A Lower Bound for the Degree of the Minimal Polynomial of the Kronecker Product

Cristina Caldeira*†
Departamento de Matemática
Universidade de Coimbra
Apartado 3008
3001-454 Coimbra
Portugal

May 23, 2002

Abstract

Using Kneser's Theorem [7, 8, 13] from Additive Group Theory we obtain a lower bound for the degree of the minimal polynomial of the Kronecker product of two linear operators. Using another result from Additive Group Theory (Kemperman's Theorem [6]), we also characterize equality cases of that lower bound, when the spectrum of the Kronecker product is not a periodic set in the multiplicative group of the algebraic closure of the underlying field.

Keywords: Minimal Polynomial; Kronecker Product

1 Introduction

Let $\mathbb{F}$ be an arbitrary field and let p be the characteristic of $\mathbb{F}$ in non-zero characteristic and $p = +\infty$ otherwise. $\overline{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$. If V is a finite dimension vector space over $\mathbb{F}$ and f is a linear operator on V then P_f is the minimal polynomial of f and $\sigma(f)$ is the spectrum of f over $\overline{\mathbb{F}}$, that is, the set of eigenvalues of f over $\overline{\mathbb{F}}$. For $v \in V$ the f-cyclic subspace of v is

$$\mathcal{C}_f(v) = \left\langle f^i(v) : i \in \mathbb{N}_0 \right\rangle .$$

If f is of simple structure then $\deg(P_f) = |\sigma(f)|$ where, for a polynomial q, $\deg(q)$ denotes its degree and $|X|$ denotes the cardinality of the set X.

*This research was done within the activities of "Centro de Matemática da Universidade de Coimbra".
† *Tel.:* 351-239-791173; *E-mail address:* caldeira@mat.uc.pt

Let V and W be two finite dimension vector spaces over $\mathbb{F}$ and let f and g be two linear operators on V and W, respectively. The *Kronecker product* of f and g is the unique linear operator on $V \otimes W$ such that

$$(f \otimes g)(v \otimes w) = f(v) \otimes g(w) , \quad \forall v \in V , \ \forall w \in W .$$

The *Kronecker sum* of f and g is $f \otimes I_W + I_V \otimes g$. Using the fact that $\deg(P_{f\otimes I_W + I_V \otimes g})$ equals the maximum of the dimensions of $(f \otimes I_W + I_V \otimes g)$-cyclic subspaces, Dias da Silva and Hamidoune proved [5] that

$$\deg(P_{f\otimes I_W + I_V \otimes g}) \geq \min\{p, \deg(P_f) + \deg(P_g) - 1\} . \tag{1}$$

Considering simple structure linear operators and since

$$\sigma(f \otimes I_W + I_V \otimes g) = \sigma(f) + \sigma(g) ,$$

from (1), Dias da Silva and Hamidoune proved [5] that, for A and B finite non-empty subsets of $\mathbb{F}$,

$$|A + B| \geq \min\{p, |A| + |B| - 1\} .$$

When $\mathbb{F}$ is the field of integers modulo a prime, p, this result is known as Cauchy-Davenport Theorem [2, 3, 4].

In order to obtain a lower bound for the degree of the minimal polynomial of the Kronecker product we use a slightly different method. We use a technique used (when $\mathbb{F} = \mathbb{C}$) by Marcus and Shafqat Ali in [11, 12] to obtain lower bounds for the degrees of minimal polynomials of additive commutator operators and Jordan operators. A lower bound for $|\sigma(f \otimes g)|$ and information about elementary divisors of $f \otimes g$ will allow us to obtain a lower bound for $\deg(P_{f\otimes g})$.

The lower bound for $|\sigma(f \otimes g)|$ is obtained from the fact that

$$\sigma(f \otimes g) = \sigma(f)\sigma(g)$$

and from Kneser's Theorem [7, 8, 13], applied on the multiplicative group of the algebraic closure of $\mathbb{F}$.

In certain conditions the lower bound we obtain for $\deg(P_{f\otimes g})$ is

$$\deg(P_{f\otimes g}) \geq \deg(P_f) + \deg(P_g) - 1 . \tag{2}$$

Using Kemperman's Theorem [6] we characterize the linear operators f and g for which equality is attained in (2).

