Treball final de màster

MÀSTER DE
MATEMÀTICA AVANÇADA

Facultat de Matemàtiques
Universitat de Barcelona

On the Minimality of GT-systems

Autor: Martí Salat Moltó

Directora:	**Dra. Rosa María Miró-Roig**
Realitzat a:	**Departament de Matemàtiques i Informàtica**

Barcelona,	**June 27, 2018**

Abstract

In this work we address the minimality problem of GT-systems in three variables introduced in [8]. To study this problem, we consider an $N \times N$ generic sparse circulant matrix M with only three non-zero entries per row: x_0, x_a and x_b. We consider $d_{(N;0,a,b)}$ (resp. $p_{(N;0,a,b)}$) the number of non-zero coefficients in the expansion of the determinant (resp. the permanent) of M. The minimality of a GT-system is translated to the equality between $d_{(N;0,a,b)}$ and $p_{(N;0,a,b)}$ with $\gcd(a,b,N) = 1$. We prove that this equality holds in some open cases giving rise to new minimality results.

Keywords. *Circulant matrix, minimal GT-system, permanent, weak Lefschetz property.*

Contents

Introduction

From the late 19th century, mathematicians have brought interest in the study of circulant matrices and their determinant. Namely, a circulant $N \times N$ matrix is any matrix M of type

$$M = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{N-1} \\ a_1 & a_2 & a_3 & \cdots & a_0 \\ a_2 & a_3 & a_4 & \cdots & a_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{N-1} & a_0 & a_1 & \cdots & a_{N-2} \end{pmatrix} = \mathrm{Circ}(a_0, \ldots, a_{N-1}).$$

Circulant matrices appear in very different areas of mathematics, such as signal processing, statistics or graph theory. In particular, to compute the determinant of a circulant matrix is a longstanding problem. It was treated by Catalan, Sylvester or later by Ore in [14]. When we consider the coefficients $a_0, \ldots, a_{N-1}$ to be variables rather than elements of a field k, we are considering a symbolic circulant matrix. To be clearer, in this case we write $x_0, \ldots, x_{N-1}$ instead of $a_0, \ldots, a_{N-1}$. Although it has been addressed from different perspectives, it remains an open problem to find a computable enclosed formula for the coefficients of a symbolic circulant matrix determinant. Moreover, it is not known a characterization for the non-zero coefficients among them. We will contribute to this open problem in the first chapter of this work.

On the other hand, for any matrix M we can associate its permanent $\mathrm{per}(M)$. The computation of $\mathrm{per}(M)$ is a hard problem. Actually, Valiant in [17] proved that the computation of the permanent of a binary matrix is a $\#P-$problem. However, in the case of circulant matrices, Brualdi and Newman proved in [1] that the solutions of the system

$$\left.\begin{array}{rcl} \alpha_0 + \alpha_1 + \cdots + \alpha_{N-1} & = & N \\ \alpha_1 + 2\alpha_2 + \cdots + (N-1)\alpha_{N-1} & \equiv & 0 \pmod{N} \end{array}\right\}$$

give exactly the terms $a_0^{\alpha_0} \cdots a_{N-1}^{\alpha_{N-1}}$ with non-zero coefficient in the expansion of the permanent of the $N \times N$ symbolic circulant matrix. Moreover, if a term $a_0^{\alpha_0} \cdots a_{N-1}^{\alpha_{N-1}}$ has non-zero coefficient in the expansion of the determinant $\det(\mathrm{Circ}(a_0, \ldots, a_{N-1}))$, then it must satisfy also this congruence. The reciprocal, however, is not always true. Therefore, a question arise: when does this reciprocal hold? As soon as all a_i are different from zero, Thomas conjectured in [16] that this reciprocal only holds when N is a prime or a power of a prime. We will devote Section 1.2 to prove this conjecture. If we consider some $a_i = 0$, then the conjecture of Thomas is not true anymore. In Section 1.3, we study the non-zero coefficients of the expansion of $\det(\mathrm{Circ}(a_0, \ldots, a_{N-1}))$ with some $a_i = 0$. In particular we pay attention to the case in which all but three a_i are zero and the circulant matrix is largely sparse. In this sense, Theorem 1.3.9 will give the maximum generality we have at the moment to solve this open problem.

As it has been mentioned above, circulant matrices are in relation with many different problems. In [8] it was introduced a surprising relation between the problem of characterizing the non-zero elements of a generic circulant matrix and the minimality of some *Togliatti systems*. Roughly speaking, a Togliatti system is an artinian ideal $I \subset k[x_0, \ldots, x_n]$ generated by forms of the same degree d such that for a general linear form L, the multiplication-by-L map $\times L : [R/I]_{d-1} \to [R/I]_d$ fails to be injective (that is, I fails the so-called weak Lefschetz property in degree $d-1$). Togliatti systems were introduced by Mezzetti, Miró-Roig and Ottaviani in [10] and they have been studied and partially classified in [11], [9], [13] and [8]. Precisely in the latter reference the authors introduced the notion of *GT-system*: a Togliatti system $I = (F_1, \dots, F_r)$ such that the associated morphism $\varphi_I : \mathbb{P}^n \to \mathbb{P}^r$ (given by the r forms of degree d generating I) is a Galois covering of its image. When classifying GT-systems it is important to take account of its minimality (that is, I do not contain a *sub*-GT-system). One particular case of GT-systems consists of ideals $I_{(a,b,c)}$ in $k[x,y,z]$ generated by monomials of degree d invariant with respect to the action of the matrix $\begin{pmatrix} e^a & 0 & 0 \\ 0 & e^b & 0 \\ 0 & 0 & e^c \end{pmatrix}$, where e is a primitive dth root of unity. It is remarkable that the minimality of these GT-systems is tightly related to the problem of finding the non-zero coefficients of a generic circulant matrix determinant (see Remark 2.1.11). In [8], the authors proved that for d a prime or a power of a prime and $1 \leq b < c \leq d-1$, the GT-system $I_{(0,b,c)}$ is minimal, provided that $\gcd(b,c,d) = 1$. Moreover, they conjectured that for d not necessarily a prime $I_{(0,b,c)}$ is also minimal. In the second chapter we will develop these ideas, and we will partially prove this conjecture.

The work is organized as follows. In the first chapter we introduce the definition of a circulant and the ways to express its determinant. On the other hand, we study the permanent of this type of matrices. This leads us to introduce the problem of compare the coefficients of the determinant and those of the permanent. In particular, it motivates the results of Thomas in [16] and his conjecture. The following section is devoted entirely to prove the conjecture of Thomas. At this point, the next section introduces the problem to specialize a generic circulant. In this section we also give the Example 1.3.2 to show how the analog of Thomas' conjecture does not hold anymore. However, Proposition 1.3.3 and Example 1.3.4 and multiple computations made with Mathematica, motivates posing Conjecture 1.3.5. The rest of the section is devoted to study and give some partial answers to this conjecture. Finally, in the last section of the first chapter, we are interested in showing the connection between the circulant matrix determinant problem and the some special resultants of polynomials.

The second chapter starts introducing the Lefschetz properties as well as Togliatti systems as were introduced in [10]. Then, we introduce the notion of a GT-system and state some properties. In the following section, the important Remark 2.1.11 shows up the connection between the contents of Section 1.3 and the minimality problem of GT-systems. The goal of the rest of this section is providing partial answers and shed light to the conjecture of Mezzetti and Miró-Roig in [8].

Part of the results in Chapter 1 have been published in [2].

Notation: Let us fix the notation we will use in the sequel. k will denote an algebraically closed field of characteristic zero and $R = k[x_0, \dots, x_n]$ will be the polynomial ring in n variables with coefficients in k. We consider R with its standard graduation

$R = \bigoplus_{i \in \mathbb{Z}} R_i$ where R_i is the $k-$vector space of all homogeneous polynomials in R of degree i. For a homogeneous ideal $I \subset R$ we mean an ideal such that each of its generators belongs to some component R_i in the graduation. Given a homogeneous ideal $I \in R$, we consider also the graduation on $R/I = \bigoplus_{i \in \mathbb{Z}} [R/I]_i$ induced by the graduation on R. Finally, we denote the sth projective space over k by $\mathbb{P}^s$. We say that a homogeneous ideal $I = (F_1, \ldots, F_r) \subset R$ is artinian if the zero locus of $\{F_1, \ldots, F_r\}$ is $Z(I) = \{p \in \mathbb{P}^n : F_i(p) = 0, i = 1, \ldots, r\} = \emptyset$.

Acknowledgements

Però no us penseu que sempre serà així!

I would like to thank my advisor. No tinc paraules suficients per agrair-li els ànims que sempre m'ha donat i la seva dedicació.

