Received: 2 June 2021 | Revised: 15 October 2021 | Accepted: 12 January 2022

DOI: 10.1112/blms.12642

RESEARCH ARTICLE

Bulletin of the London
Mathematical Society

On a problem of Lang for matrix polynomials

Alina Ostafe

School of Mathematics and Statistics,
University of New South Wales, Sydney,
NSW, Australia

Correspondence
Alina Ostafe, School of Mathematics and
Statistics, University of New South Wales,
Sydney, NSW 2052, Australia.
Email: alina.ostafe@unsw.edu.au

Funding information
Australian Research Council,
Grant/Award Number: DP200100355;
Max Planck Institute of Mathematics

Abstract

In this paper, we consider a problem of Lang about finiteness of torsion points on plane rational curves, and prove some results towards a matrix analogue of this problem, including a full analogue for 2×2 matrices defined over $\mathbb{C}$.

MSC (2020)
11C20, 11G30, 11R58 (primary)

1 | INTRODUCTION AND STATEMENTS OF MAIN RESULTS

1.1 | Motivation

Pivotal work of Lang made it clear that the existence of multiplicative relations between coordinates of points on algebraic curves in $\mathbb{G}_m^n = (\mathbb{C} \setminus \{0\})^n$ is a very rare event, which may occur only if the curve is 'special'. In particular, the celebrated result conjectured by Lang [9, 13] in the 1960s and proved by Ihara, Serre and Tate asserts the finiteness of the so-called *torsion points* on curves, that is, points with all coordinates roots of unity. For the case of plane curves, Beukers and Smyth [2, Section 4.1] give a uniform bound for the number of such points, and Corvaja and Zannier [7] give an upper bound for the maximal order of torsion points on the curve. More precisely, one has the following result [2, Section 4.1]:

Theorem A. *An algebraic curve $F(y_1, y_2) = 0$, where $F \in \mathbb{C}[y_1, y_2]$, contains at most $11(\deg F)^2$ torsion points unless F has a factor of the form $y_1^i - \rho y_2^j$ or $y_1^i y_2^j - \rho$ for some non-negative integers i, j not both zero and some root of unity ρ.*

Theorem A in the case of plane rational curves can be reformulated as follows: given multiplicatively independent rational functions $f, g \in \mathbb{C}(x)$ (see below for the precise definition), there are at most

$$11(\deg f + \deg g)^2 \min(\deg f, \deg g) \leqslant 22(\deg f + \deg g) \deg f \cdot \deg g$$

elements $\alpha \in \mathbb{C}$ such that both $f(\alpha)$ and $g(\alpha)$ are roots of unity, see also the proof of [11, Lemma 2.2]. This has been extended to a finiteness result of elements $\alpha \in \mathbb{C}$ such that $|f(\alpha)| = |g(\alpha)| = 1$, first by Corvaja, Masser and Zannier [5] for $f(x) = x$ and $g \in \mathbb{C}[x]$, and later by Pakovich and Shparlinski [12] for the general case, improving also the bound above for genus zero curves. More precisely, we have the following result [12, Theorem 2.2]:

Theorem B. *Let $f, g \in \mathbb{C}(x)$. Then one has*

$$\#\{\alpha \in \mathbb{C} : |f(\alpha)| = |g(\alpha)| = 1\} \leqslant (\deg f + \deg g)^2,$$

unless

$$f = f_1 \circ h \qquad \text{and} \qquad g = g_1 \circ h$$

for some quotients of Blaschke products f_1 and f_2 and some rational function h.

As remarked in [12] (see the comment after Theorem 2.2 in [12]), if f and g are polynomials, then the conclusion of Theorem B holds, unless the polynomials f and g are multiplicatively dependent.

In this note, we aim at obtaining an analogue of Theorem A (for plane rational curves) for matrix polynomials.

Notation and conventions: We now set the following notation, which remains fixed for the remainder of this paper:

- For $r \geqslant 1$, $\mathsf{M}_r(\mathbb{C})$ is the set of all $r \times r$ matrices with entries in $\mathbb{C}$, $\mathrm{GL}_r(\mathbb{C})$ the set of invertible matrices, and $\mathrm{SL}_r(\mathbb{C})$ the set of matrices of determinant one.
- $I \in \mathsf{M}_r(\mathbb{C})$ is the identity matrix.
- We use 0 for both the zero scalar and the zero matrix, which shall be clear from the context.
- By a scalar matrix we mean a scalar multiple of the identity I, that is, λI for some $\lambda \in \mathbb{C}$.
- x, y_1, y_2 are "scalar" variables, that is, we apply them at elements $\lambda \in \mathbb{C}$. We reserve Z, Z_1, Z_2 for "matrix" variables, that is, we apply them at matrices $A \in \mathsf{M}_r(\mathbb{C})$.
  We also write xI for the multiplication of the variable x with the identity matrix I.
- $f, g \in \mathsf{M}_r(\mathbb{C})[Z]$ are matrix polynomials with coefficients in $\mathsf{M}_r(\mathbb{C})$, that is, polynomials of the form

$$C_d Z^d + \cdots + C_1 Z + C_0, \qquad C_i \in \mathsf{M}_r(\mathbb{C}), \quad i = 0, \ldots, d,$$

  for some $d \geqslant 1$ with $C_d \neq 0$.
- For $A \in \mathsf{M}_r(\mathbb{C})$, we write A^T for the transpose of A.
- For $A \in \mathsf{M}_r(\mathbb{C})$, $\det(A)$ is the determinant of the matrix A.
- $A \in \mathrm{GL}_r(\mathbb{C})$ is called *torsion matrix* if $A^n = I$ for some $n \geqslant 1$. A pair of matrices (A, B) is called a *torsion point* in $\mathrm{GL}_r(\mathbb{C})^2$ if both matrices A and B are torsion.

We say that two matrices $A, B \in \mathsf{M}_r(\mathbb{C})$ are *conjugate* if there exists an invertible matrix $V \in \mathsf{M}_r(\mathbb{C})$ such that

$$A = VBV^{-1}.$$

Clearly, two conjugate matrices have the same set of eigenvalues with the same multiplicities.

We say that two algebraic functions $h_1, h_2 \in \overline{\mathbb{C}(x)}$ are *multiplicatively dependent* if there is a non-zero vector $(k_1, k_2) \in \mathbb{Z}^2$ such that

$$h_1(x)^{k_1} h_2(x)^{k_2} = 1.$$

Otherwise they are called *multiplicatively independent*.