2 Auxiliary results on group theory

Let G be an abelian group with multiplicative notation. A finite *geometric progression* in G is a subset of G of the form $\{ad, ad^2, \ldots, ad^k\}$, where $k \in \mathbb{N}$, $a \in G$ and $d \in G \setminus \{1\}$. Let A and B be two non-empty subsets of G and let $g \in G$. We consider

$$AB = \{ab : a \in A \text{ and } b \in B\} ,$$

$$A^{-1} = \{a^{-1} : a \in A\}$$
$$\text{and} \qquad \nu_g(A,B) = |\{(a,b) \in A \times B : ab = g\}| .$$

Definition 1 Let A be a non-empty subset of G. The *stabilizer of A in G* is the subgroup of G,

$$H(A) = \{g \in G : gA = A\} .$$

Remark 1

(i) We have $AH(A) = A$ and therefore if A is a finite non-empty subset of G then $H(A)$ is a finite subgroup;

(ii) If H is a subgroup of G, we have $AH = A$ if and only if A is the union of H-cosets. Therefore A is the union of $H(A)$-cosets.

Definition 2 Let A be a non-empty subset of G. A is a *periodic set* if $H(A) \neq \{1\}$.

Remark 2 A non-empty finite subset A of G is periodic if and only if there exists a subgroup of G, H, such that $|H| \geq 2$ and $AH = A$.

Theorem 1 (Kneser) [7, 8, 13] *Let A and B be finite non-empty subsets of the abelian group G. Let $H = H(AB)$. Then*

$$|AB| \geq |A| + |B|$$

or

$$|AB| + |H| = |AH| + |BH| .$$

From Kneser's Theorem it is easy to obtain the following results:

Corollary 1 [13, Theorem 4.3] *Let A and B be finite non-empty subsets of the abelian group G. Let $H = H(AB)$. Then*

$$|AB| \geq |AH| + |BH| - |H| .$$

Corollary 2 *Let A and B be non-empty finite subsets of G with $|B| \geq |A| \geq 2$. Then $|AB| = |B|$ if and only if there exists a finite subgroup of G, H, such that $|H| \geq 2$, $BH = B$ and $A \subseteq aH$, for all $a \in A$.*

Corollary 3 *Let A and B be two non-empty finite subsets of the abelian group G such that $|A| \geq 2$, $B = C\dot{\cup}D$, $C \neq \emptyset$, $D \neq \emptyset$ and*

$$AC = aC\,, \quad \forall a \in A\,.$$

If AD is a periodic set and $|AD| = |A| + |D| - 1$ then also AB is a periodic set.

Proof Suppose AD is periodic. Let $H = H(AD) \neq \{1\}$. From Remark 1 we have

$$AD = \dot{\bigcup_{i=1}^{n}} c_i H \,.$$

Let $d \in D$. We have $dA \subseteq AD$ and hence

$$A \subseteq \dot{\bigcup_{i=1}^{n}} d^{-1} c_i H \,.$$

Then there exist $k \in \{1, \ldots, n\}$ and $a_1, \ldots, a_k \in A$ such that

$$A \subseteq \dot{\bigcup_{i=1}^{k}} a_i H \,.$$

We have also that

$$AH = \dot{\bigcup_{i=1}^{k}} a_i H \,.$$

From the hypothesis and Kneser's Theorem we obtain

$$|A| + |D| - 1 = |AD| = |AH| + |DH| - |H| \,.$$

Since $|DH| \geq |D|$ we have $|AH| \leq |A| + |H| - 1$. Then

$$|A| \geq |AH| - |H| + 1 = (k-1)|H| + 1 \,.$$

If $k = 1$ then $A \subseteq a_1 H$. Since $|A| \geq 2$ there exists $h \in H \setminus \{1\}$ such that $a_1 h \in A$.

If $k > 1$ then $|A| \geq (k-1)|H| + 1 \geq 2k - 1 > k$. Then in this case we have also that, for some $i \in \{1, \ldots, k\}$, there exists $h \in H \setminus \{1\}$ such that $a_i h \in A$.

Next we prove that $hAB \subseteq AB$. Let $x \in AB = AC \cup AD$. If $x \in AD$ then ($H = H(AD)$) $hx \in AD \subseteq AB$.