Voglio inoltre ringraziare a la Dott.ssa Emilia Mezzetti per le discussioni avute per Skype ed a Barcelona. In speciale per le lezioni particolari su Geometria nel corso di la sua stanza qui.

Finalment, pel seu suport, a la meva família Salat-Moltó y Gómez.

To L.

Chapter 1

Circulant matrices

This chapter is devoted to the study of circulant matrices. In the first section, we define and illustrate what a circulant matrix is, and next we state some known basic properties. As previously studied along the last century and in the last few decades, we are interested in knowing how the coefficients of a determinant or a permanent of a circulant matrix behave. Actually, this will be a very important issue to address since it is related to some problems on an *a priori* unrelated areas such as commutative algebra and geometry. In particular, the study presented in this chapter will enable us to give a complete answer to a conjecture posed by Thomas in [16] and, give a partial answer to a conjecture recently posed by Mezzetti and Miró-Roig in [8].

1.1 Definitions and basic properties

In this section, we start giving a description of a circulant matrix and we will motivate the object of study: its determinant and its permanent. Previously studied by Ore in [14], Kra and Siamanca in [5] or Wyn-Jones in [19], we mainly follow [7]. The results on this section are totally necessary to give a positive answer to the Thomas' conjecture in Section 1.2.

Definition 1.1.1: Let $M = (a_{ij})$ be an $N \times N$ matrix. M is a **circulant matrix** if, and only if $a_{ij} = a_{kl}$ whenever $j - i \equiv k - l \mod N$. That is, M is of the type

$$\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{N-1} \\ a_{N-1} & a_0 & a_1 & \cdots & a_{N-2} \\ a_{N-2} & a_{N-1} & a_0 & \cdots & a_{N-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}$$

where successive rows are circular permutations of the first row. It is a particular form of a Toeplitz matrix, i.e. a matrix whose elements are constant along the diagonals. For shortness we will denote such matrices as $\text{Circ}(a_0\, a_1 \ldots a_{N-1})$.

Circulant matrices have been studied in the last decades and they have been related to many different areas in mathematics such as digital signal processing, image compression, physics, engineering simulations, number theory or cryptography. It is a longstanding problem in algebra to find a closed formula for the coefficients of the determinant (resp. the permanent) of a circulant matrix. In the remaining part of this section we will review some known facts and properties about the determinant and the permanent of circulant matrices and we will study the behaviour of the coefficients of its determinant and compare them to those of its permanent. First of all, let us recall some definitions and fix some notation.

Definition 1.1.2: Let $M = (a_{ij})$ be an $N \times N$ matrix. Then its **determinant** and its **permanent** are, respectively:

$$\begin{aligned} \det(M) &= \sum_{\sigma\in\Sigma_N} (-1)^{\epsilon(\sigma)} a_{0\sigma(0)} \cdots a_{(N-1)\sigma(N-1)} \\ \operatorname{per}(M) &= \sum_{\sigma\in\Sigma_N} a_{0\sigma(0)} \cdots a_{(N-1)\sigma(N-1)} \end{aligned}$$

where Σ_N is the symmetric group of N elements and $\epsilon(\sigma)$ is the signature of the permutation σ.

Remark 1.1.3: Let us take a generic circulant matrix $\operatorname{Circ}(x_0\, x_1 \dots x_{N-1})$ whose entries are precisely the variables of the polynomial ring $k[x_0, \dots, x_{N-1}]$. Its N eigenvalues are $x_0 + \omega^j x_1 + \cdots + \omega^{(N-1)j} x_{N-1}$ where $\omega = e^{\frac{2\pi i}{N}}$ and $0 \leq j \leq N-1$. We can use the expression of its eigenvalues to write its determinant

$$\det\left(\operatorname{Circ}(x_0\, x_1 \dots x_{N-1})\right) = \sum_{j=0}^{N-1} (x_0 + \omega^j x_1 + \cdots + \omega^{(N-1)j} x_{N-1})$$

and also we can develop and rearrange the alternate sum of the determinant formula and give two other equivalent expressions

$$\begin{aligned} \det\left(\operatorname{Circ}(x_0\, x_1 \dots x_{N-1})\right) &= \sum_{0\leq a_0 \leq \cdots \leq a_{N-1} \leq N-1} C_{a_0,\dots,a_{N-1}} x_{a_0} \cdots x_{a_{N-1}} \\ &= \sum_{\substack{0\leq M_0,\dots,M_{N-1}\leq N \\ M_0+\cdots+M_{N-1}=N}} C^{\star}_{M_0\cdots M_{N-1}} x_0^{M_0} \cdots x_{N-1}^{M_{N-1}}. \end{aligned}$$

We notice also that we can write in the analogous way the permanent of a circulant matrix. It is immediate to see that if a coefficient $C_{a_0\cdots a_{N-1}}$ does not appear in the permanent, then the correspondent coefficient of the determinant does not appear too. However, by the alternancy nature of the determinant, a coefficient appearing in the permanent may vanish in the determinant.

In the following example we compute explicitly the determinant and the permanent of a generic circulant matrix with $N = 3,\ 4,\ 5$ and 6. In the first three cases there are no non-zero coefficient of the permanent vanishing in the determinant while in the latter case there are several non-zero coefficients of the permanent vanishing in the determinant.

Example 1.1.4:

$$\begin{aligned}
&\det(Circ(x,y,z)) = x^3 + y^3 + z^3 - 3xyz\\
&\operatorname{per}(Circ(x,y,z)) = x^3 + y^3 + z^3 + 3xyz
\end{aligned}$$

$$\begin{aligned}
&\det(Circ(x,y,z,t)) = x^4 - y^4 + z^4 - t^4 - 2x^2z^2 + 2y^2t^2 - 4x^2yt + 4xy^2z - 4yz^2t + 4xzt^2\\
&\operatorname{per}(Circ(x,y,z,t)) = x^4 + y^4 + z^4 + t^4 + 2x^2z^2 + 2y^2t^2 + 4x^2yt + 4xy^2z + 4yz^2t + 4xzt^2
\end{aligned}$$

$$\begin{aligned}
&\det(Circ(x,y,z,t,u)) = x^5 + y^5 + z^5 + t^5 + u^5 - 5x^3yu - 5x^3zt - 5xy^3z - 5y^3tu - 5xz^3u\\
&\quad -5yz^3t - 5xyt^3 - 5zy^3u - 5xtu^3 - 5yzu^3 + 5x^2y^2t + 5x^2yz^2 + 5x^2zu^2\\
&\quad +5x^2t^2u + 5xy^2u^2 + 5xz^2t^2 + 5y^2z^2u + 5y^2tu^2 + 5yt^2u^2 + 5z^2tu^2 - 5xyztu\\
&\operatorname{per}(Circ(x,y,z,t,u)) = x^5 + y^5 + z^5 + t^5 + u^5 + 5tu^3x + 5t^2ux^2 + 5t^2u^2y + 5t^3xy + 5ux^3y\\
&\quad +5u^2xy^2 + 5tx^2y^2 + 5tuy^3 + 5t^3uz + 5u^2x^2z + 5tx^3z + 5u^3yz + 15tuxyz\\
&\quad +5t^2y^2z + 5xy^3z + 5tu^2z^2 + 5t^2xz^2 + 5x^2yz^2 + 5uy^2z^2 + 5uxz^3 + 5tyz^3
\end{aligned}$$

