

Interactions Between Brauer Configuration Algebras and Classical Cryptanalysis to Analyze Bach's Canons

Agustín Moreno Cañadas¹, Pedro Fernando Fernández Espinosa², José Gregorio Rodríguez Nieto³, Odette M. Mendez⁴, Ricardo Hugo Arteaga-Bastidas⁵.

Abstract

Since their introduction, Brauer configuration algebras (BCAs) and their specialized messages have helped research in several fields of mathematics and sciences. This paper deals with a new perspective on using such algebras as a theoretical framework in classical cryptography and music theory. It is proved that some block cyphers define labeled Brauer configuration algebras. Particularly, the dimension of the BCA associated with a ciphertext-only attack of the Vigenere cryptosystem is given by the corresponding key's length and the captured ciphertext's coincidence index.

On the other hand, historically, Bach's canons have been considered solved music puzzles. However, due to how Bach posed such canons, the question remains whether their solutions are only limited to musical issues. This paper gives alternative solutions based on the theory of Brauer configuration algebras to some of the puzzle canons proposed by Bach in his Musical Offering (BWV 1079) and the canon à 4 Voc: Perpetuus (BWV 1073). Specifically to the canon à 6 Voc (BWV 1076), canon 1 à 2 (also known as the crab canon), and canon à 4 Quaerendo Invenietis. These solutions are obtained by interpreting such canons as ciphertexts (via route and transposition cyphers) of some specialized Brauer messages. In particular, it is noted that the structure or form of the notes used in such canons can be described via the shape of the most used symbols in Bach's works.

¹Universidad Nacional de Colombia (Bogotá)

²Universidad de Caldas (Manizales)

³Universidad Nacional de Colombia (Medellín)

⁴Universidad Nacional de Colombia (Manizales)

⁵Universidad Nacional de Colombia (Bogotá)

1 Introduction

Brauer configuration algebras were introduced in 2017 to research algebras of wild representation type [1, 2]. Soon afterwards, it was discovered that such algebras are helpful tools for investigating different fields of mathematics and sciences due to their combinatorial nature. These algebras are induced by special systems of multisets, which are suitable tools to deal with the theory of integer partitions and enumerative combinatorics [3, 4]. Brauer messages associated with Brauer configurations have been used in cryptography to study the behavior of some provably secure hash functions or to give alternative descriptions to the schedule of an AES (Advanced Encryption Standard) key [5, 6]. This paper shows that behind the definition of some block cyphers is a Brauer configuration algebra whose invariants allow giving properties of the corresponding cryptographic system.

We will see that cryptanalysis of a Vigenere cryptosystem provides formulas for the dimension of its associated Brauer configuration algebra and its center. Similar results can be obtained for the Brauer configuration algebra associated with the permutation (transposition) cryptosystem. In fact, the dimension of the Brauer configuration algebra associated with a ciphertext obtained by permutation (or via a permutation network) equals the dimension of the Brauer configuration algebra associated with the corresponding plaintext.

Musical compositions are another example of the presence of Brauer's messages. These musical contents can be seen as ciphertexts of specialized Brauer messages via an appropriated transposition.

In the Baroque period, musical canons were musical pieces proposed by composers as puzzles to be solved with the help of some predefined hints. Bach proposed some of the most celebrated canons in music history in his Musical Offering [7]. We remember that in this work, Bach proposed ten canons based on a single theme that King Frederick the Great proposed. Up-to-date, it is accepted that Bach's canons were solved by two of Bach's former students, Johann Friedrich Agricola and Johann Philip Kirnberger [8, 10, 11, 9].

According to some of Bach's biographers [10, 11, 12, 13, 14, 15, 16, 17, 18, 19], it is easy to think that many of the canons need to be solved taking into account another point of view because it is generally

accepted that Bach used a particular type of symbolism in his music. We recall that Bach was used to including musical cryptograms in his works. For instance, his well-known motif is included in musical pieces such as the Art of Fugue or the Brandenburg Concerto No. 2 [20]. In this line, this paper proposes to consider some of Bach's canons as ciphertexts obtained by the transposition of some Brauer messages in such a way that such messages allow to recover part of Bach's data and symbolism via a route deciphering.

1.1 Motivations

One of the main characteristics of Brauer configuration algebras is their capacity to be adapted in different contexts, provided its combinatorial definition [1]. The interaction of such algebras with different sciences and mathematics fields has allowed new perspectives to investigate the underlying theoretical frameworks [5, 6, 21, 22, 23, 24, 25, 26, 27].

This paper is focused on the interaction between classical cryptanalysis, music theory, and Brauer configuration algebras. We give formulas for the dimension of the Brauer configuration algebras induced by ciphertexts obtained via some block cyphers and music pieces interpreted as ciphertexts of some route and transposition cyphers. These procedures permit us to give alternative solutions to some of the canons proposed by Bach.

1.2 Contributions

The main results of this paper are Theorems 1, 2, 3, 4 with Proposition 1. Furthermore, the Brauer analysis of Bach canons à 6 Voc (BWV 1076), 1 à 2 (crab canon), and à 4 Quaerendo Invenietis realized in Section 3.4.

Theorem 1 proves that the Brauer configuration algebras associated with the plaintext and ciphertext of a permutation cryptosystem coincide. Theorems 2, 3 and Proposition 1 give formulas for the dimensions of the Brauer configuration algebra and the corresponding center associated with a Vigenere ciphertext.

Theorem 4 gives conditions for a musical piece written on the usual Western staff to be a specialization of a suitable Brauer configuration. Section 3.5 is devoted to the Brauer analysis of some of Bach's canons.

In particular, some commonly used symbols in Bach's works are built by representing musical notes as points in the plane. Such points are vertices of graphs induced by the canons. The graphs' edges are obtained by connecting consecutive classes of musical notes (i.e., consecutive points) appropriately.

The organization of this paper goes as follows: Background, main definitions and notation are given in section 2; we remind definitions of multisets (Section 2.2), Brauer configuration algebras (Section 2.2.1) and some of their properties. Section 2.3 is devoted to reminding basic facts about cryptography. We present the main results in section 3. Concluding remarks are given in section 4.

2 Preliminaries

This section provides basic definitions and notations regarding Brauer configuration algebras, and cryptography [1, 2, 5, 6, 28, 29, 30, 31, 32].

2.1 Background

Brauer configuration algebras (BCAs) were introduced by Green and Schroll in 2017 [1, 2]. Soon afterwards, several works were written to apply these algebras in different fields of mathematics and sciences. On one hand, Espinosa and Rios wrote their doctoral dissertations based on these algebras [29, 30]. Espinosa et al. introduced the notion of a message and specialized message of a Brauer configuration to give a formula for the number of perfect matchings of a snake graph associated with some Kronecker modules [29, 26]. Rios [30] used such algebras to describe particular classes of Dyck paths and integer friezes. This approach allows Dyck-Brauer messages to obtain alternative formulas for cluster variables associated with cluster algebras of type A_n [31, 33].

Angarita et al. [23] used BCAs to define alternative methods to protect biometric databases, and Fúneme et al. [6] introduced Brauer messages to examine the performance of some provably secure hash functions as those defined by Zémor and Tillich [34] and Sosnovski [35] based on the Cayley graph of some semigroups.

Relationships between BCAs and the graph energy theory were given by Agudelo et al. [25], who calculated the trace norm of some matrices induced by so-called $\{0, 1\}$ -Brauer configurations. It is worth noting that Espinosa [29] also studied relationships between the graph energy theory and Brauer messages.

Ballester-Bolinches et al. [21] used BCAs to give solutions to the Yang-Baxter equation. To do that, the authors specialized Brauer messages to define some skew braces in the sense of Rump [36]. Espinosa and Ballester-Bolinches et al. [22] also gave solutions to the Yang-Baxter equation via previous works written by Espinosa regarding the interaction between the Kronecker algebra, snake graphs theory and the theory of Brauer configuration algebras.

Relationships between cryptography and Brauer configuration algebras were given by Marin et al. [5], who define the schedule of an AES (Advanced Standard Encryption) key in terms of appropriated mutations of Brauer messages. In this work, such messages allow solutions to some generalizations of the Chicken Mc Nugget problem, particularly the Frobenius problem.

On the other hand, it is worth pointing out that throughout history, Bach's work has been a source of a plethora of research, from the study of the symbology used to write his compositions to determining their corresponding fractal dimensions [7, 8, 14, 9, 10, 11, 12, 18, 20, 37, 38, 39, 40, 41, 42]. For instance, Smend [38] applied gematria to name the number 14 as the Bach number ($BACH=2+1+3+8=14$), and Tatlow discusses the use of cryptograms in Bach's work in [9]. Furthermore, Niitsuma and Tomita studied Bach's writing in [40]. Bach journal, published by the Riemenschneider Bach Institute and Understanding Bach journal, edited by Ruth Tatlow, are devoted to Bach works in the Baroque era. Several papers published in these journals regard Bach's canons and his writing stylism, including his famous motif [13, 17, 16, 19, 18, 20, 42, 43, 44].

Sylvestre and Costa [14] and Shafer [12] studied some relationships between Bach's work, Fibonacci numbers and Fourier analysis.

It is worth noting, that the theory of graphs is a helpful tool to analyze symbolic music structure, which is an open problem in Music Information Retrieval (MIR) in this regard Hernandez-Olivan et al.

[45] used adjacency matrices of some graphs to segment symbolic music by its form or structure. According to them, the notes of a music piece $\mathfrak{M}$ can be seen as vertices of an appropriated graph $(V^{\mathfrak{M}}, E^{\mathfrak{M}})$ and the set $E^{\mathfrak{M}}$ of edges between two of them is partitioned into three sets, i.e., $E^{\mathfrak{M}} = E^{on} \cup E^{cons} \cup E^h$, where E^{on} consists of the edges connecting notes in the same onset, E^{cons} consists of the edges connecting consecutive notes in time. And E^h which is the set of edges linking overlapping notes in time.

On the other hand, Szeto et al. [46] defined posets (partially ordered sets) to facilitate pattern matching in post-tonal music analysis by using some pitch-class sets. In this work, the authors introduced the notion of stream, defined as the perceptual impression of connected series of musical notes. Whereas, stream segregation is the process of grouping musical notes into streams. According to them, the vertices or points of the corresponding Hasse diagram are given by events, and the main objective of the clustering algorithm is to connect an event to its nearest sequential event.

We also remind that Jeong et al. [47] presented a graph neural network to learn note representation from music scores in Western notation.

In this paper, we combine the techniques introduced by Hernandez Oliván et al. and Szeto et al. to construct appropriated graphs which can be read as symbols commonly used by Bach in his works.

In the sequel, we introduce some helpful notation and definitions regarding BCAs and classical cryptography.

2.2 Multisets

A *multiset* is a set with possibly repeated elements. Formally, a multiset is a pair of type (M, f) where M is a set and $f : M \rightarrow \mathbb{N}$ is a map from M to the set of nonnegative integers. In this case, if $m \in M$ then $f(m)$ is said to be the *multiplicity* of m [4, 48].

A *permutation* of a multiset (M, f) is a word w whose letters are given by the set M whereas the number of occurrences of a given letter in w is given by the map f . In this paper, we assume that the word

$w(M)$ of a multiset (M, f) with $M = \{m_1, m_2, \dots, m_s\}$ is given by a fixed permutation with the form

$$w(M) = m_1^{f(m_1)} m_2^{f(m_2)} \dots m_s^{f(m_s)}. \quad (1)$$

Note that there are $(f(m_1) + f(m_2) + \dots + f(m_s))!$ permutations associated with the multiset (M, f) .

If (M_1, f_1) and (M_2, f_2) are multisets with $M_1 = \{m_{1,1}, \dots, m_{1,r}\}$ and $M_2 = \{m_{2,1}, \dots, m_{2,s}\}$ then

$$\begin{aligned} (M_1, f_1) \cup (M_2, f_2) &= (M_1 \cup M_2, f_{1,2}) \text{ with } f_{1,2}(x) = \max\{f_1(x), f_2(x)\}. \\ (M_1, g_1) \cap (M_2, g_2) &= (M_1 \cap M_2, g_{1,2}) \text{ with } g_{1,2}(x) = \min\{f_1(x), f_2(x)\}. \end{aligned} \quad (2)$$

Let $\mathcal{M} = \{(M_1, f_1), (M_2, f_2), \dots, (M_h, f_h)\}$ be a collection of multisets such that if

$$w(M_i) = (m_{i,1})^{f_i(m_{i,1})} (m_{i,2})^{f_i(m_{i,2})} \dots (m_{i,s_i})^{f_i(m_{i,s_i})} \text{ then } \sum_{j=1}^{s_i} f_i(m_{i,j}) > 1.$$

In such a case. If $M = \bigcup_{i=1}^h M_i$, $\bigcap_{x \in I} M_x$ is the interception of all multisets containing an element $y \in M$ with $I \subseteq \{1, 2, \dots, h\}$ a fixed set of indices, and $f_x(y)$ is the frequency of y in M_x then $\sum_{x \in I} f_x(y)$ is said to be the *valency* of y denoted $val(y)$. We endow the set $\mathfrak{I}_y = \{M_x \mid x \in I\}$ with a linear order $<$.

If $x, x' \in I$, $z \in M_x \cap M_{x'}$, $z \notin \bigcap_{M_x \in \mathfrak{I}_y} M_x$, and $M_x < M_{x'}$ then the linear order $\prec$ associated with $\mathfrak{I}_z$ is defined in such a way that $M_x \prec M_{x'}$. Particularly, for $x \in I$ fixed and $f_x(y) > 1$, there is a subchain $\mathfrak{M}_{x,y} = M_x^{(1)} < M_x^{(2)} < \dots < M_x^{f_x(y)}$ where M_x^i is associated with a unique copy of M_x named the *expansion* of M_x induced by y .

A collection of multisets $\mathcal{M} = \{(M_1, f_1), \dots, (M_t, f_t)\}$ is said to be a *system of multisets of type M*, if $M = \bigcup_{j=1}^t M_j$. And it is endowed with a map $\nu : M \rightarrow \mathbb{N}^+ \times \mathbb{N}^+$ such that $\nu(m) = (j, val(m))$, for each $m \in M$.

Green and Schroll [1] named vertices the elements of M . The positive integer j in a pair $(j, \text{val}(m))$ associated with a vertex m is the multiplicity value $\mu(m)$ according to them. It is worth pointing out that $\mu(m)$ does not deal with the multiplicity of m as an element of a multiset. In particular, $m \in M$ is said to be non-truncated (truncated) provided that $\mu(m)\text{val}(m) > 1$ ($\mu(m)\text{val}(m) = 1$). Thus, the multiplicity function μ classifies the set of vertices M into the set of truncated and non-truncated vertices. In this work, if $\text{val}(m) = 1$, it is assumed that $\mu(m) = 2$. Therefore, the considered vertices are non-truncated.

If $y \in M_{i_1} \cap M_{i_2} \cap \dots \cap M_{i_t}$ then a *successor sequence* $\mathcal{S}_y$ associated with y is a chain with the form

$$M_{i_1}^{(1)} < \dots < M_{i_1}^{(f(i_1, y))} < M_{i_2}^{(1)} < \dots < M_{i_2}^{(f(i_2, y))} < \dots < M_{i_t}^{(1)} < \dots < M_{i_t}^{(f(i_t, y))} \quad (3)$$

Successor sequence (3) can be written in the form:

$$\mathfrak{M}_{i_1, y} < \mathfrak{M}_{i_2, y} < \dots < \mathfrak{M}_{i_t, y}. \quad (4)$$

A *Brauer configuration* is a system of multisets of type M endowed with a function ν and an orientation $\mathcal{O}$ which is obtained by adding a relation $M_{i_t}^{(f(i_t, y))} < M_{i_1}^{(1)}$ ($M_{i_t} < M_{i_1}$) to each successor sequence $\mathcal{S}_y$, associating in this fashion a family of equivalent circular orders to any $y \in M$. In this case, the multisets (M_i, f_i) are called *polygons*. We let $\mathcal{M} = (M, \mathcal{M}_1, \nu, \mathcal{O})$ denote a Brauer configuration with $\mathcal{M}_1 = \{(M_1, f_1), \dots, (M_h, f_h)\}$, map ν and orientation $\mathcal{O}$ defined as above [1, 2].

Note that the completed successor sequences or circular orders associated with a given vertex y have the form

$$M_{i_s}^{(j)} < \dots < M_{i_s}^{(f(i_s, y))} < \dots < M_{i_t}^{(f(i_t, y))} < M_{i_1}^{(1)} < \dots < M_{i_s}^{(j-1)}. \quad (5)$$

The *message* $M(\mathcal{M})$ of a Brauer configuration is the concatenation of the words $w(M_i)$, i.e.,

$$M(\mathcal{M}) = w(M_1)w(M_2) \dots w(M_h). \quad (6)$$

We say that a Brauer configuration $\mathcal{M}$ is $\mathfrak{S}$ -labeled if each multiset (M_i, f_i) is labeled by a permutation $\pi_i \in \mathfrak{S}_{f_i(m_{i,1})+f_i(m_{i,2})+\dots+f_i(m_{i,s_i})}$, where $\mathfrak{S}_n$ denotes the symmetric group with n elements. Such a labeling means that the permutation π_i is applied to the word $w(M_i)$ for each $1 \leq i \leq h$ [29, 5]. In such a case we write

$$M(\mathcal{M}^{\pi_1, \dots, \pi_h}) = w(M_1, \pi_1) \dots w(M_h, \pi_h) = w(\pi_1(M_1)) \dots w(\pi_h(M_h)). \quad (7)$$

Remark 1. *Since Brauer messages are defined by concatenating a fixed set of words given by a set of suitable permutations, we assume that all the Brauer configurations presented in this paper are $\mathfrak{S}$ -labeled. i.e., polygons are defined by words obtained after the application of an appropriated permutation.*

The Brauer quiver $Q_{\mathcal{M}} = (Q_0, Q_1, s, t)$ (or simply Q , if no confusion arises) induced by a Brauer configuration $\mathcal{M} = (M, \mathcal{M}_1, \nu, \mathcal{O})$ is defined in such a way that there is a bijective correspondence between its set of vertices Q_0 and the set of polygons $\mathcal{M}_1$. In such a case, each covering $(M_i, f_i) < (M_j, f_j)$ in a circular ordering defines an arrow from (M_i, f_i) to (M_j, f_j) in Q_1 .