Suppose that $x \notin AD$. Then $x \in AC = a_i C$ and there exists $c \in C$ such that $x = a_i c$. It follows that

$$hx = (a_i h)c \in AC \subseteq AB \,.$$

Then $h \in H(AB)$. Since $h \neq 1$ we conclude that AB is periodic. ■

Definition 3 [6, definition on page 78 and remark on page 82] Let (A, B) be a pair of finite non-empty subsets of the abelian group G. The pair (A, B) is said to be an *elementary pair* if it satisfies, at least, one of the following conditions:

(i) $|A| = 1$ or $|B| = 1$;

(ii) A and B are geometric progressions in G of the same rate, d, where $d \in G$ has order (not necessarily finite) greater than or equal to $|A| + |B| - 1$;

(iii) A is not periodic and there exist H, finite subgroup of G, $c \in G$ and $a \in A$ such that $A \subseteq aH$ and $B = c((AH) \setminus A)^{-1}$;

(iv) There exists $H \neq \{1\}$ finite subgroup of G such that each one of the sets A and B is a subset of an H-coset, $|A| + |B| = |H| + 1$ and there exists at least one $g \in AB$ such that $\nu_g(A, B) = 1$.

Remark 3

(1) If (A, B) satisfies (ii) then AB is a geometric progression with rate d and there exists $g \in AB$ such that $\nu_g(A, B) = 1$;

(2) If (A, B) satisfies (iii) then $AB = (cH) \setminus \{c\}$ [6, Lemma 4.2];

(3) If (A, B) satisfies (iv) then AB is an H-coset [6, Lemma 4.1];

(4) If (A, B) is an elementary pair then $|AB| = |A| + |B| - 1$;

(5) If (A, B) satisfies (iii) then B is not periodic, $B \subseteq (ca^{-1})H$ e $A = c((BH) \setminus B)^{-1}$. It follows that if (A, B) is an elementary pair then also (B, A) is elementary and of the same type.

Let H be a subgroup of G. We denote by Π_H the canonical surjection of G onto G/H,

$$\begin{array}{rccc} \Pi_H : & G & \longmapsto & G/H \\ & g & \longrightarrow & gH\,. \end{array}$$

Remark 4 If H is a finite subgroup of G and A is a finite subset of G then

$$|\Pi_H(A)| = \frac{|AH|}{|H|}\,.$$

Theorem 2 (Kemperman)[6, teorema 5.1] *Let $(G, \cdot)$ be an abelian group with, at least, two elements. Let A and B be two non-empty finite subsets of G. Then*

$$|AB| = |A| + |B| - 1$$

and

$$\textit{if } AB \textit{ is a periodic set then there exists } g \in AB \textit{ such that } \nu_g(A, B) = 1\,,$$

if and only if there exist A_1 and B_1 non-empty subsets of A and B, respectively and a subgroup J of G, with, at least, two elements, satisfying:

(i) *The pair* (A_1, B_1) *is elementary and each one of the sets* A_1*,* B_1 *is contained in a* J*-coset;*

(ii) $(A_1B_1) \cap ((A \setminus A_1)B) = \emptyset$ *and* $(A_1B_1) \cap (A(B \setminus B_1)) = \emptyset$*;*

(iii) *The sets* $A \setminus A_1$ *and* $B \setminus B_1$ *are unions of* J*-cosets;*

(iv) $|\Pi_J(A)\Pi_J(B)| = |\Pi_J(A)| + |\Pi_J(B)| - 1$.

Remark 5 If $A_1 \neq A$ or $B_1 \neq B$ then, from (iii), it follows that J is finite.

By $\overline{\mathbb{F}}^*$ we denote the multiplicative group of the field $\overline{\mathbb{F}}$. For $d \in \overline{\mathbb{F}}^*$, $\langle d \rangle$ denotes the cyclic subgroup of $\overline{\mathbb{F}}^*$, $\{d^i : i \in \mathbb{Z}\}$.

We will be interested in applying Kemperman's Theorem in the group $\overline{\mathbb{F}}^*$, so first we will characterize the finite periodic subsets and the elementary pairs in this group.

