Circulant matrices and Galois-Togliatti systems

Pietro De Poi [a,1], Emilia Mezzetti [b,1], Mateusz Michałek [c,d,*,2], Rosa Maria Miró-Roig [e,3], Eran Nevo [f,4]

[a] *Dipartimento di Scienze Matematiche, Informatiche e Fisiche, Università degli Studi di Udine, Via delle Scienze 206, 33100 Udine, Italy*
[b] *Dipartimento di Matematica e Geoscienze, Università degli Studi di Trieste, Via A. Valerio 12/1, 34127 Trieste, Italy*
[c] *Max Planck Institute for Mathematics in the Sciences, Inselstr. 22, 04103 Leipzig, Germany*
[d] *Mathematical Institute of the Polish Academy of Sciences, Śniadeckich 8, 00-956 Warszawa, Poland*
[e] *Facultat de Matemàtiques i Informatica, Universitat de Barcelona, Gran Via de les Corts Catalanes 585, 08007 Barcelona, Spain*
[f] *Institute of Mathematics, Hebrew University, Givat Ram, Jerusalem 91904, Israel*

MSC:
15B05; 15A05; 13E10; 14M25

Keywords:
Circulant matrix
Permanent
Weak Lefschetz property
Laplace equations
Monomial ideals
Togliatti systems

A B S T R A C T

The goal of this article is to compare the coefficients in the expansion of the permanent with those in the expansion of the determinant of a three-lines circulant matrix. As an application we solve a conjecture stated in [17] concerning the minimality of GT-systems.

* Corresponding author.
E-mail addresses: pietro.depoi@uniud.it (P. De Poi), mezzette@units.it (E. Mezzetti), wajcha2@poczta.onet.pl (M. Michałek), miro@ub.edu (R.M. Miró-Roig), nevo@math.huji.ac.il (E. Nevo).

[1] Member of INdAM - GNSAGA and supported by PRIN "Geometry of algebraic varieties" 2015EYPTSB - PE1.
[2] Supported by the Polish National Science Centre grant no. 2015/19/D/ST1/01180.
[3] Partially supported by MTM2016–78623-P.
[4] Partially supported by grants ISF1695/15, ISF-NRF2528/16 and ISF-BSF2016288.

1. Introduction

Circulant matrices appear naturally in many areas of mathematics. In the last decades, for instance, they have been related to holomorphic mappings ([7]), cryptography, coding theory ([10]), digital signal processing ([9]), image compression ([22]), physics ([2]), engineering simulations, number theory, theory of statistical designs ([12]), etc. Even if the basic facts about these matrices can be proved in elementary way, many questions about them are subtle and remain still open (see, for instance, [11]).

Our interest in this topic was originally motivated by its connections, exposed in [17], with a class of homogeneous ideals of a polynomial ring failing the Weak Lefschetz Property. In that context, the first question relevant to us was that of determining which monomials in the entries of a "generic" circulant matrix appear explicitly in the development of its determinant.

More precisely, let us denote by $\mathrm{Circ}(x_0, x_1 \ldots, x_{d-1})$ the circulant matrix of the form

$$\begin{pmatrix} x_0 & x_1 & x_2 & \cdots & x_{d-1} \\ x_{d-1} & x_0 & x_1 & \cdots & x_{d-2} \\ x_{d-2} & x_{d-1} & x_0 & \cdots & x_{d-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & x_3 & \cdots & x_0 \end{pmatrix},$$

where $x_0, \ldots, x_{d-1}$ are complex numbers, or more generally elements of a ring. Every summand of the determinant $\det \mathrm{Circ}(x_0, x_1 \ldots, x_{d-1})$ is of the form

$$c_{i_0,\ldots,i_{d-1}} x_0^{i_0} \cdots x_{d-1}^{i_{d-1}},$$

where $c_{i_0,\ldots,i_{d-1}} \in \mathbb{Z}$ and $i_0 + \cdots + i_{d-1} = d$. The question is: for which indices $i_0, \ldots, i_{d-1}$ is the coefficient $c_{i_0,\ldots,i_{d-1}}$ different from zero?

An analogous question can be posed for the permanent of $\mathrm{Circ}(x_0, x_1 \ldots, x_{d-1})$. In this case the answer was given in [4], where it was proved that the monomials appearing with non-zero coefficient are precisely those whose exponents satisfy the two conditions:

$$\begin{cases} i_0 + \cdots + i_{d-1} = d \\ 0i_0 + 1i_1 + 2i_2 + \cdots + (d-1)i_{d-1} \equiv 0 \pmod{d}. \end{cases} \tag{1}$$

Clearly, conditions (1) are necessary for the non-vanishing of the coefficient $c_{i_0,\ldots,i_{d-1}}$ in $\det \mathrm{Circ}(x_0, x_1 \ldots, x_{d-1})$. It has been recently proved that they are also sufficient if and only if $d > 1$ is a power of a prime number ([25], [6]).

A more general question is to find a formula for the coefficient $c_{i_0,\ldots,i_{d-1}}$. This problem had already been considered in 1951 by Ore [23], who gave an explicit expression. Other expressions were given more recently in [14], [29]. However, they are not always easy to apply in order to decide if $c_{i_0,\ldots,i_{d-1}}$ vanishes or not.

In this article, we are interested in the so-called r-lines circulant matrices, i.e. circulant matrices $\mathrm{Circ}(x_0, x_1 \ldots, x_{d-1})$ of order $d > r$, where $d - r$ among $x_0, \ldots, x_{d-1}$ are specialized to 0. We ask if for some pairs (r, d), $r < d$, conditions (1) are sufficient for the non-vanishing of the corresponding coefficient in the determinant.

Our main result is Theorem 2.3, where we prove that conditions (1) are sufficient in the case of 3-lines circulant matrices of order d, of the form

$$\mathrm{Circ}(x, 0, \ldots, 0, y, 0, \ldots, 0, z, 0, \ldots, 0),$$

where y appears in position a (counting from zero), z appears in position b, and $\mathrm{GCD}(a, b, d) = 1$.

We also give examples of:

- 3-lines circulant matrices with $\mathrm{GCD}(a,b,d) \neq 1$,
- r-lines circulant matrices with $r \geq 4$ and similar GCD equal to one,

for which the analogous property fails. Moreover, we prove that the coefficient of any specific monomial in a 3-lines circulant determinant is always equal, up to the sign, to the analogous coefficient in the permanent of the same matrix under the assumption $\mathrm{GCD}(a,b,d) = 1$.

Our results are inspired by and extend a previous result, concerning 3-lines circulant matrices of the special form $\mathrm{Circ}(x, y, 0, \ldots, 0, z, 0, \ldots, 0)$, given by Loehr, Warrington and Wilf [13]. This case, i.e. $a = 1$, was also studied by Codenotti and Resta [5] who gave an expression for twice the permanent as a sum of four related determinants. This setting easily extends to the cases when at least one of $\mathrm{GCD}(a,d)$, $\mathrm{GCD}(b,d)$, $\mathrm{GCD}(b-a,d)$ equals 1.