$$\begin{aligned}
&\det(Circ(x,y,z,t,u,v)) = x^6 - y^6 + z^6 - t^6 + u^6 - v^6 + 6t^4uz + 6t^4vy + 3t^4x^2 - 6t^3u^2y-\\
&\quad 12t^3uvx - 2t^3v^3 - 6t^3vz^2 - 12t^3xyz - 2t^3y^3 + 6t^2u^3x + 9t^2u^2v^2 - 9t^2u^2z^2+\\
&\quad 18t^2uxy^2 + 18t^2v^2xz - 9t^2v^2y^2 - 3t^2x^4 + 6t^2xz^3+\\
&\quad 9t^2y^2z^2 - 6tu^4v + 12tu^3yz - 18tu^2x^2y - 12tuv^3z+\\
&\quad 12tuvx^3 + 12tuvz^3 - 12tuy^3z + 6tv^4y - 6tv^3x^2-\\
&\quad 18tvx^2z^2 + 6tvy^4 - 6tx^2y^3 + 12tx^3yz - 6tyz^4-\\
&\quad 6u^4xz - 3u^4y^2 + 6u^3v^2z + 12u^3vxy + 2u^3x^3 + 2u^3z^3 - 6u^2v^3y - 9u^2v^2x^2-\\
&\quad 18u^2vyz^2 + 9u^2x^2z^2 + 3u^2y^4 + 6uv^4x + 18uv^2y^2z-\\
&\quad 12uvxy^3 - 6ux^4z + 6ux^3y^2 - 6uxz^4 + 6uy^2z^3 + 3v^4z^2-\\
&\quad 12v^3xyz - 2v^3y^3 + 6v^2x^3z + 9v^2x^2y^2 - 3v^2z^4 - 6vx^4y + 12vxyz^3 - 6vy^3z^2+\\
&\quad 2x^3z^3 - 9x^2y^2z^2 + 6xy^4z\\
&\operatorname{per}(Circ(x,y,z,t,u,v)) = x^6 + y^6 + z^6 + t^6 + u^6 + v^6 + 6t^4uz + 6t^4vy + 3t^4x^2 + 6t^3u^2y+\\
&\quad 12t^3uvx + 2t^3v^3 + 6t^3vz^2 + 12t^3xyz + 2t^3y^3 + 6t^2u^3x + 9t^2u^2v^2 + 9t^2u^2z^2 + 24t^2uvyz+\\
&\quad 12t^2ux^2z + 18t^2uxy^2 + 18t^2v^2xz + 9t^2v^2y^2 + 12t^2vx^2y + 3t^2x^4 + 6t^2xz^3+\\
&\quad 9t^2y^2z^2 + 6tu^4v + 12tu^3yz + 24tu^2vxz + 12tu^2vy^2 + 18tu^2x^2y + 12tuv^3z+\\
&\quad 24tuv^2xy + 12tuvx^3 + 12tuvz^3 + 24tuxyz^2 + 12tuy^3z + 6tv^4y + 6tv^3x^2+\\
&\quad 12tv^2yz^2 + 18tvx^2z^2 + 24tvxy^2z + 6tvy^4 + 6tx^2y^3 + 12tx^3yz + 6tyz^4+\\
&\quad 6u^4xz + 3u^4y^2 + 6u^3v^2z + 12u^3vxy + 2u^3x^3 + 2u^3z^3 + 6u^2v^3y + 9u^2v^2x^2+\\
&\quad 18u^2vyz^2 + 9u^2x^2z^2 + 12u^2xy^2z + 3u^2y^4 + 6uv^4x + 12uv^2xz^2 + 18uv^2y^2z+\\
&\quad 24uvx^2yz + 12uvxy^3 + 6ux^4z + 6ux^3y^2 + 6uxz^4 + 6uy^2z^3 + 3v^4z^2+\\
&\quad 12v^3xyz + 2v^3y^3 + 6v^2x^3z + 9v^2x^2y^2 + 3v^2z^4 + 6vx^4y + 12vxyz^3 + 6vy^3z^2+\\
&\quad 2x^3z^3 + 9x^2y^2z^2 + 6xy^4z
\end{aligned}$$

The key fact here is that 3, 4 and 5 are prime or power of a prime integer, while 6 is composite. As we will see in Theorem 1.2.1 this fact characterizes completely this phenomenon. In the following, we will first state some formulas regarding the coefficients $C_{a_0 \cdots a_{N-1}}$ of the determinant of a circulant matrix and next we will use them to compare to those of the permanent. As we will see, it is a hard problem to compute these coefficients and even to decide whether they vanish or not. In fact, the combinatorics lying under the form of a general coefficient are related to a general notion of partitions of integers and become very involved.

1.1.1 The coefficients of the determinant and the permanent

In this subsection, we collect some formulas regarding the coefficients of the expansion of the determinant of a circulant matrix. In the following we fix a generic circulant matrix $\mathrm{Circ}_N := \mathrm{Circ}(x_0\, x_1 \ldots x_{N-1})$ and we refer to $C_{[a]}$ as a general coefficient $C_{a_0 \ldots a_{N-1}}$ explained above.

Proposition 1.1.5: *If $a_0 + a_1 + \cdots + a_{N-1} = M_1 + 2M_2 + \cdots + (N-1)M_{N-1} \not\equiv 0 \mod N$, then $C_{[a]} = C^{\star}_{M_0 \cdots M_{N-1}} = 0$.*

Proof. See [7, Theorem 1]. □

This result is a first step to determine the vanishing coefficients of the determinant of a circulant matrix. Actually from a previous result of Hall in [4], Brualdi and Newman proved in [1] the following result, which determine the non-zero coefficient of the expansion of $per(\mathrm{Circ}_N)$:

Proposition 1.1.6: *The solutions of the system*

$$\left.\begin{array}{rcl} M_0 + M_1 + M_2 + \cdots + M_{N-1} & = & N \\ M_1 + 2M_2 + \cdots + (N-1)M_{N-1} & \equiv & 0 \mod N \end{array}\right\}$$

parametrize completely the set of non-vanishing coefficients appearing in $\mathrm{per}(\mathrm{Circ}_N)$.

Proof. See [1, Theorem 1]. □

This result motivates denoting with $p(N)$ (resp. $d(N)$) the number of non-zero coefficients appearing in the permanent (resp. the determinant) of Circ_N. For example, $d(3) = 4 = p(3)$, $d(4) = 10 = p(4)$, $d(5) = 26 = p(5)$ but $d(6) = 68 < 80 = p(6)$. As noticed above we have $p(N) \geq d(N)$ and in fact we have more:

Proposition 1.1.7: *Let $N \geq 3$ be a prime. If $0 \leq M_0, \ldots, M_{N-1} \leq N$ satisfies*

$$\left.\begin{array}{rcl} M_0 + M_1 + M_2 + \cdots + M_{N-1} & = & N \\ M_1 + 2M_2 + \cdots + (N-1)M_{N-1} & \equiv & 0 \mod N \end{array}\right\},$$

then the coefficient $C^{\star}_{M_0 \cdots M_{N-1}} \neq 0$. In particular, for N prime $d(N) = p(N)$.

Proof. See [7, Corollary 4]. □

From this result and using the theory of symmetric functions, H. Thomas proved that the equality also holds when N is a power of a prime:

Proposition 1.1.8: *If $N \geq 3$ is a power of a prime, then $d(N) = p(N)$.*

Proof. See [16, Theorem]. □

Remark 1.1.9: It is not always true that $d(N) = p(N)$. As we have seen above $d(6) = 68 < 80 = p(6)$.

In [16], Thomas conjectured that the equality $d(N) = p(N)$ only holds for N a power of prime, i.e:

Conjecture 1.1.10 ([16]): *Let $N \geq 3$ be an integer. It holds that $d(N) = p(N)$ if and only if N is a power of prime.*

The conjecture is true as we will see in next subsection. We end this subsection recalling a result on the vanishing of the coefficients of $\det(\mathrm{Circ}_N)$ that will be very useful to prove Thomas' conjecture:

Lemma 1.1.11: *For $N = M_0 + M_1 + 3$ with $M_0, M_1 \geq 1$, the coefficient $c_{0\cdots 01\cdots 1 a_{N-3}, a_{N-2} a_{N-1}}$ with $M_1 + a_{N-3} + a_{N-2} + a_{N-1} \equiv 0 \pmod N$ is zero if N divides $(M_1+2)(M_1+1)$ and either*

- *$a_{N-3} \leq a_{N-2} < N - M_1$, $a_{N-3} + a_{N-2} = N + 1 - \frac{(M_1+2)(M_1+1)}{N}$ and $a_{N-1} = M_0 + 2 + \frac{(M_1+2)(M_1+1)}{N}$, or*

- *$N - M_1 \leq a_{N-2} \leq a_{N-3}$, $a_{N-2} + a_{N-1} = N + 1 + \frac{(M_0+2)(M_0+1)}{N}$ and $a_{N-3} = M_0 + 2 - \frac{(M_0+2)(M_0+1)}{N}$.*

Proof. See [7, Corollary 6]. □

1.2 Thomas' conjecture

This section is entirely devoted to prove the Thomas' conjecture. Indeed, we have:

Theorem 1.2.1: *Let $N \geq 3$ be an integer. Then $d(N) = p(N)$ if and only if N is a power of a prime.*

Proof. From Proposition 1.1.8 we get one direction. For the converse, we use the Lemma 1.1.11. We assume that N is not a power of prime and we write $N = nm$ with $n, m > 1$ and $\gcd(m, n) = 1$. We will find an $N-$tuple $0 \leq M_0, \ldots, M_{N-1} \leq N$ satisfying the equation of Proposition 1.1.6, such that $C^{\star}_{M_0 \cdots M_{N-1}} = 0$. To construct this $N-$tuple we first apply the Bézout's identity to $\gcd(m, n) = 1$, to find integers $1 \leq \lambda, \mu$ such that $\lambda m = 1 + \mu n$ and $\lambda m, \mu n \leq N$. From these integers we define $M_1 := \mu n - 1$ and we have

$$(M_1+1)(M_1+2) = \mu n(\mu n + 1) = \mu n \lambda n = \lambda \mu N \Longrightarrow N | (M_1+1)(M_1+2)$$