Lemma 1 *Let* J *be a finite subgroup of* $\overline{\mathbb{F}}^*$*, with order* n*. Then*

$$J = \left\{x \in \overline{\mathbb{F}}^* : x^n = 1\right\} = \langle d \rangle \ ,$$

for some $d \in \overline{\mathbb{F}}^*$*, with finite order* n*. Moreover, if* p *is finite then* $n \not\equiv 0 \pmod{p}$*.*

Proof Let $J = \{a_1, a_2, \ldots, a_n\}$ with $a_i \neq a_j$ if $i \neq j$. For all i, $a_i^n = a_i^{|J|} = 1$ and so

$$J \subseteq \left\{x \in \overline{\mathbb{F}}^* : x^n = 1\right\} .$$

From

$$\left|\left\{x \in \overline{\mathbb{F}}^* : x^n = 1\right\}\right| \leq n$$

it follows that

$$J = \left\{x \in \overline{\mathbb{F}}^* : x^n = 1\right\} .$$

Suppose p is finite and divides n. Then $n = pq$ for some integer $q \geq 1$ and

$$\begin{aligned} x \in J \ &\Rightarrow \ x^n = 1 \\ &\Rightarrow \ (x^q)^p = 1 \\ &\Rightarrow \ (x^q - 1)^p = 0 \\ &\Rightarrow \ x^q - 1 = 0\,. \end{aligned}$$

Hence

$$|J| \leq \left|\left\{x \in \overline{\mathbb{F}}^* : x^q = 1\right\}\right| \leq q < n\,,$$

but this is a contradiction. Then p does not divide n and we can take a primitive n-root of the unity for d. ■

From this Lemma and Remark 1 we obtain:

Lemma 2 *Let A be a finite non-empty subset of $\overline{\mathbb{F}}^*$. Then A is periodic if and only if A is of the form*

$$A = \dot{\bigcup_{i=1}^{s}} a_i \langle d \rangle = \dot{\bigcup_{i=1}^{s}} \{x \in \overline{\mathbb{F}}^* : x^n = a_i^n\} ,$$

for some $s \in \mathbb{N}$, $a_1, a_2, \ldots, a_s \in A$ and $d \in \overline{\mathbb{F}}^*$ with order $n \geq 2$ such that $n \not\equiv 0 \pmod{p}$ (if p is finite).

Lemma 3 *Let (A, B) be a pair of finite non-empty subsets of $\overline{\mathbb{F}}^*$. The pair (A, B) is an elementary pair in the group $\overline{\mathbb{F}}^*$ if and only if it satisfies, at least, one of the following conditions:*

(I) $|A| = 1$ *or* $|B| = 1$*;*

(II) *A and B are geometric progressions in $\overline{\mathbb{F}}^*$ of the same rate, d, where $d \in \overline{\mathbb{F}}^*$ has order (not necessarily finite) greater than or equal to $|A| + |B| - 1$;*

(III) *A is not periodic and there exist $a \in A$, $d \in \overline{\mathbb{F}}^*$ with finite order k such that $k \not\equiv 0 \pmod{p}$ (if p is finite) and $c \in \overline{\mathbb{F}}^*$ satisfying*

$$A \subsetneqq a \langle d \rangle$$

and

$$B = c\,(a \langle d \rangle \setminus A)^{-1} \;;$$

(IV) *There exist $a, a_1 \in A$, $d \in \overline{\mathbb{F}}^*$ with finite order k such that $k \not\equiv 0 \pmod{p}$(if p is finite) and $c \in \overline{\mathbb{F}}^*$ satisfying*

$$A \subseteq a \langle d \rangle$$

and

$$B = c\,(a \langle d \rangle \setminus A)^{-1} \dot{\cup} \{c a_1^{-1}\} .$$

Proof Using Lemma 1 it is easy to prove that (A, B) is elementary of type (iii) if and only if (A, B) satisfies (III).

Suppose (A, B) is elementary of type (iv) and let us prove that (A, B) satisfies (IV). Using Lemma 1 and considering d such that $H = \{1, d, \ldots, d^{k-1}\}$ it is easy to prove that

$$A = a\{d^{i_1}, d^{i_2}, \ldots, d^{i_r}\}$$

and

$$B = b\{d^{j_1}, d^{j_2}, \ldots, d^{j_s}\} ,$$

where $r + s = k + 1$, $0 = i_1 < i_2 < \cdots < i_r \leq k - 1$ and $0 = j_1 < j_2 < \cdots < j_s \leq k - 1$. Let $c \in AB$ be such that $\nu_c(A, B) = 1$. There exist $u \in \{1, 2, \ldots, r\}$ and $v \in \{1, 2, \ldots, s\}$ such that