2.2.1 Brauer Configuration Algebras

A Brauer configuration algebra $\Lambda_{\mathcal{M}}$ (or simply Λ if no confusion arises) is a bound quiver algebra $\Lambda_{\mathcal{M}} = kQ_{\mathcal{M}}/\langle \rho \rangle$ induced by a Brauer quiver $Q_{\mathcal{M}}$ bounded by an ideal $I = \langle \rho \rangle$ generated by a set of relations ρ of the following types [1, 2]:

- $C_i^{\mu(i)} - C_j^{\mu(j)}$ if i and j are vertices in the same polygon (M_i, f_i) and C_x is a cycle defined by circular relations. These cycles are said to be *special cycles*.
- $C^{\mu(i)}a$ if a is the first arrow of a special cycle C_i associated with a vertex i .
- ab if $a, b \in Q_1$ are arrows of different special cycles and ab is an element of the path algebra induced by $Q_{\mathcal{M}}$.

Remark 2. *Green and Schroll [1] proved that Brauer configuration algebras are symmetric and multiserial and that there is a bijective correspondence between the indecomposable projective $\Lambda_{\mathcal{M}}$ -modules and the*

polygons in $\mathcal{M}_1$. Furthermore, the number of summands in the heart of an indecomposable projective $\Lambda_{\mathcal{M}}$ -module P with $\text{rad}^2 P \neq 0$ equals the number of non-truncated vertices in the corresponding polygon. Particularly, it holds that

$$\dim_k \Lambda_{\mathcal{M}} = 2|\mathcal{M}_1| + \sum_{m \in M} \text{val}(m)(\text{val}(m)\mu(m) - 1). \quad (8)$$

Sierra [32] obtained the following formula for the dimension of the center $Z(\Lambda_{\mathcal{M}})$ of a connected Brauer configuration algebra.

$$\dim_k Z(\Lambda_{\mathcal{M}}) = 1 + |\mathcal{M}_1| - |M| + \sum_{m \in M} \mu(m) + \#(\text{Loops}(Q_{\mathcal{M}})) - |\{m \in M \mid \text{val}(m) = 1\}|. \quad (9)$$

2.3 Cryptography

This section reminds the definition of well-known cryptosystems [28]. Some of them related to the theory of Brauer configuration algebras.

A cryptosystem or cryptographic system is a quintuple of the form $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where

- $\mathcal{P}$ is a finite set of possible plaintexts.
- $\mathcal{C}$ is a finite set of possible ciphertexts.
- $\mathcal{K}$ is a finite set of possible keys.
- $\mathcal{E}(\mathcal{D})$ is a set of encryption (decryption) functions such that for each $K \in \mathcal{K}$, it holds that $e_K : \mathcal{P} \rightarrow \mathcal{C} \in \mathcal{E}$ ($d_K : \mathcal{C} \rightarrow \mathcal{P} \in \mathcal{D}$), and $d_K(e_K(x)) = x$, for each $x \in \mathcal{P}$.

The permutation cryptosystem and the Vigenere cryptosystem are examples of classical cryptosystems associated with Brauer configuration algebras. The following section will be devoted to clarifying these relationships.

The permutation or transposition cryptosystem is defined in such a way that for fixed integers $n, m > 1$, it holds that $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n^m$, in this case $\mathcal{K} = \mathfrak{S}_m$ is the set of all m -element permutations. For $\pi \in \mathfrak{S}_m$ and $x = (x_1, x_2, \dots, x_m) \in \mathcal{P}$, $e_{\pi}(x) = (x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(m)})$. Whereas, for $y = (y_1, y_2, \dots, y_m) \in \mathcal{C}$, $d_{\pi}(y_1, y_2, \dots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \dots, y_{\pi^{-1}(m)})$.

The following is an example of this kind of encryption for $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^4$, and $\pi = (3 \ 4 \ 1 \ 2)$.

<i>Y</i>	<i>O</i>	<i>H</i>
<i>P</i>	<i>T</i>	<i>Y</i>
<i>C</i>	<i>R</i>	<i>A</i>
<i>R</i>	<i>G</i>	<i>P</i>

(10)

Applying π^{-1} to each block, it is obtained the following array:

<i>C</i>	<i>R</i>	<i>A</i>
<i>R</i>	<i>G</i>	<i>P</i>
<i>Y</i>	<i>O</i>	<i>H</i>
<i>P</i>	<i>T</i>	<i>Y</i>

(11)

The path shown in figure 1 gives rise to the plaintext CRYPTOGRAPHY. So, it is considered as a route cypher.

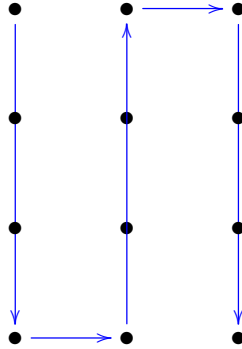


Figure 1: The route (path) used to decrypt the message (11) obtained via permutation.

For fixed integers $m, n > 1$ fixed, $\mathbb{Z}_n^m = \mathcal{P} = \mathcal{C} = \mathcal{K}$ in the Vigenere cryptosystem. In such a case, for a given key $K = (k_1, k_2, \dots, k_m) \in \mathcal{K}$, $x = (x_1, x_2, \dots, x_m) \in \mathcal{P}$, and $y = (y_1, y_2, \dots, y_m) \in \mathcal{C}$, it holds that

$$\begin{aligned} e_K(x) &= (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m) \mod n \\ d_K(y) &= (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m) \mod n \end{aligned} \quad (12)$$

The Vigenere cryptosystem is vulnerable to a ciphertext-only attack introduced by Friedman [28]. It is based on the coincidence index of a text. In such a case, it is assumed that n is the size of the underlying alphabet. For instance, $n = 26$ if the language is English. The *index of coincidence* $\mathcal{J}(T)$ of a string T of alphabetic characters (which is the probability that two random elements of T be identical) is given by the following formula:

$$\mathcal{J}(T) = \sum_{i=0}^{25} \frac{f_i(f_i - 1)}{n(n - 1)}. \quad (13)$$

Where $n = |T|$ and for each i , f_i denotes the frequency of the i th character in T (f_0 for A, f_1 for B, and so on).

Suppose T and T' are strings of alphabetic characters. In that case, the *mutual index of coincidence* (which is the probability that a random element of T is identical to an element of T') is given by the following formula.

$$M\mathcal{J}(T, T') = \sum_{i=0}^{25} \frac{f_i f'_i}{nn'}. \quad (14)$$

Where $n = |T|$, $n' = |T'|$ and f_i (f'_i) denotes the frequency of the i th character in T (T').

The coincidence index attack is based on the fact that modulo the length of the key, identical characters are encrypted by the same alphabetic character. So, if y is a ciphertext obtained by a Vigenere key $k = (k_1, k_2, \dots, k_m)$ of length m . Then y can be split into m lists $y_1, y_2, \dots, y_m$ whose indices are all close to 0.065.

Since the lists $y_1, y_2, \dots, y_m$ are obtained by applying an appropriated shift $\mathfrak{s}$ and computing the different mutual indices of coincidence $M\mathcal{J}(y_i, y_j^{\mathfrak{s}}) = \frac{\sum_{i=0}^{25} f_i f'_{i-\mathfrak{s}}}{nn'}$. Then a set of equations with the form $k_i - k_j = \mathfrak{s}_0$ is built for each of these comparisons, where $\mathfrak{s}_0$ is a value for which $M\mathcal{J}(y_i, y_j^{\mathfrak{s}_0})$ is close to 0.065. The solution of the obtained

system of linear equations (modulo 26) gives the Vigenere key used to obtain the ciphertext y . Particularly, if m is the length of the key then $J(y_i) \sim 0.065$ for any $1 \leq i \leq m$.

3 Main Results

This section gives the main results regarding the dimension of Brauer configurations algebras associated with polyalphabetic cryptosystems, mutations of Brauer configurations, and iterated cyphers. Subsections 3.3 and 3.4 are devoted to the Brauer analysis of musical content, subsection 3.4 analyzes Bach's canons.

3.1 Brauer Configuration Algebras Associated with the Permutation Cryptosystem

Suppose that $y = y_1 y_2 \dots y_m$ is a ciphertext obtained by encrypting a plaintext x divided into m blocks $x_1, x_2, \dots, x_m$ not necessarily of the same size, i.e., $x = x_1 x_2 \dots x_m$, with $|x_i| = s_i = |y_i| > 1$. The encryption and decryption rules are given by the following identities:

$$\begin{aligned} e_K(x) &= e_{\pi_1}(x_1) e_{\pi_2}(x_2) \dots e_{\pi_m}(x_m) = \pi_1(x_1) \pi_2(x_2) \dots \pi_m(x_m). \\ d_K(y) &= d_{\pi_1^{-1}}(x_1) d_{\pi_2^{-1}}(x_2) \dots d_{\pi_m^{-1}}(x_m) = \pi_1^{-1}(x_1) \pi_2^{-1}(x_2) \dots \pi_m^{-1}(x_m). \end{aligned} \quad (15)$$

where $\pi_i \in \mathfrak{S}_i$ for $1 \leq i \leq m$.

Plaintexts and ciphertexts in the transposition cryptosystem define labeled Brauer configurations bearing in mind that x can be seen as a Brauer message of a labeled Brauer configuration $\mathcal{M}$ of the form

$$\begin{aligned} x &= M(\mathcal{M}) = (w(x_1), \sigma_1)(w(x_2), \sigma_2) \dots (w(x_m), \sigma_m), \quad \sigma_i \in \mathfrak{S}_i \quad 1 \leq i \leq m. \\ x_i &= \sigma_i(w(x_i)). \end{aligned} \quad (16)$$

Where for each i , $w(x_i) = x_{i,1}^{f_{i,1}} x_{i,2}^{f_{i,2}} \dots x_{i,m_i}^{f_{i,m_i}}$ ($f_{i,1} + f_{i,2} + \dots + f_{i,m_i} = s_i$) is a word determining the polygon $U_i \in \mathcal{M}_1 = \{U_1, U_2, \dots, U_m\}$. Note that, $x_{i,j}$ is a character of a fixed alphabet $\mathcal{A}$. Thus, $\mathcal{M} = (M, \mathcal{M}_1, \mu, \mathcal{O})$, where

- $M = \{x_{i,j} \mid 1 \leq i \leq m, 1 \leq j \leq s_i\}$.
- $\mathcal{M}_1 = \{w(x_i) \mid 1 \leq i \leq m\}$.
- $\mu(x_{i,j}) = 1$ ($\mu(x_{i,j}) = 2$) if $\text{val}(x_{i,j}) > 1$ ($\text{val}(x_{i,j}) = 1$).
- $(w(x_1), \sigma_1) < (w(x_2), \sigma_2) < \dots < (w(x_m), \sigma_m)$ in successor sequences.

In the same fashion the ciphertext $y = \pi_1(x_1)\pi_2(x_2)\dots\pi_m(x_m)$ is a labeled Brauer message $M(\mathcal{M}^{\pi_1, \pi_2, \dots, \pi_m})$ obtained by permuting vertices in x_i for $1 \leq i \leq m$. We let $\Lambda_{\mathcal{M}}$ ($\Lambda_{\mathcal{M}^{\pi_1, \dots, \pi_m}}$) denote the labeled Brauer configuration algebra defined by the plaintext x (ciphertext y).

The following result holds:

Theorem 1. $\Lambda_{\mathcal{M}} = \Lambda_{\mathcal{M}^{\pi_1, \dots, \pi_m}}$.

Proof. Note that the system of permutations $\pi_1, \pi_2, \dots, \pi_m$ does not change vertices, polygons nor the orientation of the polygons in successor sequences defining the Brauer configuration $\mathcal{M}$. $\square$

3.2 Brauer configuration Algebras Associated with the Cryptanalysis of the Vigenere Cryptosystem

Suppose that y is a captured ciphertext of a Vigenere cryptosystem. We can assume that y contains all the characters of an alphabet $\mathcal{A}$ of a natural language $\mathcal{L}$ and the frequency f_j of any $j \in \mathcal{A}$ is greatest than 1. If m is the length of the key $K = (k_1, k_2, \dots, k_m)$ then y is a concatenation of m lists $y_1, y_2, \dots, y_m$. Thus y can be seen as a Brauer message $M(\mathfrak{C})$ such that:

- $\mathfrak{C}_0 = \mathcal{A}$.
- $\mathfrak{C}_1 = \{y_1, y_2, \dots, y_m\}$.
- $\mu(i) = 1$, for any $i \in \mathcal{A}$.
- $y_1 < y_2 < \dots < y_m$ in successor sequences.

We have the following result:

Theorem 2. *Let $\Lambda_{\mathfrak{C}}$ be a Brauer configuration algebra induced by a Vigenere ciphertext y obtained with a key of length m . Then*

$$\dim_k \Lambda_{\mathfrak{C}} = 2m + |y|(|y| - 1)\mathcal{I}(y). \quad (17)$$

Proof. Since the size of the key is m . Then $|\mathfrak{C}_1| = m$ and $\mathcal{I}(y) = \sum_{i \in \mathcal{A}} \frac{f_i(f_i-1)}{|y|(|y|-1)}$. $\square$

The following result regards the dimension $\dim_k Z(\Lambda_{\mathfrak{C}})$ of the center of the algebra $\Lambda_{\mathfrak{C}}$ induced by a Vigenere ciphertext y .

Theorem 3. *Let $\Lambda_{\mathfrak{C}}$ be the Brauer configuration algebra induced by a Vigenere ciphertext y and $y_1, y_2, \dots, y_m$ are its corresponding lists obtained with a key of length m . Then if $f_{i,j}$ denotes the frequency of the j th alphabetic character in the list y_i , it holds that*

$$\dim_k Z(\Lambda_{\mathfrak{C}}) = 1 + m + \sum_{i=1}^m \sum_{j \in \mathcal{A}} (f_{i,j} - 1). \quad (18)$$

Proof. Since the length of the key is m then $|\mathfrak{C}_1| = m$. Furthermore, the number of loops associated with the j th character-vertex of the alphabet $\mathcal{A}$ in the list-polygon y_i is $f_{i,j} - 1$. $\square$

As an example, the Vigenere ciphertext

$$C = \text{OOPAELRIXFGGBWDODDEPK} \quad (19)$$

is obtained from the plaintext

$$\text{classicalcryptography} \quad (20)$$

with the key

$$\text{MDPI} \quad (21)$$

This scheme induces the Brauer configuration $\mathfrak{C} = (\mathfrak{C}_0, \mathfrak{C}_1, \mu, \mathcal{O})$ such that

- $\mathfrak{C}_0 = \{O, P, A, E, L, R, I, X, F, G, B, W, D, K\}$.
- $\mathfrak{C}_1 = \{y_1 = \{O, E, X, B, D, K\}, y_2 = \{O, L, F, W, D\}, y_3 = \{P, R, G, D, E\}, y_4 = \{A, I, G, O, P\}\}$.
- $\mu(O) = \mu(P) = \mu(E) = \mu(G) = \mu(D) = 1, \quad \mu(j) = 2$, for the remaining vertices $j \in M$.
- $y_1 < y_2 < y_3 < y_4$ in successor sequences.

$$\begin{aligned}
S_O &= y_1 < y_2 < y_4, \\
S_P &= y_3 < y_4, \\
S_A &= y_4, \\
S_E &= y_1 < y_3, \\
S_L &= y_2, \\
S_R &= y_3, \\
S_I &= y_4, \\
S_X &= y_1, \\
S_F &= y_2, \\
S_G &= y_3 < y_4, \\
S_B &= y_1, \\
S_W &= y_2, \\
S_D &= y_1 < y_2 < y_3, \\
S_K &= y_1.
\end{aligned} \tag{22}$$

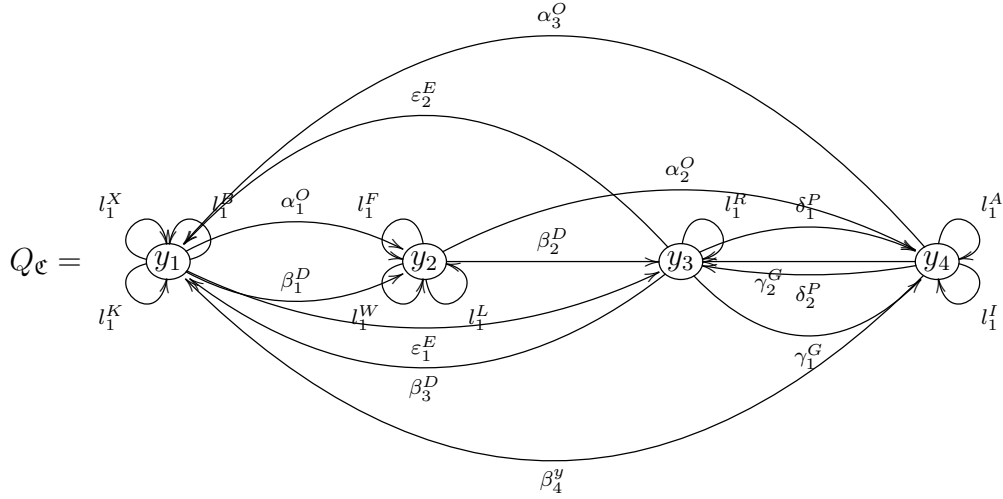


Figure 2: Brauer quiver of a Vigenere ciphertext.

