DIVISIBILITY CONSTRAINTS ON DEGREES OF FACTOR MAPS

PAUL TROW

(Communicated by Kenneth R. Meyer)

Abstract. We show that the degree of a finite-to-one factor map \( f: \Sigma_A \to \Sigma_B \) between shifts of finite type is constrained by the factors of \( \chi_A \) and \( \chi_B \). A special case of these constraints is that if \( 2 \text{rank}^* B > \text{rank}^* A \), then the degree of \( f \) is a unit in \( \mathbb{Z}[1/\det^* B] \) (where \( \text{rank}^* A \) is the rank of the Jordan form away from 0 of \( A \), and \( \det^* B \) is the determinant of the Jordan form away from 0 of \( B \)).

0. Introduction

The degree of a finite-to-one factor map \( f: \Sigma_A \to \Sigma_B \) between irreducible shifts of finite type is the largest positive integer \( d \) such that every \( y \in \Sigma_B \) has \( d \) mutually separated inverse images. This concept was introduced in [H] for endomorphisms of full shifts. In [B], M. Boyle showed that, given \( \Sigma_A \) and \( \Sigma_B \), there exists a finite set \( E \) of positive integers such that if \( f: \Sigma_A \to \Sigma_B \) has degree \( d \), then \( d = e \nu \), where \( e \in E \) and \( \nu \) is a unit in \( \mathbb{Z}[1/\lambda] \), where \( \lambda \) is the dominant eigenvalue of \( A \). In [T2], this result was extended to apply to any nonzero eigenvalue \( \gamma \) that has the same algebraic multiplicity in \( \chi_A \) and \( \chi_B \). In this paper we give further constraints on the possible degrees of a finite-to-one factor map, given certain assumptions on the factors of \( \chi_A \) and \( \chi_B \) (see Theorem 8 and Corollary 9).

1. Background

We give some basic definitions concerning shifts of finite type. For a more thorough introduction to symbolic dynamics, see [AM] or [PT].

Let \( A \) be an \( n \times n \), nonnegative, integral matrix, and let \( G(A) \) be the directed graph on \( n \) vertices, with \( A_{ij} \) edges from vertex \( i \) to vertex \( j \). Let \( \mathcal{E}_A = \{\text{edges of } G(A)\} \). We define the shift of finite type \( \Sigma_A = \{x \in \mathbb{Z}^n : x_{i+1} \text{ follows } x_i \text{ for all } i\} \), where \( x_{i+1} \text{ follows } x_i \) if the terminal vertex of \( x_i \) is the initial vertex of \( x_{i+1} \). \( \Sigma_A \) is a compact metric space under the product topology.

\( A \) is irreducible if for each \( i, j \), there exists \( n = n(i, j) \) such that \( A^n_{ij} > 0 \). \( \Sigma_A \) is irreducible if \( A \) is. A factor map \( f: \Sigma_A \to \Sigma_B \) is a continuous,
surjective map which commutes with the shift. \( f \) is finite-to-one if there exists \( N \in \mathbb{Z}^+ \) such that \( \# f^{-1}(y) \leq N \), for all \( y \in \sum_B \). By [CP, Corollary 4.5], this is equivalent to \( h(\sum_A) = h(\sum_B) \).

If \( D \) is a principal ideal domain, and \( g, h \in D \), we denote the greatest common divisor of \( g \) and \( h \) by \((g, h)\). If \( p(x) \in \mathbb{Z}[x] \), we denote the degree of \( p(x) \) by \( \deg p(x) \).

If \( A \) is a square, integral matrix, and \( \chi_A = p(x)x^r \), where \( r \) is the largest power of \( x \) which divides \( \chi_A \), let \( \chi_A^* = p(x) \), \( \text{rank}^* A = \deg p(x) \), and \( \det^* A = \text{constant term of } p(x) \).

If \( F \) is a field, \( A \) is a square matrix over \( F \), and \( g(x) \) is a factor of \( \chi_A \), we denote the null space of \( g(A) \) by \( N(g(A)) \). If \( V \) is a vector space over \( F \), we denote the dual space of \( V \) by \( V^* \). If \( W \) is a subspace of \( V \), the annihilator of \( W \), denoted \( \text{Ann} W \), is \( \{ f \in V^* : f(w) = 0 \text{ for all w } \in W \} \).