$$c = (\underbrace{a d^{i_u}}_{\in A})(\underbrace{b d^{j_v}}_{\in B}) .$$

For $\ell = 1, 2, \ldots, s$ with $\ell \neq v$ we have

$$bd^{j_\ell} = ca^{-1}d^{-i_u - j_v + j_\ell}\,.$$

Since $d^{-i_u-j_v+j_\ell} \in H$, there exists $t \in \{0, 1, \ldots, k-1\}$ such that $bd^{j_\ell} = ca^{-1}d^{k-t}$. Suppose $t \in \{i_1, i_2, \ldots, i_r\}$. Then

$$c = (\underbrace{ad^t}_{\in A})(\underbrace{bd^{j_\ell}}_{\in B})\,.$$

But this contradicts $\nu_c(A, B) = 1$, because $bd^{j_v} \neq bd^{j_\ell}$. Then $t \notin \{i_1, i_2, \ldots, i_r\}$. It follows that

$$b\left\{d^{j_\ell} : \ell = 1, 2, \ldots, s, \ell \neq v\right\} = ca^{-1}\left\{d^{k-t} : t \in \{0, 1, \ldots, k-1\} \setminus \{i_1, \ldots, i_r\}\right\}\,.$$

Let $a_1 = ad^{i_u}$. Since $bd^{j_v} = ca^{-1}d^{k-i_u} = ca_1^{-1}$ we obtain that B is of the required form.

Now suppose (A, B) satisfies (IV). Consider the subgroup $H = \langle d \rangle = \{1, d, \ldots, d^{k-1}\}$. Then $A \subseteq aH$, $B \subseteq ca^{-1}H$ and

$$|A| + |B| = |H| + 1\,.$$

In order to prove that (A, B) is elementary of type (iv) it remains to prove that $\nu_g(A, B) = 1$ for some g. We shall prove that $\nu_c(A, B) = 1$. Let $A = a\{d^{i_1}, d^{i_2}, \ldots, d^{i_r}\}$, where $0 = i_1 < i_2 < \cdots < i_r \leq k-1$. We have

$$c = \underbrace{a_1}_{\in A}\underbrace{(ca_1^{-1})}_{\in B}\,.$$

Suppose

$$c = (\underbrace{ad^t}_{\in A})b\,,$$

for some $t \in \{i_1, \ldots, i_r\}$ and $b \in B \setminus \{ca_1^{-1}\}$. Then $b = ca^{-1}d^{k-j}$ for some $j \in \{0, 1, \ldots, k-1\} \setminus \{i_1, \ldots, i_r\}$. Hence

$$d^{t+k-j} = 1$$

and $t - j \equiv 0 \pmod{k}$. Since $t - j \in [-k+1, k-1]$, it must be $t = j$ and this is a contradiction. Then $\nu_c(A, B) = 1$. ■

Applying Kemperman's Theorem in the group $\overline{\mathbb{F}}^*$ we obtain

Corollary 4 *Let A and B be two non-empty finite subsets of $\overline{\mathbb{F}}^*$ and suppose that AB is not periodic. Then*

$$|AB| = |A| + |B| - 1$$

if and only if

the pair (A, B) is elementary of one of the types (I),(II) or (III) (types considered in Lemma 3) *or*

there exist a positive integer $n \geq 2$ *such that* $n \not\equiv 0 \pmod p$, $d \in \overline{\mathbb{F}}^*$ *with order* n, $a_1, a_2, \ldots, a_k \in A$, *and* $b_1, b_2, \ldots, b_\ell \in B$ *such that*

(i) $A = A_1 \dot{\bigcup} \left(\dot{\bigcup}_{i=2}^{k} a_i \langle d \rangle \right)$, $A_1 \subseteq a_1 \langle d \rangle$,

$B = B_1 \dot{\bigcup} \left(\dot{\bigcup}_{j=2}^{\ell} b_j \langle d \rangle \right)$, $B_1 \subseteq b_1 \langle d \rangle$,

where (A_1, B_1) *is elementary;*

(ii) $\left(a_1 b_1 a_i^{-1} b_j^{-1}\right) \neq 1$ *if* $(i, j) \neq (1, 1)$;

(iii) $|\{a_i^n b_j^n : i = 1, 2, \ldots, k\,,\ j = 1, 2, \ldots, \ell\}| = k + \ell - 1$.

Remark 6 If AB is periodic, conditions given in Corollary 4 are sufficient for $|AB| = |A| + |B| - 1$.