As a direct consequence of Theorem B, one already has an immediate result for matrix polynomials $f, g \in \mathsf{M}_r(\mathbb{C})[Z]$ such that all the eigenvalues of $f(\lambda I)$ and $g(\lambda I)$, $\lambda \in \mathbb{C}$, are of absolute value one. More precisely, one has:

Corollary 1.1. *Let $f, g \in \mathsf{M}_r(\mathbb{C})[Z]$ be such that* $\det(f(xI))$ *and* $\det(g(xI))$ *are multiplicatively independent in $\mathbb{C}(x)$. Then there are at most*

$$r^2(\deg f + \deg g)^2$$

elements $\lambda \in \mathbb{C}$ such that $f(\lambda I)$ and $g(\lambda I)$ satisfy

$$|\det(f(\lambda I))| = |\det(g(\lambda I))| = 1.$$

In particular, there are at most finitely many elements $\lambda \in \mathbb{C}$ such that all eigenvalues of $f(\lambda I)$ and $g(\lambda I)$ are of absolute value one.

Remark 1.2. The condition that $\det(f(xI))$ and $\det(g(xI))$ are multiplicatively independent in $\mathbb{C}(x)$ in Corollary 1.1 can be reformulated as follows: there is no non-zero vector $(k_1, k_2) \in \mathbb{Z}^2$ such that

$$f(xI)^{k_1} g(xI)^{k_2} \in \mathrm{SL}_r(\mathbb{C}).$$

Indeed, $\det(f(xI))$ and $\det(g(xI))$ are multiplicatively independent in $\mathbb{C}(x)$ if and only if there is no non-zero vector $(k_1, k_2) \in \mathbb{Z}^2$ such that

$$\det(f(xI))^{k_1} \det(g(xI))^{k_2} = \det\left(f(xI)^{k_1} g(xI)^{k_2}\right) = 1,$$

which implies the above condition.

We also note that if $f, g \in \mathbb{C}[Z]$, then for any matrix $A \in \mathsf{M}_r(\mathbb{C})$, by the spectral theorem on eigenvalues, the eigenvalues of $f(A)$ are $f(\lambda_i)$, $i = 1, \dots, r$, where $\lambda_1, \dots, \lambda_r$ are the eigenvalues of A, and similarly for g. Thus, if $f(A)^n = I$ for some n, then all $f(\lambda_i)$, $i = 1, \dots, r$, are roots of unity, and similarly for g. We thus reduce the problem to the classical Lang problem, that is, Theorem A. Similarly, if all eigenvalues of $f(A)$ and $g(A)$ are of absolute value one, then we reduce the problem to Theorem B.

If $f, g \in \mathsf{M}_r(\mathbb{C})[Z]$ with coefficients $C_i = c_i I, i = 1, \dots, \deg f$, and similarly for g, then we are in the case above, that is, $f \in \mathbb{C}[Z]$ is given by

$$f(Z) = \sum_{i=0}^{\deg f} c_i Z^i,$$

and similarly for g, and thus the discussion above applies, again.

Theorem A is also intimately related to the question of giving uniform bounds for the degree of $\gcd(f^n - 1, g^m - 1)$, $n, m \geqslant 1$, for some polynomials $f, g \in \mathbb{C}[x]$, which was initially considered by Ailon and Rudnick [1] and later in [11] and further extended in several ways by other authors. It is worth mentioning that matrices have already been considered in this context in [1], that is, the authors give results for $\gcd(A^n - I)$, $n \geqslant 1$, for a matrix A defined over $\mathbb{Z}$, cyclotomic extensions or $\mathbb{C}[T]$ (here, by the greatest common divisor of a matrix we mean the greatest common divisor of all entries of the matrix). Moreover, in [6], Corvaja, Rudnick and Zannier study the growth of the order of matrices in reduction modulo integers $N \geqslant 1$ as N goes to infinity.

We note that the finiteness result in Theorem A has been extended to higher-order multiplicative relations of points on curves in $\mathbb{G}_m^n$ defined over $\overline{\mathbb{Q}}$ by Bombieri, Masser and Zannier [3], and then further generalised in [4, 10].

We conclude this section with a rather vague question towards obtaining a full matrix analogue of Theorem A for torsion points on plane curves.

Question 1.3. Let $F \in \mathsf{M}_r(\mathbb{C})[Z_1, Z_2]$. Under what conditions on F are there, up to conjugacy, finitely many torsion points $(A_1, A_2) \in \mathrm{GL}_r(\mathbb{C})^2$ such that $F(A_1, A_2) = 0$?

In this paper, we give an answer for the 2×2 matrix analogue of Theorem A in the case of plane rational curves.

1.2 | Main results

Informally, given matrix polynomials $f, g \in \mathsf{M}_r(\mathbb{C})[Z]$, we would like to have a finiteness result for the set of matrices $A \in \mathsf{M}_r(\mathbb{C})$, such that $f(A)$ and $g(A)$ are 'roots' of the identity matrix. In this paper, we are able to prove this in any dimension r for matrices $A \in \mathsf{M}_r(\mathbb{C})$ that commute with the coefficients of both f and g, as well as for arbitrary matrices $A \in \mathsf{M}_2(\mathbb{C})$ in dimension two.

It is clear that, in the case of matrices, one cannot expect a finiteness result as in Theorem A. Indeed, let f have the coefficients $c_i I$, $c_i \in \mathbb{C}$, $i = 0, \dots, \deg f$, and let $A \in \mathsf{M}_r(\mathbb{C})$ be such that $f(A)^n = I$ for some n. Then any matrix conjugate to A is also a solution to $f(Z)^n = I$, and similarly for g. Thus, one can only expect a finiteness result *up to conjugacy*.

Our first result gives an answer towards Lang's problem for matrices which commute with the coefficients of the polynomials f and g. More precisely, we have:

Theorem 1.4. *Let $f, g \in \mathsf{M}_r(\mathbb{C})[Z]$ be such that any eigenvalue of $f(xI)$ and any eigenvalue of $g(xI)$ are multiplicatively independent functions in $\overline{\mathbb{C}(x)}$. Then, up to conjugacy, there are at most*

$$2\big(22r^5(\deg f + \deg g)(\deg f \cdot \deg g)\big)^r$$

matrices $A \in \mathsf{M}_r(\mathbb{C})$ which commute with the coefficients of f and g, such that $(f(A), g(A))$ is a torsion point in $\mathrm{GL}_r(\mathbb{C})^2$.

The proof reduces to considering scalar specialisations, see Lemma 2.2 (in Section 2.2), and thus relies on Theorem A above.

As an example, one can consider all coefficients of f and g to be matrices in $\mathbb{C}[B]$ for some fixed $B \in \mathsf{M}_r(\mathbb{C})$. Then Theorem 1.4 gives finiteness, up to conjugacy, of the set of matrices $A \in \mathsf{M}_r(\mathbb{C})$ which commute with B, such that $(f(A), g(A))$ is a torsion point.