To use the Lemma 1.1.11, we have to see first that $M_1 \leq N - 4$. However, $M_1 = \mu n - 1 = \lambda m - 2 \leq N - 2$. So, it is enough to see that M_1 cannot be $N - 3$. Indeed, if $M_1 = N - 3$, then $\mu n + 1 = M_1 + 2 = N - 1$ and so $\mu n = N - 2 = nm - 2$ which implies that $n|2$. Since we are assuming that $n > 1$ we obtain $n = 2$ and $\mu = m - 1$. In particular $\lambda m = 1 + \mu n = 1 + (m-1)2 = 2m - 1$ which implies that $m|1$ which is a contradiction since we assume

$m > 1$. In order to use Lemma 1.1.11, we define:

$$\begin{aligned} M_0 &:= nm - \mu n - 2 \\ A_2 &:= nm - \mu n \\ A_1 &:= \mu n - \mu\lambda + 1 \\ A_3 &:= nm - \mu n + \lambda\mu \end{aligned}$$

Since $M_1 \leq N - 4$, then $M_0 = N - M_1 - 3 \geq 1$. We have that $M_1 + A_1 + A_2 + A_3 = \mu n - 1 + nm - \mu n + \mu n - \mu\lambda + 1 + nm - \mu n + \lambda\mu = 2N \equiv 0 \pmod{N}$.

Finally we will see that these integers satisfy the first condition of Lemma 1.1.11. Choosing $(a_{N-3}, a_{N-2}, a_{N-1}) := (A_1, A_2, A_3)$.

Since $\mu \leq m$, then $\mu n - \mu\lambda \leq mn - m\lambda \Leftrightarrow \mu n - \mu\lambda + 1 \leq mn - m\lambda + 1 = mn - \mu n$. Then $A_1 \leq A_2$. On the other hand, since $\frac{(M_1+1)(M_1+2)}{N} = \mu\lambda$, we have $A_1 + A_2 = nm - \lambda\mu + 1 = N - \frac{(M_1+1)(M_1+2)}{N} + 1$ and $A_3 = nm - \mu n + \lambda\mu = M_0 + 2 + \frac{(M_1+1)(M_1+2)}{N}$. Therefore the coefficient $C_{0\cdots 01\cdots 1A_1A_2A_3}$ vanishes in the determinant. □

This theorem will be applied in Chapter 2 to find the first examples of non-minimal monomial $GT-$systems.

1.3 Specialization of the generic circulant

Let us consider $r \leq N-1$ and $0 \leq \alpha_0 < \cdots < \alpha_{r-1} \leq N-1$ be an $r-$tuple of integers. We can define $\operatorname{Circ}_{(N;\alpha_0,\dots,\alpha_{r-1})} := (\operatorname{Circ}_N)_{|(0,\dots,0,x_{\alpha_0},0,\dots,0,x_{\alpha_i},0,\dots,0,x_{\alpha_{r-1}},0\dots,0)}$ where x_{a_i} is located at the $a_i + 1$ position. Notice that $\operatorname{Circ}_{(N;\alpha_0,\dots,\alpha_{r-1})}$ is nothing but the specialization of Circ_N to $\{x_i = 0 \, : \, i \notin \{\alpha_0, \dots, \alpha_{r-1}\}\}$. On the same spirit let us denote $d_{(N;\alpha_0,\dots,\alpha_{r-1})}$ (resp. $p_{(N;\alpha_0,\dots,\alpha_{r-1})}$) the number of different monomials that appear in the expansion of $\det(\operatorname{Circ}_{(N;\alpha_0,\dots,\alpha_{r-1})})$ (resp. $\operatorname{per}(\operatorname{Circ}_{(N;\alpha_0,\dots,\alpha_{r-1})})$) with non-zero coefficient. Recall that only when N is a power of a prime we have $p(N) = d(N)$. However, let N not be a power of a prime, and suppose that all the non-zero coefficients of $\operatorname{per}(\operatorname{Circ}_N)$, vanishing in $\det(\operatorname{Circ}_N)$ involve only the variables $\{x_i \, : \, i \notin \{\alpha_0, \dots, \alpha_{r-1}\}\}$. Then, when we specialize there will be no non-zero coefficient of $\operatorname{per}(\operatorname{Circ}_{(N;\alpha_0,\dots,\alpha_{r-1})})$ vanishing in $\det(\operatorname{Circ}_{(N;\alpha_0,\dots,\alpha_{r-1})})$. In particular, $d_{(N;\alpha_0,\dots,\alpha_{r-1})} = p_{(N;\alpha_0,\dots,\alpha_{r-1})}$. Therefore we can see that the picture becomes slightly more involved. Actually, we have the following direct corollary from Theorem 1.2.1:

Corollary 1.3.1: *If $N \geq 3$ is a power of a prime, then for any $0 \leq \alpha_0 < \cdots < \alpha_{r-1} \leq N-1$ $r-$tuple of integers, it holds $d_{(N;\alpha_0,\dots,\alpha_{r-1})} = p_{(N;\alpha_0,\dots,\alpha_{r-1})}$.*

Proof. Notice that the monomials appearing in $\det\left(\operatorname{Circ}_{(N;\alpha_0,\dots,\alpha_{r-1})}\right)$ will appear with the same coefficient in $\det(\operatorname{Circ}_N)$, and the monomials appearing in $\det(\operatorname{Circ}_N)$ and not appearing in $\det(\operatorname{Circ}_{(N;\alpha_0,\dots,\alpha_{r-1})})$ are precisely those involving at least one variable in $\{x_i \, : \, i \notin \{\alpha_0, \dots, \alpha_{r-1}\}\}$. The same occurs changing det by per. Now, using Proposition 1.2.1, since N is a power of a prime we have $p(N) = d(N)$. Then, if we write by A the set of monomials appearing in $\det(\operatorname{Circ}_N)$ (or equivalently in $\operatorname{per}(\operatorname{Circ}_N)$) involving at least one variable in $\{x_i : i \notin \{\alpha_0, \dots, \alpha_{r-1}\}\}$ we have $d_{(N;\alpha_0,\dots,\alpha_{r-1})} = d(N) - \#A = p(N) - \#A = p_{(N;\alpha_0,\dots,\alpha_{r-1})}$ as we wanted. □

However, the converse is not true anymore as it is shown in the following example:

Example 1.3.2: If $N = 6$, $r = 3$ and $(\alpha_0, \alpha_1, \alpha_2) = (0, 1, 3)$ we have:

$$\mathrm{Circ}_{(6;0,1,3)} = \begin{pmatrix} x & y & 0 & t & 0 & 0 \\ 0 & x & y & 0 & t & 0 \\ 0 & 0 & x & y & 0 & t \\ t & 0 & 0 & x & y & 0 \\ 0 & t & 0 & 0 & x & y \\ y & 0 & t & 0 & 0 & x \end{pmatrix}$$

$$\det(\mathrm{Circ}_{(6;0,1,3)}) = -t^6 + 3t^4x^2 - 3t^2x^4 + x^6 - 2t^3y^3 - 6tx^2y^3 - y^6,$$

$$\mathrm{per}(\mathrm{Circ}_{(6;0,1,3)}) = t^6 + 3t^4x^2 + 3t^2x^4 + x^6 + 2t^3y^3 + 6tx^2y^3 + y^6.$$

Hence, $d_{(6;0,1,3)} = p_{(6;0,1,3)} = 7$. Observe that we can compare it with the determinant and the permanent of the generic circulant Circ_6 computed in Example 1.1.4 where the family $\{t^2uvyz,\ t^2ux^2z,\ t^2vx^2y,\ tu^2vxz,\ tu^2vy^2,\ 24tuv^2xy,\ tuxyz^2,\ tv^2yz^2,\ tvxy^2z,\ u^2xy^2z,\ uv^2xz^2,\ uvx^2yz\}$ consists of all the monomials appearing in the permanent $\mathrm{per}(\mathrm{Circ}_6)$ such that their coefficients vanish in the determinant $\det(\mathrm{Circ}_6)$. Notice that all of them involve the variable z or u or v, and these are precisely the variables from where we are projecting in our example.