3 Auxiliary results on elementary divisors

Let $V \neq \{0\}$ and $W \neq \{0\}$ be two finite dimension vector spaces over $\mathbb{F}$. Let f and g be two linear operators on V and W, respectively. We consider the elementary divisors of f, g and $f \otimes g$ over $\overline{\mathbb{F}}$.

If the field $\mathbb{F}$ is a field of zero characteristic there is a well-known result [1, 15][10, chapter 7,Theorem 1.4] that characterizes the elementary divisors of the Kronecker product $f \otimes g$ in terms of the elementary divisors of f and g. That result is no longer valid over a field of finite characteristic.

The following Lemma is easily proved by induction on ℓ.

Lemma 4 *Let* k *and* q *be positive integers and let* C *and* D *be square matrices, over* $\mathbb{F}$, *of order* q *that commute. Let* F *be the square matrix of order* kq *defined by*

$$F = \begin{bmatrix} C & D & 0 & \cdots & 0 \\ & C & D & \ddots & \vdots \\ & & \ddots & \ddots & 0 \\ & 0 & & \ddots & D \\ & & & & C \end{bmatrix}.$$

For $\ell \in \mathbb{N}$,

$$F^{\ell} = \begin{bmatrix} F_1^{(\ell)} & F_2^{(\ell)} & \cdots & \cdots & F_k^{(\ell)} \\ & F_1^{(\ell)} & F_2^{(\ell)} & \ddots & \vdots \\ & & \ddots & \ddots & \vdots \\ & 0 & & \ddots & F_2^{(\ell)} \\ & & & & F_1^{(\ell)} \end{bmatrix},$$

where, for $j = 1, 2, \ldots, k$,

$$F_j^{(\ell)} = \begin{cases} \binom{\ell}{j-1} C^{\ell-j+1} D^{j-1} & \text{if} \quad 1 \le j \le \ell+1 \\ 0 & \text{if} \qquad j \ge \ell+2 \end{cases} .$$

Lemma 5 *If f and g are cyclic linear operators on V and W, respectively, with $P_f = (X-a)^k$ and $P_g = (X-b)^q$ ($k, q \ge 1$), then*

(a) *If $ab \neq 0$, $p \ge k$ and $p \ge q$,*

$$P_{f\otimes g} = (X - ab)^{\min\{p, k+q-1\}};$$

(b) *If $ab \neq 0$ and $p < \max\{k, q\}$, $P_{f\otimes g} = (X-ab)^t$, where*

$$t \;=\; \min\left\{ \ell \in [\max\{k,q\}, k+q-1] \cap \mathbb{N} : \binom{\ell}{j-1} \equiv 0 \pmod{p}, \right. \\ \left. \forall j \in \{\ell - q + 2, \ldots, k\} \right\} > p;$$

(c) *If $a = b = 0$, $P_{f\otimes g} = X^{\min\{k,q\}}$;*

(d) *If $a \neq 0$ e $b = 0$, $P_{f\otimes g} = X^q$;*

(e) *If $a = 0$ e $b \neq 0$, $P_{f\otimes g} = X^k$.*

Proof Since $\sigma(f \otimes g) = \{ab\}$, the minimal polynomial $P_{f\otimes g}$ has the form $(X-ab)^t$, where $t \in \mathbb{N}$. For $n \in \mathbb{N}$ let U_n denote the square matrix of order n with ones in $(i, i+1)$ entries and zeros elsewhere.

There exist basis of V and W in respect which f and g have matricial representations $A = aI_k + U_k$ and $B = bI_q + U_q$, respectively. Then there exists a basis of $V \otimes W$ in respect which $f \otimes g$ has matricial representation

$$A \otimes B = abI_{kq} + bU_k \otimes I_q + aI_k \otimes U_q + U_k \otimes U_q .$$

Suppose $ab \neq 0$.