The second part of this article is devoted to describing applications of Theorem 2.3; it concerns mainly the minimality of Galois-Togliatti systems in three variables. These systems, abbreviated GT-systems, form a class of ideals of a polynomial ring introduced and studied in [17]. A GT-system in three variables is the homogeneous artinian ideal $I^d_{a,b}$ of $R := \mathbb{K}[x_0, x_1, x_2]$, generated by all forms of degree d, that are invariant under the action of a diagonal matrix $M_{a,b} := \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^a & 0 \\ 0 & 0 & e^b \end{pmatrix}$, where e is a d-th root of the unit. Note that the group generated by $M_{a,b}$ is the cyclic group of order d provided $\mathrm{GCD}(a,b,d) = 1$, and that all actions of this group on R can be represented by a matrix of the form $M_{a,b}$. In [17] it was proved that, if $\mathrm{GCD}(a,b,d) = 1$, then the ideal $I^d_{a,b}$ is a Togliatti system. This means that it fails the Weak Lefschetz Property in degree $d-1$, i.e. for a general linear form L (equivalently, for all linear forms), the multiplication map $\times L \colon (R/I^d_{a,b})_{d-1} \longrightarrow (R/I^d_{a,b})_d$ is not injective. The authors then conjectured that $I^d_{a,b}$ is a minimal Togliatti system. As an application of Theorem 2.3 we prove this conjecture.

Next we outline the structure of this paper. Section 2 contains our main results about circulant matrices. After introducing r-lines circulant matrices, we give a precise formulation of the problems we want to study (Question 2.2). We then state our main theorems (Theorems 2.3 and 2.4) and produce some examples showing that our results are optimal (Examples 2.6 and 2.7). Subsection 2.2 contains the proofs of the two theorems; it relies on a series of lemmas, aiming to describe the structure, in the symmetric group on d elements, of the permutations that contribute non-trivially in the development of the circulant determinants we study. Section 3 is devoted to the application of the results of Section 2 to Togliatti systems. We first recall the background about the Weak Lefschetz Property and Togliatti systems, in particular minimal monomial Togliatti systems and GT-systems, and the conjecture on the minimality of GT-systems in three variables. Finally, Theorem 3.8 shows how the conjecture follows from the results of Section 2. In Section 4 we indicate a computational complexity application of our main result.

Notation. Throughout this paper $\mathbb{K}$ will be an algebraically closed field of characteristic zero, $R = \mathbb{K}[x_0, x_1, \ldots, x_n]$ and $\mathbb{P}^n = \mathrm{Proj}(\mathbb{K}[x_0, x_1, \ldots, x_n])$. For any polynomial $F \in R$, we denote by $[F]_{i_0,i_1,\ldots,i_n}$ the coefficient of the monomial $x_0^{i_0} x_1^{i_1} \cdots x_n^{i_n}$ in F. Hence, we have $F = \sum_{i_0,i_1,\ldots,i_n} [F]_{i_0,i_1,\ldots,i_n} x_0^{i_0} x_1^{i_1} \cdots x_n^{i_n}$. Let S_d denote the symmetric group on d elements.

2. Three-lines circulant matrices

This section is devoted to the study of circulant matrices and their determinant and permanent. They have been previously studied by Ore [23], Kra and Simanca [11], Wyn-Jones [29] and Malenfant [14]; we will mainly follow Loehr, Warrington and Wilf [13]. Let us start by recalling their definition:

Definition 2.1. Let $M = (y_{i,j})$ be a $d \times d$ matrix. M is a *circulant matrix* if, and only if $y_{i,j} = y_{k,l}$ whenever $j - i \equiv l - k \pmod{d}$. That is, M is of the type

$$\begin{pmatrix} x_0 & x_1 & x_2 & \cdots & x_{d-1} \\ x_{d-1} & x_0 & x_1 & \cdots & x_{d-2} \\ x_{d-2} & x_{d-1} & x_0 & \cdots & x_{d-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & x_3 & \cdots & x_0 \end{pmatrix}$$

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 short we denote such matrices as $\mathrm{Circ}_d(x_0, x_1 \ldots, x_{d-1})$ or simply Circ_d.

We now define an *r-lines circulant matrix* as follows: we fix an integer $r \leq d$ and an r-tuple of integers $0 \leq \alpha_0 < \cdots < \alpha_{r-1} \leq d-1$ and define

$$\mathrm{Circ}_{(d;\alpha_0,\ldots,\alpha_{r-1})} := (\mathrm{Circ}_d)(0,\ldots,0,x_{\alpha_0},0,\ldots,0,x_{\alpha_i},0,\ldots,0,x_{\alpha_{r-1}},0\ldots,0)$$

where x_{α_i} is located at the $\alpha_i + 1$ position. Notice that $\mathrm{Circ}_{(d;\alpha_0,\ldots,\alpha_{r-1})}$ is nothing but the specialization of Circ_d to $\{x_i = 0 \mid i \notin \{\alpha_0,\ldots,\alpha_{r-1}\}\}$. Let us denote by $D_{(d;\alpha_0,\ldots,\alpha_{r-1})}$ (resp. $P_{(d;\alpha_0,\ldots,\alpha_{r-1})}$) the number of different monomials that appear with non-zero coefficient in the expansion of the determinant $\det(\mathrm{Circ}_{(d;\alpha_0,\ldots,\alpha_{r-1})})$ (resp. permanent $\mathrm{per}(\mathrm{Circ}_{(d;\alpha_0,\ldots,\alpha_{r-1})})$). We always have $D_{(d;\alpha_0,\ldots,\alpha_{r-1})} \leq P_{(d;\alpha_0,\ldots,\alpha_{r-1})}$ and we are lead to pose the following questions:

Question 2.2. *Fix integers $r \leq d$ and an r-tuple of integers $0 \leq \alpha_0 < \cdots < \alpha_{r-1} \leq d-1$.*

(1) *Is $D_{(d;\alpha_0,\ldots,\alpha_{r-1})} = P_{(d;\alpha_0,\ldots,\alpha_{r-1})}$?*
(2) *More strongly, comparing coefficients, is*

$$[\det(\mathrm{Circ}_{(d;\alpha_0,\ldots,\alpha_{r-1})})]_{d-A_1-\cdots-A_{r-1},A_1,\ldots,A_{r-1}} =$$
$$\pm[\mathrm{per}(\mathrm{Circ}_{(d;\alpha_0,\ldots,\alpha_{r-1})})]_{d-A_1-\cdots-A_{r-1},A_1,\ldots,A_{r-1}}?$$

In this paper, we deal with 3-lines circulant matrices. Without loss of generality we can always assume $\alpha_0 = 0$ and we set $a = \alpha_1$ and $b = \alpha_2$. We answer both questions affirmatively under the condition $\mathrm{GCD}(a,b,d) = 1$:

Theorem 2.3. *Fix integers $d \geq 3$ and $1 \leq a < b \leq d-1$. Assume $\mathrm{GCD}(a,b,d) = 1$. Then, $[\det(\mathrm{Circ}_{(d;0,a,b))})]_{d-A-B,A,B} = \pm[\mathrm{per}(\mathrm{Circ}_{(d;0,a,b))})]_{d-A-B,A,B}$. In particular, $D_{(d;0,a,b)} = P_{(d;0,a,b)}$.*

The case $a = 1$ in the above theorem was established in [13], and our proof strategy largely follows theirs. In fact, our proof gives the sign, as well as a combinatorial interpretation of the magnitude, for the coefficients of $\det(\mathrm{Circ}_{(d;0,a,b))})$:

Theorem 2.4. *Fix integers $d \geq 3$ and $1 \leq a < b \leq d-1$ such that $\mathrm{GCD}(a,b,d) = 1$. Then, for any nonnegative integers A, B such that $A + B \leq d$,*