If \( \mathcal{L} \subseteq \mathbb{Z}^n \), \( \mathcal{L} \) is called a sublattice. \( \mathcal{L} \) is closed if \( \mathcal{L} = (\mathcal{L}) \cap \mathbb{Z}^n \), where \( (\mathcal{L}) \) denotes the rational span of \( \mathcal{L} \).

2. Main results

Definition 1. Let \( p(x) \) be a monic, integral polynomial, and \( p(x) = \prod_{i=1}^l p_i^{e_i}(x) \) be the unique factorization of \( p(x) \) in \( \mathbb{Z}[x] \), where the \( p_i(x) \) are distinct, monic, irreducible polynomials. Any factor of \( p(x) \) which is a product of some of the \( p_i^{e_i}(x) \) is called a complete factor of \( p(x) \). If \( g(x) \) is a complete factor of \( p(x) \), and \( h(x) \) is a complete factor of \( p(x)/g(x) \), then \( h(x) \) is called a complementary complete factor of \( p(x) \).

If \( f: \sum_A \rightarrow \sum_B \) is a finite-to-one factor map, then \( \chi_B^* \) divides \( \chi_A^* \) (see [K, Corollary A]). If \( g_B(x) = \prod p_i^{f_i}(x) \) is a complete factor of \( p(x) = \chi_B^* \), then \( g_A(x) = \prod p_i^{f_i}(x), f_i \geq e_i \), is a complete factor of \( \chi_A^* \), where \( f_i \) is the power to which \( p_i \) is raised in \( \chi_A^* \). Then \( g_A(x) \) is called the corresponding complete factor of \( \chi_A^* \).

Lemma 2. Let \( B \) be a \( k \times k \) integral matrix, and let \( g(x) \) be a complete factor of \( \chi_B \). Then there is a closed, \( B \)-invariant sublattice \( \mathcal{L} \subseteq N(g(B)) \) such that \( \text{rank} \mathcal{L} = \deg g(x) \).

Proof. Let \( \mathcal{L} = N(g(B)) \cap \mathbb{Z}^k \). By the Primary Decomposition Theorem ([HK, Theorem 12, p. 189]), \( \text{rank} \mathcal{L} = \deg g(x) \).

We now consider a sublattice \( \mathcal{L} \) reduced over \( \mathbb{Z}/p\mathbb{Z} \), for \( p \) a prime. Lemmas 4–6 are elementary results from linear algebra.

Definition 3. For \( p \) a fixed prime, let \( \pi: \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \) denote the natural homomorphism \( k \rightarrow k + p\mathbb{Z} \). Denote \( \pi(k) \) by \( \overline{k} \). If \( A = (a_{ij}) \) is an \( n \times n \) integral matrix, let \( \overline{A} \) denote the \( n \times n \) matrix over \( \mathbb{Z}/p\mathbb{Z} \) given by \( \overline{A}_{ij} = \overline{a}_{ij} \). If \( v = (v_1, \ldots, v_n) \in \mathbb{Z}^n \), let \( \overline{v} \in (\mathbb{Z}/p\mathbb{Z})^n \) be defined by \( \overline{v} = (\overline{v}_1, \ldots, \overline{v}_n) \). If \( \mathcal{L} \subseteq \mathbb{Z}^n \), let \( \overline{\mathcal{L}} = \{ \overline{v} : v \in \mathcal{L} \} \).
Lemma 4. If $A$ is an $n \times n$ integral matrix and $\mathcal{L} \subseteq \mathbb{Z}^n$ is a closed sublattice, then $\mathcal{L}$ is an $A$-invariant subspace of $(\mathbb{Z}/p\mathbb{Z})^n$ and $\text{rank} \mathcal{L} = \text{dim} \mathcal{L}$.

**Proof.** It is easy to check that $\mathcal{L}$ is an $A$-invariant subspace. To see that $\text{rank} \mathcal{L} = \text{dim} \mathcal{L}$, choose an integral basis $\mathcal{B} = \{\beta_1, \ldots, \beta_k\}$ for $\mathcal{L}$. We claim that $\mathcal{B} = \{\bar{\beta}_1, \ldots, \bar{\beta}_k\}$ is a basis for $\mathcal{L}$. If $\bar{v} \in \mathcal{L}$, where $v \in \mathcal{L}$, then $v = \sum_{i=1}^k c_i \beta_i$, for some $c_i \in \mathbb{Z}$, since $\mathcal{B}$ is an integral basis for $\mathcal{L}$. Therefore $\bar{v} = \sum_{i=1}^k c_i \bar{\beta}_i$, so $\mathcal{B}$ spans $\mathcal{L}$. If $\sum_{i=1}^k \bar{c}_i \bar{\beta}_i = (0, \ldots, 0)$, then $p$ divides $(\sum_{i=1}^k c_i \beta_i)_j$, for $1 \leq j \leq n$. It follows that $v = \sum_{i=1}^k (c_i/p) \beta_i \in \mathcal{L}$, since $v \in \langle \mathcal{L} \rangle \cap \mathbb{Z}^n$ and $\mathcal{L}$ is closed. This implies that $c_i/p \in \mathbb{Z}$, since $\mathcal{B}$ is an integral basis for $\mathcal{L}$. Therefore $\bar{c}_i = \bar{0}$, so $\mathcal{B}$ is linearly independent. It follows that $\text{rank} \mathcal{L} = \text{dim} \mathcal{L}$. □