Let $C = A \otimes B - (ab)I_{kq} = aI_k \otimes U_q + U_k \otimes B$. Then

$$C = \begin{bmatrix} aU_q & B & 0 & \cdots & 0 \\ & aU_q & B & \ddots & \vdots \\ & & \ddots & \ddots & 0 \\ & 0 & & \ddots & B \\ & & & & aU_q \end{bmatrix}.$$

Since B and aU_q commute, using the previous Lemma, we know that for $\ell \in \mathbb{N}$, C^ℓ is of the form

$$C^\ell = \begin{bmatrix} C_1^{(\ell)} & C_2^{(\ell)} & \cdots & \cdots & C_k^{(\ell)} \\ & C_1^{(\ell)} & C_2^{(\ell)} & \ddots & \vdots \\ & & \ddots & \ddots & \vdots \\ & 0 & & \ddots & C_2^{(\ell)} \\ & & & & C_1^{(\ell)} \end{bmatrix}, \tag{3}$$

where, for $j = 1, \ldots, k$,

$$C_j^{(\ell)} = \begin{cases} \binom{\ell}{j-1} a^{\ell-j+1} U_q^{\ell-j+1} B^{j-1} & \text{if} \quad 1 \le j \le \ell+1 \\ 0 & \text{if} \quad j \ge \ell+2 \end{cases}.$$

Let $\ell \in \mathbb{N}$. If $\ell \le q-1$, $U_q^\ell \neq 0$ and $(a \neq 0)$

$$C_1^{(\ell)} = a^\ell U_q^\ell \neq 0\,.$$

If $\ell \le k-1$,

$$C_{\ell+1}^{(\ell)} = B^\ell \neq 0 \ (b \neq 0)\,.$$

Hence we have proved that, for $\ell \in \{1, \ldots, \max\{k-1, q-1\}\}$, $C^\ell \neq 0$.

Next we prove that $C^{k+q-1} = 0$. For $j = 1, \ldots, k$,

$$C_j^{(k+q-1)} = \binom{k+q-1}{j-1} a^{k+q-j} U_q^{k+q-j} B^{j-1}$$

and this block is zero because $k+q-j \ge q$ and therefore $U_q^{k+q-j} = 0$. From (3) we have $C^{k+q-1} = 0$.

(a) Suppose $p \ge k$ and $p \ge q$.

For $\max\{k, q\} \le \ell \le \min\{p-1, k+q-2\}$,

$$C_k^{(\ell)} = \binom{\ell}{k-1} a^{\ell-k+1} U_q^{\ell-k+1} B^{k-1}\,.$$

The $(1, \ell-k+2)$-entry of this matrix is $a^{\ell-k+1}\binom{\ell}{k-1} b^{k-1} \neq 0$. Then $C^\ell \neq 0$.

Next we prove that $C^p = 0$. For $j = 1, \ldots, k$,

$$C_j^{(p)} = \binom{p}{j-1} a^{p-j+1} U_q^{p-j+1} B^{j-1} .$$

For $j = 2, \ldots, k$ we have $1 \le j-1 \le p-1$ and therefore $\binom{p}{j-1} \equiv 0 \pmod{p}$. For $j = 1$ we have $C_1^{(p)} = a^p U_q^p$ and this matrix is zero because $p \ge q$. Since C^p is of the form (3) we conclude that $C^p = 0$.

(b) Suppose $p < \max\{k, q\}$. We have already proved that

$$C^\ell \neq 0 , \quad \ell = 1, \ldots, \max\{k-1, q-1\} ,$$

and that

$$C^{k+q-1} = 0 .$$

Then $\max\{k, q\} \le t \le k+q-1$.

For $\ell = \max\{k, q\}, \ldots, k+q-2$, C^ℓ is of the form (3), where

$$C_j^{(\ell)} = \binom{\ell}{j-1} a^{\ell-j+1} U_q^{\ell-j+1} B^{j-1} , \quad j = 1, \ldots, k .$$

Since $U_q^{\ell-j+1} \neq 0 \Leftrightarrow j \ge \ell - q + 2$ we have

$$C_j^{(\ell)} = \begin{cases} \binom{\ell}{j-1} a^{\ell-j+1} U_q^{\ell-j+1} B^{j-1} & \text{if} \quad \ell - q + 2 \le j \le k \\ 0 & \text{if} \quad 1 \le j \le \ell - q + 1 \end{cases} .$$