(1) *$[\det(\mathrm{Circ}_{(d;0,a,b))})]_{d-A-B,A,B} \neq 0$ if and only if $d|(aA+bB)$.*

Further, assuming $d|(aA+bB)$, then:

(2) *the sign of $[\det(\mathrm{Circ}_{(d;0,a,b))})]_{d-A-B,A,B}$ is $+$ if and only if at least one of $\mathrm{GCD}(A, B, \frac{aA+bB}{d})$ and $A+B-1$ is even; and*

(3) *the magnitude of* $[\det(\mathrm{Circ}_{(d;0,a,b)})]_{d-A-B,A,B}$ *equals the number of permutations in* S_d *with cycle decomposition* $C_1 \circ C_2 \circ \cdots \circ C_k$*, where* $k = \mathrm{GCD}(A, B, \frac{aA+bB}{d})$*, and each* C_i *has length* $A+B$ *and consists of exactly* A *elements* j *with* $C_i(j) \equiv j+a$ *and* B *elements* j *with* $C_i(j) \equiv j+b$*, modulo* d*.*

Remark 2.5. For $r = 2$ we may assume $\alpha_0 = 0$ and $\alpha_1 = a$ divides d, with x on the main diagonal and y on another nontrivial diagonal of the circulant $d \times d$-matrix. One easily verifies that all coefficients of the determinant $\det(\mathrm{Circ}_{(d;0,a)})$ equal up to sign to the corresponding coefficients in the permanent $\mathrm{per}(\mathrm{Circ}_{(d;0,a)})$, and are given by the explicit formula

$$\det(\mathrm{Circ}_{(d;0,a)}) = \sum_{s=0}^{a} (-1)^{(a-s)(\frac{d}{a}-1)} \binom{a}{s} x^{\frac{ds}{a}} y^{\frac{d(a-s)}{a}}.$$

However, for $r = 3$, the following example shows that the assumption $\mathrm{GCD}(a, b, d) = 1$ cannot be dropped from Theorem 2.3:

Example 2.6. Indeed, we take $(a, b, d) = (2, 6, 12)$. We compute the permanent and the determinant of $\mathrm{Circ}_{(12;0,2,6)}$ and get:

$$\begin{aligned}\det(\mathrm{Circ}_{(12;0,2,6)}) = {} & x^{12} - 6x^{10}y^2 + 15x^8y^4 - 20x^6y^6 + 15x^4y^8 - 6x^2y^{10} + \\ & + y^{12} - 12x^8yz^3 + 32x^6y^3z^3 - 24x^4y^5z^3 + 4y^9z^3 - 2x^6z^6 + 42x^4y^2z^6 + 18x^2y^4z^6 + \\ & + 6y^6z^6 + 12x^2yz^9 + 4y^3z^9 + z^{12}\end{aligned}$$

and

$$\begin{aligned}\mathrm{per}(\mathrm{Circ}_{(12;0,2,6)}) = {} & x^{12} + 6x^{10}y^2 + 15x^8y^4 + 20x^6y^6 + 15x^4y^8 + 6x^2y^{10} + \\ & + y^{12} + 12x^8yz^3 + 40x^6y^3z^3 + 48x^4y^5z^3 + 24x^2y^7z^3 + 4y^9z^3 + 2x^6z^6 + 42x^4y^2z^6 + \\ & + 30x^2y^4z^6 + 6y^6z^6 + 12x^2yz^9 + 4y^3z^9 + z^{12}.\end{aligned}$$

Therefore, we have

$$D_{(12;0,2,6)} = 18 < P_{(12;0,2,6)} = 19$$

and

$$[\det(\mathrm{Circ}_{(12;0,2,6))})]_{6,3,3} = 32 \neq [\mathrm{per}(\mathrm{Circ}_{(12;0,2,6))})]_{6,3,3} = 40.$$

Example 2.7. For r-lines circulant matrices with $r \geq 4$ Theorem 2.3 is no longer true. In fact,

1. For $r = 4$, we have $D_{(6;0,2,4,5)} < P_{(6;0,2,4,5)}$ since the monomial xz^2uv^2 appears in $\mathrm{per}(\mathrm{Circ}(x, 0, z, 0, u, v))$ but it does not appear in $\det(\mathrm{Circ}(x, 0, z, 0, u, v))$ (see [6] and [5, Example 3]).
2. Assume $r \geq 5$. We choose two prime integers p and q such that $p < q$ and $r \leq pq$. Set $d = pq$. We will first prove that $D_{(d;0,1,\ldots,d-1)} < P_{(d;0,1,\ldots,d-1)}$. To this end we exhibit a d-tuple $A_0, A_1, \ldots, A_{d-1}$ such that

$$\begin{aligned} A_0 + 2A_1 + \cdots + dA_{d-1} &\equiv 0 \pmod{d} \\ A_0 + A_1 + \cdots + A_{d-1} &= d \end{aligned}$$

and

$$[\det(\mathrm{Circ}_{(d;0,1,\dots,d-1)})]_{A_0,A_1,\dots,A_{d-1}} = 0.$$

We apply Bezout's theorem and we write $\lambda q = 1+\mu p$ with $1 \le \lambda, \mu$ and $\lambda q < d$. We define $A_0 = d-\mu p-2$, $A_1 = \mu p-1$, $A_{d-\mu p} = A_{\mu p-\mu\lambda+1} = A_{d-\mu p+\lambda\mu} = 1$, and $A_i = 0$ for $i \neq 0, 1, d-\mu p, \mu p-\mu\lambda+1, d-\mu p+\lambda\mu$. By the proof of [6, Theorem 3.5], $[\det(\mathrm{Circ}_{(d;0,1,\dots,d-1)})]_{A_0,A_1,\dots,A_{d-1}} = 0$, i.e. the monomial $x_0^{d-\mu p-2}x_1^{\mu p-1}x_{d-\mu p}x_{\mu p-\lambda\mu+1}x_{d-\mu p+\lambda\mu}$ appears in $\mathrm{per}(\mathrm{Circ}(x_0, x_1 \dots, x_{d-1}))$ but it does not appear in $\det(\mathrm{Circ}(x_0, x_1 \dots, x_{d-1}))$. Therefore, $D_{(d;0,1,\dots,d-1)} < P_{(d;0,1,\dots,d-1)}$.
Since $5 \le r \le d$, for any choice of an r-tuple $(a_0, a_1, \dots, a_{r-1})$ containing $\{0, 1, d-\mu p, \mu p-\mu\lambda+1, d-\mu p+\lambda\mu\}$, the monomial $x_0^{d-\mu p-2}x_1^{\mu p-1}x_{d-\mu p}x_{\mu p-\lambda\mu+1}x_{d-\mu p+\lambda\mu}$ appears in the permanent of the $d \times d$ r-lines circulant matrix $\mathrm{Circ}_{(d;a_0,a_1,\dots,a_{r-1})}$ but it does not appear in the determinant. Therefore, $D_{(d;a_0,a_1,\dots,a_{r-1})} < P_{(d;a_0,a_1,\dots,a_{r-1})}$ and we are done.