The following relations define the admissible ideal $I_{\mathfrak{C}}$ with $M = \{\alpha_{i_1}^{j_1}, \beta_{i_2}^{j_2}, \gamma_{i_3}^{j_3}, \delta_{i_4}^{j_4}, \varepsilon_{i_5}^{j_5}\}$.

- $m_{i_s}^{j_s} n_{i_t}^{j_t}, \quad m_{i_s}^{j_s} \neq n_{i_t}^{j_t}, \quad m_{i_s}^{j_s}, n_{i_t}^{j_t} \in M.$
- $(l_1^j)^2$, for all the possible values of j .
- $\alpha_1^O \alpha_2^O \alpha_3^O = \beta_1^D \beta_2^D \beta_3^D = \varepsilon_1^E \varepsilon_2^E.$
- $\alpha_2^O \alpha_3^O \alpha_1^O = \beta_2^D \beta_3^D \beta_1^D.$
- $\gamma_1^G \gamma_2^G = \beta_3^D \beta_1^D \beta_2^D = \varepsilon_2^E \varepsilon_1^E = \delta_1^P \delta_2^P.$
- $\gamma_2^G \gamma_1^G = \alpha_3^O \alpha_1^O \alpha_2^O = \delta_2^P \delta_1^P.$
- $C_i^j f$, if C_i^j is a special cycle and f is its first arrow.

It holds that

$$\begin{aligned} \dim_k \Lambda_{\mathfrak{C}} &= 35, \\ \dim_k Z(\Lambda_{\mathfrak{C}}) &= 1 + 18 + 5 - 14 + 4 + 9 - 9 = 14, \\ \mathcal{J}(C) &= \frac{\dim_k \Lambda_{\mathfrak{C}} - 2(4)}{21(20)} = \frac{27}{420} = 0,0642. \end{aligned} \tag{23}$$

Proposition 1. *Let $\Lambda_{\mathcal{M}}$ be a Brauer configuration algebra induced by a Brauer configuration $\mathcal{M} = (M, \mathcal{M}_1, \mu, \mathcal{O})$ with $\mathcal{M}_1 = \{(U_1, f_1), \dots, (U_m, f_m)\}$ and for any $u_{i,j} \in U_i$, $1 \leq i \leq m$ it holds that $f_i(u_{i,j}) = 1$. And there are n vertices α such that $\text{val}(\alpha) = 1$. Then*

$$\dim_k Z(\Lambda_{\mathcal{M}}) = m + n + 1. \tag{24}$$

Proof. Note that $\#(\text{Loops}(Q_{\mathcal{M}})) = |\{i \in M \mid \text{val}(i) = 1\}|$, and $\sum_{i \in M} \mu(i) = 2n + |M| - n = n + |M|$. Thus, $\dim_k Z(\Lambda_{\mathcal{M}}) = 1 + m + n + |M| - |M| = 1 + m + n$. We are done. $\square$

3.3 Brauer Configuration Algebras Associated with Musical Content

This section proves that some musical contents give rise to Brauer configuration algebras.

Let $\mathcal{A} = \mathcal{X} \cup \mathcal{S}_0$ be an alphabet of a language whose letters or vertices are partitioned into two sets $\mathcal{X}$ and $\mathcal{S}_0$, $\mathcal{X}$ is endowed with a partial order $\preceq$ and a subset of real numbers $\mathcal{T} = \{t_1, t_2, \dots, t_k\}$. Elements $s \in \mathcal{S}_0$ are said to be constants. Each element $x_i \in \mathcal{X}$ is labeled by a unique element $t_i \in \mathcal{T}$. Therefore, each element $x_i \in \mathcal{X}$ can be seen as an ordered pair of the form (x_i, t_i) and

$$\mathcal{X} = \{(x_1, t_1), (x_2, t_2), \dots, (x_k, t_k)\} \quad (25)$$

$(x_i, t_i) \trianglelefteq (x_j, t_j)$ if and only if $x_i \preceq x_j$ or $t_i \leq t_j$ (the usual real numbers order).

In this case,

$$\min(\mathcal{X}) = x_1 \trianglelefteq x_2 \trianglelefteq \dots \trianglelefteq x_{k-1} \trianglelefteq x_k = \max(\mathcal{X}) \quad (26)$$

$\mathcal{X}$ is endowed with a circular order of the form

$$\mathbf{c}_h = (x_h, t_h) \trianglelefteq (x_{h+1}, t_{h+1}) \trianglelefteq \dots \trianglelefteq (x_k, t_k) \trianglelefteq (x_1, t_1) \trianglelefteq \dots \trianglelefteq (x_{h-1}, t_{h-1}) \trianglelefteq (x_h, t_h), \quad 1 \leq h \leq k.$$

Numbers t_j in pairs (x_j, t_j) are given by coverings $x_{j-1} \preceq x_j$, i.e.,

$$x_{j-1} \preceq x_j \longrightarrow t_j. \quad (27)$$

If numbers t_j are predefined, then (if no confusion arises), we will omit their use in the notation of the pairs constituting a set $\mathcal{X}$.

The words $\mathfrak{w} \in \mathcal{X}^*$ defined by the set $\mathcal{X}$ have the form:

$$\mathfrak{w} = \mathfrak{z}_1^{F_1} \mathfrak{z}_2^{F_2} \dots \mathfrak{z}_s^{F_s}. \quad (28)$$

For each $1 \leq i \leq s$, $\mathfrak{z}_i \in \mathcal{X}_j \subset \mathcal{X}^*$ for some integer $j \geq 1$. Where, $\mathcal{X}_j$ consists of length j words with the shape:

$$(x_{i_{h,1}}, t_{i_{h,1}})(x_{i_{h,2}}, t_{i_{h,2}}) \dots (x_{i_{h,j}}, t_{i_{h,j}}), \quad 1 \leq h \leq n_j. \quad (29)$$

To define operators, we will assume the notation $(x_{i_{h,j}}, t_{i_{h,j}}) = \mathfrak{y}_{i_{h,j}}$.

We let F_i denote an integral vector $F_i = (f_{i,1}, f_{i,2}, \dots, f_{i,j})$ such that

$$\mathfrak{z}_i^{F_i} = (x_{i_{h,1}}, t_{i_{h,1}})^{f_{i,1}} (x_{i_{h,2}}, t_{i_{h,2}})^{f_{i,2}} \dots (x_{i_{h,j}}, t_{i_{h,j}})^{f_{i,j}}. \quad (30)$$

Where $(x_{i_{h,1}}, t_{i_{h,1}})^{f_{i,1}} = \underbrace{(x_{i_{h,1}}, t_{i_{h,1}}) \dots (x_{i_{h,1}}, t_{i_{h,1}})}_{f_{i,1} \text{--times}}.$

Operators

Two maps $\sigma_{r_{\mathfrak{v}_{i_h,j}}}$ and φ_h are defined in such a way that if $\mathfrak{w}$ is given as in (28) then

$$\sigma_{r_{\mathfrak{v}_{i_h,j}}}(\mathfrak{v}_{i_{h'},j'}) = \begin{cases} (x_{i_{h,1}}, t_{i_{h,1}} + \frac{(t_{i_{h,1}})(r_{\mathfrak{v}_{i_h,j}})}{2}), & \text{if } h = h' \text{ and } j = j', \\ \mathfrak{v}_{i_{h'},j'}, & \text{otherwise.} \end{cases}$$

$$r_{\mathfrak{v}_{i_h,j}} \in \mathbb{R}.$$

$$\varphi_h((x_{i_{p,j}}, t_{i_{p,j}})^{f_{p,j}}) = (x_{i_{p,j}}, t_{i_{p,j}})^{f_{p,j} + h f_{p,j}} \quad (31)$$

$$\begin{aligned} \sigma_2(x_{i-1}, t_{i-1}) &= (x_i, 2t_{i-1}) = (x_i, t_i) \\ \sigma_{-2}(x_i, t_i) &= (x_{i-1}, 0) = (x_{i-1}, t_{i-1}) \\ \sigma_x(\sigma_{-x})((x_i, t_i)) &= (x_i, t_i). \end{aligned} \quad (32)$$

Note that in the cycle $\mathfrak{c}_h$, it holds that $(x_{h+k}, t_{h+k}) = \sigma_{2k}(x_h, t_h)$.

Grouping Symbols

Letters within a word $\mathfrak{w}$ or in different words can be grouped using parentheses, brackets and braces. Often, parentheses are used to group letters with the same coordinates. Whereas brackets and braces group letters within a word with the same frequency.

$$\underbrace{((x_1, t_1)^{f_1}(x_1, t_1)^{f_1} \dots (x_1, t_1)^{f_1}(x_1, t_1)^{f_i})}_{n\text{-times}} = (x_1, t_1)^{\underbrace{f_1 + f_1 + \dots + f_1 + f_i}_{n\text{-veces}}} \quad (33)$$

$$\mathfrak{w} = \underbrace{(x_{i_1}, t_{i_1})^{f_{i_1}}(x_{i_2}, t_{i_2})^{f_{i_2}} \dots ((x_{i_s}, t_{i_s})^{f_{i_s}}(x_{i_s}, t_{i_s})^{f_{i_s}})}_{w_1} \underbrace{(x_{j_1}, t_{j_1})^{f_{j_1}}(x_{j_2}, t_{j_2})^{f_{j_2}} \dots (x_{j_r}, t_{j_r})^{f_{j_r}}}_{w_r} \quad (34)$$

$$\mathfrak{w} = \underbrace{\{(x_{i_1}, t_{i_1})(x_{i_2}, t_{i_2}) \dots (x_{i_s}, t_{i_s})\}^{f_{j_0}}}_{w_1} \underbrace{(x_{j_1}, t_{j_1})^{f_{j_1}}(x_{j_2}, t_{j_2})^{f_{j_2}} \dots (x_{j_r}, t_{j_r})^{f_{j_r}}}_{w_r} \quad (35)$$

$$(x_{i_1}, t_{i_1}) \trianglelefteq (x_{i_2}, t_{i_2}) \trianglelefteq \cdots \trianglelefteq (x_{i_s}, t_{i_s}).$$

We let $\sigma_{r,x}^\Gamma$ denote a function which applies σ_r to each occurrence of a vertex $x \in \Gamma_0$, where Γ_0 is the set of vertices of a Brauer configuration whose polygons are given by words of type $\mathfrak{w}$ (see (28), (33)-(35)).

$$\mathfrak{a}^\Gamma = \{\sigma_{r,x}^\Gamma \mid x \in \Gamma_0, r \in \mathbb{R}\} \quad (36)$$

$\mathfrak{a}^\Gamma$ can be considered part of a Γ *labeling*, which contains symbols giving information on the ordering and number of vertices in the polygons.

Identities (37) gives the words determining polygons of a Brauer configuration $\Gamma = (\Gamma_0, \Gamma_1, \mu, \mathcal{O})$ with

- $\Gamma_0 = \{a, e, g, \sigma_{-1}(b), \sigma_{-1}(g), c_0, d_0\}$.
- $\varphi_{\frac{n}{2}}(x)^n = x^{n+\frac{n}{2}}$.
- $\sigma_{-1}(x^n) = (\sigma_{-1}(x))^n$.
- c_0 and d_0 are constants.
- π_j are labeling denoting appropriated permutations.
- $w_i < w_j$ if $i < j$ for successor sequences.
- $\mu(\alpha) = 2$ or $\mu(\alpha) = 1$ if the valency of a vertex α is whether 1 or greatest than 1.

$$\begin{aligned} w_1 &= (\varphi_8(e^{16})\sigma_{-1}(\varphi_8(g^{16}))a^{16}d_0^8e^8, \pi_1) \\ w_2 &= (d_0^8\sigma_{-1}(g^8)d_0^8\sigma_{-1}(b^8)\varphi_8(a^{16})d_0^8, \pi_2) \\ w_3 &= (\varphi_8(e^{16})\sigma_{-1}(\varphi_8(g^{16}))a^{16}d_0^8g^8, \pi_3) \\ w_4 &= (d_0^8\varphi_{16}(e^{32})c_0^{16}, \pi_4) \\ w_5 &= (\varphi_8(e^{16})\sigma_{-1}(g^{16})a^{16}d_0^8e^8, \pi_5) \\ w_6 &= (d_0^8\sigma_{-1}(g^8)d_0^8\sigma_{-1}(b^8)\varphi_8(a^{16})d_0^8, \pi_6) \\ w_7 &= (\varphi_8(e^{16})\sigma_{-1}(\varphi_8(g^{16}))a^{16}d_0^8g^8, \pi_7) \\ w_8 &= (\varphi_8(e^{16})\sigma_{-1}(\varphi_8(g^{16}))a^{16}d_0^8g^8, \pi_8) \\ w_9 &= (d_0^8\varphi_{16}(e^{32})c_0^{16}, \pi_9) \end{aligned} \quad (37)$$

$$\begin{aligned} \dim_k \Lambda_\Gamma &= 90426 \\ \dim_k Z(\Lambda_\Gamma) &= 612 \end{aligned}$$

The following result regards Western musical writing without considering ornaments or interpretation symbols (e.g. fermata, coda, crescendo-decrescendo symbols or any other dynamic symbol, which can be included as label polygons).

Theorem 4. *Any musical piece $\mathcal{M}$ written with the standard staff notation can be seen as a transposition ciphertext of the message $M(\mathfrak{M})$ of a Brauer configuration $\mathfrak{M}$ with the following properties: $\mathfrak{M} = (\mathfrak{M}_0, \mathfrak{M}_1, \mu, \mathcal{O})$.*

- $\mathfrak{M}_0 = \{a < \sigma_{-1}(b) < b < \sigma_{-1}(c) < c < d < \sigma_{-1}(e) < e < \sigma_{-1}(f) < f < \sigma_{-1}(g) < g < a\} \cup \mathcal{H} \cup \mathcal{S}_0$.
- $\mathcal{H} = \{\varphi_{\frac{k}{2}}(x^k) \mid x = a, b, \dots, g, k = 2^t \text{ for some } t > 0\}$.
- $\mathcal{S}_0 = \{a_0, b_0, c_0, d_0, e_0, f_0, g_0\}$.
- Any labeled polygon $U \in \mathfrak{M}_1$ (by a key $(\mathcal{K}_i, \mathfrak{s}_i)$) is determined by a word of type (28) and (33, 28, 35) with $f_{i,j} = 2^n + k2^{n/2}$, $k, n \geq 0$. We assume that if $\mathfrak{M}_1 = \{U_1, U_2, \dots, U_k\}$ then $\mathcal{K}_i$ is a permutation of the vertices $x_{i,j}$ in polygon U_i and $\mathfrak{s}_i \leq 64$ is the total number of its vertices counting repetitions.

•

$$\mu(\alpha) = \begin{cases} 2, & \text{if } \text{val}(\alpha) = 1, \\ 1, & \text{Otherwise.} \end{cases}$$

- The orientation $\mathcal{O}$ is given by enumerating the words $w_1 < w_2 < \dots < w_n$ associated with the polygons of Γ_1 ($|\Gamma_1| = n$) and assuming this order to build the successor sequences.

Proof Consider the following equivalences:

1. $x^{64} \longleftrightarrow (\mathfrak{c}, x)$
 $x^{32} \longleftrightarrow (\mathfrak{d}, x)$
 $x^{16} \longleftrightarrow (\mathfrak{e}, x)$
 $x^8 \longleftrightarrow (\mathfrak{f}, x)$
 $x^4 \longleftrightarrow (\mathfrak{g}, x)$
 $x^2 \longleftrightarrow (\mathfrak{h}, x)$

Finally, the sixty fourth note and its rest have associated the vertices x^1 and g_0 respectively.

2.

$$\begin{aligned} \sigma_{-1}(x) &= \flat x. \\ \sigma_1(x) &= \sharp x. \\ \sigma_{-n}\sigma_n(x) &= \natural x. \end{aligned} \tag{38}$$

$$3. \varphi_{32}(x^{64}) \longleftrightarrow (\mathfrak{O}, x), \quad \varphi_{16}(x^{32}) \longleftrightarrow (\mathfrak{D}, x), \quad \varphi_8(x^{16}) \longleftrightarrow (\mathfrak{d}, x) \dots$$

$$4. \begin{array}{ll} a_0^{64} \longleftrightarrow & \text{—} \\ b_0^{32} \longleftrightarrow & \text{—} \\ c_0^{16} \longleftrightarrow & \mathfrak{z} \\ d_0^8 \longleftrightarrow & \gamma \\ e_0^4 \longleftrightarrow & \mathfrak{y} \\ f_0^2 \longleftrightarrow & \mathfrak{y} \end{array}$$

$$5. \begin{array}{ll} a \longleftrightarrow & C \\ b \longleftrightarrow & D \\ c \longleftrightarrow & E \\ d \longleftrightarrow & F \\ e \longleftrightarrow & G \\ f \longleftrightarrow & A \\ g \longleftrightarrow & B \end{array}$$

6. Standard scales are given by the following cycles.

- (a) $a < b < c < d < e < f < g < a$.
- (b) $d < \sigma_{-1}(e) < e < \sigma_{-1}(f) < f < \sigma_{-1}(g) < g < a < \sigma_{-1}(b) < b < \sigma_{-1}(c) < c < d$
- (c) $a < \sigma_{-1}(b) < b < \sigma_{-1}(c) < c < d < \sigma_{-1}(e) < e < \sigma_{-1}(f) < f < \sigma_{-1}(g) < g < a$
- (d) $\frac{x+y}{2} = \sigma_{-1}(y) = \sigma_1(x)$, if $x < y$.

