its associated automaton is non-deterministic.  $\square$

For example, using the polynomial  $p(x) = x^8 + x^4 + x^3 + 1$  and a set  $Hex = \{0 = 0000, 1 = 0001, 2 = 0010, \dots, A = 1010, \dots, F = 1111\}$  of polynomials to define a seed  $(\Gamma, \mathcal{X})$ . With  $\mathcal{X} = (x_1, x_2, x_3, x_4)$  can be denoted as follows:

$$\begin{aligned} x_1 &= (AF, C0, 13, 10), \\ x_2 &= (D0, B3, 8A, F2), \\ x_3 &= (CE, C4, 62, 3D), \\ x_4 &= (A2, 74, 79, 7D). \end{aligned}$$

$$\begin{aligned}
\Gamma &= (\Gamma_0, \Gamma_1, \mu, \mathcal{O}), \\
\Gamma_0 &= \{0, 1\}, \\
\Gamma_1 &= \{w(0) = \{10101111 \dots 00010000\}, w(1) = \{11010000 \dots 11110010\}, \dots\}, \\
\mu(0) &= \mu(1) = 1, \\
w(0) &< w(1) < w(2) < w(3).
\end{aligned} \tag{5.64}$$

Then

$$M(\Gamma) = (AC03D27)^{(3)}(F14)^{(2)}(B8E69)^{(1)}$$

which builds a solution for a diophantine equation  $\mathcal{D}(15, 32, \{3, 2, 1\})$  with the form:

$$\begin{aligned}
\lambda_1 + \lambda_2 + \lambda_3 &= 15, \\
3\lambda_1 + 2\lambda_2 + \lambda_3 &= 32.
\end{aligned}$$

For a given polynomial  $p(x) = w(i) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7 \in \mathbb{F}$ , the map  $\tau(p(x)) = \tau(x_i)$  associated with a mutation of the seed  $(\Gamma, \mathcal{X})$  is defined in such a way that

$$\begin{aligned}
\tau(x_i) &= \sum_{s=0}^7 b_s x^s + v_{i/4,0}, \\
b_j &= a_j + a_{j+4} + a_{j+5} + a_{j+6} + a_{j+7} + c_j, \\
(c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7) &= (1, 1, 0, 0, 0, 1, 1, 0), \\
\mathcal{H}(x_1, x_2, x_3, x_4) &= (\tau(x_2), \tau(x_3), \tau(x_4), \tau(x_1)), \quad m_0 = 10.
\end{aligned} \tag{5.65}$$

The following is the list of vectors  $v_{j,0}$ ,  $1 \leq j \leq 10$ .

$$\begin{aligned}
v_{1,0} &\leftarrow 01000000 \\
v_{2,0} &\leftarrow 02000000 \\
v_{3,0} &\leftarrow 04000000 \\
v_{4,0} &\leftarrow 08000000 \\
v_{5,0} &\leftarrow 10000000 \\
v_{6,0} &\leftarrow 20000000 \\
v_{7,0} &\leftarrow 41000000 \\
v_{8,0} &\leftarrow 81000000 \\
v_{9,0} &\leftarrow 1B000000 \\
v_{10,0} &\leftarrow 36000000
\end{aligned} \tag{5.66}$$

For  $m_0 = 10$ , any mutation of this seed gives rise to a solution of a diophantine equation of type  $(n_1 \leq 16, 32, \mathcal{K}_m)$  with  $\mathcal{K}_m$  being a set of the form:

$$\begin{aligned}\mathcal{K}_m &= \{1, 2, 3\}, \\ \mathcal{K}_m &= \{1, 2, 3, 4\}, \\ \mathcal{K}_m &= \{1, 2, 3, 4, 5\}, \\ \mathcal{K}_m &= \{1, 2, 3, 4, 7\}, \\ \mathcal{K}_m &= \{1, 2, 3, 4, 7\}, \\ \mathcal{K}_m &= \{1, 2, 3, 4, 8\}.\end{aligned}$$