2.1. Notation

For a permutation σ of d elements $I := \{0, \dots, d-1\}$ and an integer q, we define

$$S_{q,\sigma} := \{i \in I \mid \sigma(i) \equiv i + q \pmod d\}.$$

Let:

$$P_{a,b,d,A,B} := \{\sigma \in S_d \mid |S_{a,\sigma}| = A, |S_{b,\sigma}| = B, |S_{0,\sigma}| = d - A - B\}.$$

The permutations in $P_{a,b,d,A,B}$ can be characterized as those in S_d where each i is either fixed, i.e. $\sigma(i) = i$, or translated a or b steps forward, i.e. $\sigma(i) \equiv i+a$ or $\sigma(i) \equiv i+b \pmod d$, and further, the second situation $\sigma(i) \equiv i + a$ happens exactly A times and the last one exactly B times. Clearly,

Lemma 2.8. *The following equalities hold:*

$$[\det(\mathrm{Circ}_{(d;0,a,b)})]_{d-A-B,A,B} = \sum_{\sigma \in P_{a,b,d,A,B}} \mathrm{sgn}(\sigma),$$

$$[\mathrm{per}(\mathrm{Circ}_{(d;0,a,b)})]_{d-A-B,A,B} = \sum_{\sigma \in P_{a,b,d,A,B}} |\mathrm{sgn}(\sigma)| = |P_{a,b,d,A,B}|. \quad \square$$

We often work with cyclic indices, say modulo d: an element in $\mathbb{Z}/d\mathbb{Z}$ is uniquely determined by an element in $s \in I = \{0, \dots, d-1\}$; by abuse of notation, we frequently identify in what follows this integer s with its class in $\mathbb{Z}/d\mathbb{Z}$. With this identification, we will write $s_1 < s_2 < s_3 < \cdots$, with $s_i \in \mathbb{Z}/d\mathbb{Z}$ if, for the corresponding elements in I we have $0 < s_2 - s_1 < s_3 - s_1 < \cdots$.

Example 2.9. We have $4 < 1 < 2$ modulo 5, as $0 < 2 < 3$. On the other hand it is not true that $1 < 3 < 2$.

2.2. Structure of permutations

In this subsection we fix a permutation $\sigma \in P_{a,b,d,A,B}$ and its canonical cycle decomposition $\sigma = C_1 \circ C_2 \circ \cdots \circ C_k$. We set $A_i = |S_{a,C_i}|$, $B_i = |S_{b,C_i}|$ and "winding number" $\ell_i = \frac{A_i a + B_i b}{d}$. Our aim is to prove, in steps, that the canonical cycle decomposition $\sigma = C_1 \circ C_2 \circ \cdots \circ C_k$ must be of a very special type, as described in Theorem 2.4(3), and in particular all permutations $\sigma \in P_{a,b,d,A,B}$ have the same cycle structure, hence the same sign, implying Theorem 2.3.

The following lemma is a straightforward generalization of [13, Lemma 7], where the case $a = 1$ was considered. We include the proof for the sake of completeness.

Lemma 2.10. *For any integer i, $1 \leq i \leq k$, we have* $\mathrm{GCD}(A_i, B_i, \ell_i) = 1$.

Proof. Let $g := \mathrm{GCD}(A_i, B_i, \ell_i)$. We consider the cycle $C_i = (s_1, \ldots, s_w)$, where $w = A_i + B_i$ and $s_j \in \mathbb{Z}/d\mathbb{Z}$. Let $w = gw'$. To simplify notation we assume that the indexes j of each s_j are considered modulo w. We know that $s_{j+1} - s_j$ is congruent either to a or b. Hence, we may represent C_i as a word W of length w with letters a, b:

$$W := s_2 - s_1, s_3 - s_2, \ldots, s_w - s_{w-1}, s_1 - s_w =: p_1 \cdots p_w.$$

Claim: There exists a subword $W' = p_{w_0+1}, p_{w_0+2}, \ldots, p_{w_0+w'}$ of the word W such that:

1. the number of a's in W' equals A_i/g and
2. the number of b's in W' equals B_i/g.

Proof of the claim. As the length of the word W' is fixed to be w', the number of letters b is determined by the number of letters a in it. Hence, it is enough to find W' that satisfies the first condition.

The word W is a concatenation of g words of length w/g:

$$W = W_1 \cdots W_g.$$

If one of the W_j's has A_i/g letters a the claim follows. Hence, we assume each of them has either strictly more or strictly less letters a then A_i/g. As the total number of letters a in W equals A_i, it is not possible that all words W_j have simultaneously more or simultaneously less letters a then A_i/g. Thus, we may find two consecutive words W_j, W_{j+1} and assume without loss of generality that W_j has less and W_{j+1} has more than A_i/g letters a. Consider the sequence of all subwords of W_jW_{j+1} of length w' ordering them by the starting index:

$$W_j = W'_1, W'_2, \ldots, W'_{w'+1} = W_{j+1}.$$

The word W'_{s+1} is shifted by one index to the right, with respect to the word W'_s. In particular, W'_{s+1} is getting exactly one additional letter and looses exactly one letter. Hence, the number of letters a in W'_s and W'_{s+1} may differ by at most one. In particular, as the starting word $W_j = W'_1$ has less than A_i/g letters a and the last word $W_{j+1} = W'_{w'+1}$ has more than A_i/g letters a, there must exist a word $W' = W'_s$ with precisely A_i/g letters a. □

We may cyclically permute the entries $(s_1, \ldots, s_w)$ of C_i. By the Claim we may assume that in the multiset $\{s_2 - s_1, s_3 - s_2, \ldots, s_{w'} - s_{w'-1}, s_{w'+1} - s_{w'}\}$ there are precisely A_i/g differences a and B_i/g differences b. Summing up all the elements of this multiset modulo d we obtain:

$$s_{w'+1} - s_1 = a\frac{A_i}{g} + b\frac{B_i}{g} = \frac{aA_i + bB_i}{g} = \frac{\ell_i d}{g} = \frac{\ell_i}{g}d \equiv 0 \pmod{d}.$$

Hence, $s_{w'+1} \equiv s_1$. As the cycle C_i was assumed to be primitive, the s_j's must be all distinct. Hence, $w' + 1 = 1$ modulo w, which means that $w' = w$ and $g = 1$. □

Lemma 2.11. *Suppose $\ell_1 = \ell_2 = 1$. Then $A_1 = A_2$ and $B_1 = B_2$.*

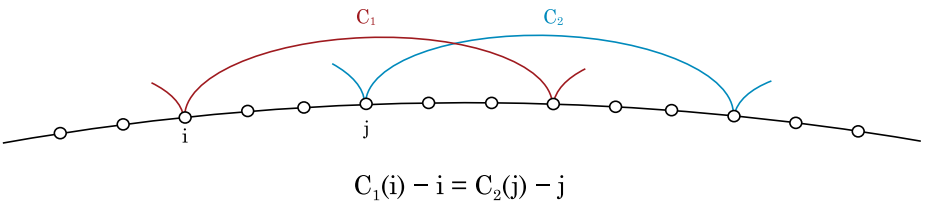

Fig. 1. Two cycles C_1 and C_2 with $i < j < C_1(i)$ as in the Claim in proof of Lemma 2.11.