7. Measures are given by the polygons in $\mathfrak{M}_1$.

8. Grouping symbols (parentheses, brackets, and braces) in polygons define slurs, ties, tuples and chords.

Therefore, the musical piece $\mathcal{M}$ is nothing but a ciphertext of a transposition cryptosystem $S = (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where

$$\mathcal{P} = \{a, b, \dots, g, \sigma_{-1}(b), \sigma_{\pm 1}(c), \sigma_{\pm 1}(e), \sigma_{\pm 1}(f), \sigma_{\pm 1}(g)\} \bigcup \mathcal{H} \bigcup \mathfrak{S}_0,$$

$$\mathcal{C} = \{(\mathfrak{n}, x) \mid \mathfrak{n} \text{ is a musical note and } x \in \mathcal{P}\}.$$

$$\mathcal{K} = \{n \in \mathbb{N} \mid n = 2^k, 1 \leq k \leq 6\}.$$

$$e_{2^k}(x) = x^{2^k} = (\mathfrak{n}, x), \text{ for any } x \in \mathcal{P} \text{ the duration of } \mathfrak{n} \text{ is } \frac{\mathfrak{d}}{2^k} (\text{see}(\mathfrak{?})).$$

(39)

$$\begin{aligned}
d_n(\mathbf{n}, y) &= y^{2^k} \text{ if the duration of } \mathbf{n} = \frac{\mathfrak{d}}{2^k}. \text{ Furthermore,} \\
d_n(\mathfrak{b}\mathbf{n}, y) &= \sigma_{-1}(y^{2^k}). \\
d_n(\sharp\mathbf{n}, y) &= \sigma_1(y^{2^k}). \\
d_n(\natural\mathbf{n}, y) &= y^{2^k}. \\
d_n(\dot{\mathbf{n}}, y) &= \varphi_{2^{k-1}}(y^{2^k}). \\
d_n(\mathfrak{r}) &= x_0^{2^k}, \text{ where } \mathfrak{r} \text{ is a rest of duration } \frac{\mathfrak{d}}{2^k}. \quad \square
\end{aligned} \tag{40}$$

As an example the following is the musical notation of the words (37) defined by the equivalences described in Theorem 4, the corresponding labeled Brauer configuration induced by these words is said to be $\mathfrak{M}$ -reduced:

$$\begin{aligned}
(\omega_1, \mathcal{K}) &= [b^8 f^8 e^8 b^8][d^8 \sigma_{-1} g^8 e^8 b^8] \longleftrightarrow [(\mathfrak{J}, b)(\mathfrak{J}, f)(\mathfrak{J}, e)(\mathfrak{J}, b)][(\mathfrak{J}, d)(\mathfrak{b}\mathfrak{J}, g)(\mathfrak{J}, e)(\mathfrak{J}, b)] \\
(\omega_2, \mathcal{K}) &= \sigma_{-1} c^{16} [\sigma_{-1} g^8 e^8] b^{16} f^{16} \longleftrightarrow (\mathfrak{J}, c)[(\mathfrak{b}\mathfrak{J}, g)(\mathfrak{J}, e)](\mathfrak{J}, b)(\mathfrak{J}, f) \\
(\omega_3, \mathcal{K}) &= b^{16} [f^8 \sigma_{-1} c^8] a^{16} f^{16} \longleftrightarrow (\mathfrak{J}, b)[(\mathfrak{J}, f)(\mathfrak{b}\mathfrak{J}, c)](\mathfrak{J}, a)(\mathfrak{J}, f) \\
(\omega_4, \mathcal{K}) &= [b^8 f^8 e^8 b^8][d^8 \sigma_{-1} g^8 e^8 b^8] \longleftrightarrow [(\mathfrak{J}, b)(\mathfrak{J}, f)(\mathfrak{J}, e)(\mathfrak{J}, b)] \\
&\quad [(\mathfrak{J}, d)(\mathfrak{b}\mathfrak{J}, g)(\mathfrak{J}, e)(\mathfrak{J}, b)] \\
(\omega_5, \mathcal{K}) &= [\sigma_{-1} c^8 \sigma_{-1} g^8 e^8 b^8][\sigma_{-1} b^8 \sigma_{-1} b^8 \sigma_{-1} g^8 e^8] \longleftrightarrow [(\mathfrak{b}\mathfrak{J}, c)(\mathfrak{b}\mathfrak{J}, g)(\mathfrak{J}, e)(\mathfrak{J}, b)] \\
&\quad [(\mathfrak{b}\mathfrak{J}, b)(\mathfrak{b}\mathfrak{J}, b)(\mathfrak{b}\mathfrak{J}, g)(\mathfrak{J}, e)] \\
(\omega_6, \mathcal{K}) &= b^{16} [f^8 \sigma_{-1} c^8] a^{32} \longleftrightarrow (\mathfrak{J}, b)[(\mathfrak{J}, f)(\mathfrak{b}\mathfrak{J}, c)](\mathfrak{J}, a) \\
(\omega_7, \mathcal{K}) &= b^{16} [f^8 \sigma_{-1} c^8] a^{16} f^{16} \longleftrightarrow (\mathfrak{J}, b)[(\mathfrak{J}, f)(\mathfrak{b}\mathfrak{J}, c)](\mathfrak{J}, a)(\mathfrak{J}, f)
\end{aligned} \tag{41}$$

The $\mathfrak{M}$ -reduced Brauer configuration is defined as follows:

- $\mathfrak{M}_0 = \{(\mathfrak{J}, b), (\mathfrak{b}\mathfrak{J}, b), (\mathfrak{b}\mathfrak{J}, c), (\mathfrak{J}, d), (\mathfrak{J}, e), (\mathfrak{b}\mathfrak{J}, f), (\mathfrak{b}\mathfrak{J}, g), (\mathfrak{J}, a), (\mathfrak{J}, a), (\mathfrak{J}, b), (\mathfrak{b}\mathfrak{J}, c), (\mathfrak{J}, f), (\mathfrak{J}, f)\}.$
- $\Gamma_1 = \{(\omega_1, \mathcal{K}), \dots, (\omega_7, \mathcal{K})\}.$
- The successor sequences associated with vertices are defined as follows (if no confusion arises, we use the same notation for copies

of the same polygon):

$$\begin{aligned}
S_{(\mathfrak{J},b)} &= \omega_1 < \omega_1 < \omega_1 < \omega_4 < \omega_4 < \omega_4 < \omega_5, \quad \text{val}((\mathfrak{J},b)) = 7, \\
S_{(\mathfrak{b}\mathfrak{J},b)} &= \omega_5 < \omega_5, \quad \text{val}((\mathfrak{b}\mathfrak{J},b)) = 2, \\
S_{(\mathfrak{b}\mathfrak{J},c)} &= \omega_3 < \omega_5 < \omega_6 < \omega_7, \quad \text{val}((\mathfrak{J},c)) = 4, \\
S_{(\mathfrak{J},d)} &= \omega_1 < \omega_4, \quad \text{val}((\mathfrak{J},d)) = 2, \\
S_{(\mathfrak{J},e)} &= \omega_1 < \omega_1 < \omega_2 < \omega_4 < \omega_4 < \omega_5 < \omega_5, \quad \text{val}((\mathfrak{J},e)) = 7, \\
S_{(\mathfrak{J},f)} &= \omega_1 < \omega_3 < \omega_4 < \omega_6 < \omega_7, \quad \text{val}((\mathfrak{J},f)) = 5, \\
S_{(\mathfrak{b}\mathfrak{J},g)} &= \omega_1 < \omega_2 < \omega_4 < \omega_5 < \omega_5, \quad \text{val}((\mathfrak{b}\mathfrak{J},g)) = 5, \\
S_{(\mathfrak{J},a)} &= \omega_3 < \omega_7, \quad \text{val}((\mathfrak{J},a)) = 2, \\
S_{(\mathfrak{J},a)} &= \omega_6, \quad \text{val}((\mathfrak{J},a)) = 1, \\
S_{(\mathfrak{J},b)} &= \omega_2 < \omega_3 < \omega_6 < \omega_7, \quad \text{val}((\mathfrak{J},b)) = 4, \\
S_{(\mathfrak{b}\mathfrak{J},c)} &= \omega_2, \quad \text{val}((\mathfrak{b}\mathfrak{J},c)) = 1, \\
S_{(\mathfrak{J},f)} &= \omega_2 < \omega_3 < \omega_7, \quad \text{val}((\mathfrak{J},f)) = 3.
\end{aligned} \tag{42}$$

- $\mu((\mathfrak{b}\mathfrak{J},c)) = \mu((\mathfrak{J},a)) = 2$, $\mu(\alpha) = 1$, for the remaining vertices $\alpha \in \Gamma_0$.
- The signature of the key $\mathcal{K}$ is given by the pair $(\mathfrak{J}, \frac{n}{2^m})$, meaning that each polygon ω_i , $1 \leq i \leq 7$ has $\mathfrak{s}_i = n \times 2^{6-m}$ vertices (or its equivalent number).
- $\dim_k \Lambda_{\mathfrak{M}} = 14 + 162 = 176$.
- $\dim_k Z(\Lambda_{\mathfrak{M}}) = 1 + 10 + 4 - 12 + 7 + 12 - 2 = 20$ (note that, there are 2 vertices whose valency equals 1. Furthermore, the Brauer quiver $Q_{\mathfrak{M}}$ has 12 loops and 7 vertices).

Figure 3 shows the labeled Brauer message $M(\mathfrak{M}, \mathcal{K})$ written using the staff notation. Here, the label of the Brauer configuration is given by a signature of the form $\mathcal{K} = (\mathfrak{J}, \frac{2}{2}, \mathfrak{a}^{\mathfrak{M}} = \{\sigma_{-1}(c), \sigma_{-1}(g)\})$, which means that the circular order associated with the vertices is given by the following sequence (43) and that each polygon has two half notes or their equivalents.

$$d < \sigma_{-1}(e) < e < \sigma_{-1}(f) < f < \sigma_{-1}(g) < g < a < \sigma_{-1}(b) < b < \sigma_{-1}(c) < c < d \quad (43)$$



Figure 3: Ciphertext defined by the Brauer configuration (41).

Figure 4 shows the Brauer quiver $Q_{\mathfrak{M}}$ induced by the $\mathfrak{M}$ -reduced Brauer configuration (41). Here $\mathfrak{z}^j$ corresponds with a vertex $\sigma_{-1}z^j$.

The Brauer configuration algebra $\Lambda_{\mathfrak{M}}$ is bounded by an ideal I generated by relations of the following types:

- $C_j^{\mu(j)} - C_i^{\mu(i)}$, if i, j belong to the same polygon. Whereas, C_i and C_j are corresponding special cycles.
- $\alpha_s^{s'} \alpha_t^{t'}$ if $t \neq t'$.
- $(l_s^{s'})^2$, if $l_s^{s'}$ is a loop.
- $C_j^{\mu(j)} f$, if C_j is a special cycle and f is its first arrow.

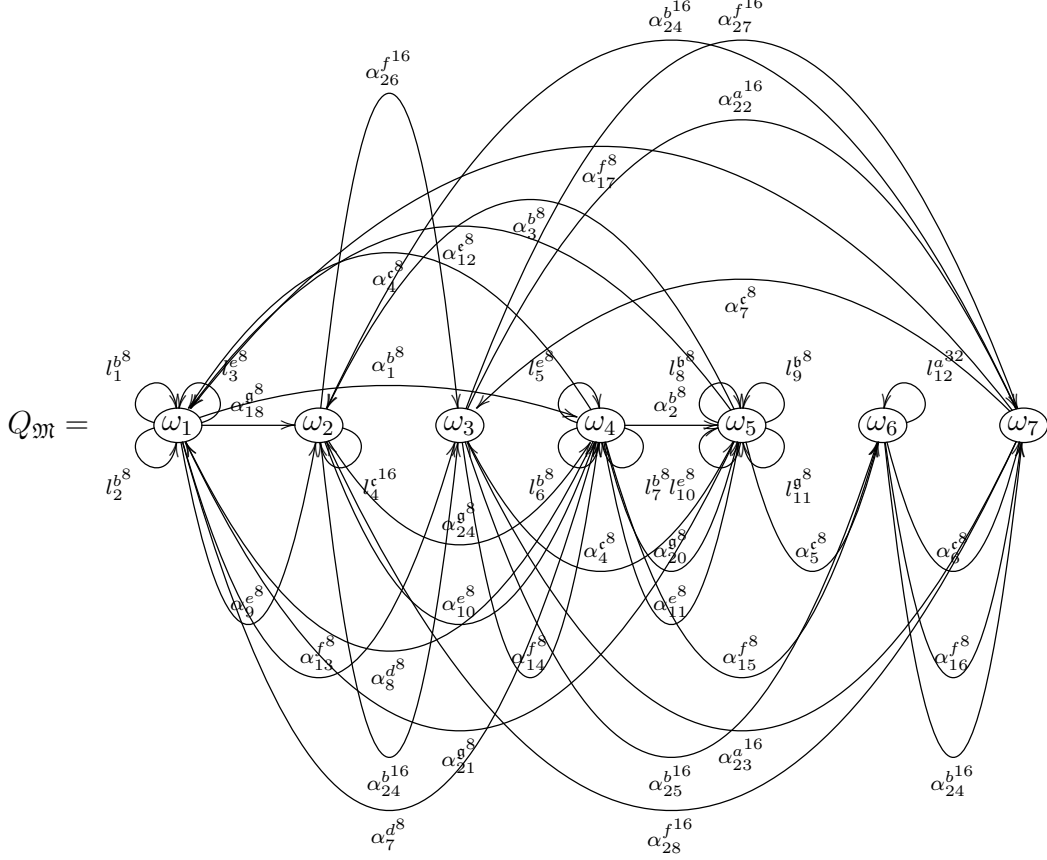


Figure 4: Brauer quiver associated with the $\mathfrak{M}$ -reduced Brauer configuration (41).

3.4 Brauer Analysis of Bach's Canons

This section gives some properties of the Brauer configuration algebras induced by Bach's canons known as canon à 6 Voc, canon à 4 Voc: Perpetuus (BWV 1073), canon 1, à 2 (the crab canon), canon à 4 Quaerendo Invenietis. The musical notes are represented in the Euclidean plane to build some of the most common symbols used by Bach in his manuscripts. In this line, Bach's canons are interpreted as ciphertexts of a transposition cryptosystem whose plaintext consists of such symbols, which give the structure or form of the studied Bach's

canons. Algorithm 1 describes the procedure:

Algorithm 1: This algorithm gives the steps to built a graph induced by the musical notes of Bach's canons.

- Choose a vertex circular order of the set $\{a, b, \dots, g\}$ according to the signature clef. The order associated with a treble, (bass, C) clef starts with the letter e , (d, a , respectively).
 - Segregate the notes into classes according to the equivalence relation $\sim$, such that $(\mathbf{n}, x) \sim (\mathbf{n}', x')$ if and only if $\mathbf{n} = \mathbf{n}'$ and $x = x'$.
 - Associate with the first occurrence of the i th note $\mathbf{n}_i$ a point $(\varepsilon^{i,1}, \varepsilon^{i,2})$ in the Euclidean plane. Where, the first coordinate $\varepsilon^{i,1}$ is a pair $(\mathbf{n}_{i,1}^1, \mathbf{n}_{i,2}^1)$, $\mathbf{n}_{i,1}^1 \in \{\circ, \flat, \natural, \dots\}$, $\mathbf{n}_{i,2}^1 \in \{a, b, c, \dots, g\}$ is given by the appearance order of the note in the musical piece.
 - $\varepsilon^{i,2}$ is an integer number assigned to the vertical coordinate of the note. The clef note has assigned the number $\varepsilon^{1,2} = 0$ and the remaining notes have assigned the number i if the vertices order is $a_0 < a_1 < \dots$, $a_i = \mathbf{n}_{i,2}^2 \in \{a, b, c, \dots, g\}$. It is positive above (below) the clef note $(\varepsilon^{1,1}, \varepsilon^{1,2})$, if it is written in standard (reversed) orientation.
 - Each letter or number is built by connecting consecutive points. If there are repeated notes only the first of them is represented in the diagram. In such a way that points $(\varepsilon^{i,1}, \varepsilon^{i,2})$ define a discrete function. Generally, two consecutive points with the same value $\varepsilon^{i,2}$ are not connected, such a connection is drawn only for aesthetic reasons as well as additional lines can be drawn to represent a symbol containing a cycle (e.g., A, B, α). If necessary, lines of the previous symbol can be used to construct a new one. In particular, vertical lines can be used to represent rests.
-

Figure 5 shows examples of symbols and letters that can be built using Algorithm 1. Bach was used to inverting some of these symbols in his manuscripts (see Figures 3.4 and 6, where Bach's monogram in his famous wax seal is built upon his initials. And a bass symbol is used to write the number 6).