In this section, we will address this problem to have a more complete picture of what occurs. Since the determinant of a matrix is invariant (modulus sign) for permutation of rows, and since the matrix is circulant, given a specialization $(\alpha_0, \dots, \alpha_{r-1})$, we can always choose a row with a nonzero first entry as a first row. Therefore, we can assume in the following $\alpha_0 = 0$. Let us start recalling a useful result due to Loehr, Warrington and Wilf:

Proposition 1.3.3: *Let $N \geq 3$ and $2 \leq a \leq N-1$ be integers. Then $d_{(N;0,1,a)} = p_{(N;0,1,a)}$.*

Proof. See [6, Theorem 2]. □

Observe that this result applies to all circulant matrices such that the first row is of the type $(x_0, x_1, 0, \dots, 0, x_a, 0, \dots, 0)$. In particular it applies to Example 1.3.2. The following example shows there are cases in which Proposition 1.3.3 does not apply but the equality still holds:

Example 1.3.4: If $N = 6$, $r = 3$ and $(\alpha_0, \alpha_1, \alpha_2) = (0, 2, 5)$ we have:

$$\mathrm{Circ}_{(6;0,2,5)} = \begin{pmatrix} x & 0 & z & 0 & 0 & v \\ v & x & 0 & z & 0 & 0 \\ 0 & v & x & 0 & z & 0 \\ 0 & 0 & v & x & 0 & z \\ z & 0 & 0 & v & x & 0 \\ 0 & z & 0 & 0 & v & x \end{pmatrix}$$

$$\begin{aligned}\det(\mathrm{Circ}_{(6;0,2,5)}) &= x^6+z^6-v^6+6v^2x^3z+3v^4z^2-3v^2z^4+2x^3z^3,\\ \mathrm{per}(\mathrm{Circ}_{(6;0,2,5)}) &= x^6+v^6+z^6+6v^2x^3z+3v^4z^2+2x^3z^3+3v^2z^4.\end{aligned}$$

Therefore, we have $d_{(6;0,2,5)} = p_{(6;0,2,5)} = 7$.

In fact, consider the following cyclic permutation of the rows: the ith row becomes the $(i-1)$th row for $1 \leq i \leq 5$ and the 0th row becomes the 5th. The matrix we have got is $\mathrm{Circ}_{(6;0,1,3)}$ changing the variables (x,y,t) by (v,x,z). Since the determinant does not change by permutations of rows, $\det(\mathrm{Circ}_{(6;0,2,5)}) = \det(\mathrm{Circ}_{(6;0,1,3)})$ and $\mathrm{per}(\mathrm{Circ}_{(6;0,2,5)}) = \mathrm{per}(\mathrm{Circ}_{(6;0,1,3)})$ modulus a change of variables. This is not a coincidence and comes from the fact that $(0,2,5)+1 \equiv (1,3,0) \pmod 6$. In proposition 1.3.7 we will establish this property in a more general framework.

Based on the previous examples and on our calculations with the program Mathematica, we make the following guess:

Conjecture 1.3.5: *Fix $N \geq 3$ be an integer and $(\alpha_0,\alpha_1,\alpha_2) = (0,a,b)$ with $gcd(N,a,b) = 1$. It holds: $d_{(N;0,a,b)} = p_{(N;0,a,b)}$.*

In order to solve other cases and give a partial answer to this last conjecture, we need to review some symmetries among the coefficients of the generic circulant matrix.

Definition 1.3.6: Let $N \geq 3$, given an integer n and an $N-$tuple $[a_0,\dots,a_{N-1}]$, we define:

- $n+[a] := [\{\overline{n+a_0},\dots,\overline{n+a_{N-1}}\}]$.
- $n[a] := [\{\overline{na_0},\dots,\overline{na_{N-1}}\}]$.

Where $\overline{x}$ is the integer such that $0 \leq a \leq N-1$ and $x \equiv a \pmod N$, and $\{x_0,\dots,x_{N-1}\}$ means to rearrange the $N-$tuple such it becomes increasing.

These two operations play a key role in comparing the coefficients of different monomials in the determinant of the generic circulant matrix. In particular, we are interested in looking for different monomials with the same coefficient (modulus sign).

Proposition 1.3.7: *Let $N \geq 3$ be an integer and $[a] = [a_0,\dots,a_{N-1}]$ a coefficient index. Then,*

(i) for all integer n, $C_{n+[a]} = C_{[a]}$ and

(ii) for all integer n such that $\gcd(n,N) = 1$, $C_{n[a]} = (-1)^{n(N-1)}C_{[a]}$.

Proof. See [7, Proposition 2]. □

Using this Proposition we obtain another interesting result.

Proposition 1.3.8: *Let $N \geq 3$ and $1 \leq a < b \leq N$. If either $\gcd(a,N) = 1$ or $\gcd(b,N) = 1$, then $d_{(N;0,a,b)} = p_{(N;0,a,b)}$.*

Proof. We can assume without loss of generality that $\gcd(a, N) = 1$. The coefficients of $per(Circ_{(N;0,a,b)})$ are determined in Proposition 1.1.6. Hence, to prove that $d_{(N;0,a,b)} = p_{(N;0,a,b)}$ it suffices to see that for any $0 \leq M_0, M_a, M_b \leq N$ such that $M_0 + M_a + M_b = N$ and $aM_a + bM_b \equiv 0 \pmod{N}$, the coefficient $C^{\star}_{M_0 M_a M_b} = C_{0\cdots 0a\cdots ab\cdots b} \neq 0$. Let us take a triple (M_0, M_a, M_b) satisfying these equations and we see that $C_{0\cdots 0a\cdots ab\cdots b} \neq 0$. Since $\gcd(a, N) = 1$, there is $1 \leq k \leq N-1$ such that $ka \equiv 1 \pmod{N}$. So, applying Proposition 1.3.7 we have:

$$|C_{0\cdots 0a\cdots ab\cdots b}| = |C_{k[\cdots 0a\cdots ab\cdots b]}| = |C_{0\cdots 01\cdots 1(\overline{kb})\cdots(\overline{kb})}|$$

On the other hand, $C_{0\cdots 01\cdots 1(\overline{kb})\cdots(\overline{kb})}$ is a coefficient of the determinant of the circulant matrix $\mathrm{Circ}_{(N;0,1,(\overline{kb})}$. Therefore, by Proposition 1.3.3 the coefficient is non-zero and the result follows. □

This result allows us to focus on the case $(N; 0, a, b)$ with both $\gcd(a, N) > 1$ and $\gcd(b, N) > 1$. In this line we have two more results which solve a great amount of cases. In particular, we have all the ingredients to state the main theorem of this section.

Theorem 1.3.9: *Let $N \geq 3$ and $1 \leq a, b \leq N$. If $b - a \in \left(\mathbb{Z}/N\mathbb{Z}\right)^{\star}$, then $d_{(N;0,a,b)} = p_{(N;0,a,b)}$.*

Proof. By Proposition 1.1.6, to prove that $d_{(N;0,a,b)} = p_{(N;0,a,b)}$ it is enough to see that for any $0 \leq M_0, M_a, M_b \leq N$ such that $M_0 + M_a + M_b = N$ and $aM_a + bM_b \equiv 0 \pmod{N}$, the coefficient $C^{\star}_{M_0 M_a M_b} = C_{0\cdots 0a\cdots ab\cdots b} \neq 0$. Pick up (M_0, M_a, M_b) one such triple and look the coefficient $C_{0\cdots 0a\cdots ab\cdots b}$ from $\det(\mathrm{Circ}_{(N;0,a,b)})$ in the determinant of the generic circulant matrix Circ_N.

Let us first assume that $b = a + 1$. In this case we can use Proposition 1.3.7 (i) to see that

$$C_{0\cdots 0a\cdots a(a+1)\cdots(a+1)} = C_{(N-a)+[0\cdots 0a\cdots a(a+1)\cdots(a+1)]} = C_{0\cdots 01\cdots 1(N-a)\cdots(N-a)}.$$

Now we observe that this is a coefficient of the determinant of the circulant matrix $\mathrm{Circ}_{(N;0,1,N-a)}$ and by Proposition 1.3.3 it does not vanish.