The main result of the paper is a full analogue of Lang's result (in the case of plane rational curves) for 2 × 2 complex matrices. To state our result, we introduce the following notation and definition: for $f \in \mathsf{M}_2(\mathbb{C})[Z]$, we define the set

$$\mathcal{S}_f = \{\det(f(xI)), \mu_i(x), i = 1, \dots, r\}, \tag{1.1}$$

where $\mu_i(x)$, $i = 1, \dots, r$, are the eigenvalues of $f(xI)$ in $\overline{\mathbb{C}(x)}$.

Definition 1.5. We say that two polynomials $f, g \in \mathsf{M}_2(\mathbb{C})[Z]$ are *spectrally multiplicatively independent* if for any pair $(\alpha, \beta) \in \mathcal{S}_f \times \mathcal{S}_g$, where $\mathcal{S}_f$ and $\mathcal{S}_g$ are defined by (1.1), α and β are multiplicatively independent.

Remark 1.6. We note that any eigenvalue $\mu_i(x)$ of $f(xI)$ being multiplicatively independent with any eigenvalue $\eta_j(x)$ of $g(xI)$ would not necessarily imply that $\det(f(xI))$ is multiplicatively independent with all $\eta_j(x)$, $j = 1, \dots, r$, or that $\det(f(xI))$ is multiplicatively independent with $\det(g(xI))$. We need the latter conditions to apply Corollary 1.1 or Lemma 2.5 (see Section 2.2) in the proof of our main result, Theorem 1.7 below, whence the need to add $\det(f(xI)) = \prod_{i=1}^r \mu_i(x)$ to the set $\mathcal{S}_f$.

For example, if

$$f(Z) = Z^2 + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} Z + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

and

$$g(Z) = Z^2 + \begin{pmatrix} 0 & 0 \\ 1 & -1 \end{pmatrix},$$

then $\mu_1(x) = x(x+1)$, $\mu_2(x) = x(x-1)$, $\eta_1(x) = x^2$ and $\eta_2(x) = (x-1)(x+1)$, and thus $\mu_1\mu_2 = \eta_1\eta_2 = x^2(x^2-1)$.

We have the following:

Theorem 1.7. *Let $f, g \in \mathsf{M}_2(\mathbb{C})[Z]$ be spectrally multiplicatively independent and such that $f(xI)$ and $g(xI)$ are non-singular. Then, up to conjugacy, there are at most*

$$2^{25}(\deg f + \deg g)^2(\deg f \cdot \deg g)^2$$

matrices $A \in \mathsf{M}_2(\mathbb{C})$ such that $(f(A), g(A))$ is a torsion point in $\mathrm{GL}_2(\mathbb{C})^2$.

The proof of this result is based on [8, Theorem 1] (see Section 2.3), coupled with Corollary 1.1 above, Lemmas 2.2 and 2.5 (see Section 2.2).

Remark 1.8. We note that to ensure that $f(xI)$ and $g(xI)$ are non-singular, it is enough to assume, for example, that the leading matrix coefficients of f and g are non-singular matrices.

We expect that the spectral multiplicative independence condition in Theorem 1.7 holds for the overwhelming majority of pairs of matrix polynomials f and g.

We also remark that, if all the eigenvalues of $f(xI)$ and $g(xI)$ are multiplicatively independent functions in $\overline{\mathbb{C}(x)}$, then the spectral multiplicative independence condition is satisfied. For example, let

$$f(Z) = Z^d + \begin{pmatrix} a_1 & 0 \\ a_2 & a_3 \end{pmatrix} \qquad \text{and} \qquad g(Z) = Z^e + \begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix}$$

be such that $a_1, a_3, b_1, b_3 \in \mathbb{C}^*$ are multiplicatively independent. The eigenvalues of $f(xI)$ are $x^d + a_i$, $i = 1, 3$, and similarly the eigenvalues of $g(xI)$ are $x^e + b_i$, $i = 1, 3$. Since $a_1, a_3, b_1, b_3 \in \mathbb{C}^*$ are multiplicatively independent, all conditions of Theorem 1.7 are satisfied.

We obtain the following consequence of Theorem 1.7.

Corollary 1.9. *Let $F(Z_1, Z_2) = Z_1 - Z_2 - C \in \mathsf{M}_2(\mathbb{C})[Z_1, Z_2]$ be such that C is non-singular. Then, up to conjugacy, there are at most 2^{27} torsion points $(A_1, A_2) \in \mathrm{GL}_2(\mathbb{C})^2$ such that $F(A_1, A_2) = 0$.*

Remark 1.10. We note that indeed Corollary 1.9 is not necessarily true if $\det(C) = 0$. For example, let

$$F(Z_1, Z_2) = Z_1 - Z_2 - \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

For any primitive nth root of unity λ, where $n \geqslant 2$, the point

$$\left(\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \lambda & -1 \\ 0 & 1 \end{pmatrix} \right)$$

is torsion of order n. Indeed, this follows immediately since

$$\begin{pmatrix} \lambda & -1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} \lambda^n & -(\sum_{i=0}^{n-1} \lambda^i) \\ 0 & 1 \end{pmatrix}.$$

Therefore, we have infinitely many such matrices (which are not conjugate) when λ runs over all primitive nth roots of unity, $n \geqslant 2$.

In Theorems 1.4 and 1.7, we look at matrices $A \in \mathsf{M}_r(\mathbb{C})$ such that all the eigenvalues of $f(A)$ and $g(A)$ are roots of unity. We would also like to have a more general result for the case when all the eigenvalues of $f(A)$ and $g(A)$ are of absolute value one. This, then, would be an analogue of Theorem B and would extend Corollary 1.1 to non-scalar matrices. We thus formulate the following problem:

Problem 1.11. Let $f, g \in \mathsf{M}_r(\mathbb{C})[Z]$. Prove that, under certain conditions on f and g, there are, up to conjugacy, finitely many matrices $A \in \mathsf{M}_r(\mathbb{C})$ such that all the eigenvalues of $f(A)$ and $g(A)$ are of absolute value one.

2 | PRELIMINARIES

2.1 | Multiplicative independence of eigenvalues

Let $f, g \in \mathsf{M}_r(\mathbb{C})[Z]$. We define

$$\begin{aligned} P_f(x, y_1) &= \det\left(y_1 I - f(xI)\right) \in \mathbb{C}[x, y_1],\\ P_g(x, y_2) &= \det\left(y_2 I - g(xI)\right) \in \mathbb{C}[x, y_2], \end{aligned} \tag{2.1}$$

and the following two resultants

$$\begin{aligned} R_{f,g}(y_1, y_2) &= \mathrm{Res}_x\left(P_f(x, y_1), P_g(x, y_2)\right) \in \mathbb{C}[y_1, y_2],\\ T_{f,g}(y_1, y_2) &= \mathrm{Res}_x\left(P_f(x, y_1), y_2 - \det(g(xI))\right) \in \mathbb{C}[y_1, y_2]. \end{aligned} \tag{2.2}$$

We note that both $R_{f,g}$ and $T_{f,g}$ are non-zero polynomials. Indeed, assume $R_{f,g} = 0$. Then, by the definition of the resultant, the polynomials $P_f(x, y_1)$ and $P_g(x, y_2)$, as polynomials in x, share a common root $t \in \overline{\mathbb{C}(y_1)} \cap \overline{\mathbb{C}(y_2)} = \mathbb{C}$. Thus we obtain that $\det(y_1 I - f(tI)) = \det(y_2 I - g(tI)) = 0$, which is a contradiction, since both polynomials have as leading monomials y_1^r and y_2^r, respectively. Similarly, $T_{f,g}$ is a non-zero polynomial.