1	l	g
2	s	j
{(21)3}	ω	B
4=4	α	B
5	$\mathcal{S}$	U
7	M	N
0	A	

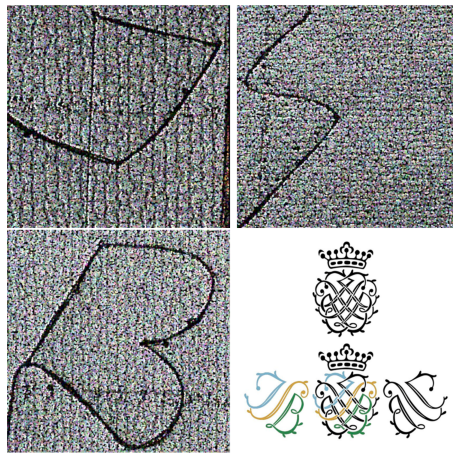
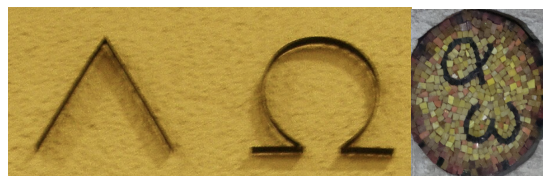


Figure 5: Symbols that are constructed using points and lines. And examples of symbols written or mentioned in Bach's manuscripts. Bach's monogram on his wax seal based on his initials and different versions of the Greek letters α and ω [49, 50].



Bach's canon Triplex â6 Voc is obtained by reducing the Brauer message (44). It allows defining the labeled Brauer configuration $\mathfrak{M}^{A6} = (\mathfrak{M}_0^{A6}, \mathfrak{M}_1^{A6}, \mu, \mathcal{O})$ whose words or polygons (45) are obtained after an appropriate segmentation.

$$c_0^{16} e^{16} c_0^{16} d^{16} c^{16} b^{16} d_0^8 [d^8 e^8 f^8] [g^8 f^8] e^{16} c_0^{16} d^{16} g^{32} f^{16} d^{16} e^{32} f^{32} g^{32} f^{16} d^{16} c_0^{16} c^{16} d^{16} e^{16} f^{16} a^{16} g^{16} f^{16} c^{16} c^{16} d^{16} e^{16}. \quad (44)$$

$$\begin{aligned} (\omega_1, \mathcal{K}) &= c_0^{16} e^{16} c_0^{16} d^{16} \longleftrightarrow \mathfrak{z}(\mathfrak{d}, e) \mathfrak{z}(\mathfrak{d}, d) \\ (\omega_2, \mathcal{K}) &= c^{16} b^{16} d_0^8 [d^8 e^8 f^8] \longleftrightarrow (\mathfrak{d}, c)(\mathfrak{d}, b) \mathfrak{v}[(\mathfrak{d}, d)(\mathfrak{d}, e)(\mathfrak{d}, f)] \\ (\omega_3, \mathcal{K}) &= [g^8 f^8] e^{16} c_0^{16} d^{16} \longleftrightarrow [(\mathfrak{d}, g)(\mathfrak{d}, f)](\mathfrak{d}, e) \mathfrak{z}(\mathfrak{d}, d) \\ (\omega_4, \mathcal{K}) &= g^{32} f^{16} d^{16} \longleftrightarrow (\mathfrak{d}, g)(\mathfrak{d}, f)(\mathfrak{d}, d) \\ (\omega_5, \mathcal{K}) &= e^{32} f^{32} \longleftrightarrow (\mathfrak{d}, e)(\mathfrak{d}, f) \\ (\omega_6, \mathcal{K}) &= g^{32} f^{16} d^{16} \longleftrightarrow (\mathfrak{d}, g)(\mathfrak{d}, f)(\mathfrak{d}, d) \\ (\omega_7, \mathcal{K}) &= c_0^{16} c^{16} d^{16} e^{16} \longleftrightarrow \mathfrak{z}(\mathfrak{d}, c)(\mathfrak{d}, d)(\mathfrak{d}, e) \\ (\omega_8, \mathcal{K}) &= f^{16} a^{16} g^{16} f^{16} \longleftrightarrow (\mathfrak{d}, f)(\mathfrak{d}, a)(\mathfrak{d}, g)(\mathfrak{d}, f) \\ (\omega_9, \mathcal{K}) &= c^{16} c^{16} d^{16} e^{16} \longleftrightarrow (\mathfrak{d}, c)(\mathfrak{d}, c)(\mathfrak{d}, d)(\mathfrak{d}, e) \end{aligned} \quad (45)$$

The successor sequences are given by the following identities:

$$\begin{aligned}
S_{\mathfrak{z}} &= \omega_1 < \omega_1 < \omega_3 < \omega_7, \\
S_{(\mathfrak{d},e)} &= \omega_1 < \omega_3 < \omega_7 < \omega_9, \\
S_{(\mathfrak{d},d)} &= \omega_1 < \omega_3 < \omega_4 < \omega_6 < \omega_7 < \omega_9, \\
S_{(\mathfrak{d},c)} &= \omega_2 < \omega_7 < \omega_9 < \omega_9, \\
S_{(\mathfrak{d},b)} &= \omega_2, \\
S_{\gamma} &= \omega_2, \\
S_{(\mathfrak{d},d)} &= \omega_2, \\
S_{(\mathfrak{d},e)} &= \omega_2, \\
S_{(\mathfrak{d},f)} &= \omega_2 < \omega_3, \\
S_{(\mathfrak{d},g)} &= \omega_3, \\
S_{(\mathfrak{d},g)} &= \omega_4 < \omega_6, \\
S_{(\mathfrak{d},f)} &= \omega_4 < \omega_6 < \omega_8 < \omega_8, \\
S_{(\mathfrak{d},e)} &= \omega_5, \\
S_{(\mathfrak{d},f)} &= \omega_5, \\
S_{(\mathfrak{d},a)} &= \omega_8, \\
S_{(\mathfrak{d},g)} &= \omega_8.
\end{aligned} \tag{46}$$

The following identities give the main properties of the Brauer con-

figuration algebra $\Lambda_{\mathfrak{M}^{A6}}$ induced by the Bach's canon â6 Voc.

$$\begin{aligned}
\mathfrak{M}_0^{A6} &= \{\mathfrak{z}, \gamma, (\mathfrak{d}, a), (\mathfrak{d}, b), (\mathfrak{d}, c), (\mathfrak{d}, d), (\mathfrak{d}, e), (\mathfrak{d}, f), (\mathfrak{d}, g), (\mathfrak{d}, d), (\mathfrak{d}, e), (\mathfrak{d}, f), \\
&\quad (\mathfrak{d}, g), (\mathfrak{d}, e), (\mathfrak{d}, f), (\mathfrak{d}, g)\}, \\
\mathfrak{M}_1^{A6} &= \{\omega_1, \dots, \omega_9\}, \quad (\text{see identities (45)}), \\
\mathcal{K} &= (\mathfrak{G}, \frac{4}{4}, d < c < b < \dots < f < e < d, 4\text{th line}) \\
\{\alpha \in \mathfrak{M}_0^{A6} \mid \text{val}(\alpha) = 1\} &= \{(\mathfrak{d}, b), \gamma, (\mathfrak{d}, d), (\mathfrak{d}, e), (\mathfrak{d}, g), (\mathfrak{d}, e), (\mathfrak{d}, f), (\mathfrak{d}, a), (\mathfrak{d}, g)\}, \\
\{\alpha \in \mathfrak{M}_0^{A6} \mid \text{val}(\alpha) = 2\} &= \{(\mathfrak{d}, f), (\mathfrak{d}, g)\}, \\
\{\alpha \in \mathfrak{M}_0^{A6} \mid \text{val}(\alpha) = 4\} &= \{\mathfrak{z}, (\mathfrak{d}, e), (\mathfrak{d}, c), (\mathfrak{d}, f)\}, \\
\{\alpha \in \mathfrak{M}_0^{A6} \mid \text{val}(\alpha) = 6\} &= \{(\mathfrak{d}, d)\}, \\
|\mathfrak{M}_0^{A6}| &= 16, \quad \text{there are 14 vertices, excluding the rests.} \\
\#Loops \mathcal{Q}_{\mathfrak{M}^{A6}} &= 12, \\
\dim_k \Lambda_{\mathfrak{M}^{A6}} &= 109, \\
\dim_k Z(\Lambda_{\mathfrak{M}^{A6}}) &= 22.
\end{aligned} \tag{47}$$



Figure 6: The reduced Brauer message of the Brauer configuration (47) gives the Bach's canon â6 Voc [51].

The following list gives the 14 points (without rests) induced by canon â6 Voc. Such points are represented in the diagram shown in Figure 7. The initials of Johann Sebastian Bach and the Greek letters alpha and omega can be built up via an appropriate connection of the points.

$$\begin{aligned}
& ((\downarrow, e); \varepsilon^1), ((\downarrow, d); \varepsilon^0), ((\downarrow, c); \varepsilon^{-1}), ((\downarrow, b); \varepsilon^{-2}), ((\downarrow, d); \varepsilon^0), ((\downarrow, e); \varepsilon^1), ((\downarrow, f); \varepsilon^2), \\
& ((\downarrow, g); \varepsilon^3), ((\downarrow, g); \varepsilon^3), ((\downarrow, f); \varepsilon^2), ((\downarrow, e); \varepsilon^1), ((\downarrow, f); \varepsilon^2), ((\downarrow, a); \varepsilon^4), ((\downarrow, g); \varepsilon^3).
\end{aligned}
\tag{48}$$

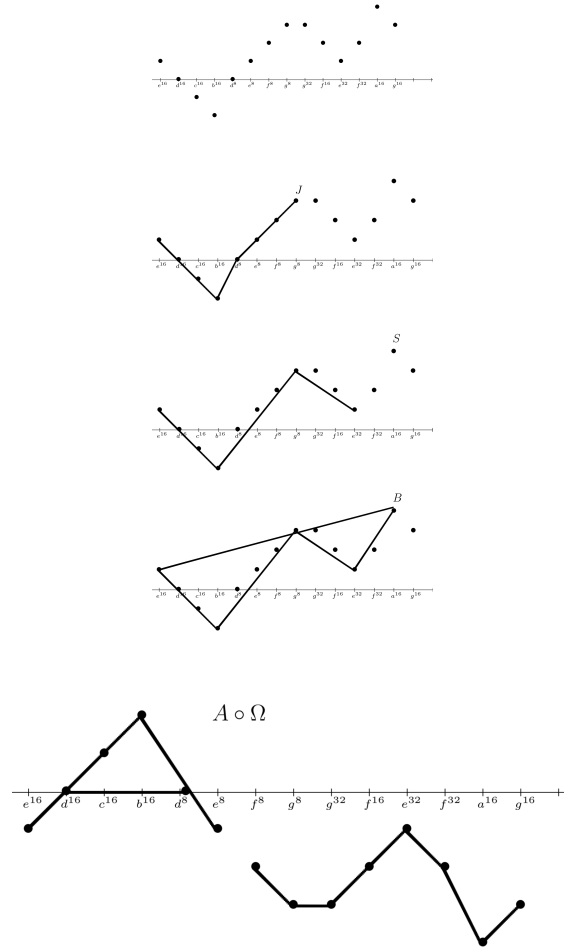


Figure 7: Fourteen vertices are enough to build up Bach's initials. Symbols alpha and omega arise by applying a reflection to these points (see Algorithm 1).

Reductions and segmentations of the Brauer message (49) give rise

to Bach's *Canon 1, a2* shown in Figure 8. Words $\omega_1 - \omega_{18}$ (see identities (50)) define the $\mathfrak{M}$ -reduced Brauer configuration $\mathfrak{M}^{A2}$.

$$\begin{aligned}
& f^{32} \sigma_{-1} d^{32} b^{32} \sigma_{-1} a^{32} \sigma_1 \sigma_{-1} g^{32} c_0^{16} (b^{16} b^{16}) \sigma_{-1} c^{32} (\sigma_1 \sigma_{-1} c^{16} c^{16}) \sigma_1 \sigma_{-1} d^{32} (\sigma_{-1} d^{16} \\
& \sigma_{-1} d^{16}) e^{16} \sigma_{-1} e^{16} f^{16} \sigma_1 \sigma_{-1} g^{16} b^{16} f^{16} c^{16} \sigma_{-1} d^{32} e^{32} f^{32} \sigma_{-1} d^{32} [b^8 c^8 b^8 f^8] [b^8 \sigma_{-1} d^8 e^8 \sigma_{-1} d^8] [c^8 b^8 \\
& \sigma_1 \sigma_{-1} a^8 \sigma_1 \sigma_{-1} g^8] [f^8 \sigma_{-1} d^8 c^8 b^8] [a^8 e^8 \sigma_{-1} d^8 c^8] [b^8 c^8 \sigma_{-1} d^8 e^8] [\sigma_{-1} d^8 c^8 b^8 \sigma_{-1} a^8] [\sigma_{-1} g^8 \sigma_{-1} a^8 b^8 c^8] \\
& [b^8 \sigma_{-1} a^8 \sigma_{-1} g^8 f^8] [\sigma_{-1} e^8 \sigma_{-1} g^8 \sigma_{-1} a^8 b^8] [\sigma_1 \sigma_{-1} a^8 \sigma_1 \sigma_{-1} g^8 f^8 e^8] [\sigma_{-1} d^8 f^8 \sigma_1 \sigma_{-1} g^8 \sigma_1 \sigma_{-1} a^8] \\
& [\sigma_1 \sigma_{-1} g^8 f^8 e^8 \sigma_{-1} d^8] [c^8 e^8 b^8 e^8] [f^8 e^8 \sigma_{-1} d^8 c^8] [\sigma_{-1} d^8 e^8 f^8 \sigma_1 \sigma_{-1} g^8] f^8 b^8 \sigma_{-1} d^8 f^8.
\end{aligned}
\tag{49}$$