Lemma 5. Let $A$ be an $n \times n$ matrix over a field $F$. Let $\overline{g}(x)$ and $\overline{h}(x)$ be factors of $\chi_A$. If $(\overline{g}(x), \overline{h}(x)) = 1$ in $F[x]$, and $v \in N(\overline{h}(A))$, $w \in N(\overline{g}(A^T))$, then $vw^T = 0$.

**Proof.** Because $(\overline{g}(x), \overline{h}(x)) = 1$, there exist $q(x), r(x) \in F[x]$ such that $\overline{g}(x)q(x) + \overline{h}(x)r(x) = 1$. Therefore $v = v\overline{g}(A)q(A)$ and $w^T = \overline{h}(A)r(A)w^T$. So $vw^T = v\overline{g}(A)q(A)\overline{h}(A)r(A)w^T = v\overline{h}(A)q(A)r(A)\overline{g}(A)w^T = 0$. □

Lemma 6. Let $U$ and $V$ be subspaces of $(\mathbb{Z}/p\mathbb{Z})^n$. Assume that $\bar{v} \bar{w}^T = \bar{0}$ for all $\bar{v} \in U$, $\bar{w} \in V$. Then $\text{dim} U \leq \text{dim} \text{Ann}(V)$.

**Proof.** It is easy to check that the linear map $\phi: (\mathbb{Z}/p\mathbb{Z})^n \to (\mathbb{Z}/p\mathbb{Z})^n$ given by $v \to f_v$, where $f_v(w) = vw^T$, is injective. Since $\phi(U) \subseteq \text{Ann}(V)$, the result follows. □

Theorem 7. Let $A$ be an $n \times n$ integral matrix, $p$ a prime, $g(x)$ a complete factor of $\chi_A^*$, with constant term $c$, and $h(x)$ a complementary complete factor of $\chi_A^*$. Assume that $(\overline{g}(x), \overline{h}(x)) = 1$ and that $(p, c) = 1$. Let $\mathcal{L}_1$ be a closed, $A$-invariant sublattice of $N(g(A))$ and $\mathcal{L}_2$ a closed, $A^T$-invariant sublattice of $N(g(A^T))$. If $p$ divides $vw^T$, for all $v \in \mathcal{L}_1$, $w \in \mathcal{L}_2$, then $\text{rank} \mathcal{L}_1 + \text{rank} \mathcal{L}_2 \leq \text{rank}^* A - \text{deg} h(x)$.