Proof. **First** we treat the special case when one of the numbers A_1, A_2, B_1, B_2 equals 0, say $B_1 = 0$. As $\ell_1 = 1$ we have $d = a \cdot A_1$ and without loss of generality we may assume that C_1 consists of all numbers divisible by a. If $B_2 = 0$ we are done. We assume $B_2 \neq 0$ in order to obtain a contradiction. Let $C_2 = (s_1, \ldots, s_w)$ for $w = A_2 + B_2$. As C_1 and C_2 are disjoint, we know that each s_i is not divisible by a. As $a|d$ and $\mathrm{GCD}(a, b, d) = 1$ we have $\mathrm{GCD}(a, b) = 1$. Let $0 \leq t < a$ be such that $tb \equiv -s_1$ modulo a. We have $A_2 a + B_2 b = d$ thus $a|B_2 b$ and hence $a|B_2$. In particular $B_2 \geq a > t$. Hence, there exists such s_{i_0} that

$$|\{1 \leq i < i_0 : s_{i+1} = s_i + b\}| = t,$$

i.e. until i_0, the cycle C_2 made exactly t jumps of size b. Modulo a we have:

$$s_{i_0} = s_1 + tb = s_1 - s_1 = 0,$$

which gives the contradiction.

Hence, from now on we assume that all A_1, A_2, B_1, B_2 are nonzero. Without loss of generality we may assume $A_1 + B_1 \leq A_2 + B_2$. Our proof is inductive on the length of the cycle C_1, i.e. on $A_1 + B_1$.

Base of induction: $A_1 + B_1 = 2$. As $A_1, B_1 \neq 0$ we have $A_1 = B_1 = 1$. Thus $d = a + b$. We also have $A_2 a + B_2 b = d = a + b$. As $A_2, B_2 \neq 0$ we must have $A_2 = B_2 = 1 = A_1 = B_1$.

Inductive step: We start by proving the following statement illustrated on Fig. 1.

Claim: There exist i, j such that:

- $C_1(i) - i = C_2(j) - j \neq 0$,
- $i < j < C_1(i)$ or $j < i < C_2(j)$ with a cyclic ordering modulo d.

Proof of the claim. We know that $A_1, B_1 \neq 0$ thus without loss of generality we may consider i' such that $C_1(i') = i' + a$ and $C_1(i' + a) = i' + a + b$. Presenting $C_2 = (s_1, \ldots, s_w)$ for $w = A_2 + B_2$, we may find $s_{j'} < i' + a < s_{j'+1}$.

If $s_{j'+1} - s_{j'} = a$, then setting $i = i'$ and $j = s_{j'}$ we obtain the desired indices.

If $s_{j'+1} - s_{j'} = b$, then we set $j = s_{j'}$ and $i = i' + a$ to conclude. □

By interchanging C_1 and C_2 and a and b if needed, by the above Claim we may assume that there are indices i, j such that $C_1(i) - i = C_2(j) - j = b$ and $i < j < C_1(i)$, cf. Fig. 1. As $\ell_1 = 1$, for $i < k < j$ we have $C_1(k) = k$.

Next, we show how to conclude in a special **Case I**, depicted on Fig. 2 when there exist i, j such that:

- for all $i < k < j$ we have $C_2(k) = k$; in other words k does not belong to any of the two cycles.

Let $d' = d - b$. We will define two disjoint cycles C_1' and C_2' that will be permutations of $\{1, 2, \ldots, d'\}$. The cycle C_i' will have exactly A_i steps of size a and $B_i - 1$ steps of size b. As $\mathrm{GCD}(d', a, b) = \mathrm{GCD}(d, a, b) = 1$ this will allow us to conclude by induction. Let $C_2 = (s_1, \ldots, j, j + b, \ldots, s_w)$ for $w = A_2 + B_2$ be presented in such a way that $s_1 < s_2 \cdots < s_w$. We define C_2' by removing $j + b$ and decreasing all indices after it

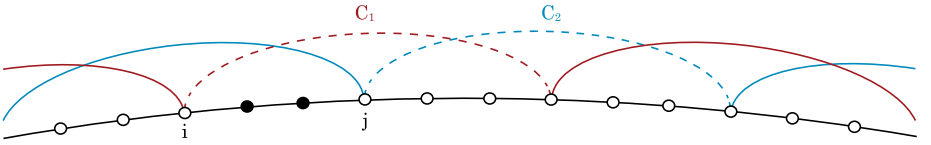

Fig. 2. Two cycles C_1 and C_2 with $i < j < C_1(i)$ as in Case I in proof of Lemma 2.11. The black dots do not belong to either cycle. The dashed lines indicate the parts of the cycles that will be contracted in the inductive proof.

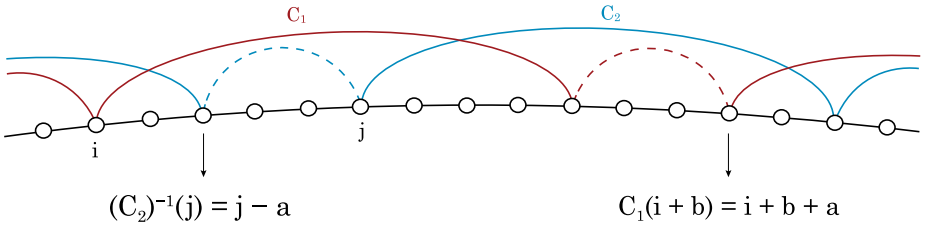

Fig. 3. Two cycles C_1 and C_2 with $i < j < C_1(i)$ as in Case II in proof of Lemma 2.11. The dashed lines indicate the parts of the cycles that will be contracted in the inductive proof.

by b: $C_2' = (s_1, \ldots, j, \ldots, s_w - b)$. Similarly, we present C_1 as $(s_1', \ldots, i, i+b, \ldots s_{w'}')$ for $w' = A_1 + B_1$. The cycle C_1' removes $i+b$ and decreases all indices after it by b: $C_1' = (s_1', \ldots, i, \ldots, s_{w'}' - b)$. The only nontrivial claim is that C_1' and C_2' are disjoint. Consider C_1'. The indices $s_1', \ldots, i$ are distinct from $s_1, \ldots, j$ as C_1 and C_2 were disjoint. Also $s_1', \ldots, i$ are distinct from $s_\ell - b > j$ for $s_\ell > j$, as $i < j$. It remains to consider elements of C_1' that are larger than i. Consider such an element $s_\ell' - b > i$. By assumption the index preceding j in C_1 is smaller than i. Thus $s_\ell' - b$ could only coincide with the second part of elements of C_2: $j = j + b - b, \ldots, s_w - b$. However, $s_\ell' - b = s_q - b$ would imply that $s_\ell' = s_q$, which is not possible. This finishes the proof in the special Case I.

Case II: If we are not in the special Case I, we must have $i < (C_2)^{-1}(j) < j$, cf. Fig. 3. This implies $j - (C_2)^{-1}(j) = a$ and $a < b$. By inverting the direction of both cycles we see that we may also assume that $C_1(i+b) = i + b + a$. In analogy to Case I, we set $d' = d - a$ and we will define two cycles C_1' and C_2'. Precisely if $C_2 = (s_1, \ldots, j-a, j, j+b, \ldots, s_w)$ let $C_2' = (s_1, \ldots, j-a, j+b-a, \ldots, s_w - a)$, and if $C_1 = (s_1', \ldots, \mathbf{i}, i+b, i+b+a, \ldots, s_{w'})$ let $C_1' = (s_1', \ldots, i, i+b, \ldots, s_{w'} - a)$. It is straightforward to check, as in the Case I, that the cycles C_1' and C_2' are disjoint. We conclude by induction. □

Remark 2.12. Lemma 2.11 may not hold when $\mathrm{GCD}(a, b, d) \neq 1$. Indeed, consider $d = 8$, $a = 2$, $b = 4$. Let $\sigma = (0, 2, 4, 6) \circ (1, 5)$. Clearly the two cycles in the decomposition do not satisfy the conclusion of the lemma.