$$\begin{aligned}
(\omega_1, \mathcal{K}) &= f^{32} \sigma_{-1} d^{32} \longleftrightarrow (\downarrow, f)(\mathfrak{b}\downarrow, d) \\
(\omega_2, \mathcal{K}) &= b^{32} \sigma_{-1} a^{32} \longleftrightarrow (\downarrow, b)(\mathfrak{b}\downarrow, a) \\
(\omega_3, \mathcal{K}) &= \sigma_1 \sigma_{-1} g^{32} c_0^{16} (b^{16} \longleftrightarrow (\mathfrak{h}\downarrow, g)\mathfrak{z}((\downarrow, b) \\
(\omega_4, \mathcal{K}) &= b^{16} \sigma_{-1} c^{32} (\sigma_1 \sigma_{-1} c^{16} \longleftrightarrow (\downarrow, b))(\mathfrak{b}\downarrow, c)((\mathfrak{h}\downarrow, c) \\
(\omega_5, \mathcal{K}) &= c^{16} \sigma_1 \sigma_{-1} d^{32} (\sigma_{-1} d^{16} \longleftrightarrow (\downarrow, c))(\mathfrak{h}\downarrow, d)((\mathfrak{b}\downarrow, d) \\
(\omega_6, \mathcal{K}) &= \sigma_{-1} d^{16} e^{16} \sigma_{-1} e^{16} f^{16} \longleftrightarrow (\mathfrak{b}\downarrow, d)(\downarrow, e)(\mathfrak{b}\downarrow, e)(\downarrow, f) \\
(\omega_7, \mathcal{K}) &= \sigma_1 \sigma_{-1} g^{16} b^{16} f^{16} c^{16} \longleftrightarrow (\mathfrak{h}\downarrow, g)(\downarrow, b)(\downarrow, f)(\downarrow, c) \\
(\omega_8, \mathcal{K}) &= \sigma_{-1} d^{32} e^{32} \longleftrightarrow (\mathfrak{b}\downarrow, d)(\downarrow, e) \\
(\omega_9, \mathcal{K}) &= f^{32} \sigma_{-1} d^{32} \longleftrightarrow (\downarrow, f)(\mathfrak{b}\downarrow, d) \\
(\omega_{10}, \mathcal{K}) &= [b^8 c^8 b^8 f^8][b^8 \sigma_{-1} d^8 e^8 \sigma_{-1} d^8] \longleftrightarrow [(\downarrow, b)(\downarrow, c)(\downarrow, b)(\downarrow, f)][(\downarrow, b)(\mathfrak{b}\downarrow, d)(\downarrow, e)(\mathfrak{b}\downarrow, d)] \\
(\omega_{11}, \mathcal{K}) &= [c^8 b^8 \sigma_1 \sigma_{-1} a^8 \sigma_1 \sigma_{-1} g^8][f^8 \sigma_{-1} d^8 c^8 b^8] \longleftrightarrow [(\downarrow, c)(\downarrow, b)(\mathfrak{h}\downarrow, a)(\mathfrak{h}\downarrow, g)] \\
&\quad [(\downarrow, f)(\mathfrak{b}\downarrow, d)(\downarrow, c)(\mathfrak{b}\downarrow, b)] \\
(\omega_{12}, \mathcal{K}) &= [a^8 e^8 \sigma_{-1} d^8 c^8][b^8 c^8 \sigma_{-1} d^8 e^8] \longleftrightarrow [(\downarrow, a)(\downarrow, e)(\mathfrak{b}\downarrow, d)(\downarrow, c)] \\
&\quad [(\downarrow, b)(\downarrow, c)(\mathfrak{b}\downarrow, d)(\downarrow, e)] \\
(\omega_{13}, \mathcal{K}) &= [\sigma_{-1} d^8 c^8 b^8 \sigma_{-1} a^8][\sigma_{-1} g^8 \sigma_{-1} a^8 b^8 c^8] \longleftrightarrow [(\mathfrak{b}\downarrow, d)(\downarrow, c)(\downarrow, b)(\mathfrak{b}\downarrow, a)] \\
&\quad [(\mathfrak{b}\downarrow, g)(\mathfrak{b}\downarrow, a)(\downarrow, b)(\downarrow, c)] \\
(\omega_{14}, \mathcal{K}) &= [b^8 \sigma_{-1} a^8 \sigma_{-1} g^8 f^8][\sigma_{-1} e^8 \sigma_{-1} g^8 \sigma_{-1} a^8 b^8] \longleftrightarrow [(\downarrow, b)(\mathfrak{b}\downarrow, a)(\mathfrak{b}\downarrow, g)(\mathfrak{b}\downarrow, g)(\downarrow, f)] \\
&\quad [(\mathfrak{b}\downarrow, e)(\mathfrak{b}\downarrow, g)(\mathfrak{b}\downarrow, a)(\downarrow, b)] \\
(\omega_{15}, \mathcal{K}) &= [\sigma_1 \sigma_{-1} a^8 \sigma_1 \sigma_{-1} g^8 f^8 e^8][\sigma_{-1} d^8 f^8 \sigma_1 \sigma_{-1} g^8 \sigma_1 \sigma_{-1} a^8] \longleftrightarrow [(\mathfrak{h}\downarrow, a)(\mathfrak{h}\downarrow, g)(\downarrow, f)(\downarrow, e)] \\
&\quad [(\mathfrak{b}\downarrow, d)(\downarrow, f)(\mathfrak{h}\downarrow, g)(\mathfrak{h}\downarrow, a)] \\
(\omega_{16}, \mathcal{K}) &= [\sigma_1 \sigma_{-1} g^8 f^8 e^8 \sigma_{-1} d^8][c^8 e^8 b^8 e^8] \longleftrightarrow [(\mathfrak{h}\downarrow, g)(\downarrow, f)(\downarrow, e)(\mathfrak{b}\downarrow, d)] \\
&\quad [(\downarrow, c)(\downarrow, e)(\downarrow, b)(\downarrow, e)] \\
(\omega_{17}, \mathcal{K}) &= [f^8 e^8 \sigma_{-1} d^8 c^8][\sigma_{-1} d^8 e^8 f^8 \sigma_1 \sigma_{-1} g^8] \longleftrightarrow [(\downarrow, f)(\downarrow, e)(\mathfrak{b}\downarrow, d)(\mathfrak{b}\downarrow, c)] \\
&\quad [(\mathfrak{b}\downarrow, d)(\downarrow, e)(\downarrow, f)(\mathfrak{h}\downarrow, g)] \\
(\omega_{18}, \mathcal{K}) &= f^8 b^8 \sigma_{-1} d^8 f^8 \longleftrightarrow (\downarrow, f)(\downarrow, b)(\mathfrak{b}\downarrow, d)(\downarrow, f)
\end{aligned} \tag{50}$$

The following data (51) and (52) give the dimension of the Brauer configuration algebra (and its center) induced by Canon's Bach 1 a2

known as the *crab canon* (see Figure 8).

$$\begin{aligned}
S_{(\flat\flat, a)} &= \omega_1, \\
S_{(\flat, b)} &= \omega_1, \\
S_{(\flat\flat, c)} &= \omega_3, \\
S_{(\flat\flat, d)} &= \omega_1 < \omega_7 < \omega_8, \\
S_{(\flat, e)} &= \omega_7, \\
S_{(\flat\flat, f)} &= \omega_1 < \omega_8, \\
S_{(\flat\flat, f)} &= \omega_1, \\
S_{(\flat, g)} &= \omega_2, \\
S_{\sharp} &= \omega_2, \\
S_{(\flat, b)} &= \omega_2 < \omega_6, \\
S_{(\flat\flat, d)} &= \omega_4, \\
S_{(\flat, e)} &= \omega_5, \\
S_{(\flat\flat, e)} &= \omega_5, \\
S_{(\flat, f)} &= \omega_5 < \omega_6, \\
S_{(\flat, g)} &= \omega_6, \\
S_{(\flat, a)} &= \omega_{10} < \omega_{11} < \omega_{14} < \omega_{14} < \omega_{16}, \\
S_{(\flat, b)} &= \omega_9 < \omega_9 < \omega_9 < \omega_{10} < \omega_{11} < \omega_{12} < \omega_{12} < \omega_{13} < \omega_{13} < \omega_{15} < \omega_{17}, \\
S_{(\flat, c)} &= \omega_9 < \omega_{10} < \omega_{10} < \omega_{11} < \omega_{11} < \omega_{12} < \omega_{12} < \omega_{15} < \omega_{16}, \\
S_{(\flat, e)} &= \omega_9 < \omega_{11} < \omega_{11} < \omega_{14} < \omega_{15} < \omega_{15} < \omega_{15} < \omega_{16} < \omega_{16}, \\
S_{(\flat, f)} &= \omega_9 < \omega_{13} < \omega_{14} < \omega_{14} < \omega_{15} < \omega_{16} < \omega_{16} < \omega_{17} < \omega_{17}, \\
S_{(\flat, g)} &= \omega_{10} < \omega_{11} < \omega_{14} < \omega_{14} < \omega_{15}, \\
S_{(\flat\flat, a)} &= \omega_{12} < \omega_{12} < \omega_{13} < \omega_{13}, \\
S_{(\flat\flat, d)} &= \omega_9 < \omega_9 < \omega_{10} < \omega_{11} < \omega_{11} < \omega_{12} < \omega_{14} < \omega_{15} < \omega_{16} < \omega_{16} < \omega_{17}, \\
S_{(\flat\flat, e)} &= \omega_{13}, \\
S_{(\flat\flat, g)} &= \omega_{12} < \omega_{13} < \omega_{13}.
\end{aligned} \tag{51}$$

$$\begin{aligned}
\mathfrak{M}_0^{A2} &= \{(\flat\flat, a), (\flat, b), (\flat\flat, c), (\flat\flat, d), (\flat, d), (\flat, e), (\flat, f), (\flat, g), \sharp, (\flat, b), \\
&\quad (\flat\flat, d), (\flat, e), (\flat\flat, e), (\flat, f), (\flat, g), (\sharp, a), (\sharp, b), (\sharp, c), (\sharp, e), (\sharp, f), \\
&\quad (\sharp, g), (\flat\sharp, a), (\flat\sharp, d), (\flat\sharp, e), (\flat\sharp, g)\}, \\
\mathfrak{M}_1^{A2} &= \{\omega_1, \dots, \omega_{13}\}, \\
\mathcal{K} &= (\mathfrak{G}; d < e < f < \dots < c < d, 4\text{th line}), \quad \text{labels polygons in } \mathfrak{M}^{A2}, \\
&\quad \omega_1 < \omega_2 < \dots < \omega_{13} \quad \text{for successor sequences,} \\
\dim_k \Lambda_{\mathfrak{M}^{A2}} &= 582, \\
|\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 1\}| &= 12, \\
|\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 2\}| &= 3, \\
|\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 3\}| &= 2, \\
|\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 4\}| &= 1, \\
|\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 5\}| &= 2, \\
|\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 9\}| &= 2, \\
|\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 11\}| &= 3, \\
\# \text{Loops}(Q_{\mathfrak{M}^{A2}}) &= 32, \\
\dim_k Z(\Lambda_{\mathfrak{M}^{A2}}) &= 46.
\end{aligned} \tag{52}$$



Figure 8: Brauer message of the Brauer configuration (52) gives Bach's canon 1 â2 [52].

$$\begin{aligned}
&((\flat, f), \varepsilon^2), ((\flat\flat, d), \varepsilon^0), ((\flat, b), \varepsilon^{-2}), ((\flat\flat, a), \varepsilon^{-3}), ((\sharp\flat, g), \varepsilon^3), \sharp, ((\flat, b), \varepsilon^{-2}), \\
&((\sharp\flat, c), \varepsilon^{-1}), ((\sharp\flat, c), \varepsilon^{-1}), ((\sharp\flat, d), \varepsilon^0), ((\flat\flat, d), \varepsilon^0), ((\flat, e), \varepsilon^1), ((\flat\flat, e), \varepsilon^1), ((\flat, f), \varepsilon^2), \\
&((\sharp\flat, g), \varepsilon^3), ((\flat, e), \varepsilon^1), ((\sharp, b), \varepsilon^{-2}), ((\sharp, c), \varepsilon^{-1}), ((\sharp, f), \varepsilon^{-5}), ((\flat\sharp, d), \varepsilon^0), ((\sharp, e), \varepsilon^1), \\
&((\sharp\sharp, a), \varepsilon^{-3}), ((\sharp\sharp, g), \varepsilon^{-4}), ((\flat\sharp, a), \varepsilon^{-3}), ((\flat\sharp, g), \varepsilon^{-4}), ((\flat\sharp, e), \varepsilon^{-7}).
\end{aligned} \tag{53}$$

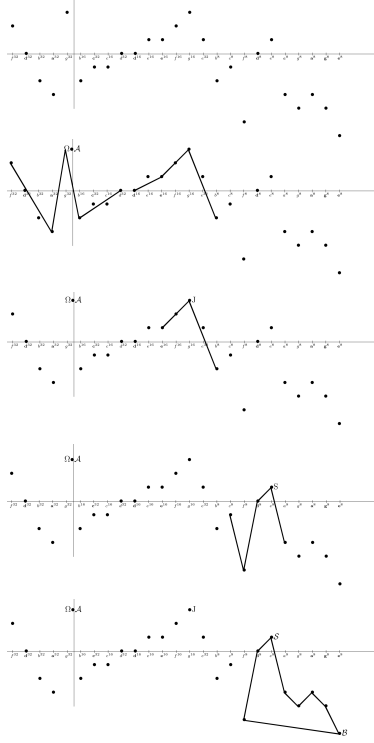


Figure 9: Letters, W, A, J,S , and B as they arise by connecting consecutive points defined by Bach's canon 1 à 2 (see Algorithm 1).

Canon's Bach a4 *Quaerendo Invenietis* is given by the $\mathfrak{M}$ -reduced Brauer message of the Brauer configuration $\mathfrak{M}^{QI} = (\mathfrak{M}_0^{QI}, \mathfrak{M}_1^{QI}, \mu, \mathcal{O})$ defined by words (54) which were obtained after appropriate segmentations of the Brauer message (58).

$$\begin{aligned}
\omega_1 &= [e^8 f^8] [\sigma_{-1} g^8 a^8 b^8 \sigma_{-1} c^8] \longleftrightarrow [(\mathfrak{J}, e)(\mathfrak{J}, f)][(\mathfrak{b}\mathfrak{J}, g)(\mathfrak{J}, a)(\mathfrak{J}, b)(\mathfrak{b}\mathfrak{J}, c)] \\
\omega_2 &= \sigma_1 d^{16} c_0^{16} c_0^{16} (b^{16} \longleftrightarrow (\# \mathfrak{J}, d) \mathfrak{J} \mathfrak{J} ((\mathfrak{J}, b) \\
\omega_3 &= [b^8] \sigma_1 a^8 f^8 \sigma_1 \sigma_{-1} g^8] (\sigma_{-1} \sigma_1 a^{32} \longleftrightarrow [(\mathfrak{J}, b)(\# \mathfrak{J}, a)(\mathfrak{J}, f)(\mathfrak{J}\mathfrak{J}, g)](\mathfrak{J}\mathfrak{J}, a) \\
\omega_4 &= [a^8] \sigma_1 \sigma_{-1} g^8 e^8 f^8] (\sigma_{-1} g^{32} \longleftrightarrow [(\mathfrak{J}, a)(\# \mathfrak{J}, g)(\mathfrak{J}, e)(\mathfrak{J}, f)](\mathfrak{b}\mathfrak{J}, g) \\
\omega_5 &= [(\sigma_{-1} g^8) f^8 \sigma_1 e^8 f^8] [(\sigma_{-1} f^8 e^8 \sigma_1 d^8 e^8)] \longleftrightarrow [((\mathfrak{b}\mathfrak{J}, g))(\mathfrak{J}, f)(\# \mathfrak{J}, e)(\mathfrak{J}, f))] \\
&\quad [((\mathfrak{b}\mathfrak{J}, f)(\mathfrak{J}, e)(\mathfrak{J}, d)(\# \mathfrak{J}, g)(\mathfrak{J}, e))] \\
\omega_6 &= [(\sigma_1 d^8 \sigma_1 \sigma_{-1} c^8 b^8 \sigma_{-1} c^8)] [(b^8 \sigma_1 d^8 f^8 a^8)] \longleftrightarrow [((\# \mathfrak{J}, d)(\mathfrak{J}\mathfrak{J}, c)(\mathfrak{J}, b)(\mathfrak{b}\mathfrak{J}, c))] \\
&\quad [((\mathfrak{J}, b)(\# \mathfrak{J}, d)(\mathfrak{J}, f)(\mathfrak{J}, a))] \\
\omega_7 &= [(\sigma_{-1} g^8 b^8 \sigma_1 d^8 e^8)] [f^8 \sigma_{-1} c^8 b^8 a^8] \longleftrightarrow [((\mathfrak{b}\mathfrak{J}, g)(\mathfrak{J}, b)(\# \mathfrak{J}, d)(\mathfrak{J}, e))] \\
&\quad [(\mathfrak{J}, f)(\mathfrak{b}\mathfrak{J}, c)(\mathfrak{J}, b)(\mathfrak{J}, a)] \\
\omega_8 &= [\sigma_{-1} g^4 f^4 e^4 \sigma_1 d^4] [e^4 e^4 \sigma_1 d^4 \sigma_{-1} c^4] [b^4 a^4 \sigma_{-1} g^4 f^4] e^{16} \longleftrightarrow [(\mathfrak{b}\mathfrak{J}, g)(\mathfrak{J}, f)(\mathfrak{J}, e)(\# \mathfrak{J}, d)] \\
&\quad [(\mathfrak{J}, e)(\mathfrak{J}, e)(\# \mathfrak{J}, d)(\mathfrak{b}\mathfrak{J}, c)][(\mathfrak{J}, b)(\mathfrak{J}, a)(\mathfrak{b}\mathfrak{J}, g)(\mathfrak{J}, f)](\mathfrak{J}, e) \\
\omega_9 &= d_0^8 [f^8 \sigma_{-1} g^8 a^8] [b^8 d^8 \sigma_1 \sigma_{-1} c^8 e^8] \longleftrightarrow \mathfrak{J}[(\mathfrak{J}, f)(\mathfrak{b}\mathfrak{J}, g)(\mathfrak{J}, a)] \\
&\quad [(\mathfrak{J}, b)(\mathfrak{J}, d)(\mathfrak{J}\mathfrak{J}, c)(\mathfrak{J}, e)] \\
\omega_{10} &= [d^8 \sigma_1 \sigma_{-1} c^4 b^4] \sigma_1 a^{16} d_0^8 [\sigma_{-1} c^8 b^8 d^8] \longleftrightarrow [(\mathfrak{J}, d)(\mathfrak{J}\mathfrak{J}, c)(\mathfrak{J}, b)](\# \mathfrak{J}, a) \gamma \\
&\quad [(\mathfrak{b}\mathfrak{J}, c)(\mathfrak{J}, b)(\mathfrak{J}, d)] \\
\omega_{11} &= [\sigma_{-1} c^8 b^4 a^4] \sigma_1 \sigma_{-1} g^{16} d_0^8 [b^8 \sigma_1 a^8 \sigma_1 \sigma_{-1} c^8] \longleftrightarrow [(\mathfrak{b}\mathfrak{J}, c)(\mathfrak{J}, b)(\mathfrak{J}, a)](\mathfrak{J}\mathfrak{J}, g) \gamma \\
&\quad [(\mathfrak{J}, b)(\# \mathfrak{J}, a)(\mathfrak{J}\mathfrak{J}, c)] \\
\omega_{12} &= [b^8 \sigma_1 \sigma_{-1} a^8 \sigma_1 \sigma_{-1} g^8 b^8] [a^8 \sigma_1 \sigma_{-1} g^8] (a^{16} \longleftrightarrow [(\mathfrak{J}, b)(\mathfrak{J}\mathfrak{J}, a)(\mathfrak{J}\mathfrak{J}, g)(\mathfrak{J}, b)] \\
&\quad [(\mathfrak{J}, a)(\mathfrak{J}\mathfrak{J}, g)]((\mathfrak{J}, a) \\
\omega_{13} &= [a^8] e^8 \sigma_1 d^8 e^8 [f^8 b^8] (b^{16} \longleftrightarrow [(\mathfrak{J}, a)(\mathfrak{J}, e)(\# \mathfrak{J}, d)(\mathfrak{J}, e)][(\mathfrak{J}, f)(\mathfrak{J}, b)]((\mathfrak{J}, b)
\end{aligned}$$