We know that $\deg_x P_f \leqslant r \deg f$ and $\deg_x P_g \leqslant r \deg g$, and $R_{f,g}$ is a polynomial of degree $\deg_x P_f$ in y_2 and of degree $\deg_x P_g$ in y_1. Similarly, $\deg \det(g(xI)) \leqslant r \deg g$, and $T_{f,g}$ is a polynomial of degree $\deg_x P_f$ in y_2 and of degree $\deg \det(g(xI))$ in y_1. We thus obtain that

$$\deg R_{f,g}, \deg T_{f,g} \leqslant r(\deg f + \deg g). \tag{2.3}$$

Lemma 2.1. *Let $f, g \in \mathsf{M}_r(\mathbb{C})[Z]$.*

(i) *If any eigenvalue of $f(xI)$ and any eigenvalue of $g(xI)$ are multiplicatively independent functions in $\overline{\mathbb{C}(x)}$, then $R_{f,g}(y_1, y_2)$ defined by (2.2) does not have a factor of the form $y_1^i y_2^j - \rho$ or $y_1^i - \rho y_2^j$ for some non-negative integers i, j not both zero and some root of unity ρ.*

(ii) *If any eigenvalue of $f(xI)$ and $\det(g(xI))$ are multiplicatively independent functions in $\overline{\mathbb{C}(x)}$, then $T_{f,g}(y_1, y_2)$ defined by (2.2) does not have a factor of the form $y_1^i y_2^j - \rho$ or $y_1^i - \rho y_2^j$ for some non-negative integers i, j not both zero and some root of unity ρ.*

Proof. The proofs for (i) and (ii) follow the same discussion, so we only provide the proof for (i).

Let $\mu_i(x)$, $i = 1, \dots, r$, be the eigenvalues of $f(xI)$ in $\overline{\mathbb{C}(x)}$, that is, the roots of the polynomial $P_f(y_1, x)$ defined by (2.1) as a polynomial in y_1. Similarly, let $\eta_j(x)$, $j = 1, \dots, r$, be the eigenvalues of $g(xI)$ in $\overline{\mathbb{C}(x)}$.

Assume that $R_{f,g}(y_1, y_2)$ has a factor of one of the forbidden forms, say $y_1^i y_2^j - \rho$ for some non-negative integers i, j not both zero and some root of unity ρ. We note that any point on the curve

$R_{f,g}(y_1,y_2)=0$ is of the form $(\mu_k(t),\eta_\ell(t))$ for some $1\leqslant k,\ell\leqslant r$ and some $t\in\mathbb{C}$. Indeed, let $(t_1,t_2)\in\mathbb{C}^2$ be such that $R_{f,g}(t_1,t_2)=0$. Then, by definition of the resultant $R_{f,g}$, the two polynomials

$$\det(t_1I-f(xI))=\prod_{i=1}^{r}(t_1-\mu_i(x)),\det(t_2I-g(xI))=\prod_{i=1}^{r}(t_2-\eta_i(x))$$

have a common root $x=t\in\mathbb{C}$. This implies $t_1=\mu_k(t)$ and $t_2=\eta_\ell(t)$ for some k,ℓ. Since $y_1^iy_2^j-\rho$ is a factor of $R_{f,g}$, there are infinitely many $(t_1,t_2)\in\mathbb{C}^2$ which are roots of this factor, and thus we deduce that there are infinitely many $t\in\mathbb{C}$ such that

$$\mu_k(t)^i\eta_\ell(t)^j=\rho$$

for some $1\leqslant k,\ell\leqslant r$. Since μ_k and η_ℓ are algebraic functions, we conclude that $\mu_k(x)^i\eta_\ell(x)^j=\rho$, which contradicts our hypothesis.

The case when $R_{f,g}(y_1,y_2)$ has a factor of the form $y_1^i-\rho y_2^j$ is treated entirely similar. A similar discussion applies for (ii), replacing only $\det(t_2I-g(xI))$ above with the polynomial $t_2-\det(g(xI))$. □

2.2 | Scalar specialisations

Two of the main tools for the proof of Theorems 1.4 and 1.7 are the following results which apply, again, to scalar matrices λI, however for which the matrices $f(\lambda I)$ and $g(\lambda I)$ satisfy different conditions than in Corollary 1.1. More precisely, we have:

Lemma 2.2. *Let $f,g\in\mathsf{M}_r(\mathbb{C})[Z]$ be such that any eigenvalue of $f(xI)$ and any eigenvalue of $g(xI)$ are multiplicatively independent functions in $\overline{\mathbb{C}(x)}$. Then there are at most*

$$22r^5(\deg f+\deg g)\deg f\cdot\deg g$$

elements $\lambda\in\mathbb{C}$ such that

$$f(\lambda I)^n-I\qquad\text{and}\qquad g(\lambda I)^m-I$$

are singular matrices for some $n,m\geqslant 1$.

Proof. We use a similar approach as for the proof of [1, Theorem 3], reducing the problem to an application of Theorem A.

Let $\lambda\in\mathbb{C}$ be such that $f(\lambda I)^n-I$ and $g(\lambda I)^m-I$ are singular matrices for some $n,m\geqslant 1$. This implies that $J^n_{f(\lambda I)}$ and $J^m_{g(\lambda I)}$, which are triangular matrices, have at least one element 1 on the main diagonal, where $J_{f(\lambda I)}$ and $J_{g(\lambda I)}$ are Jordan normal forms of $f(\lambda I)$ and $g(\lambda I)$, respectively.

Let $u_{\lambda,i},v_{\lambda,j}\in\mathbb{C}$, $i,j=1,\dots,r$, be the eigenvalues of $f(\lambda I),g(\lambda I)$, respectively, that is, $u_{\lambda,i}$ are the (not necessarily distinct) roots of the polynomial $P_f(\lambda,y_1)$ and $v_{\lambda,j}$ are the (not necessarily distinct) roots of the polynomial $P_g(\lambda,y_2)$, where $P_f(x,y_1)$ and $P_g(x,y_2)$ are defined by (2.1). Consequently, there exist $i,j\in\{1,\dots,r\}$ such that $u^n_{\lambda,i}=1$ and $v^m_{\lambda,j}=1$, that is, both $u_{\lambda,i}$ and $v_{\lambda,j}$ are roots of unity.