Lemma 2.13. *For any $1 \leq i, j \leq k$ we have $A_i = A_j$ and $B_i = B_j$.*

Proof. Without loss of generality we assume $i = 1$ and $j = 2$.

Our aim is to rearrange the cycles C_1 and C_2, possibly changing a, b, d, in such a way that we can apply Lemma 2.11.

Reduction 1: We first reduce to the situation when $a|d$ and $\mathrm{GCD}(a, b) = 1$. Precisely, we construct new cycles, without changing A_1, A_2, B_1, B_2 and d, however with new a' and b', such that $\mathrm{GCD}(a', b') = 1$ and $a'|d$.

Let $a' := \mathrm{GCD}(a, d)$ and $a = za'$. Let $z' < d$ be such that $z \cdot z' \equiv 1$ modulo d. Let $d > b' := bz'$ modulo d. We rearrange the rests $\{0, 1, \ldots, d-1\}$ modulo d by multiplying them by z'. Precisely, we change the cycle $C_1 = (s_1, \ldots, s_{A_1+B_1})$ and $C_2 = (s_1', \ldots, s_{A_2+B_2}')$ respectively to $C_1' = (z's_1, \ldots, z's_{A_1+B_1})$ and $C_2' = (z's_1', \ldots, z's_{A_2+B_2}')$. These are clearly two disjoint cycles with possible differences a' and b'. Further

$a'|d$ and $\mathrm{GCD}(a', b', d) = \mathrm{GCD}(a', bz', d)$. Note that $\mathrm{GCD}(a', b, d) = 1$ (as $a'|a$) and $\mathrm{GCD}(a', z', d) = 1$ (as z' and d are coprime), hence $\mathrm{GCD}(a', b', d) = 1$.

Reduction 2: Let C_i' be as above, $i = 1, 2$. We now reduce to the case of winding numbers $\ell_1 = \ell_2 = 1$. Let $m := \mathrm{GCD}(\ell_1, \ell_2)$ and $\ell_1 = m\ell_1'$, $\ell_2 = m\ell_2'$.

Let $d' = dm\ell_1'\ell_2' = d\,\mathrm{LCM}(\ell_1, \ell_2)$. We extend the cycle C_1' (that is a permutation of d elements) to a cycle C_1'' (that is a permutation of d' elements) as follows. Say $C_1' = (c_1, \ldots, c_{A_1+B_1})$, where c_1 is the smallest integer appearing in C_1'. We may encode it as a word, with letters a' and b', of length $A_1 + B_1$:

$$w := c_2 - c_1, \ldots, c_{A_1+B_1} - c_{A_1+B_1-1}.$$

We concatenate the word w with itself ℓ_2' times, obtaining a word $w^{\circ\ell_2'}$ with exactly $A_1\ell_2'$ letters a' and $B_1\ell_2'$ letters b'. The word $w^{\circ\ell_2'}$ encodes the cycle C_1'', that starts at c_1 with differences $c_{i+1} - c_i$ equal to either a' or b', according to $w^{\circ\ell_2'}$. In the analogous way we obtain a cycle C_2'' with $A_2\ell_1'$ differences a' and $B_2\ell_2'$ differences b'.

We are now in position to apply Lemma 2.11. As $a'|d$, we must have $\mathrm{GCD}(a', b') = 1$. In particular, $\mathrm{GCD}(a', b', d') = 1$. Further, the cycles C_1'' and C_2'' have their winding numbers $\ell_1'' = \ell_2'' = 1$. They are also disjoint, as their reductions modulo d coincide with C_1 and C_2 that are disjoint. Hence, by Lemma 2.11, $A_1\ell_2' = A_2\ell_1'$ and $B_1\ell_2' = B_2\ell_1'$.

In particular, $\ell_1'|A_1\ell_2'$ and as $\mathrm{GCD}(\ell_1', \ell_2') = 1$ we have $\ell_1'|A_1$. In the same way $\ell_1'|B_1$ and by definition $\ell_1'|\ell_1$. Thus, by Lemma 2.10 we must have $\ell_1' = 1$. Analogously $\ell_2' = 1$. Hence, indeed $A_1 = A_2$ and $B_1 = B_2$. □

Recall $A = \sum_{i=1}^k A_i$, $B = \sum_{i=1}^k B_i$, and let $\ell := \frac{aA+bB}{d}$.

Lemma 2.14. *We have* $k = \mathrm{GCD}(A, B, \ell)$.

Proof. By Lemma 2.13 we know that $A = kA_1$, $B = kB_1$ and $\ell = k\ell_1$. We conclude by Lemma 2.10:

$$k = k\,\mathrm{GCD}(A_1, B_1, \ell_1) = \mathrm{GCD}(kA_1, kB_1, k\ell_1) = \mathrm{GCD}(A, B, \ell). \quad \square$$

By Lemma 2.8, the results of this subsection imply Theorems 2.3 and 2.4. □

3. On the minimality of GT-systems

In this section, we will apply the results on the determinant of a three-lines circulant matrix obtained in the previous section to study the minimality of GT-systems and to solve a conjecture stated by Mezzetti and Miró-Roig in [17]. To state this conjecture we need first to introduce some definitions.

Definition 3.1. Let $I \subset R$ be a homogeneous artinian ideal. We say that I has the *Weak Lefschetz Property* (WLP, for short) if there is a $L \in [R/I]_1$ such that, for all integers j, the multiplication map

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

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

To establish whether an ideal $I \subset R$ has the WLP is a difficult and challenging problem and even in simple cases, such as complete intersections, much remains unknown about the presence of the WLP. Recently the failure of the WLP has been connected to a large number of problems, that appear to be unrelated at first glance. For example, in [15], Mezzetti, Miró-Roig and Ottaviani proved that the failure

of the WLP is related to the existence of varieties satisfying at least one Laplace equation of order greater than 2; we recall that a k-dimensional variety $X \subset \mathbb{P}^n$ *satisfies r Laplace equations of order d* if for any parametrization $F = F(t_1, \dots, t_k)$ of X around a smooth, general point, F satisfies a system of r (linearly independent) PDE's with constant coefficients of order d. Their result is the following:

Theorem 3.2. *([15, Theorem 3.2]) Let $I \subset R$ be an artinian ideal generated by r homogeneous polynomials $F_1, \dots, F_r$ 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 $F_1, \dots, F_r$ become k-linearly dependent on a general hyperplane H of $\mathbb{P}^n$;*
(3) *the n-dimensional variety $X = \overline{\mathrm{Im}(\varphi)}$ where $\varphi \colon \mathbb{P}^n \dashrightarrow \mathbb{P}^{\binom{n+d}{d}-r-1}$ is the rational map associated to $(I^{-1})_d$, satisfies at least one Laplace equation of order $d-1$.*

The above result motivated the following definitions:

Definition 3.3. 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 3.2.
(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 defining a monomial Togliatti system.

These definitions were introduced in [15] and [16] and the names are in honor of Eugenio Togliatti who proved that for $n = 2$ the only smooth Togliatti system of cubics is

$$I = (x_0^3, x_1^3, x_2^3, x_0x_1x_2) \subset \mathbb{K}[x_0, x_1, x_2]$$

(see [3], [26] and [27]). The systematic study of Togliatti systems was initiated in [15] and for recent results the reader can see [18], [16], [1], [20] and [17]. Precisely in the latter reference the authors introduced the notion of *GT-system* which we recall now.