Finally, let us assume that $b > a + 1$. Since by hypothesis $b - a \in \left(\mathbb{Z}/N\mathbb{Z}\right)^{\star}$ we can consider its inverse k and we have $k(b - a) \equiv 1 \pmod{N}$ or equivalently $kb \equiv ka + 1 \pmod{N}$. Then applying Proposition 1.3.7 (ii) we have:

$$|C_{0\cdots 0a\cdots ab\cdots b}| = |C_{k[0\cdots 0a\cdots ab\cdots b]}| = |C_{[\{0\cdots 0(\overline{ka})\cdots(\overline{ka})(\overline{ka+1})\cdots(\overline{ka+1})\}]}|.$$

To this last coefficient we can apply the previous case to see that it does not vanish, and the result follows. □

As a consequence of this theorem we have the following corollary:

Corollary 1.3.10: *If $N \geq 3$, $1 \leq a, b \leq N$, $\gcd(a, b, N) = 1$ and $Supp(N) \subset Supp(a) \cup Supp(b)$, then $d_{(N;0,a,b)} = p_{(N;0,a,b)}$.*

Proof. It is enough to see that the condition $\mathrm{Supp}(N) \subset \mathrm{Supp}(a) \cup \mathrm{Supp}(b)$ implies that $b - a$ is coprime with N. Indeed, let us assume that $\gcd(b - a, N) > 1$, then there exists

p a prime such that $p|N$ and $p|(b-a)$. In particular $p \in \text{Supp}(N) \subset \text{Supp}(a) \cup \text{Supp}(b)$. Assume that $p \in \text{Supp}(a)$, then $p|(b-a)$ and $p|a$. So, $p|b$ too and then $p|gcd(a,b,N) = 1$, which is a contradiction. Therefore, we cannot suppose that $\gcd(b-a,N) > 1$ and hence $b-a$ is coprime with N. □

Observe that there are cases in which Corollary 1.3.10 does not apply but Theorem 1.3.9 does. For instance, if $(N;0,a,b) = (70;0,2,5)$, then $\text{Supp}(70) = \{2,5,7\}$ and $\text{Supp}(2) \cup \text{Supp}(5) = \{2,5\}$. So we cannot apply Corollary 1.3.10 but, since $5-2=3$ which is coprime with 70 we can yet apply Theorem 1.3.9. However, there are cases in which even though we cannot apply Theorem 1.3.9, the equality still holds. Consider $(N;0,a,b) = (30;0,2,5)$. We cannot apply Theorem 1.3.9 because $2-5=3$ which is not coprime with 30. Nevertheless, using the computer algebra system Mathematica we have obtained:

$$\begin{aligned}\det(\text{Circ}_{(30;0,2,5)}) = {} & -t^{30} - 60t^{25}v^3x^2 - 1170t^{20}v^6x^4 + 3t^{20}x^{10} - 2t^{15}v^{15} - 8210t^{15}v^9x^6 - \\ & 730t^{15}v^3x^{12} + 165t^{10}v^{18}x^2 - 16095t^{10}v^{12}x^8 + 7050t^{10}v^6x^{14} - 3t^{10}x^{20} - \\ & 420t^5v^{21}x^4 - 3906t^5v^{15}x^{10} - 3240t^5v^9x^{16} - 210t^5v^3x^{22} - v^{30} + 5v^{24}x^6 - \\ & 10v^{18}x^{12} + 10v^{12}x^{18} - 5v^6x^{24} + x^{30}\end{aligned}$$

$$\begin{aligned}\text{per}(\text{Circ}_{(30;0,2,5)}) = {} & t^{30} + 60t^{25}v^3x^2 + 1170t^{20}v^6x^4 + 3t^{20}x^{10} + 2t^{15}v^{15} + 8210t^{15}v^9x^6 + \\ & 730t^{15}v^3x^{12} + 165t^{10}v^{18}x^2 + 16095t^{10}v^{12}x^8 + 7050t^{10}v^6x^{14} + 3t^{10}x^{20} + \\ & 420t^5v^{21}x^4 + 3906t^5v^{15}x^{10} + 3240t^5v^9x^{16} + 210t^5v^3x^{22} + v^{30} + 5v^{24}x^6 + \\ & 10v^{18}x^{12} + 10v^{12}x^{18} + 5v^6x^{24} + x^{30}\end{aligned}$$

Remark 1.3.11: Observe that for any $3 \leq N \leq 29$ it holds that N is at most a product of two power of primes. In particular, the first value by which there can be integers $1 \leq a < b \leq N$ with $\gcd(a,N) > 1$ and $\gcd(b,N) > 1$, and such that Theorem 1.3.9 cannot be applied is $N = 30$. For example, as showed above $(N;0,a,b) = (30;0,2,5)$. Moreover, this remark also allows us to conclude that Conjecture 1.3.5 is true for $N \leq 41$. Indeed, for $31 \leq N \leq 41$ $\#\text{Supp}(N) \leq 2$.

1.4 Connections to other areas

The study of the determinant of a circulant matrix has been largely studied along the 20th century. In particular, the problem of finding an enclosed formula for the coefficients of $\det(\text{Circ}_N)$ was treated in a lot of detail by Ore in [14]. In his article, Ore find a formula to compute a coefficient of $\det(\text{Circ}_N)$ making use of integer partitions and a formula of Faà di Bruno. However, computing the coefficients using this formula becomes rapidly a very hard problem. Developing these ideas, Malenfant found in [7, Theorem 3] another formula involving integer partitions that in some cases can be simplified to get an easier expression of the coefficients. Another approach different from finding such an enclosed formula consists of finding connections to other concepts and problems of other areas in mathematics. To see one of these relations, pointed out by Ore in [14, Section 5], let us review some basic facts about the resultant of two polynomials.

Definition 1.4.1: Let $f = a_0 + a_1x + \cdots + a_rx^r$ and $g = b_0 + b_1x + \cdots + b_sx^s$ be two polynomials. Then the **Resultant** of f and g is the determinant of the Sylvester matrix of f and g

$$Syl(f,g) = \begin{pmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & & 0 & b_1 & b_0 & & 0 \\ a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 \\ a_r & a_{r-1} & & a_1 & b_s & b_{s-1} & & b_1 \\ 0 & a_r & \ddots & a_2 & 0 & b_s & \ddots & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_r & 0 & 0 & \cdots & b_s \end{pmatrix}$$

which has the first s columns with entries on the coefficients of f and the next r columns made by the coefficients of g. We denote $Res(f,g) = \det(Syl(f,g))$.

The resultant is an algebraic tool arising in a great variety of problems and results in commutative algebra, algebraic geometry or algebraic computational theory. One property, which will turn out to be very useful in our case, is the following:

Proposition 1.4.2: *Let f and g be polynomials in $k[x]$. Then*

$$Res(f,g) = \prod_{\alpha \in g^{-1}(0)} f(\alpha) = \prod_{\beta \in f^{-1}(0)} g(\beta).$$

Observe that, given an integer $N \geq 3$, the Nth roots of unity are precisely the roots of the polynomial $\varphi_N := x^N - 1$. On the other hand, let us consider the circulant matrix Circ_N whose first row is given by $(a_0\, a_1\, \cdots\, a_{N-1})$. By Remark 1.1.3, its determinant can be written as

$$\begin{aligned} \det(\mathrm{Circ}_N) &= \prod_{j=0}^{N-1} (a_0 + a_1\zeta^j + \cdots + a_{N-1}\zeta^{j(N-1)}) \\ &= \prod_{\alpha \in \varphi_N^{-1}(0)} (a_0 + a_1\alpha + \cdots + a_{N-1}\alpha^{N-1}). \end{aligned}$$

Where ζ is a primitive Nth root of unity. Using Proposition 1.4.2, if we consider the polynomial $f = a_0 + a_1x + \ldots + a_{N-1}x^{N-1}$ associated to Circ_N we obtain that

$$\det(\mathrm{Circ}_N) = Res(\varphi_N, f).$$

Therefore, we have found that studying the determinant of $N \times N$ circulant matrices is equivalent to study the resultants with respect to the polynomial φ_N. This observation has been very useful for checking the minimality of certain Togliatti systems and GT-systems in [3] (work in progress).

Chapter 2

Applications to the minimality of GT-systems

In this chapter, we apply the results from Chapter 1 about the coefficients of the determinant of a specialized generic circulant matrix to state new contributions to the conjecture on the minimality of GT-systems. After recalling the definition of the WLP and reviewing its basic properties, we define GT-systems as were introduced in [8]. Then, we show how to apply the knowledge of the determinant of the circulant matrix to study the minimality of GT-systems. Finally, we show how the results given in the last section of Chapter 1 allow us to give a partial answer to a previous conjecture of Mezzetti and Miró-Roig in [8].

2.1 Preliminaries

In this section we will collect and illustrate all the definitions and results about the weak Lefschetz property which are necessary to define the notion of GT-system.

Definition 2.1.1: Let $I \subset R$ be a homogeneous artinian ideal. We say that I has Weak Lefschetz Property (WLP) if there is a $L \in [R/I]_1$ such that, for all integers j, the multiplication map

$$\times L : [R/I]_{j-1} \to [R/I]_j$$

has maximal rank, i.e. it is either injective or surjective.