Notice that, since $P_f(\lambda, u_{\lambda,i}) = P_g(\lambda, v_{\lambda,j}) = 0$, one also has

$$R_{f,g}(u_{\lambda,i}, v_{\lambda,j}) = 0$$

for all i, j, where $R_{f,g}$ is defined by (2.2). Moreover, from the above discussion, there exist i, j such that $(u_{\lambda,i}, v_{\lambda,j})$ is a torsion point on the curve $R_{f,g}(y_1, y_2) = 0$.

Since, by our hypothesis and Lemma 2.1 (i), $R_{f,g}$ does not have any of the special factors mentioned in the statement of Theorem A, it follows from Theorem A and (2.3) that there are at most

$$11(\deg R_{f,g})^2 \leqslant 11r^2(\deg f + \deg g)^2$$

torsion points (ζ_1, ζ_2) on the curve $R_{f,g}(y_1, y_2) = 0$. Each such point $(\zeta_1, \zeta_2) = (u_{\lambda,i}, v_{\lambda,j})$ for some i, j corresponds to at most $r \min(\deg f, \deg g)$ values of λ. Indeed, since $R_{f,g}(\zeta_1, \zeta_2) = 0$, λ is a common root of the polynomials $P_f(x, \zeta_1), P_g(x, \zeta_2)$. We note that both polynomials $P_f(x, \zeta_1), P_g(x, \zeta_2)$ are non-zero, since, otherwise, ζ_1 or ζ_2 would be an eigenvalue of $f(xI)$ or $g(xI)$, respectively. However, since ζ_1 or ζ_2 are roots of unity, this contradicts the multiplicative independence assumption on the eigenvalues of $f(xI)$ and $g(xI)$.

Taking the contribution from each $i, j \leqslant r$, we conclude that there at most

$$11r^5(\deg f + \deg g)^2 \min(\deg f, \deg g) \leqslant 22r^5(\deg f + \deg g) \deg f \cdot \deg g$$

possibilities for such $\lambda \in \mathbb{C}$, which concludes the proof. □

Remark 2.3. It is worth mentioning that Lemma 2.2 is equivalent to the following reformulation: Let $f, g \in \mathsf{M}_r(\mathbb{C})[Z]$ be as in Lemma 2.2. Then there are at most

$$22r^5(\deg f + \deg g) \deg f \cdot \deg g$$

elements $\lambda \in \mathbb{C}$ such that $f(\lambda I)$ and $g(\lambda I)$ have each at least one eigenvalue that is a root of unity.

Remark 2.4. When $r = 1$, the conditions in Corollary 1.1 and Lemma 2.2 are equivalent to the polynomials f and g being multiplicatively independent, and, in this case, we recover Theorem A.

Lemma 2.5. *Let $f, g \in \mathsf{M}_r(\mathbb{C})[Z]$ be such that any eigenvalue of $f(xI)$ and $\det(g(xI))$ are multiplicatively independent functions in $\overline{\mathbb{C}(x)}$. Then there are at most*

$$22r^4(\deg f + \deg g) \deg f \cdot \deg g$$

elements $\lambda \in \mathbb{C}$ such that

$$f(\lambda I)^n - I \text{ is singular} \qquad \text{and} \qquad \det(g(\lambda I))^m = 1$$

for some $n, m \geqslant 1$.

Thus, in Lemma 2.5, we look at $\lambda \in \mathbb{C}$ such that $f(\lambda I)$ has an eigenvalue a root of unity and $\det(g(\lambda I))$ is a root of unity.

Proof. The proof follows exactly the same lines as the proof of Lemma 2.2, but, instead of the polynomial $R_{f,g}$, we consider $T_{f,g}$ defined by (2.2).

Indeed, let $\lambda \in \mathbb{C}$ be such that $f(\lambda I)^n - I$ is singular for some $n \geqslant 1$ and $\det(g(\lambda I))$ is a root of unity. As observed above, this means that an eigenvalue of $f(\lambda I)$ is a root of unity, which we denote, as in the previous proof, by $u_{\lambda,i}$ for some $i = 1, \dots, r$. Since

$$T_{f,g}(u_{\lambda,i}, \det(g(\lambda I))) = 0,$$

we are, again, in the situation of looking at torsion points on the algebraic curve $T_{f,g}(y_1, y_2)$=0 and apply Theorem A. Using (2.3) and applying Lemma 2.1 (ii) and Theorem A, we obtain at most

$$11(\deg T_{f,g})^2 \leqslant 11r^2(\deg f + \deg g)^2$$

torsion points (ζ_1, ζ_2) on the curve $T_{f,g}(y_1, y_2) = 0$. Each such torsion point $(\zeta_1, \zeta_2) = (u_{\lambda,i}, \det(g(\lambda I)))$ for some $i = 1, \dots, r$, corresponds, again, to at most $r \min(\deg f, \deg g)$ values of λ. Taking the contribution from each $i \leqslant r$, we conclude that there at most

$$11r^4(\deg f + \deg g)^2 \min(\deg f, \deg g) \leqslant 22r^4(\deg f + \deg g) \deg f \cdot \deg g$$

possibilities for such $\lambda \in \mathbb{C}$, which concludes the proof. □

2.3 | Singular differences of powers of matrices

In this section, we consider only 2×2 matrices. For matrices $A, B \in \mathrm{GL}_2(\mathbb{C})$, we define the set

$$S_{A,B} = \{(n, m) \in \mathbb{Z}^2 \ : \ A^n - B^m \text{ is singular}\}. \tag{2.4}$$

In [8, Theorem 1], Evertse and Tijdeman give a classification of pairs of matrices (A, B) such that the set $S_{A,B}$ is infinite. This is our main tool in the proof of Theorem 1.7. For completeness, we present their result in this section, and, for this, we say that two pairs of matrices (A, B) and (A_1, B_1) are *similar*, if there exists a matrix $V \in \mathrm{GL}_2(\mathbb{C})$ such that

$$A = VA_1V^{-1} \qquad \text{and} \qquad B = VB_1V^{-1}.$$

Moreover, we say that (A, B) is *related* to (A_1, B_1) if

$$(A, B) \ \text{is similar to} \ (A_1, B_1), (B_1, A_1), (A_1^T, B_1^T) \text{ or } (B_1^T, A_1^T).$$

We define now four pairs of matrices (A_1, B_1) for which S_{A_1,B_1} is infinite, see [8] for more details.