**Proof.** Let $\text{deg} h(x) = s$, and let $r$ be the largest power of $x$ which divides $\chi_A$. Clearly, $\text{rank}^* A = n - r$. Since $(p, c) = 1$, it is easy to see that $(\overline{g}(x), \overline{x}) = 1$. Let $h_1(x) = h(x)x^r$. Then $(\overline{g}(x), \overline{h_1}(x)) = 1$. We have $\dim N(h_1(A)) \leq \dim N(\overline{h_1}(A))$, since $N(h_1(A)) \cap \mathbb{Z}^n$ projects onto a subspace of $N(\overline{h_1}(A))$ whose dimension equals $\dim N(h_1(A)) \cap \mathbb{Z}^n$, by Lemma 4. Also, $\dim N(h_1(A)) = \text{deg} h_1(x) = s + r$ by the Primary Decomposition Theorem ([HK, Theorem 12]), since $h_1(x)$ is a complete factor of $\chi_A$. So $\dim N(\overline{h_1}(A)) \geq s + r$. Also, we have $\bar{v} \bar{w}^T = \bar{0}$ for all $\bar{v} \in \mathcal{L}_1$, $\bar{w} \in \mathcal{L}_2$, since $p$ divides $vw^T$. Let $U$ be the span over $\mathbb{Z}/p\mathbb{Z}$ of $N(\overline{h_1}(A))$ and $\mathcal{L}_1$. Since $\mathcal{L}_1 \subseteq N(\overline{g}(A))$ and $(\overline{g}(x), \overline{h_1}(x)) = 1$, it is easy to see that $N(\overline{h_1}(A)) \cap \mathcal{L}_1 = \{0\}$, so that $\dim U = \dim N(\overline{h_1}(A)) + \dim \mathcal{L}_1 \geq s + r + \dim \mathcal{L}_1$. Also, since
\( \mathcal{F}_2 \subseteq N(\overline{g}(A^T)) \), it follows from Lemma 5 that \( \overline{v} \overline{w}^T = \overline{0} \), for all \( \overline{v} \in U, \overline{w} \in \mathcal{F}_2 \). By Lemma 6, \( s + r + \dim \mathcal{F}_1 \leq \dim U \leq \dim \text{Ann}(\mathcal{F}_2) \). Since \( \dim \mathcal{F}_2 + \dim \text{Ann}(\mathcal{F}_2) = \dim(\mathbb{Z}/p\mathbb{Z})^n = n \) (by [HK, Theorem 17, p. 98]), we have \( s + r + \dim \mathcal{F}_1 + \dim \mathcal{F}_2 \leq n \) or \( \dim \mathcal{F}_1 + \dim \mathcal{F}_2 \leq n - r - s = \text{rank}^*A - \deg h(x) \). Since \( \dim \mathcal{F}_1 = \text{rank} \mathcal{L}_1 \) and \( \dim \mathcal{F}_2 = \text{rank} \mathcal{L}_2 \), by Lemma 4, the result follows. \( \square \)

**Theorem 8.** Suppose that \( \sum_A \) and \( \sum_B \) are irreducible shifts of finite type, and that \( f: \sum_A \to \sum_B \) is a finite-to-one factor map of degree \( d \). Suppose that \( g_B(x) \) is a complete factor of \( \chi_B^* \) and \( g_A(x) \) is the corresponding complete factor of \( \chi_A^* \), where the constant term of \( g_A(x) \) is \( c \), and that \( h(x) \) is a complementary complete factor of \( \chi_A^* \). Let \( p \) be a prime which divides \( d \), and assume that \( (\overline{g}_A(x), \overline{h}(x)) = 1 \) and that \( 2\deg g_B(x) > \text{rank}^*A - \deg h(x) \). Then \( p \) divides \( c \).

**Proof.** By [KMT, Theorem 2.3] and [T2, Definition 1.4 and Lemma 1.6] (substituting \( \mathbb{Q} \) for \( \mathbb{C} \)), there exist \( \sum_A \) topologically conjugate to \( \sum_A \), and \( \sum_B \) conjugate to \( \sum_B \), a rational \( A \)-invariant subspace \( V \), a rational \( A^T \)-invariant subspace \( W \), and surjective linear maps \( \phi: V \to \mathbb{Q}^k \) and \( \theta: W \to \mathbb{Q}^k \) (where \( \hat{B} \) is \( k \times k \)) such that \( vA\phi = \nu \phi \hat{B} \) and \( wA^T \theta = w\theta \hat{B}^T \), for all \( v \in V \), \( w \in W \). By [W, Corollary 4.8], \( \chi_A^* = \chi_A^* \) and \( \chi_B^* = \chi_B^* \), so \( g_B(x) \) is a complete factor of \( \chi_B^* \), \( g_A(x) \) is the corresponding complete factor of \( \chi_A^* \), and \( h(x) \) is a complementary complete factor of \( \chi_A^* \). It follows from Lemma 2 and duality that there exist a closed \( A \)-invariant sublattice \( \mathcal{L}_1 \subseteq N(g_A(A)) \cap V \) and a closed \( A^T \)-invariant sublattice \( \mathcal{L}_2 \subseteq N(g_A(A^T)) \cap W \) such that \( \text{rank} \mathcal{L}_1 = \text{rank} \mathcal{L}_2 = \deg g_B(x) \). So \( \text{rank} \mathcal{L}_1 + \text{rank} \mathcal{L}_2 = 2\deg g_B(x) > \text{rank}^*A - \deg h(x) \). In [T2, Theorem 2.5], it is shown that if \( v \in V \) and \( w \in W \) are \( \mathbb{Z} \)-vectors, then \( d \) divides \( vw^T \), and so \( p \) divides \( vw^T \). If \( (p, c) = 1 \), then by Theorem 7 there would exist \( v \in \mathcal{L}_1 \) and \( w \in \mathcal{L}_2 \) such that \( p \) does not divide \( vw^T \), contradicting the previous statement. Therefore \( p \) divides \( c \). \( \square \)