Example 2.1.2: The ideal $I = (x^3, y^3, z^3, (x+y+z)^3)$ has de WLP. Indeed, for a general linear form $L = ax + by + cz$ we have to see that $\times L : [R/I]_j \to [R/I]_{j+1}$ has maximal rank for each j. Since $[R/I]_0 = R_0$, $[R/I]_1 = R_1$ and $[R/I]_2 = R_2$, we can start looking for $j = 2$. Since $\dim[R/I]_2 = 6$ and $\dim[R/I]_3 = 6$, if we see that $\times L$ is injective, we are done. If we pick $P = a_1x^2 + a_2xy + a_3xz + a_4y^2 + a_5yz + a_6z^2 \in R_2 = [R/I]_2$, we have $LP = aa_1x^3 + (aa_2 + ba_1)x^2y + (aa_4 + ba_2)xy^2 + ba_4y^3 + (aa_3 + ca_1)x^2z + (aa_5 + ba_3 + ca_2)xyz + (ba_5 + ca_4)y^2z + (aa_6 + ca_3)xz^2 + (ba_6 + ca_5)yz^2 + ca_6z^3$. Hence, in $[R/I]_3$ we have $LP \equiv (aa_2 + ba_1)x^2y + (aa_4 + ba_2)xy^2 + (aa_3 + ca_1)x^2z + (aa_5 + ba_3 + ca_2)xyz + (ba_5 + ca_4)y^2z + (aa_6 + ca_3)xz^2 + (ba_6 + ca_5)yz^2$. If we suppose that $LP \equiv 0$ in $[R/I]_3$ so $LP \in I = (x^3, y^3, z^3, (x+y+z)^3)$. This leads to a linear system in which the only solution is $a_1 = a_2 = a_3 = a_4 = a_5 = a_6 = 0$, using that $abc \neq 0$. Since $\times L : [R/I]_2 \to [R/I]_3$ is injective and $\dim[R/I]_2 = 6 = \dim[R/I]_3$, then $\times L$ is bijective and, in particular it is surjective. On the other hand, it was proved in [12, Proposition 2.1] that if $\times L : [R/I]_{j_0-1} \to [R/I]_{j_0}$

is surjective in some degree j_0, then $\times L : [R/I]_{j-1} \to [R/I]_j$ is surjective for all $j \geq j_0$. Applying this result in our case, the surjectivity for $\times L : [R/I]_{j-1} \to [R/I]_j$ for $j \geq 4$ follows.

On the other hand, the ideal $I = (x^3, y^3, z^3, xyz)$ fails the WLP in degree 2. Since I is a monomial ideal, it is enough to check the WLP for the particular linear form $L = x + y + z$ instead of for a general linear one (see for instance [12, Proposition 2.2]). We will see that $\operatorname{Ker}(\times L : R_2 \to [R/I]_3)$ has a nontrivial element. Actually, imposing that $(x+y+z)(a_1x^2 + a_2xy + a_3xz + a_4y^2 + a_5yz + a_6z^2) \equiv 0$ in $[R/I]_3$ gives rise to a linear system of equations in $\{a_1, \dots, a_6\}$ which is indeterminate with one degree of freedom. The solutions are $\{(\lambda, -\lambda, -\lambda, \lambda, -\lambda, \lambda) : \lambda \in k\}$. Therefore, the form $(x^2 + y^2 + z^2 - xy - xz - yz \in \operatorname{Ker}(\times L)$ and therefore the multiplication map $\times L$ is not injective.

It is a hard problem to establish whether certain artinian ideals have or fail the WLP. For instance, even though Stanley in [15] and Watanabe in [18] proved that a general artinian complete intersection has the WLP, it is already an open problem to determine if *every* complete intersection in codimension bigger than 3 has the WLP. In the last decades the study of the WLP has been related to other areas of mathematics, such as combinatorics or geometry. For instance, Mezzetti, Miró-Roig and Ottaviani found in [10] a relation between the failure of the WLP and the existence of a projection of a Veronese variety satisfying Laplace equations:

Theorem 2.1.3: *Let $I \subset R$ be an artinian ideal generated by r homogeneous polynomials $F_1, ..., F_r$ of degree d and let I^{-1} be its Macaulay inverse system. If $r \leq \binom{n+d-1}{n-1}$, then the following conditions are equivalent:*

(1) the ideal I fails the WLP in degree $d-1$;

(2) the homogeneous forms $F_1, ..., F_r$ become k-linearly dependent on a general hyperplane H of $\mathbb{P}^n$;

(3) the n-dimensional variety X associated to the Macaulay inverse system I^{-1} satisfies at least one Laplace equation of order $d-1$.

Proof. See [10, Theorem 3.2]. □

This important result motivated the following definitions:

Definition 2.1.4: Let $I \subset R$ be an artinian ideal generated by r forms of degree d, and $r \leq \binom{n+d-1}{n-1}$. We will say:

(i) I is a *Togliatti system* if it satisfies one of three equivalent conditions in Theorem 2.1.3.

(ii) I is a *monomial Togliatti system* if, in addition, I can be generated by monomials.

(iii) I is a *smooth Togliatti system* if, in addition, the rational variety X is smooth.

(iv) A monomial Togliatti system I is *minimal* if there is no proper subset of the set of generators of I defining a monomial Togliatti system.

Remark 2.1.5: The name is in honour to the italian mathematician E. Togliatti who proved that the only smooth Togliatti system of cubics in $k[x,y,z]$ is (x^3, y^3, z^3, xyz).

In the remaining of this section, we focus our attention on defining and studying a particular class of Togliatti system introduced in [8, Problem 2.6]: the so-colled GT-systems.

Definition 2.1.6: A **GT-system** is an artinian ideal $I \subset k[x,y,z]$ generated by forms $F_1, \ldots, F_r$ of degree d such that:

i) I is a Togliatti system.

ii) The regular map $\varphi_I : \mathbb{P}^2 \to \mathbb{P}^{r-1}$ defined by $(F_1, \ldots, F_r)$ is a Galois covering of degree d with cyclic Galois group $\mathbb{Z}/d$.

To study these types of Togliatti systems we need to fix some notation about the representations of the cyclic groups $\mathbb{Z}/d$ as subgroups of $GL(3, \mathbb{C})$. Namely, we have the following result.

Proposition 2.1.7: *Let $d \in \mathbb{Z}$. Any representation of $\mathbb{Z}/d$ on $GL(3, \mathbb{C})$ can be diagonalized and, in particular it is represented by a matrix of the form*

$$M_{a,b,c} := \begin{pmatrix} e^a & 0 & 0 \\ 0 & e^b & 0 \\ 0 & 0 & e^c \end{pmatrix}$$

where e is a primitive dth root of 1, $0 \le a \le b \le c \le d-1$ *and* $\gcd(a,b,c,d) = 1$.

Proof. Since $\mathbb{Z}/d$ is cyclically generated by $\bar{1}$, it is enough to consider a 3×3 matrix M representing $\bar{1} \in \mathbb{Z}/d$. That is $M^d = \mathrm{Id}$ and $M^k \neq \mathrm{Id}$ for $1 \le k \le d-1$. Therefore, if we consider the polynomial $F(X) = X^d - 1$, we have that $F(M) = 0$. In particular, the minimal polynomial $m(x)$ of M divides F. Observe that the roots of F are exactly all the dth roots of unity. Then, the three roots of the minimal polynomial are precisely three roots of unity. We can write them in terms of a primitive dth root of unity e: e^a, e^b and e^c. In particular, M diagonalizes to the matrix $M_{a,b,c}$ in the statement. Finally, since $M^d = \mathrm{Id}$ and for $1 \le k \le d-1$, $M^k \neq \mathrm{Id}$, the condition $\gcd(a,b,c,d) = 1$ follows. □

Let us fix a an integer d and a matrix $M_{a,b,c}$. Then Z/d acts on $k[x,y,z]$ by means of the matrix $M_{a,b,c}$ as follows:

$$\langle M_{a,b,c} \rangle \curvearrowright k[x,y,z] \text{ such that } M_{a,b,c} \cdot P(x,y,z) := P(e^a x, e^b y, e^c z).$$

It is worthwhile to mention the following result.

Proposition 2.1.8: *Let $d \ge 3$ and let $M_{a,b,c}$ be any matrix representing the cyclic group $\mathbb{Z}/d$. Then the ideal $I \subset k[x,y,z]$ generated by all the forms of degree d invariant under the action of $M_{a,b,c}$ is monomial.*

Proof. See, for instance, [8, Theorem 3.1]. □

Remark 2.1.9: Since we are working in the projective space and its homogeneous coordinates, $[e^a x, e^b y, e^c z] = [x, e^{b-a} y, e^{c-a} z]$. Hence, without loss of generality we can assume that $a = 0$ and then we consider only matrices of the type $M_{0,a,b}$. Moreover, abusing with the notation we write $M_{a,b}$ instead of $M_{0,a,b}$.