(I) $A_1^\ell = \begin{pmatrix} \theta & * \\ 0 & * \end{pmatrix}$ and $B_1^s = \begin{pmatrix} \theta & * \\ 0 & * \end{pmatrix}$ for some integers ℓ, s not both zero, and some non-zero $\theta \in \mathbb{C}$.

(II) $A_1^\ell = \begin{pmatrix} \theta & 0 \\ 0 & \kappa \end{pmatrix}$ and $B_1^s = \begin{pmatrix} 0 & \zeta \\ \zeta & 0 \end{pmatrix}$ for some integers ℓ, s with $\ell s \neq 0$ and some non-zero $\theta, \kappa, \zeta \in \mathbb{C}$ such that $\theta\kappa = \zeta^2$.

(III) $A_1^{\ell} = \begin{pmatrix} \theta & 0 \\ 0 & \kappa \end{pmatrix}$ and $B_1^s = \begin{pmatrix} 2\zeta+\theta & 2(\zeta+\theta) \\ -(\zeta+\theta) & -\zeta-2\theta \end{pmatrix}$ for some integers ℓ, s with $\ell s \neq 0$ and some non-zero $\theta, \kappa, \zeta \in \mathbb{C}$ such that $\kappa\zeta = \theta^2$.

(IV) $A_1 = \begin{pmatrix} \alpha & \alpha \\ 0 & \alpha \end{pmatrix}$ and $B_1 = \begin{pmatrix} (1-\sqrt{\zeta\mu})\rho & \zeta\rho \\ -\mu\rho & (1+\sqrt{\zeta\mu})\rho \end{pmatrix}$, for some $\alpha, \rho, \zeta, \mu \in \mathbb{C}$ such that $\mu \neq 0$, α and ρ are not roots of unity, and

$$(\alpha^n - \rho^m)^2 = \mu nm\alpha^n\rho^m \quad \text{for infinitely many } (n,m) \in \mathbb{Z}^2.$$

Remark 2.6. We note that for pairs (A_1, B_1) of type IV above, both A_1 and B_1 have a double eigenvalue, namely α and ρ, respectively.

We can now state the result of Evertse and Tijdeman [8, Theorem 1].

Theorem 2.7. *Let (A, B) be a pair of matrices in* $\mathrm{GL}_2(\mathbb{C})$ *such that the set $S_{A,B}$ is infinite. Then (A, B) is related to a pair (A_1, B_1) of type I, II, III or IV.*

3 | PROOFS OF MAIN RESULTS

3.1 | Proof of Theorem 1.4

The proof follows as a simple application of Lemma 2.2. Indeed, let $A \in \mathsf{M}_r(\mathbb{C})$ be such that A commutes with each of the coefficients of f and g, and such that

$$f(A)^n = I \qquad \text{and} \qquad g(A)^m = I \tag{3.1}$$

for some $n, m \geqslant 1$.

Using the commutativity assumption on A, simple computations show that there exist polynomials $Q_{n,A}, Q_{m,A} \in \mathsf{M}_r(\mathbb{C})$ depending on n, m and A, such that

$$f(xI)^n - f(A)^n = Q_{n,A}(xI)(xI - A),$$
$$g(xI)^m - g(A)^m = Q_{m,A}(xI)(xI - A).$$

Therefore, using (3.1), we obtain that

$$\det(xI - A) \mid \gcd\left(\det(f(xI)^n - I), \det(g(xI)^m - I)\right).$$

We note that both polynomials $\det(f(xI)^n - I)$ and $\det(g(xI)^m - I)$ are non-zero. Indeed, assume, for example, $\det(f(xI)^n - I) = 0$. Then writing

$$\det(f(xI)^n - I) = \prod_{i=1}^{n} \det(f(xI) - \zeta^i I),$$

where $\zeta \in \mathbb{C}$ is an nth root of unity, we conclude that $\det(f(xI) - \zeta^i I) = 0$ for some $i = 1, \ldots, n$. Thus ζ^i is an eigenvalue of $f(xI)$, and similarly for g. This contradicts our multiplicative independence assumption on the eigenvalues of $f(xI)$ and $g(xI)$.

Thus, every eigenvalue of A is a root of the greatest common divisor above. In other words, for any eigenvalue $\lambda \in \mathbb{C}$ of A, the matrices $f(\lambda I)^n - I$ and $g(\lambda I)^m - I$ are singular. The conclusion now follows from Lemma 2.2, that is, there are at most

$$L = 22r^5(\deg f + \deg g)\deg f \cdot \deg g$$

possibilities for each of the eigenvalues of A.

We now partition the set $\{1, \dots, r\}$ into k ordered parts, $1 \leqslant k \leqslant r$, where each such part corresponds to a Jordan block of A, and thus to one eigenvalue λ. The number of such partitions is $\binom{r-1}{k-1}$, and each set in a partition corresponds to at most L values of $\lambda \in \mathbb{C}$. Summing over all k we obtain at most

$$\sum_{k=1}^{r} \binom{r-1}{k-1} L^k = L \sum_{k=0}^{r-1} \binom{r-1}{k} L^k = L(L+1)^{r-1} \leqslant L^r (1 + 1/L)^{L/2} \leqslant 2L^r$$

possible Jordan normal forms, which concludes the proof.

3.2 | Proof of Theorem 1.7

We start by remarking that the spectral multiplicative independence assumption ensures that the conditions in Corollary 1.1 and Lemmas 2.2 and 2.5 are satisfied, and thus we can apply these results, see the end of the proof.

Let $A \in \mathsf{M}_2(\mathbb{C})$ be such that

$$f(A)^n = I \qquad \text{and} \qquad g(A)^m = I \tag{3.2}$$

for some $n, m \geqslant 1$. This implies that the eigenvalues of $f(A)$ and $g(A)$ are all roots of unity.

Let λ be an eigenvalue of A and $\mathbf{v}$ the corresponding eigenvector, that is, one has

$$A\mathbf{v} = \lambda \mathbf{v}. \tag{3.3}$$

We note that, if $f(\lambda I)$ is singular, then this implies that $\det(f(\lambda I)) = 0$, that is, λ is a zero of a non-zero polynomial (by our hypothesis) of degree at most $2 \deg f$. Thus, there are at most $2 \deg f$ such elements λ, which we exclude from the discussion below. The same discussion applies for $g(\lambda I)$, thus, from now on, we assume that both $f(\lambda I)$ and $g(\lambda I)$ are non-singular.