Definition 3.4. A *GT-system* is an artinian ideal $I \subset \mathbb{K}[x_0, x_1, \dots, x_n]$ generated by r forms $F_1, \dots, F_r$ of degree d such that:

i) I is a Togliatti system.
ii) The regular map $\phi_I \colon \mathbb{P}^n \to \mathbb{P}^{r-1}$ defined by $(F_1, \dots, F_r)$ is a Galois covering of degree d with cyclic Galois group $\mathbb{Z}/d\mathbb{Z}$.

Any representation of the cyclic group $\mathbb{Z}/d\mathbb{Z}$ as subgroup of $GL(n+1, \mathbb{K})$ can be diagonalized. In particular it is represented by a matrix of the form

$$M := M_{\alpha_0, \alpha_1, \dots, \alpha_n} = \begin{pmatrix} e^{\alpha_0} & 0 & \dots & 0 \\ 0 & e^{\alpha_1} & \dots & 0 \\ & & \dots & \\ 0 & 0 & \dots & e^{\alpha_n} \end{pmatrix}$$

where e is a primitive dth root of 1 and $\alpha_0, \alpha_1, \dots, \alpha_n$ are integers with

$$\mathrm{GCD}(\alpha_0, \alpha_1, \dots, \alpha_n, d) = 1.$$

It follows (see [6, Proposition 4.6]) that the above definition is equivalent to the next one:

Definition 3.5. Fix integers $3 \leq d \in \mathbb{Z}$, $2 \leq n \in \mathbb{Z}$, with $n \leq d$, and $0 \leq \alpha_0 \leq \alpha_1 \leq \cdots \leq \alpha_n \leq d$, e a primitive d-th root of 1 and $M_{\alpha_0,\alpha_1,\dots,\alpha_n}$ a representation of $\mathbb{Z}/d\mathbb{Z}$ in $GL(n+1, \mathbb{K})$. A *GT-system* will be an ideal

$$I^d_{\alpha_0,\dots,\alpha_n} \subset \mathbb{K}[x_0, x_1, \dots, x_n]$$

generated by all forms of degree d invariant under the action of $M_{\alpha_0,\alpha_1,\dots,\alpha_n}$ provided the number of generators $\mu(I^d_{\alpha_0,\dots,\alpha_n}) \leq \binom{n+d-1}{n-1}$.

Remark 3.6. It is an immediate consequence of the above description that the ideal $I^d_{\alpha_0,\dots,\alpha_n}$ is always monomial, i.e. a GT-system is a monomial Togliatti system.

Remark 3.7. Indeed in the proof of [6, Proposition 4.6], the authors observed that $I := I^d_{\alpha_0,\dots,\alpha_n}$ fails the Weak Lefschetz Property from degree $d-1$ to degree d, because for any linear form $\ell \in R$ the induced map $\times\ell : [R/I]_{d-1} \longrightarrow [R/I]_d$ is not injective. By [19, Proposition 2.2], since I is monomial, it is enough to check it for $\ell = x_0 + x_1 + \cdots + x_n$. This is equivalent to prove that there exists a form $F_{d-1} \in R$ of degree $d-1$ such that $(x_0 + x_1 + \cdots + x_n) \cdot F_{d-1} \in I$. Consider $F_{d-1} = (e^{\alpha_0}x_0 + e^{\alpha_1}x_1 + \cdots + e^{\alpha_n}x_n)(e^{2\alpha_0}x_0 + e^{2\alpha_1}x_1 + \cdots + e^{2\alpha_n}x_n)\dots(e^{(d-1)\alpha_0}x_0 + e^{(d-1)\alpha_1}x_1 + \cdots + e^{(d-1)\alpha_n}x_n)$. The homogeneous form of degree d, $F = (x_0 + x_1 + \cdots + x_n) \cdot F_{d-1}$ is invariant under the action of $M_{\alpha_0,\alpha_1,\dots,\alpha_n}$, hence, it belongs to I.

In the following, since we are interested in the projective space and in the action of $M_{\alpha_0,\alpha_1,\dots,\alpha_n}$ up to proportionality, we will assume that the first exponent α_0 is equal to zero. Moreover, R will always denote the polynomial ring in three variables: $R = \mathbb{K}[x, y, z]$.

To determine the minimality of a GT-system is a subtle problem. In [17], in the case of three variables, the second and fourth authors proved that the ideal $I^d_{0,a,b}$ always satisfies the condition on the number of generators $\mu(I) \leq d+1$, and conjectured the following, which we now prove using Theorem 2.3:

Theorem 3.8. *([17, Conjecture 4.6]) Let $d \geq 3$ be an integer and $M_{a,b}$ be a 3×3-matrix representing the cyclic group $\mathbb{Z}/d\mathbb{Z}$ with $1 \leq a < b \leq d-1$ such that $\mathrm{GCD}(a, b, d) = 1$. Let $I = I^d_{0,a,b} \subset R = \mathbb{K}[x, y, z]$ be the ideal generated by all the monomials of degree d invariant under the action of $M_{a,b}$. Then I is a minimal GT-system.*

Proof. As observed in Remark 3.7, the form

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

is in the kernel of $\times(x + y + z) : [R/I]_{d-1} \to [R/I]_d$, so the dimension of the kernel is ≥ 1, thus I is a GT-system. We now work towards showing its minimality.
Claim: The dimension of the kernel K_{d-1} of $\times(x + y + z) : [R/I]_{d-1} \to [R/I]_d$ is one.

Proof of the claim. We will prove that F_{d-1} generates K_{d-1}.

Assume that $G_{d-1}(x, y, z)$ is a form of degree $d-1$ which belongs to K_{d-1}. We will prove that $(x+e^a y+e^b z)$ divides $G_{d-1}(x, y, z)$. Analogously the other factors of F_{d-1} divide $G_{d-1}(x, y, z)$, and we are done. Since $G_{d-1}(x, y, z)$ belongs to K_{d-1}, we have $(x + y + z)G_{d-1}(x, y, z) \in I$. So the form $H(x, y, z) := (x + y + z)$ $G_{d-1}(x, y, z)$ of degree d is in I.

Since $H(x,y,z)$ belongs to I, it is invariant under the action of $M_{a,b}$ and we have

$$(x+e^a y+e^b z)G_{d-1}(x,e^a y,e^b z) = H(x,e^a y,e^b z) = H(x,y,z) = (x+y+z)G_{d-1}(x,y,z),$$

which allows us to conclude that $(x+e^a y+e^b z)$ divides $G_{d-1}(x,y,z)$. □

Our next claim is that the Togliatti system I is minimal if and only if all monomials of degree d, which are invariant under the action of $M_{a,b}$, appear with non-zero coefficient in the form

$$C_{d;a,b} := (x+y+z)(x+e^a y+e^b z)\cdots(x+e^{(d-1)a}y+e^{(d-1)b}z) = (x+y+z)F_{d-1}. \tag{2}$$

One implication is obvious. For the other, assume that I is not a minimal Togliatti system: this means that there is an ideal J, strictly contained in I, which is again a Togliatti system. Let $G_1,\dots,G_s$ be a system of generators of J. Then for any linear form ℓ there is a form G such that ℓG is a linear combination of $G_1,\dots,G_s$. In particular, $(x+y+z)G$ belongs to I, therefore G is in the kernel of the map $\times(x+y+z)\colon [R/I]_{d-1} \to [R/I]_d$. Since the kernel has dimension one, by the Claim, it follows that G is a scalar multiple of F_{d-1}. We conclude that not all invariant monomials appear with non-zero coefficient in $C_{d;a,b}$.