**Remark 17.** For  $m_0 > 1$  and a fixed seed, the dimension of an algebra  $\Lambda_{\Phi^{m_0}}$  and its center  $Z(\Lambda_{\Phi^{m_0}})$  can be estimated by using some statistical methods. For instance, we use a sample of  $10^6$  random seeds in order to obtain confidence intervals for these values. Such samples allow us to infer that if  $m_0 = 10$  then  $P_r(7499 \leq \dim_{\mathbb{F}} \Lambda_{\Phi^{m_0}} \leq 8067)$  and  $P_r(199 \leq \dim_{\mathbb{F}} Z(\Lambda_{\Phi^{m_0}}) \leq 221)$  are both greater than 0,99. Where  $P_r(X)$  denotes the probability of an event  $X$ . As shown by the computational data obtained.

## 5.8 Criptographic applications

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity, and electronic data protection [33, 35].

The National Institute of Standards and Technology (NIST) started developing AES in 1997 when it announced the need for an alternative to the Data Encryption Standard (DES), which became vulnerable to brute-force attacks.

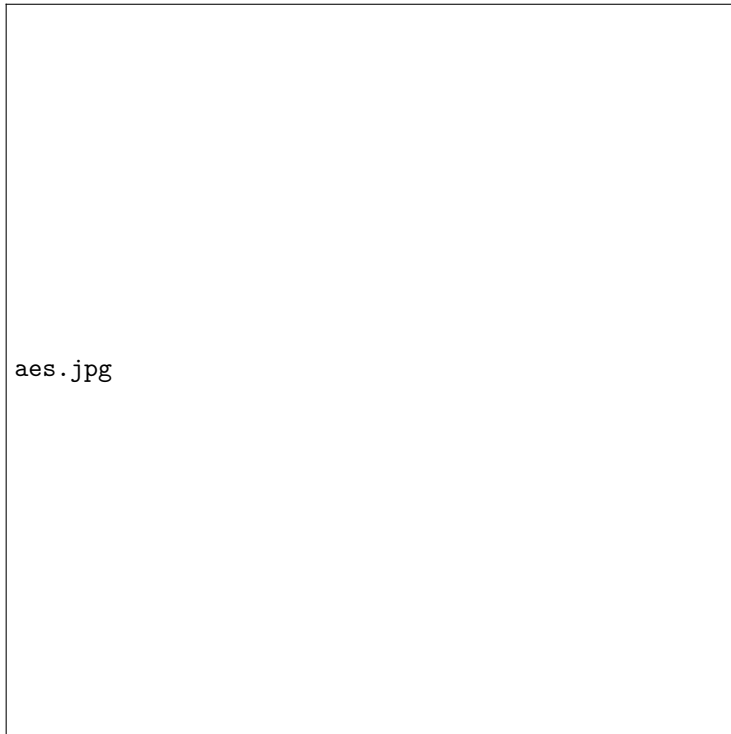
NIST stated that the newer, advanced encryption algorithm would be unclassified and must be "capable of protecting sensitive government information well into the XXI century." It was intended to be easy to implement in hardware and software and restricted environments (such as a smart card) and offer decent defenses against various attack techniques.

AES was created for the U.S. government with other programs that provide encryption services. However, non-governmental organizations choosing to use AES are subject to limitations created by U.S. export control.

AES includes three block ciphers: AES-128, AES-192, and AES-256. AES-128 uses a 128-bit key length to encrypt and decrypt a block of messages, while AES-192 uses a 192-bit key length and AES-256 a 256-bit key length in order to encrypt and decrypt messages. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192, and 256 bits, respectively.

Symmetric, also known as the secret key, ciphers use the same key for encrypting and decrypting, so the sender and the receiver must both know – and use – the same secret key. The government classifies information into three categories: Confidential, Secret, or Top Secret. All key lengths can be used to protect the Confidential and Secret levels. Top Secret information requires either 192- or 256-bit key lengths.