(54)

$$\begin{aligned}
\omega_{14} &= b^{16}[a^8\sigma_{-1}g^8]a^{16}[\sigma_{-1}g^8f^8] \longleftrightarrow (\downarrow, b)[(\downarrow, a)(\flat\downarrow, g)](\downarrow, a)[(\flat\downarrow, g)(\downarrow, f)] \\
\omega_{15} &= [\sigma_{-1}g^4a^4\sigma_{-1}g^4f^4](e^{16}[e^8]f^8\sigma_{-1}g^8a^8) \longleftrightarrow [(\flat\downarrow, g)(\downarrow, a)(\flat\downarrow, g)(\downarrow, f)]((\downarrow, e) \\
&\quad [(\downarrow, e)(\downarrow, f)(\flat\downarrow, g)(\downarrow, a)]) \\
\omega_{16} &= [b^8\sigma_{-1}c^8b^8a^8][\sigma_{-1}g^8f^8e^8\sigma_{-1}g^8] \longleftrightarrow [(\downarrow, b)(\flat\downarrow, c)(\downarrow, b)(\downarrow, a)] \\
&\quad [(\flat\downarrow, g)(\downarrow, f)(\downarrow, e)(\flat\downarrow, g)] \\
\omega_{17} &= (f^{32}[f^8]e^8\sigma_1d^8f^8) \longleftrightarrow ((\downarrow, f)[(\downarrow, f)](\downarrow, e)(\sharp\downarrow, d)(\downarrow, f)) \\
\omega_{18} &= (e^{32}[e^8]d^8\sigma_1\sigma_{-1}c^8e^8) \longleftrightarrow ((\downarrow, e)[(\downarrow, e)](\downarrow, d)(\sharp\downarrow, c)(\downarrow, e)) \\
\omega_{19} &= d^{16}d_0^8d^8a^{16}d_0^8\sigma_{-1}c^8 \longleftrightarrow (\downarrow, d)\gamma(\downarrow, d)(\downarrow, a)\gamma(\flat\downarrow, c) \\
\omega_{20} &= b^{16}d_0^8e^8\sigma_1d^8d_0^8b^8 \longleftrightarrow (\downarrow, b)\gamma(\downarrow, e)(\sharp\downarrow, d)\gamma(\downarrow, b) \\
\omega_{21} &= e^{16}c^{16}a^{16}b^{16} \longleftrightarrow (\downarrow, e)(\downarrow, c)(\downarrow, a)(\downarrow, b) \\
\omega_{22} &= [e^8e^4f^4]\varphi_8b^{16}[a^4\sigma_{-1}g^4] \longleftrightarrow [(\downarrow, e)(\downarrow, e)(\downarrow, f)](\downarrow, b)[(\downarrow, a)(\flat\downarrow, g)] \\
\omega_{23} &= [f^8\sigma_1d^8e^8f^8]b^{16}c_0^{16} \longleftrightarrow [(\downarrow, f)(\sharp\downarrow, d)(\downarrow, e)(\downarrow, f)](\downarrow, b)\sharp \\
\omega_{24} &= d_0^8[\sigma_1\sigma_{-1}c^8\sigma_1\sigma_{-1}d^8e^8]f^{32} \longleftrightarrow \gamma[(\sharp\downarrow, c)(\sharp\downarrow, d)(\downarrow, e)](\downarrow, f) \\
\omega_{25} &= d_0^8[b^8\sigma_1\sigma_{-1}c^8\sigma_1d^8]e^{32} \longleftrightarrow \gamma[(\downarrow, b)(\sharp\downarrow, c)(\sharp\downarrow, d)](\downarrow, e) \\
\omega_{26} &= c_0^{16}b^{16}\sigma_{-1}c^{16}f^{16} \longleftrightarrow \sharp(\downarrow, b)(\flat\downarrow, c)(\downarrow, f) \\
\omega_{27} &= [f^4\sigma_{-1}g^4]a^{16}\sigma_{-1}g^8[a^8f^8]\sigma_1d^{16} \longleftrightarrow [(\downarrow, f)(\flat\downarrow, g)](\downarrow, a)(\flat\downarrow, g) \\
&\quad [(\downarrow, a)(\downarrow, f)](\sharp\downarrow, d) \\
\omega_{28} &= e^{16}d_0^8\sigma_{-1}g^8\sigma_{-1}c^8d_0^8\sigma_1d^8 \longleftrightarrow (\downarrow, e)\gamma(\flat\downarrow, g)(\flat\downarrow, c)\gamma(\sharp\downarrow, d)
\end{aligned} \tag{55}$$

$$\begin{aligned}
S_{(\mathfrak{A},e)} &= \omega_1 < \omega_4 < \omega_5 < \omega_5 < \omega_7 < \omega_9 < \omega_{13} < \omega_{13} < \omega_{15} < \omega_{16} < \omega_{17} < \\
&\omega_{18} < \omega_{18} < \omega_{20} < \omega_{22} < \omega_{23} < \omega_{24}, \quad val((\mathfrak{A},e)) = 17. \\
S_{(\mathfrak{A},f)} &= \omega_1 < \omega_3 < \omega_4 < \omega_5 < \omega_5 < \omega_6 < \omega_7 < \omega_9 < \omega_{13} < \omega_{14} < \omega_{15} \\
&\omega_{16} < \omega_{17} < \omega_{17}, \quad val((\mathfrak{A},f)) = 14. \\
S_{(\mathfrak{B},g)} &= \omega_1 < \omega_5 < \omega_7 < \omega_9 < \omega_{13} < \omega_{14} < \omega_{14} < \omega_{15} < \omega_{16} < \omega_{16} < \\
&\omega_{22} < \omega_{27} < \omega_{28}, \quad val((\mathfrak{A},e)) = 13. \\
S_{(\mathfrak{A},a)} &= \omega_1 < \omega_4 < \omega_6 < \omega_7 < \omega_9 < \omega_{12} < \omega_{12} < \omega_{13} < \omega_{14} < \omega_{15} < \omega_{16} < \\
&\omega_{22} < \omega_{27}, \quad val((\mathfrak{A},a)) = 13. \\
S_{(\mathfrak{A},b)} &= \omega_1 < \omega_3 < \omega_6 < \omega_6 < \omega_7 < \omega_7 < \omega_9 < \omega_{10} < \omega_{11} < \omega_{12} < \omega_{12} \\
&< \omega_{13} < \omega_{16} < \omega_{16} < \omega_{20} < \omega_{25}, \quad val((\mathfrak{A},b)) = 16. \\
S_{(\mathfrak{B},c)} &= \omega_1 < \omega_5 < \omega_6 < \omega_7 < \omega_{11} < \omega_{16} < \omega_{19}, \quad val((\mathfrak{B},c)) = 8. \\
S_{(\sharp\mathfrak{A},d)} &= \omega_2 < \omega_{20} < \omega_{27}, \quad val((\sharp\mathfrak{A},d)) = 3. \\
S_{\mathfrak{Z}} &= \omega_2 < \omega_2 < \omega_{23} < \omega_{26}, \quad val(\mathfrak{Z}) = 4. \\
S_{(\mathfrak{A},b)} &= \omega_2 < \omega_{13} < \omega_{14} < \omega_{20} < \omega_{21} < \omega_{23} < \omega_{26}, \quad val((\mathfrak{A},b)) = 7. \\
S_{(\sharp\mathfrak{A},a)} &= \omega_3, \quad val((\sharp\mathfrak{A},d)) = 1. \\
S_{(\sharp\mathfrak{A},g)} &= \omega_3 < \omega_4 < \omega_{12} < \omega_{12}, \quad val((\sharp\mathfrak{A},g)) = 4. \\
S_{(\mathfrak{A},a)} &= \omega_3, \quad val((\mathfrak{A},a)) = 1. \\
S_{(\mathfrak{B},g)} &= \omega_4, \quad val((\mathfrak{B},g)) = 1. \\
S_{(\sharp\mathfrak{A},e)} &= \omega_5, \quad val((\sharp\mathfrak{A},e)) = 1. \\
S_{(\mathfrak{B},f)} &= \omega_5, \quad val((\mathfrak{B},f)) = 1. \\
S_{(\sharp\mathfrak{A},d)} &= \omega_5 < \omega_6 < \omega_6 < \omega_7 < \omega_{13} < \omega_{17} < \omega_{23} < \omega_{25} < \omega_{28}, \quad val((\sharp\mathfrak{A},d)) = 9.
\end{aligned}$$

(56)

$$\begin{aligned}
S_{(\mathfrak{A},c)} &= \omega_6 < \omega_9 < \omega_{11} < \omega_{18} < \omega_{24} < \omega_{25}, \quad \text{val}((\mathfrak{A},c)) = 6. \\
S_{(\mathfrak{b}\mathfrak{A},g)} &= \omega_8 < \omega_8 < \omega_{15} < \omega_{15} < \omega_{22} < \omega_{27}, \quad \text{val}((\mathfrak{b}\mathfrak{A},g)) = 6. \\
S_{(\mathfrak{A},f)} &= \omega_8 < \omega_8 < \omega_{15} < \omega_{22} < \omega_{27}, \quad \text{val}((\mathfrak{b}\mathfrak{A},g)) = 5. \\
S_{(\mathfrak{A},e)} &= \omega_8 < \omega_8 < \omega_8 < \omega_{22}, \quad \text{val}((\mathfrak{b}\mathfrak{A},g)) = 4. \\
S_{(\mathfrak{A}\mathfrak{A},d)} &= \omega_8 < \omega_8, \quad \text{val}((\mathfrak{A}\mathfrak{A},d)) = 2. \\
S_{(\mathfrak{b}\mathfrak{A},c)} &= \omega_8, \quad \text{val}((\mathfrak{b}\mathfrak{A},d)) = 1. \\
S_{(\mathfrak{A},b)} &= \omega_8 < \omega_{10} < \omega_{11}, \quad \text{val}((\mathfrak{A},b)) = 3. \\
S_{(\mathfrak{A},a)} &= \omega_8 < \omega_{11} < \omega_{15} < \omega_{22}, \quad \text{val}((\mathfrak{A},a)) = 4. \\
S_{(\mathfrak{A},e)} &= \omega_8 < \omega_{15} < \omega_{21} < \omega_{28}, \quad \text{val}((\mathfrak{A},b)) = 4. \\
S_{\gamma} &= \omega_9 < \omega_{10} < \omega_{11} < \omega_{19} < \omega_{19} < \omega_{20} < \omega_{20} < \omega_{24} < \omega_{25} < \\
&\omega_{28} < \omega_{28}, \quad \text{val}(\gamma) = 11. \\
S_{(\mathfrak{A},d)} &= \omega_9 < \omega_{10} < \omega_{10} < \omega_{18} < \omega_{19} < \omega_{24}, \quad \text{val}((\mathfrak{A},c)) = 6. \\
S_{(\mathfrak{A},c)} &= \omega_{10}, \quad \text{val}((\mathfrak{A},c)) = 1. \\
S_{(\mathfrak{A}\mathfrak{A},a)} &= \omega_{10}, \quad \text{val}((\mathfrak{A}\mathfrak{A},a)) = 1. \\
S_{(\mathfrak{A},g)} &= \omega_{11}, \quad \text{val}((\mathfrak{A},g)) = 1. \\
S_{(\mathfrak{A}\mathfrak{A},a)} &= \omega_{11}, \quad \text{val}((\mathfrak{A}\mathfrak{A},a)) = 1. \\
S_{(\mathfrak{A},a)} &= \omega_{12} < \omega_{14} < \omega_{19} < \omega_{21} < \omega_{27}, \quad \text{val}((\mathfrak{A},a)) = 5. \\
S_{(\mathfrak{A},f)} &= \omega_{17} < \omega_{24}, \quad \text{val}((\mathfrak{A},f)) = 2. \\
S_{(\mathfrak{A},e)} &= \omega_{18} < \omega_{25}, \quad \text{val}((\mathfrak{A},e)) = 2. \\
S_{(\mathfrak{A},d)} &= \omega_{19}, \quad \text{val}((\mathfrak{A},d)) = 1. \\
S_{(\mathfrak{A}\mathfrak{A},c)} &= \omega_{21} < \omega_{28}, \quad \text{val}((\mathfrak{A}\mathfrak{A},c)) = 2. \\
S_{(\mathfrak{A},b)} &= \omega_{22}, \quad \text{val}((\mathfrak{A},b)) = 1. \\
S_{(\mathfrak{A},f)} &= \omega_{26}, \quad \text{val}((\mathfrak{A},f)) = 1.
\end{aligned}$$

(57)

The following Brauer message (58) gives rise to Bach's canon Quaerendo Invenietis.

$$\begin{aligned}
& [e^8 f^8][\sigma_{-1}g^8 a^8 b^8 \sigma_{-1}c^8]\sigma_1 d^{16} c_0^{16} c_0^{16} (b^{16}[b^8]\sigma_1 a^8 f^8 \sigma_1 \sigma_{-1}g^8)(\sigma_{-1}\sigma_1 a^{32} \\
& [a^8]\sigma_1 \sigma_{-1}g^8 e^8 f^8)(\sigma_{-1}g^{32}[(\sigma_{-1}g^8)f^8 \sigma_1 e^8 f^8)][(\sigma_{-1}f^8 e^8 \sigma_1 d^8 e^8)][(\sigma_1 d^8 \sigma_1 \sigma_{-1}c^8 b^8 \sigma_{-1}c^8)] \\
& [(b^8 \sigma_1 d^8 f^8 a^8)[(\sigma_{-1}g^8 b^8 \sigma_1 d^8 e^8)][f^8 \sigma_{-1}c^8 b^8 a^8][\sigma_{-1}g^4 f^4 e^4 \sigma_1 d^4][e^4 e^4 \sigma_1 d^4 \sigma_{-1}c^4] \\
& [b^4 a^4 \sigma_{-1}g^4 f^4]e^{16} d_0^8 [f^8 \sigma_{-1}g^8 a^8][b^8 d^8 \sigma_1 \sigma_{-1}c^8 e^8][d^8 \sigma_1 \sigma_{-1}c^4 b^4]\sigma_1 a^{16} d_0^8 [\sigma_{-1}c^8 b^8 d^8] \\
& [\sigma_{-1}c^8 b^4 a^4]\sigma_1 \sigma_{-1}g^{16} d_0^8 [b^8 \sigma_1 a^8 \sigma_1 \sigma_{-1}c^8][b^8 \sigma_1 \sigma_{-1}a^8 \sigma_1 \sigma_{-1}g^8 b^8][a^8 \sigma_1 \sigma_{-1}g^8](a^{16} \\
& [a^8]e^8 \sigma_1 d^8 e^8)[f^8 b^8](b^{16} b^{16})[a^8 \sigma_{-1}g^8]a^{16}[\sigma_{-1}g^8 f^8][\sigma_{-1}g^4 a^4 \sigma_{-1}g^4 f^4](e^{16}[e^8]f^8 \\
& \sigma_{-1}g^8 a^8)[b^8 \sigma_{-1}c^8 b^8 a^8][\sigma_{-1}g^8 f^8 e^8 \sigma_{-1}g^8](f^{32}[f^8]e^8 \sigma_1 d^8 f^8)(e^{32}[e^8]d^8 \sigma_1 \sigma_{-1}c^8 e^8) \\
& d^{16} d_0^8 a^{16} d_0^8 \sigma_{-1}c^8 b^{16} d_0^8 e^8 \sigma_1 d^8 d_0^8 b^8 e^{16} c^{16} a^{16} b^{16} [e^8 e^4 f^4] \varphi_8 b^{16} [a^4 \sigma_{-1}g^4] \\
& [f^8 \sigma_1 d^8 e^8 f^8] b^{16} c_0^{16} d_0^8 [\sigma_1 \sigma_{-1}c^8 \sigma_1 \sigma_{-1}d^8 e^8] f^{32} d_0^8 [b^8 \sigma_1 \sigma_{-1}c^8 \sigma_1 d^8] e^{32} c_0^{16} b^{16} \sigma_{-1}c^{16} f^{16} \\
& [f^4 \sigma_{-1}g^4] a^{16} \sigma_{-1}g^8 [a^8 f^8] \sigma_1 d^{16} e^{16} d_0^8 \sigma_{-1}g^8 \sigma_{-1}c^8 d_0^8 \sigma_1 d^8.
\end{aligned} \tag{58}$$