The idea of the proof is to show that the sets $S_{f(A), f(\lambda I)}$ and $S_{g(A), g(\lambda I)}$ defined by (2.4) are infinite. Then, applying Theorem 2.7, we obtain that $(f(A), f(\lambda I))$ and $(g(A), g(\lambda I))$ are related to pairs of matrices of type I, II or III as defined in Section 2.3 (we will see that type IV cannot occur). This will allow us to conclude that one of $f(\lambda I)$ and $g(\lambda I)$ has an eigenvalue which is a root of unity, while the other matrix will have the same property or the product of its eigenvalues is a root of unity. Applying, then, Corollary 1.1, Lemma 2.2 or 2.5, we will conclude that there are finitely many such $\lambda \in \mathbb{C}$. Since this discussion applies for any eigenvalue λ of A, we conclude the proof.

First, we remark that, using (3.3), for any integer $i \geqslant 1$, one has

$$A^i \mathbf{v} = \lambda^i \mathbf{v},$$

which implies

$$f(A)\mathbf{v} = f(\lambda I)\mathbf{v},$$

or, equivalently,

$$(f(A) - f(\lambda I))\mathbf{v} = 0.$$

Since $\mathbf{v} \in \mathbb{C}^2$ is a non-zero vector, we conclude that the matrix $f(A) - f(\lambda I)$ is singular, and similarly for g.

Moreover, using our hypothesis (3.2), we obtain, for any integer $k \geqslant 1$,

$$f(A)^{kn+1} = f(A) \qquad \text{and} \qquad g(A)^{km+1} = g(A).$$

Thus, for any integer $k \geqslant 1$, the matrices

$$f(A)^{kn+1} - f(\lambda I) \qquad \text{and} \qquad g(A)^{km+1} - g(\lambda I)$$

are singular, which implies that the sets $S_{f(A),f(\lambda I)}$ and $S_{g(A),g(\lambda I)}$ defined by (2.4) are infinite. Therefore, Theorem 2.7 tells us that $(f(A), f(\lambda I))$ and $(g(A), g(\lambda I))$ are related to pairs of type I, II, III or IV as defined in Section 2.3.

We only consider the pair $(f(A), f(\lambda I))$, a similar argument also applies to $(g(A), g(\lambda I))$.

Let $(f(A), f(\lambda I))$ be related to (A_1, B_1) of type I, II, III or IV, which means that $(f(A), f(\lambda I))$ is similar to one of

$$(A_1, B_1), (B_1, A_1), (A_1^T, B_1^T) \text{ or } (B_1^T, A_1^T).$$

(I) We assume first that $(f(A), f(\lambda I))$ is similar to (A_1, B_1), where the pair (A_1, B_1) is such that

$$A_1^\ell = \begin{pmatrix} \theta & * \\ 0 & * \end{pmatrix} \qquad \text{and} \qquad B_1^s = \begin{pmatrix} \theta & * \\ 0 & * \end{pmatrix}$$

for some integers ℓ, s not both zero, and some non-zero $\theta \in \mathbb{C}$.

Using (3.2), since $f(A)^{\ell n} = I$ is similar to $A_1^{\ell n}$, we obtain that θ is an nth root of unity (we note that, if $\ell = 0$, then $\theta = 1$).

Since $f(\lambda I)$ is similar to B_1, and θ is an eigenvalue of B_1^s, we conclude that $f(\lambda I)^s$ has an eigenvalue θ which is a root of unity, and, thus, $f(\lambda I)$ has also an eigenvalue which is a root of unity.

We note that a similar discussion applies for the case when $(f(A), f(\lambda I))$ is similar to one of $(B_1, A_1), (A_1^T, B_1^T), (B_1^T, A_1^T)$, which concludes this case.

(II)

(i) We assume first that $(f(A), f(\lambda I))$ is similar to (A_1, B_1), where the pair (A_1, B_1) is such that

$$A_1^\ell = \begin{pmatrix} \theta & 0 \\ 0 & \kappa \end{pmatrix} \qquad \text{and} \qquad B_1^s = \begin{pmatrix} 0 & \zeta \\ \zeta & 0 \end{pmatrix}$$

for some integers ℓ, s with $\ell s \neq 0$ and some non-zero $\theta, \kappa, \zeta \in \mathbb{C}$ such that

$$\theta\kappa = \zeta^2. \tag{3.4}$$

The same discussion as for case (I) concludes that both θ and $\varkappa$ are nth roots of unity, and thus, by (3.4), ζ is also a root of unity. Since ζ and $-\zeta$ are the eigenvalues of B_1^s, and $f(\lambda I)$ is similar to B_1, we conclude, again, that both eigenvalues of $f(\lambda I)$ are roots of unity, and thus $\det(f(\lambda I))$ is a root of unity.

(ii) We assume now that $(f(A), f(\lambda I))$ is similar to (B_1, A_1). As in the previous discussions, since $f(A)$ is similar to B_1 and ζ is an eigenvalue of B_1^s, we conclude that ζ is a root of unity. Using the relation (3.4), we conclude that $\theta\varkappa$ is a root of unity, and, thus, so is $\det(A_1^\ell)$. Therefore, $\det(A_1)$ is a root of unity.

Moreover, since $f(\lambda I)$ is similar to A_1, we conclude that $\det(f(\lambda I)) = \det(A_1)$, and thus $\det(f(\lambda I))$ is also a root of unity.

A similar discussion applies for the case when $(f(A), f(\lambda I))$ is similar to one of $(A_1^T, B_1^T), (B_1^T, A_1^T)$, which concludes this case.

(III) We assume first that $(f(A), f(\lambda I))$ is similar to (A_1, B_1), where the pair (A_1, B_1) is such that

$$A_1^\ell = \begin{pmatrix} \theta & 0 \\ 0 & \varkappa \end{pmatrix} \qquad \text{and} \qquad B_1^s = \begin{pmatrix} 2\zeta + \theta & 2(\zeta + \theta) \\ -(\zeta + \theta) & -\zeta - 2\theta \end{pmatrix}$$

for some integers ℓ, s with $\ell s \neq 0$ and some non-zero $\theta, \varkappa, \zeta \in \mathbb{C}$ such that

$$\varkappa\zeta = \theta^2.$$

The same considerations as for cases (I) and (II) (i) apply, and thus we obtain that both θ and $\varkappa$ are roots of unity, which in turn implies that ζ is also a root of unity. Noting now that the eigenvalues of B_1^s are ζ and $-\theta$, we conclude that the eigenvalues of B_1, and thus of $f(\lambda I)$, are roots of unity, and thus $\det(f(\lambda I))$ is a root of unity.

A similar discussion applies for the case when $(f(A), f(\lambda I))$ is similar to one of $(B_1, A_1), (A_1^T, B_1^T), (B_1^T, A_1^T)$, which concludes this case.

(IV) If $f(A)$ is similar to A_1 or A_1^T, then α is a root of unity, which contradicts the assumption in (IV) in Section 2.3. Thus, we can only have that $(f(A), f(\lambda I))$ is similar to (B_1, A_1) or (B_1^T, A_1^T). However, this, again, implies that ρ is an eigenvalue of $f(A)$, and thus a root of unity, which is not possible.