We easily 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:

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

or, equivalently, the monomials appearing in the permanent $\mathrm{per}(\mathrm{Circ}_{(d;0,a,b)})$ with non-zero coefficient are exactly all the monomials of degree d invariant by the action of $M_{a,b}$.

Thus, to conclude the proof we need the equality $D_{(d;0,a,b)} = P_{(d;0,a,b)}$ to hold, which is indeed the case by Theorem 2.3. □

Remark 3.9. It is worthwhile to underline the following interpretation of our results in terms of representation theory of cyclic matrix groups.

In the proof of Theorem 3.8 we have proved that a monomial of degree d in three variables is invariant under the action of the cyclic matrix group of order d, generated by $M_{a,b}$, if and only if it appears with non-zero coefficient in the form $C_{d;a,b}$ of (2). So we get information about a minimal system of generators for the homogeneous component of degree d of the ring of invariants of these representations.

Up to a coefficient d, the polynomial $C_{d;a,b}$ is the image of the linear form $x+y+z$ under the Reynolds operator. This is in fact the same point of view of Emmy Noether, when she proved the finiteness of the ring of invariants of a polynomial ring under the action of a finite matrix group [21].

From Example 2.7 it follows that a similar result is not true for polynomials in r variables, with $r \geq 4$.

4. Computational complexity

The task of computing the permanent of a d by d (0/1)-matrix is computationally hard (#P-complete), by a celebrated theorem of Valiant [28], and remains so even when there are only 3 nonzero entries per row [8]. The best known upper bounds to compute the permanent are exponential in d, by Ryser [24]. Theorem 2.4 immediately tells us that computing the permanent of $\mathrm{Circ}_{(d;0,a,b)}$, when $\mathrm{GCD}(a,b,d)=1$, can be done in polynomial time in d, say by computing $\det(\mathrm{Circ}_{(d;0,a,b)}) \in \mathbb{Z}[x,y,z]$ via polynomial interpolation (evaluating it on $O(d^2)$ points suffices).

Acknowledgements

This work was started at the workshop "Lefschetz Properties and Jordan Type in Algebra, Geometry and Combinatorics," held at Levico (Trento) in June 2018. The authors thank the Centro Internazionale per la Ricerca Matematica (CIRM) for its support. We also thank Nati Linial and Amir Shpilka for helpful discussions on the computational complexity aspects and for pointing us to [5].

References

[1] C. Almeida, A.V. Andrade, R.M. Miró-Roig, Gaps in the number of generators of monomial Togliatti systems, J. Pure Appl. Algebra 223 (4) (2019) 1817–1831.
[2] J. Bae, Circulant matrix factorization based on Schur algorithm for designing optical multimirror filters, Jpn. J. Math. 45 (2006) 5163–5168.
[3] H. Brenner, A. Kaid, Syzygy bundles on $\mathbb{P}^2$ and the weak Lefschetz property, Ill. J. Math. 51 (2007) 1299–1308.
[4] R. Brualdi, M. Newman, An enumeration problem for a congruence equation, J. Res. Natl. Bur. Stand. B, Math. Sci. 74B (1970) 37–40.
[5] B. Codenotti, G. Resta, Computation of sparse circulant permanents via determinants, Linear Algebra Appl. 355 (2002) 15–34.
[6] L. Colarte, E. Mezzetti, R.M. Miró-Roig, M. Salat, On the coefficients of the permanent and the determinant of a circulant matrix. Applications, Proc. Am. Math. Soc. 147 (2) (2019) 547–558.
[7] J.P. D'Angelo, Invariant holomorphic mappings, J. Geom. Anal. 6 (1996) 163–179.
[8] P. Dagum, M. Luby, M. Mihail, U. Vazirani, Polytopes, permanents, and graphs with large factors, in: Proceedings of the 27th IEEE Symposium on Foundation of Computer Science, 1988.
[9] B. Fischer, J. Modersitzki, Fast inversion of matrices arising in image processing, Numer. Algorithms 22 (1999) 1–11.
[10] S. Georgiou, C. Kravvaritis, New good quasi-cyclic codes over GF(3), Int. J. Algebra 1 (2007) 11–24.
[11] I. Kra, S.R. Simanca, On circulant matrices, Not. Am. Math. Soc. 59 (3) (2012) 368–377.
[12] S. Kounias, C. Koukouvinos, N. Nikolaou, A. Kakos, The nonequivalent circulant D-optimal designs for $n \equiv 2 \bmod 4$, $n = 54$, $n = 66$, J. Comb. Theory, Ser. A 65 (1994) 26–38.
[13] N.A. Loehr, G.S. Warrington, H.S. Wilf, The combinatorics of a three-line circulant determinant, Isr. J. Math. 143 (1) (2004) 141–156.
[14] J. Malenfant, On the matrix-element expansion of a circulant determinant, arXiv:1502.06012.
[15] E. Mezzetti, R. Miró-Roig, G. Ottaviani, Laplace equations and the weak Lefschetz property, Can. J. Math. 65 (2013) 634–654.
[16] E. Mezzetti, R.M. Miró-Roig, The minimal number of generators of a Togliatti system, Ann. Mat. Pura Appl. 195 (2016) 2077–2098.
[17] E. Mezzetti, R.M. Miró-Roig, Togliatti systems and Galois coverings, J. Algebra 509 (2018) 263–291.
[18] M. Michałek, R.M. Miró-Roig, Smooth monomial Togliatti systems of cubics, J. Comb. Theory, Ser. A 143 (2016) 66–87.
[19] J. Migliore, R. Miró-Roig, U. Nagel, Monomial ideals, almost complete intersections and the weak Lefschetz property, Trans. Am. Math. Soc. 363 (2011) 229–257.
[20] R.M. Miró-Roig, M. Salat, On the classification of Togliatti systems, Commun. Algebra 46 (6) (2018) 2459–2475.
[21] E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen, Math. Ann. 77 (1915) 89–92.
[22] N. Nguyen, P. Milanfar, G. Golub, A computationally efficient superresolution image reconstruction algorithm, IEEE Trans. Image Process. 10 (2001) 573–583.
[23] O. Ore, Some studies on cyclic determinants, Duke Math. J. 18 (2) (1951) 343–354.
[24] H.J. Ryser, Combinatorial Mathematics, Carus Mathematical Monograph, vol. 14, 1963.
[25] H. Thomas, The number of terms in the permanent and the determinant of a generic circulant matrix, J. Algebraic Comb. 20 (2004) 55–60.
[26] E. Togliatti, Alcuni esempî di superficie algebriche degli iperspazî che rappresentano un'equazione di Laplace, Comment. Math. Helv. 1 (1929) 255–272.
[27] E. Togliatti, Alcune osservazioni sulle superficie razionali che rappresentano equazioni di Laplace, Ann. Mat. Pura Appl. (4) 25 (1946) 325–339.
[28] L.G. Valiant, The complexity of computing the permanent, Theor. Comput. Sci. 8 (1979) 189–201.
[29] A. Wyn-Jones, Circulants, available in www.circulants.org/circ/circall.pdf.