**Corollary 9.** Suppose that \( \sum_A \) and \( \sum_B \) are irreducible shifts of finite type, and \( f: \sum_A \to \sum_B \) is a finite-to-one factor map of degree \( d \). If \( 2\text{rank}^*B > \text{rank}^*A \), then every prime which divides \( d \) also divides \( \det^*B \). Therefore \( d \) is a unit in \( \mathbb{Z}[1/\det^*B] \).

**Proof.** Take \( g_B(x) = \chi_B^* \), \( g_A(x) = \chi_A^* \), and \( h(x) = 1 \). For any prime \( p \), the condition \( (\overline{g}_B(x), \overline{h}(x)) = 1 \) holds trivially. Since \( \deg g_B(x) = \text{rank}^*B \), \( \deg g_A(x) = \text{rank}^*B \), and the constant term of \( \chi_B^* \) is \( \det^*B \), the result follows from Theorem 8. \( \square \)

**Example 10.** Suppose that \( \sum_A \) and \( \sum_B \) are irreducible shifts of finite type, and that \( \chi_A^* = (x - 2)(x - 1)^3 \) and \( \chi_B^* = (x - 2)(x - 1)^2 \). Take \( g_B(x) = (x - 1)^2 \), \( g_A(x) = (x - 1)^3 \), and \( h(x) = x - 2 \). Observe that for any prime \( p \), \( (\overline{g}_A(x), \overline{h}(x)) = 1 \). Since \( 2\deg g_B(x) = 4 > \text{rank}^*A - \deg h(x) = 4 - 1 = 3 \),
and the constant term of $g_A(x)$ is 1, if $f: \sum_A \rightarrow \sum_B$ is a factor map, then the degree of $f$ is 1, by Theorem 8.

We remark that if we assume only that $\chi_A^* = (x - 2)(x - 1)^2$ and $\chi_B^* = (x - 2)(x - 1)$, we cannot draw the same conclusion. However, by applying Corollary 9, we can conclude that the degree of $f$ is a power of 2, but we do not have an example of a factor map between shifts with the given characteristic polynomials (modulo $x$) which has degree 2. Does such a factor map exist?

Example 11. This example shows that Corollary 9 is sharp, in general. Let

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$ and $B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$.

Then there exists a factor map $f: \sum_A \rightarrow \sum_B$, of degree 2, which is right and left resolving (and therefore constant-to-one). Then $f$ is defined as a map on states, sending states 1 and 2 of $\sum_A$ to state 1 of $\sum_B$ and states 3 and 4 of $\sum_A$ to state 2 of $\sum_A$. Note that $\det^* B = -1$, so 2 does not divide $\det^* B$, but that $2 \operatorname{rank}^* B = 4 = \operatorname{rank}^* A$.

Example 12. This example shows that the condition that $(\overline{g}(x), \overline{h}(x)) = 1$ in Theorem 8 is necessary. Let

$$A = \begin{bmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 2 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$ and $B = \begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}$.

There exists a factor map $f: \sum_A \rightarrow \sum_B$ of degree 2, similar to the one in the previous example, and $f$ maps states 1 and 2 of $\sum_A$ to state 1 of $\sum_B$ and states 3 and 4 of $\sum_A$ to state 2 of $\sum_B$. Let $p = 2$. Observe that $\chi_B = (x - 2)(x + 1)$ and $\chi_A = (x - 2)(x + 1)(x^2 - x + 2)$. Let $g_B(x) = x + 1 = g_A(x)$ and $h(x) = (x - 2)(x^2 - x + 2)$. Note that $2 \deg g_B(x) = 2 > \operatorname{rank}^* A - \deg h(x) = 4 - 3 = 1$, but that $(\overline{g}_A(x), \overline{h}(x)) \neq 1$, since $\overline{g}_A(x) = x + 1$ and $\overline{h}(x) = x^2(x + 1)$. Also, the conclusion of Theorem 8 does not hold, since the degree of $f$ is not 1.

References


Department of Mathematical Sciences, Memphis State University, Memphis, Tennessee 38152