Similarly as above, one concludes that either $g(\lambda I)$ has one eigenvalue which is a root of unity (as in case (I)) or the product of its eigenvalues, and thus $\det(g(\lambda I))$, is a root of unity (as in cases (II) and (III)).

To conclude the finiteness of the set of $\lambda \in \mathbb{C}$ as above, we consider all possible combinations for $f(\lambda I)$ and $g(\lambda I)$ in the cases (I), (II) and (III). For each combination, we obtain the following bounds for the cardinality of the set of such $\lambda \in \mathbb{C}$:

- If both $f(\lambda I)$ and $g(\lambda I)$ have each one eigenvalue a root of unity (occurring in case (I)), then, by Lemma 2.2, we obtain at most

$$22 \cdot 2^5 (\deg f + \deg g) \deg f \cdot \deg g \leqslant 2^{10} (\deg f + \deg g) \deg f \cdot \deg g$$

possibilities for each of the eigenvalues of such A.

- If $|\det(f(\lambda I))| = |\det(g(\lambda I))| = 1$ (occurring when both $(f(A), f(\lambda I))$ and $(g(A), g(\lambda I))$ fall in any of the cases (II) and (III)), we apply Corollary 1.1 to obtain at most

$$2^2 (\deg f + \deg g)^2$$

possibilities for each of the eigenvalues of such A.

- When $(f(A), f(\lambda I))$ falls in case (I) and $(g(A), g(\lambda I))$ falls in one of the cases (II) or (III), or the other way around, we apply Lemma 2.5 to obtain

  $$22 \cdot 2^4(\deg f + \deg g)\deg f \cdot \deg g$$

  possibilities for each of the eigenvalues of such A.
  Thus, this case contributes in total with

  $$22 \cdot 2^5(\deg f + \deg g)\deg f \cdot \deg g$$

  possibilities for each of the eigenvalues of A in this case.

Also taking into account the contribution of at most

$$2^2 \deg f \deg g$$

elements $\lambda \in \mathbb{C}$ for which $\det(f(\lambda I)) = 0$ or $\det(g(\lambda I)) = 0$, which we excluded at the beginning of the proof, and putting everything together, we obtain at most

$$\begin{aligned} &2\big(22 \cdot 2^5(\deg f + \deg g)\deg f \cdot \deg g\big) + 2^2(\deg f + \deg g)^2 + 2^2 \deg f \deg g \\ &\qquad \leqslant 2^{12}(\deg f + \deg g)\deg f \cdot \deg g = J \end{aligned}$$

possibilities for each of the eigenvalues of A.

We now conclude the proof by observing, as in the proof of Theorem 1.4, that there are at most

$$J(J+1) \leqslant 2J^2 \leqslant 2^{25}(\deg f + \deg g)^2(\deg f \cdot \deg g)^2$$

possible Jordan forms.

3.3 | Proof of Corollary 1.9

The result follows directly from Theorem 1.7 applied to the polynomials $f(Z) = Z$ and $g(Z) = Z - C$. The determinants of $f(xI)$ and $g(xI)$ are given by

$$\det(f(xI)) = x^2 \qquad \text{and} \qquad \det(g(xI)) = x^2 - \operatorname{tr}(C)x + \det(C),$$

where $\operatorname{tr}(C)$ is the trace of the matrix C. Since $\det(C) \neq 0$, the two determinants are multiplicatively independent.

The eigenvalue of $f(xI)$ is x with multiplicity two, and a simple computation shows that the eigenvalues of $g(xI)$ are given by

$$\left(2x - \operatorname{tr}(C) \pm \sqrt{\operatorname{tr}(C)^2 - 4\det(C)}\right)/2.$$

We notice that these latter eigenvalues are multiplicatively independent with x, and thus with $\det(f(xI))$ as well, since, again, $\det(C) \neq 0$. The bound now follows from Theorem 1.7, which concludes the proof.

ACKNOWLEDGEMENTS

The author is very grateful to Daniel Raoul Perez, Zeev Rudnick, Igor Shparlinski and Umberto Zannier for many discussions and useful comments on preliminary versions of the paper, which improved it significantly. The author thanks Umberto Zannier for suggesting the formulation of Question 1.3 and considering Corollary 1.9. The author is also grateful to the referee for their useful comments.

The author was partially supported by the Australian Research Council Grant DP200100355. The author also gratefully acknowledges the hospitality and generosity of the Max Planck Institute of Mathematics (which fully supported the author for 11 months in 2020, during a very challenging Covid-19 time), where this project was initiated.

Open access publishing facilitated by University of New South Wales, as part of the Wiley - University of New South Wales agreement via the Council of Australian University Librarians.

JOURNAL INFORMATION

The *Bulletin of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

REFERENCES

1. N. Ailon and Z. Rudnick, *Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$*, Acta Arith. **113** (2004), 31–38.
2. F. Beukers and C. J. Smyth, *Cyclotomic points on curves*, Number Theory for the Millenium I (Urbana, Illinois, 2000), A K Peters, 2002, 67–85.
3. E. Bombieri, D. Masser, and U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups*, Int. Math. Res. Not. **20** (1999), 1119–1140.
4. E. Bombieri, D. Masser, and U. Zannier, *On unlikely intersections of complex varieties with tori*, Acta Arith. **133** (2008), 309–323.
5. P. Corvaja, D. Masser, and U. Zannier, *Sharpening 'Manin-Mumford' for certain algebraic groups of dimension 2*, Enseign. Math. **59** (2013), 1–45.
6. P. Corvaja, Z. Rudnick, and U. Zannier, *A lower bound for periods of matrices*, Comm. Math. Phys. **252** (2004), 535–541.
7. P. Corvaja and U. Zannier, *On the maximal order of a torsion point on a curve in $\mathbb{G}_m^n$*, Rend. Lincei Mat. Appl. **19** (2008), 73–78.
8. J.-H. Evertse and R. Tijdeman, *Singular differences of powers of 2×2-matrices*, Compos. Math. **104** (1996), 199–216.
9. S. Lang, *Fundamentals of Diophantine geometry*, Springer, New York, 1983.
10. G. Maurin, *Courbes algébriques et équations multiplicatives*, Math. Ann. **341** (2008), 789–824.
11. A. Ostafe, *On some extensions of the Ailon-Rudnick theorem*, Monatsh. Math. **181** (2016), 451–471.
12. F. Pakovich and I. E. Shparlinski, *Level curves of rational functions and unimodular points on rational curves*, Proc. Amer. Math. Soc. **148** (2020), 1829–1833.
13. U. Zannier, *Lecture notes on Diophantine analysis*, Publ. Scuola Normale Superiore, Pisa, 2009.