There are ten rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. A round consists of several processing steps that include substitution, transposition, and mixing of the input plaintext to transform it into the final ciphertext output. The following is a scheme of the encryption-decryption processes.



**Figure:** AES design [35].

In the cryptosystem AES, a plaintext, also called state is a sequence of 16 bytes. The encryption process also generates a 16-bytes sequence using 128-bit, 192-bit, or 256-bit keys. Such length depends on the number of rounds developed in the encryption process, 10, 12, or 14, respectively.

Each round in an encryption process requires four different transformations:

1. SubBytes,

2. ShiftRows,
3. MixColumns,
4. AddRoundKey.

For the last round the function MixColumns is not executed.

The next table gives all the possible outputs of the transformation SubBytes [33]:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

The key schedule is how all the keys to be used in the encryption process are generated. Such keys are called subkeys. For keys of 128 bits (or 16 bytes) of length, the process generates 11 subkeys, the initial key, the nine main rounds, and the final round.

The following is the list of vectors  $v_{j,0}$ ,  $1 \leq j \leq 10$  for a key of length 128 bits.

$$\begin{aligned}
 v_{1,0} &\leftarrow 01000000 \\
 v_{2,0} &\leftarrow 02000000 \\
 v_{3,0} &\leftarrow 04000000 \\
 v_{4,0} &\leftarrow 08000000 \\
 v_{5,0} &\leftarrow 10000000 \\
 v_{6,0} &\leftarrow 20000000 \\
 v_{7,0} &\leftarrow 41000000 \\
 v_{8,0} &\leftarrow 81000000 \\
 v_{9,0} &\leftarrow 1B000000 \\
 v_{10,0} &\leftarrow 36000000
 \end{aligned} \tag{5.67}$$

The expanded key can be seen as an array of 32-bit words numbered from 0 to 43 (0 for the initial key), words that are a multiple 4 ( $w_4, w_8, \dots, w_{40}$ ) are calculated as follows:

1. Applying the RotWord and SuBytes transformation to the previous word  $w_{i-1}$ , ( $\text{SubBytes}(\text{RotWord}(x_1, x_2, x_3, x_4)) = \text{SuBytes}(x_2, x_3, x_4, x_1)$ ).
2. Adding (XOR) this result to the word 4 positions earlier  $w_{i-4}$  plus a round constant called RCON,
3. The remaining 32-bit words  $w_i$  are calculated by adding (XOR) the previous word  $w_{i-1}$ , with the word 4 positions earlier.

The following result is a consequence of the description of the AES-key schedule.

**Theorem 17.** *For  $m_0 = 10$ ,  $l = 4$ ,  $p(x) = x^8 + x^4 + x^3 + 1$  and vectors RCON given in (5.67), it holds that the set of polygons  $\Phi_1^{10}$  (see (4.30)) of  $\Phi^{10}$  obtained by mutation rules given in (5.65) is the AES-key schedule given by the message associated to a seed  $(\Gamma, \mathcal{X} = (x_1, x_2, x_3, x_4))$ .*

*Proof.* The key-schedule is obtained by applying mutation rules (5.65) and (5.67) to  $\mathcal{X} = (x_1, x_2, x_3, x_4)$ . In such a case,

$$\tau(x_i) = \begin{cases} \text{SubBytes}(\text{RotWord}(x_i)) + \text{RCON}(i/4), & \text{if } i \equiv 0 \pmod{4}, \\ x_{i-1} + x_{i-4}, & \text{otherwise.} \end{cases}$$

□

## 5.9 AES Mutation

Considering the construction and definition of the AES key itinerary for a 128-bit key it is natural to associate a configuration cluster defined as follows:

1. Seed  $(\Gamma, \mathcal{X})$ , with  $\mathcal{X} = (x_0, x_1, x_2, x_3)$  where  $x_i \in \mathbb{F}^4$  and  $\mathbb{F} = \mathbb{Z}_2[x]/\langle p(x) \rangle$  with  $p(x) = x^8 + x^4 + x^3 + 1$ .

$$\begin{aligned} \Gamma &= (\Gamma_0, \Gamma_1, \mu, \mathcal{O}), \\ \Gamma_0 &= \{0, 1\}, \\ \Gamma_1 &= \{w(0), w(1), \dots, w(N-1)\}, \\ \mu(0) &= \mu(1) = 1, \end{aligned} \tag{5.68}$$

2.  $M(\Gamma, \mathcal{X})$  is defined as:

- $x'_0 = x_0 + \mathcal{H}(x_3)$ , where  $\mathcal{H}(x_3) = \text{SubWord}(\text{RotWord}(x_3)) + \text{RCON}$  with  $\text{RCON} = (1, 0, 0, 0) \in \mathbb{F}^4$  at the start of the mutations
- $x'_i = x_i + x'_{i-1}$  for  $0 < i$ .
- $\text{RCON}' = \text{RCON} \cdot x$ .

This configuration cluster is such that if the message of the seed is equal to the bit extension of an AES key, then the polynomials of  $\Phi^{10}$  have as a message the itinerary of the initial key and therefore define an automaton that recognizes the key itinerary.

**Corollary 2.** *There exists an integer  $N$  for which  $S_{N-1}(K^{0,a}) = K^{M,a}$ , for some  $0 \leq M < N$ .*

*Proof.* For  $l = 4$ ,  $p(x) = x^8 + x^4 + x^3 + 1$  and vectors RCON given in (5.67), it holds that the set of polygons  $\Phi_1^{m_0}$  (see (4.30)) of  $\Phi^{m_0}$  obtained by the mutation rules given in (5.65) is the AES-key schedule of a seed-key  $(\Gamma, \mathcal{R} = (x_1, x_2, x_3, x_4)) = K^{0,a}$ . Thus, the result holds as a direct consequence of Theorem 14.  $\square$