Now we have all the background necessary to state the following important result:

Theorem 2.1.10: *Let $d \geq 3$ be an integer and $M_{a,b}$ be a matrix representing the cyclic group $\mathbb{Z}/d$ with $1 \leq a < b \leq d-1$ such that $\gcd(a,b,d) = 1$. Let also $I \subset k[x,y,z]$ be the ideal generated by all the monomials of degree d invariant under the action of $M_{a,b}$. Then I is a GT-system.*

Proof. See, for instance, [8, Theorem 3.4]. □

Remark 2.1.11: In the proof of Theorem 2.1.10, the authors observed that the form $F_{d-1} := (x + e^a y + e^b z) \cdots (x + e^{d-1)a} y + e^{(d-1)b} z)$ was in the kernel of $\times(x+y+z) : [R/I]_{d-1} \to [R/I]_d$. In [12, Proposition 2.2] it is proved that for monomial ideals it is enough to check the WLP for the linear form $x + y + z$ instead of for a general linear form L. In particular, these two facts give the failure of the WLP in degree $d-1$. Furthermore, this implies that the form

$$C_d := (x+y+z)(x + e^a y + e^b z) \cdots (x + e^{d-1)a} y + e^{(d-1)b} z) \in I \tag{2.1}$$

and then, it is generated by the monomials invariant under the action of $M_{a,b}$. The authors in [8] observed the following: let us consider the monomial ideal $J \subset k[x,y,z]$ generated by all the monomials obtained from the expansion of C_d. If we see that $J \subsetneq I$, then by the same argument J fails the WLP in degree $d-1$ and therefore J is also a Togliatti system. In particular I would not be minimal.

2.2 The minimality problem

In this section, we retake the study of GT-systems from the persepective of their minimality. As we have introduced in Remark 2.1.11, to study if a GT-system is a minimal Togliatti system is equivalent to study the non-zero coefficients of the expansion of the form C_d defined in (2.1). In the following we will show the relation that this problem has with the results of Chapter 1 and the theory of the circulant matrices.

Given integers $d \geq 3$ and $1 \leq a < b \leq d-1$ such that $\gcd(a,b,d) = 1$, and the matrix $M_{a,b}$ representing the cyclic group $\mathbb{Z}/d$. We denote by $I_{(d;a,b)}$ the ideal $I \subset k[x,y,z]$ generated by all the monomials of degree d invariant under the action of $M_{a,b}$. By Theorem 2.1.10 we know that $I_{(d;a,b)}$ is a GT-system. We also denote by

$$C_{(d;a,b)} := (x+y+z)(x + e^a y + e^b z) \cdots (x + e^{d-1)a} y + e^{(d-1)b} z)$$

the form of degree d introduced in Remark 2.1.11. By the Remark 1.1.3 and using the notation of Chapter 1 we observe that $C_{(d;a,b)}$ coincides with the determinant of the circulant matrix $\mathrm{Circ}_{(d;0,a,b)}$. On the other hand, a monomial $x^\alpha y^\beta z^\gamma$ of degree d is invariant under the action of $M_{a,b}$ if, and only if it satisfies the following system of equations:

$$\begin{cases} \alpha+\beta+\gamma &= d \\ a\beta+b\gamma &\equiv 0 \pmod{d} \end{cases}$$

Using Proposition 1.1.6, this is equivalent to say that the coefficient of $\operatorname{per}(\operatorname{Circ}_{(d;0,a,b)})$ correspondent to the multiplicities $(M_0, M_a, M_b) = (\alpha, \beta, \gamma)$ is non-zero. In particular, the monomials appearing in the permanent $\operatorname{per}(\operatorname{Circ}_{(d;0,a,b)})$ with non-zero coefficient are exactly all the monomials of degree d invariant by the action of $M_{a,b}$.

Summing up, we depart from the problem of finding which monomials generating $I_{(d;a,b)}$ appear with non-zero coefficient of $C_{(d;a,b)}$. By the above reasoning, this is equivalent to the problem of finding which monomials with non-zero coefficient in $\operatorname{per}(\operatorname{Circ}_{(d;0,a,b)})$ appear with non-zero coefficient in $\det(\operatorname{Circ}_{(d;0,a,b)})$. Or, in other words, it is the same as asking when does the equality $d_{(d;0,a,b)} = p_{(d;0,a,b)}$ hold. From this remark, it follows a restatement of Conjecture 1.3.5 in terms of GT-systems, previously posed by Mezzetti and Miró-Roig in [8, Conjecture 4.6].

Conjecture 2.2.1: *For any integers $d \geq 3$ and $1 \leq a < b \leq d-1$ such that $\gcd(a,b,d) = 1$. Then, $I_{(d;a,b)}$ is a minimal GT-system.*

Using the results obtained in Section 1.3, we can answer a lot of cases of this conjecture. Namely, we have the following theorem:

Theorem 2.2.2: *Let $d \geq 3$ and $1 \leq a < b \leq d-1$ be integers such that $\gcd(a,b,d) = 1$. Then*

- *i) If either $\gcd(a,d) = 1$ or $\gcd(b,d) = 1$, then the GT-system $I_{(d;a,b)}$ is minimal.*
- *ii) If both $\gcd(a,d) > 1$ and $\gcd(b,d) > 1$, and $b-a \in \left(\mathbb{Z}/d\mathbb{Z}\right)^{\star}$, then $I_{(d;a,b)}$ is minimal.*
- *iii) In particular, if $Supp(d) = Supp(a) \cup Supp(b)$, then $I_{(d;a,b)}$ is minimal.*

Proof. The i) part follows directly from Proposition 1.3.8. The ii) part is a reestatement of Theorem 1.3.9. Finally, the iii) part is deduced from the ii) part as in Corollary 1.3.10. □

Bibliography

[1] R. Brualdi and M. Newman, *An enumeration problem for a congruence equation.* J. Res. Nat. Bur. Standards. Sect. B **74B** (1970), 37–40.

[2] L. Colarte, E. Mezzetti, R. M. Miró-Roig and M. Salat, *On the coefficients of the permanent and the determinant of a circulant matrix. Applications.* Proc. AMS. (to appear).

[3] L. Colarte, E. Mezzetti, R. M. Miró-Roig and M. Salat, *On the minimality of GT-systems.* Work in progress.

[4] M. Hall, Jr. *A combinatorial problem on abelian groups.* Proc. Amer. Math. Soc. **3** (1952), 584–587.

[5] I. Kra and S. R. Siamanca *On circulant matrices.* Notices AMS **59** (3) (2012), 368-377.

[6] N. A. Loehr, G. S. Warrington and H. S. Wil, *The combinatorics of a three-line circulant determinant.* Isr. J. Math. **143** No. 1 (2004), 141–156.

[7] J. Malenfant, *On the Matrix-Element Expansion of a Circulant Determinant.* ArXiv:1502.06012.

[8] E. Mezzetti and R.M. Miró-Roig, *Togliatti systems and Galois coverings.* J. Algebra (2018), http://doi.org/10.1016/j.jalgebra.2018.05.014. Available on arXiv:1611.05620.

[9] E. Mezzetti and R. M. Miró-Roig, *The minimal number of generators of a Togliatti system.* Annali di Matematica Pura ed Applicata, **195** (2016) 2077–2098.

[10] E. Mezzetti, R.M. Miró-Roig and G. Ottaviani, *Laplace Equations and the Weak Lefschetz Property*, Canad. J. Math. **65** (2013), 634–654.

[11] M. Michałek and R. M. Miró-Roig, *Smooth monomial Togliatti systems of cubics.* J. Comb. Th., Ser. A **143** (2016) 66–87.

[12] J. Migliore, R. M. Miró-Roig and U. Nagel, *Monomial ideals, almost complete intersections and the weak Lefschetz property.* Trans. Amer. Math. Soc. **363** No. 1 (2011), 229–257.

[13] R. M. Miró-Roig and M. Salat, *On the Classification of Togliatti systems.* Commun. in Alg. **46** No. 6 (2018), 2459–2475.

[14] O. Ore *Some studies on cyclic determinants.* Duke Math J. **18** No. 2 (1951), 343–354.

[15] R. P. Stanley, *Weyl groups, the hard Lefschetz theorem, and the Sperner property.* SIAM J. on Algebraic and Discrete Methods, **1** No. 2 (1980) 168–184.

[16] H. Thomas, *The number of terms in the permanent and the determinant of a generic circulant matrix.* J. Alg. Comb. **20** (2004), 55–60.

[17] L. G. Valiant, *The Complexity of Computing the Permanent*, Theoretical Computer Science **8** No. 2 (1979) 189–201.

[18] J. Watanabe *The Dilworth number of Artinian rings and finite posets with rank function*, Commutative Algebra and Combinatorics, Advanced Studies in Pure Math. **11** (1987), 303–312.

[19] A. Wyn-Jones *Circulants.* Available in www.circulants.org/circ/circall.pdf.