Note that,

$$\begin{aligned}
\mathfrak{M}_0^{QI} &= \mathfrak{M}_0^{QI,4} \cup \mathfrak{M}_0^{QI,8} \cup \mathfrak{M}_0^{QI,16} \cup \mathfrak{M}_0^{QI,32} \cup \mathfrak{M}_0^{QI,R}, \\
\mathfrak{M}_0^{QI,4} &= \{(\mathfrak{A}, a), (\mathfrak{A}, c), (\mathfrak{A}, d), (\mathfrak{A}, f), (\mathfrak{A}, g), (\# \mathfrak{A}, b), (\flat \mathfrak{A}, e)\}, \\
\mathfrak{M}_0^{QI,8} &= \{(\mathfrak{A}, a), (\mathfrak{A}, b), (\mathfrak{A}, c), (\mathfrak{A}, d), (\mathfrak{A}, e), (\mathfrak{A}, f), (\mathfrak{A}, g), (\flat \mathfrak{A}, a), (\# \mathfrak{A}, b), \\
& (\# \mathfrak{A}, c), (\flat \mathfrak{A}, d), (\flat \mathfrak{A}, e), (\# \mathfrak{A}, f), (\flat \mathfrak{A}, f)\}, \\
\mathfrak{M}_0^{QI,16} &= \{(\mathfrak{A}, a), (\mathfrak{A}, b), (\mathfrak{A}, c), (\mathfrak{A}, d), (\mathfrak{A}, e), (\mathfrak{A}, f), (\mathfrak{A}, g), \\
& (\flat \mathfrak{A}, a), (\# \mathfrak{A}, b), (\# \mathfrak{A}, f), (\mathfrak{A}, g)\}, \\
\mathfrak{M}_0^{QI,32} &= \{(\mathfrak{A}, c), (\mathfrak{A}, d), (\mathfrak{A}, e), (\mathfrak{A}, f)\}, \\
\mathfrak{M}_0^{QI,R} &= \{\gamma, \mathfrak{z}\}, \\
\mathfrak{M}_1^{QI} &= \{\omega_1, \dots, \omega_{28}\} \quad (\text{see, identities (54)}), \\
\mathcal{K} &= (\mathfrak{A}, e < f < \dots < d < e, \text{1st line}), \text{ labels polygons in } \mathfrak{M}^{QI},
\end{aligned} \tag{59}$$

$$\begin{aligned}
& |\{\alpha \in \mathfrak{M}_0^{QI} \mid \text{val}(\alpha) = 1\}| = 13 \\
& |\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 2\}| = 4, \\
& |\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 3\}| = 2, \\
& |\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 4\}| = 5, \\
& |\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 5\}| = 2, \\
& |\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 6\}| = 3, \\
& |\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 7\}| = 1, \\
& |\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 8\}| = 1, \\
& |\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 9\}| = 1, \\
& |\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 11\}| = 1, \\
& |\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 13\}| = 2, \\
& |\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 14\}| = 1, \\
& |\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 16\}| = 1, \\
& |\{\alpha \in \mathfrak{M}_0^{A2} \mid \text{val}(\alpha) = 17\}| = 1, \\
& \# \text{Loops } Q_{\mathfrak{M}^{QI}} = 38, \\
& \dim_k \Lambda_{\mathfrak{M}^{QI}} = 1565, \\
& \dim_k Z(\Lambda_{\mathfrak{M}^{QI}}) = 67.
\end{aligned} \tag{60}$$

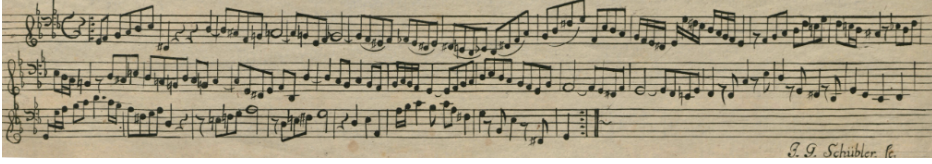


Figure 10: Brauer message (58) gives rise to Bach's canon â4 Quaerendo Invenietis.

The following points defined by canon â4 Quaerendo Invenietis are represented in Figure 11. If such points are connected then it is possible to drawn the letters J, S, and B and the letters A and W (see Figure 3.4). The scheme allows built numbers 1,2,3, and 8 in Figure 12.

$$\begin{aligned}
& ((\flat, e), \varepsilon^0), ((\flat, f), \varepsilon^1), ((\flat\flat, g), \varepsilon^2), ((\flat, a), \varepsilon^3), ((\flat, b), \varepsilon^4), ((\flat\flat, c), \varepsilon^5), ((\sharp\flat, d), \varepsilon^{-1}), \sharp \\
& ((\sharp\flat, b), \varepsilon^4), ((\sharp\flat, a), \varepsilon^3), ((\sharp\flat, g), \varepsilon^2), ((\flat, a), \varepsilon^3), ((\flat\flat, g), \varepsilon^2), ((\sharp\flat, e), \varepsilon^0), ((\flat\flat, f), \varepsilon^1), \\
& ((\sharp\flat, d), \varepsilon^{-1}), ((\flat\flat, g), \varepsilon^2), ((\flat, f), \varepsilon^1), ((\flat, e), \varepsilon^0), ((\sharp\flat, d), \varepsilon^{-1}), ((\flat\flat, c), \varepsilon^5), ((\flat, b), \varepsilon^4), \\
& ((\flat, a), \varepsilon^3), ((\flat, e), \varepsilon^0), \gamma, ((\flat, d), \varepsilon^6), ((\sharp\flat, c), \varepsilon^5), ((\sharp\flat, c), \varepsilon^5), ((\sharp\flat, a), \varepsilon^3), ((\sharp\flat, g), \varepsilon^2), \\
& ((\flat, a), \varepsilon^3), ((\flat, f), \varepsilon^1), ((\flat, e), \varepsilon^0), ((\flat, d), \varepsilon^{-1}), ((\flat\flat, c), \varepsilon^{-2}), ((\flat, b), \varepsilon^{-3}), ((\flat, b), \varepsilon^{11}), \\
& ((\flat, f), \varepsilon^1).
\end{aligned}
\tag{61}$$

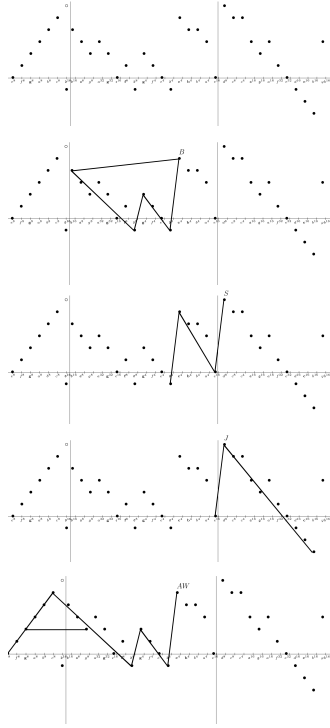


Figure 11: Letters J, S, B, A and W also arise from points defined by canon
 â4 Quaerendo Invenietis (see Algorithm 1).

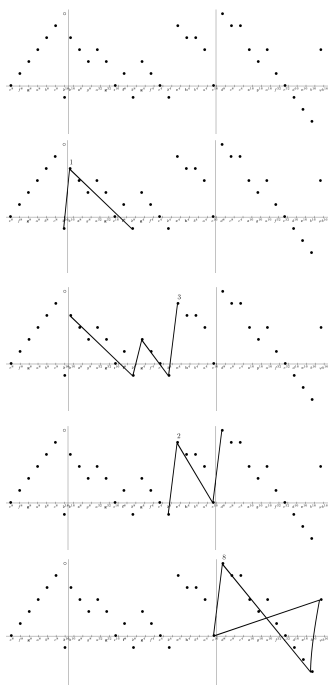


Figure 12: Numbers, 1,3,2, and 8 can be built up via canon â4 Quaerendo Invenietis.

4 Concluding Remarks and Future Work

Brauer configuration algebras are a theoretical framework to investigate block cyphers. In particular, Western musical writing can be analyzed via Brauer configuration algebras. Such analysis allows for determining relationships between notes and measures in a musical piece by assuming that these are ciphertexts of classical cryptosystems whose plaintexts are defined by appropriated Brauer configurations. Due to these procedures, a Brauer analysis can be applied to some of the canons proposed by Bach in his Musical Offering. Musical notes in these canons have a structure or form based on some of the commonly used Bach's symbols.

Future Work

This work applies Brauer's analysis to some of Bach's canons. Analyzing the remaining Bach canons in his Musical Offering is another

task to be developed in the future. Proving, in particular, that the structure or form of such canons is also based on Bach's symbols.

References

- [1] Green, E.L.; Schroll, S. Brauer configuration algebras: A generalization of Brauer graph algebras. *Bull. Sci. Math.* **2017**, *121*, 539–572.
- [2] Schroll, S. Brauer Graph Algebras. In *Homological Methods, Representation Theory, and Cluster Algebras, CRM Short Courses*; Assem I., Trepode S., Eds.; Springer: Cham, Switzerland, 2018. 177–223.
- [3] Stanley, R.P. Enumerative Combinatorics. Cambridge University Press, Cambridge, UK, 1999; Volume 2.
- [4] Andrews, G.E. The Theory of Partitions. Cambridge University Press, Cambridge, UK, 2010.
- [5] Cañadas, A.M.; Gaviria, I.D.M.; Vega, J.D.C. Relationships between the Chicken McNugget Problem, Mutations of Brauer Configuration Algebras and the Advanced Encryption Standard. *Mathematics* **2021**, *9*, 1937.
- [6] Angarita, M.A.O; Cañadas, A.M.; Fúneme, C.C. Mendez, O.M.; Serna, R.J. Cayley Hash Values of Brauer Messages and Some of Their Applications in the Solutions of Systems of Differential Equations. *Computation* **2022**, *10* (9), 1–31.
- [7] Rasmussen, M. The Musical Offering: A Musical Pedagogical Workshop by J.S. Bach, or The Musical Geometry of Bach's Puzzle Canons.
Available online: [https://schillerinstitut.dk/moweb/musical offering.htm](https://schillerinstitut.dk/moweb/musical%20offering.htm) (accessed on 25 September 2023).
- [8] Hofstadter, D.R. Gödel, Escher, Bach: an Eternal Golden Braid, 20th anniversary ed. Basic Books, New York, USA, 1999.
- [9] Tatlow, R. Bach and the Riddle of the Number Alphabet. Cambridge University Press, New York, USA, 2000.
- [10] Milka, A. Rethinking J.S. Bach's Musical Offering (Translated from Russian by Marina Ritzarev). Cambridge Scholar Publishing, Newcastle upon Tyne, UK, 2019.

- [11] Christoph, W. The Bach canon at Harvard and its dedicatee: a riddle finally solved. *Harvard Library Bulletin* **2014**, *24*(3), 104-109.
- [12] Shafer, J. The two-part and three-part inventions of Bach: A Mathematical Analysis. Honors Project. East Texas Baptist University School of Fine Arts Department of Music, 2010.
- [13] Wissner, R.A. First mathematics then Music: J. S. Bach, Glenn Gould, and the evolutionary supergenius in the outer limits' "the sixth finger". *Bach* **2019**, *50*(1), 76–92.
- [14] Sylvestre, L.; Costa, M. The mathematical architecture of Bach's The Art of Fugue. *Il Saggiatore Musicale*. **2010**, *17*(2), 175–195.
- [15] Collins, D.; Schloss, W. A. M. An unusual effect in the canon per tonos from J.S. Bach musical offering. *Music Perception* **2001**, *19*(2), 141–154.
- [16] Collins, D. Musical terminology in the canonical works of Bach: An historical context. *Bach* **2012**, *26*(1), 91–101.
- [17] De Coul, T.O. The augmentation in J.S. Bach's Musicalishes Opfer. *Bach* **2006**, *37*(1), 50–77.
- [18] Butler, G. J.S. Bach's "Hudeman" canon BWV 1074: A note engraving and printing history. *Bach* **1994**, *25*(1), 5–10.
- [19] Greer, M. Masonic Allusions in the dedications of two canons by J.S. Bach: BWV 1078 and 1075. *Bach* **2012**, *43*(2), 1–45.
- [20] Barber, E. Bach and the B-A-C-H motive. *Bach* **1971**, *2*(2), 3–5.
- [21] Cañadas, A.M.; Ballester-Bolinches, A.; Gaviria, I.D.M. Solutions of the Yang-Baxter equation arising from Brauer configuration algebras. *Computation* **2022**, *11*, 1–17.
- [22] Cañadas, A.M.; Espinosa, P.F.F; Ballester-Bolinches, A. Solutions of the Yang-Baxter equation and automaticity related to Kronecker modules. *Computation* **2023**, *11*(3), 1-17.
- [23] Cañadas, A.M.; Angarita, M.A.O. Brauer configuration algebras for multimedia based cryptography and security applications. *Multimed. Tools Appl.* **2021**, *80*, 23485–23510.
- [24] Angarita, M.A.O. Human Interaction Proofs Based on Emerging and Multistable Images: A Practical Application of the Theory of Representation of Algebras. Ph.D. Thesis, Universidad Nacional de Colombia, BTA, Colombia, 2019.

- [25] Agudelo, N.; Cañadas, A.M.; Gaviria, I.D.M.; Espinosa, P.F.F. $\{0, 1\}$ -Brauer configuration algebras and their applications in the graph energy theory. *Mathematics* **2021**, *9*, 1–18.
- [26] Cañadas, A.M.; Espinosa, P.F.F.; Agudelo, N.; . Brauer configuration algebras defined by snake graphs and Kronecker modules. *ERA* **2022**, *30* (8), 3087-3110.
- [27] Cañadas, A.M.; Espinosa, P.F.F.; Rios, G.B. Wargaming with quadratic forms and Brauer configuration algebras. *Mathematics* **2022**, *10*, 729.
- [28] Stinson, D.; Paterson, M. *Cryptography: Theory and Practice*, 4th ed.; Chapman and Hall/CRC Press: Boca Raton, FL, USA, 2019.
- [29] Espinosa, P.F.F. *Categorification of Some Integer Sequences and Its Applications*. Ph.D. Thesis, Universidad Nacional de Colombia, BTA, Colombia, 2021.
- [30] Rios, G.B. *Dynkin Functions and Its Applications*. Ph.D. Thesis, Universidad Nacional de Colombia, BTA, Colombia, 2020.
- [31] Cañadas, A.M.; Gaviria, I.D.M.; Rios, G.B.; Espinosa, P.F.F. Coxeter’s frieze patterns arising from Dyck Paths. *Ricerche de Matematica* **2023**, *72*, 867-889.
- [32] Sierra, A. The dimension of the center of a Brauer configuration algebra. *J. Algebra* **2018**, *510*, 289–318.
- [33] Cañadas, A.M.; Rios, G.B. Dyck paths categories and its relationships with cluster algebras. *Journal of Algebra and Its Applications* **2021**, *23*(1).
- [34] Tillich, J.P.; Zémor, G. Hash functions and graphs with large girths. In *Advances in Cryptology-EUROCRYPT’91*; Springer: Berlin/Heidelberg, Germany, 1991; Volume 547, pp. 508-511.
- [35] Sosnovski, B. *Cayley Graphs of Semigroups and Applications to Hashing*. Ph.D. Thesis, City University of New York, New York, USA, 2016.
- [36] Rump, W. Modules over braces. *Algebra Discret. Math* **2006**, *2*, 127-137.
- [37] Tatlow, R. *Bach’s numbers: compositional and significance*. Cambridge University Press, New York, USA, 2016.

- [38] Madden, C. *Fractals in Music: Introductory Mathematics for Musical Analysis*, 2nd Ed. High Art Press, Salt Lake City, USA, 2007.
- [39] Hsu, K.; Hsu, J.A. Fractal geometry of music. *Proc. National Academy of Sciences of the United States of America* **1990**, *87*(3), 938–941.
- [40] Niitsuma, M.; Tomita, Y. Classifying Bach’s handwritten C-clefs, Proceedings: 12th ISMIR **2011**.
- [41] Franklin, D.O. Reading Bach’s notation. *Bach* **2017**, *48*(1), 63–80.
- [42] Wollny, P. Observations on the autograph of the B-minor mass. *Bach* **2016**, *47*(2), 27–46.
- [43] Hachohen, R. Exploring the limits: the tonal, the gestural, and the allegorical in Bach’s Musical Offering. *Understanding Bach* **2006**, *1*, 19–38.
- [44] Currie, R.N.A neglected guide to Bach’s use of number symbolism-Part I. *Bach* **1974**, *5*(1), 23–32.
- [45] Hernandez-Olivan, C; Llamas, S.R.; Beltran, J.R. Symbolic Music Structure Analysis with Graph Representations and Change-point Detection Methods. *ArXiv* 2303. 13881. 2023.
- [46] Szeto, W.M.; Wong, M.H. A graph-theoretical approach for pattern matching in post-tonal music analysis. *Journal of New Music Research* **2006**, *35*(4), 307–321.
- [47] Jeong, D.; Taegyun, K; Yoojin, K; Juhan, N. Graph Neural Network for Music Score Data and Modeling Expressive Piano Performance. In *Proceedings of the 36th International Conference on Machine Learning*. **2019**, *97*(2), 3060–3070.
- [48] Costa, da F.L. An introduction to multisets. *ArXiv/abs/2110.12902*. 2021.
- [49] Monogram of Johann Sebastian Bach. Available online: [https://commons.wikimedia.org/wiki/Category: Monogram of Johann Sebastian Bach](https://commons.wikimedia.org/wiki/Category:Monogram_of_Johann_Sebastian_Bach). File:Bach Seal.svg (accessed on 13 July 2023).
- [50] Alpha and Omega. Available online: [https://commons.wikimedia.org/wiki/Category:Alpha Omega](https://commons.wikimedia.org/wiki/Category:Alpha_Omega) (accessed on 13 July 2023).

- [51] Bach, J.S. Canon BWV 1076.jpg. Canon triplex à 6 Voc.
Available online:
[https://commons.wikimedia.org/wiki/File:Canon BWV 1076.jpg](https://commons.wikimedia.org/wiki/File:Canon_BWV_1076.jpg)
(accessed on 10 August 2023).
- [52] Bach, J.S. Canon à 2. Available online:
<https://vmirror.imslp.org/files/imglnks/usimg/0/06/IMSLP341226-PMLP04550-bach8.pdf>
(accessed on 10 August 2023).
- [53] Bach, J.S. Canon à 4 Quaerendo Invenietis. Available online:
<https://vmirror.imslp.org/files/imglnks/usimg/1/1b/IMSLP341241-PMLP04550-bach9.pdf>
(accessed on 16 August 2023).