## References

- [1] M.A.O. Angarita, *Human Interaction Proofs Based on Emerging Images; A Practical Application of the Theory of Representation of Algebras*, UNAL, Colombia, 2019. PhD Dissertation.
- [2] I. Assem, D. Simson, and A. Skowronski, *Elements of the Representation Theory of Associative Algebras*, Cambridge University Press, Cambridge UK, 2006. 1–457.
- [3] I. Canakci and R. Schiffler, *Snake graph calculus and cluster algebras from surfaces*, *J. Algebra* **382** (2013), 240-281.
- [4] ———, *Cluster algebras and continued fractions*, *Compositio Mathematica* **154** (2018), no. 3, 565-593.
- [5] A.M. Cañadas, J.D. Camacho, and I. D. Marin, *Relationships between the Chicken McNugget Problem, Mutations of Brauer Configuration Algebras and the Advanced Encryption Standard*, *Mathematics* **9** (2021), no. 16.
- [6] A.M. Cañadas and M.A.O. Angarita, *Brauer configuration algebras for multimedia based encryption and applications*, *Multimed Tools Appl* **80** (2021), 23485-23510.
- [7] S.T. Chapman and C. O’Neill, *Factoring in the Chicken McNugget monoid*, *Mathematics Magazine* **91** (2015), no. 5, 323-336.
- [8] F. Curtis, *On formulas for the Frobenius number of a numerical semigroup.*, *Mathematica Scandinavica* **67** (1990), 190.
- [9] J.A. De Loera, *The many aspects of counting lattice points in polytopes*, *Mathematische Semesterberichte* (2005), 175-195.
- [10] S. Eilenberg, *Automata, Languages, and Machines*, Vol. B, Academic Press, 111 Fifth Avenue, New York, New York 10003, 1974.
- [11] P.F.F. Espinosa, *Categorification of Integer Sequences and Its Applications*, National University of Colombia, 2020. PhD Dissertation.
- [12] S. Fomin, M. Shapiro, and D. Thurston, *Cluster algebras and triangulated surfaces. Part I: Cluster complexes.*, *Acta Math.* **201** (2008), 83-146.
- [13] S. Fomin and A. Zelevinsky, *Cluster algebras. I: Foundations.*, *J. Amer. Math. Soc.* **15** (2002), 497-529.
- [14] ———, *Cluster algebras. II: Finite type classification.*, *Invent. Math.* **154** (2003), no. 1, 63-121.
- [15] ———, *Cluster algebras. IV: Coefficients.*, *Compositio Mathematica* **143** (2007), 112-164.
- [16] P. Gabriel and A.V. Roiter, *Representations of Finite Dimensional Algebras*, *Algebra VIII*, *Encyclopedia of Math. Sc.*, vol. 73, Springer-Verlag, 1992. 177p.
- [17] E.L. Green and S. Schroll, *Brauer configuration algebras: A generalization of Brauer graph algebras*, *Bull. Sci. Math.* **141** (2017), 539–572.
- [18] G. H. Hardy, E. M. Wright, D. R. Heath-Brown, and J. H. Silverman, *An Introduction to the Theory of Numbers*, Oxford University Press, 2008.
- [19] E. C. i Llópez, *Some Contributions to the Algebraic Theory of Automata*, *Facultat de Ciències Matemàtiques Universitat de València*, 2015.
- [20] B. Keller, *Cluster algebras, quiver representations and triangulated categories*, Cambridge University Press, 2010. In T. Holm, Jørgensen and R. Rouquier (Eds.), *Triangulated Categories* (London Mathematical Society Lecture Note Series, 76-160).
- [21] G. Musiker, R. Schiffler, and L. Williams, *Positivity for cluster algebras from surfaces*, *Adv. Math.* **227** (2011), 2241-2308.
- [22] S.Y. Oudot, *Persistence Theory: From Quiver Representations to Data Analysis*, American Mathematical Society, 2015.

- [23] J.E. Pin and X. Soler-Escrivà, *Languages and formations generated by  $D_4$  and  $Q_8$* , Theoretical Computer Science **800** (2019), 155-172.
- [24] J.L. Ramírez-Alfonsín, *Complexity of the Frobenius problem*, Combinatorica **16** (1996), 143-147.
- [25] ———, *The Diophantine Frobenius Problem*, Vol. 16, Oxford University Press, 1996. 1-457.
- [26] S. Rees, *The Automata that define Representations of monomial algebras*, Algebr Represent Theor **11** (2008), 207-214.
- [27] J. Rutten, A. Ballester-Bolinches, and E.C. i Llópez, *Varieties and covarieties of languages*, ENTCS **298** (2013), 7-28.
- [28] I. K. Rystsov, *Affine Automata and Classical Fractals*, Cybernetics and Systems Analysis **54** (2018), 11-20.
- [29] J. Sakarovitch, *Elements of Automata Theory*, Cambridge University Press, 2013.
- [30] R. Shiffler, *Quiver Representations*, Springer, 2010.
- [31] S. Schroll, *Brauer Graph Algebras*, Springer, Cham, 2018. In: Assem I., Trepode S. (eds), Homological Methods, Representation Theory, and Cluster Algebras, CRM Short Courses, 177-223.
- [32] A. Sierra, *The dimension of the center of a Brauer configuration algebra*, J. Algebra **510** (2018), 289-318.
- [33] D.R. Stinson and M.B. Paterson, *Cryptography; Theory and Practice*, Chapman and Hall/CRC, 2018.
- [34] G. M. Ziegler, *Lectures on Polytopes*, Springer, 1998.
- [35] *AES*, Vol. <https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard>, TechTarget.