For $\ell - q + 2 \le j \le k$, the $(1, \ell - j + 1)$-entry of matrix $a^{\ell-j+1} U_q^{\ell-j+1} B^{j-1}$ is $a^{\ell-j+1} b^{j-1} \neq 0$. Then, for $j \in \{\ell - q + 2, \ldots, k\}$,

$$C_j^{(\ell)} = 0 \Leftrightarrow \binom{\ell}{j-1} \equiv 0 \pmod{p} .$$

Hence

$$C^\ell = 0 \Leftrightarrow \forall j \in [\ell - q + 2, k] \cap \mathbb{N} , \ \binom{\ell}{j-1} \equiv 0 \pmod{p}$$

and

$$t = \min \left\{ \ell \in [\max\{k, q\}, k+q-1] \cap \mathbb{N} : \binom{\ell}{j-1} \equiv 0 \pmod{p} , \right. \\ \left. \forall j \in \{\ell - q + 2, \ldots, k\} \right\} .$$

Proofs of other cases are similar. ∎

Lemma 6 *Let f and g be two linear operators on V and W respectively.*

(a) *Let $(X-a)^k$ and $(X-b)^q$ be elementary divisors,over $\overline{\mathbb{F}}$, of f and g respectively.*

If $p \geq k$, $p \geq q$ and $ab \neq 0$ then

$$(X-ab)^{\min\{p,k+q-1\}} \text{is an elementary divisor, over } \overline{\mathbb{F}}\,,\ \text{of } f \otimes g\,;$$

If $p < \max\{k,q\}$ and $ab \neq 0$ then $f \otimes g$ has an elementary divisor, over $\overline{\mathbb{F}}$,of the form $(X-ab)^t$, where

$$t \;=\; \min\left\{\ell \in [\max\{k,q\}, k+q-1] \cap \mathbb{N} : \binom{\ell}{j-1} \equiv 0 \pmod{p}, \right.$$
$$\left. \forall j \in \{\ell-q+2,\ldots,k\}\right\} > p\,;$$

If $a=b=0$ then $X^{\min\{k,q\}}$ is an elementary divisor, over $\overline{\mathbb{F}}$, of $f \otimes g$;

If $a \neq 0$ and $b=0$ then X^q is an elementary divisor, over $\overline{\mathbb{F}}$, of $f \otimes g$;

If $a=0$ and $b \neq 0$ then X^k is an elementary divisor, over $\overline{\mathbb{F}}$, of $f \otimes g$;

(b) *If $c \neq 0$, $(X-c)^t$is an elementary divisor, over $\overline{\mathbb{F}}$, of $f \otimes g$ and $(X-c)^{t+1}$ does not divide $P_{f\otimes g}$ (in $\overline{\mathbb{F}}[X]$), then there exist $(X-a)^k$ and $(X-b)^q$ elementary divisors, over $\overline{\mathbb{F}}$, of f and g respectively, with $ab=c$ and such that either*
$p \geq k$, $p \geq q$ and $t = \min\{p, k+q-1\}$
or
$p < \max\{k,q\}$ and

$$t \;=\; \min\left\{\ell \in [\max\{k,q\}, k+q-1] \cap \mathbb{N} : \binom{\ell}{j-1} \equiv 0 \pmod{p}, \right.$$
$$\left. \forall j \in \{\ell-q+2,\ldots,k\}\right\} > p\,.$$

Proof This Lemma follows from the previous one since, if A and B are similar, over $\overline{\mathbb{F}}$, to

$$\bigoplus_{i=1}^{r}(a_iI_{n_i}+U_{n_i}) \quad \text{and} \quad \bigoplus_{j=1}^{s}\left(b_jI_{m_j}+U_{m_j}\right)\,,$$

respectively, then $A \otimes B$ is similar, over $\overline{\mathbb{F}}$, to

$$\bigoplus_{i=1}^{r}\bigoplus_{j=1}^{s}(a_iI_{n_i}+U_{n_i}) \otimes (b_jI_{m_j}+U_{m_j})\,,$$

and the elementary divisors, over $\overline{\mathbb{F}}$, of $A \otimes B$ are obtained considering the elementary divisors of all matrices

$$(a_iI_{n_i}+U_{n_i}) \otimes (b_jI_{m_j}+U_{m_j})\,, \quad i=1,\ldots,r,\ j=1,\ldots,s\,.$$

■

Lemma 7 *Let f and g be two linear operators on V and W respectively. Then $P_{f\otimes g} = P_{g\otimes f}$.*

Proof It is easy to prove that if $q(X)$ is an annihilating polynomial of $f \otimes g$ then $q(X)$ is an annihilating polynomial of $g \otimes f$. ■

4 Lower bound for the degree of the minimal polynomial of the Kronecker product

Assuming that none of the spectra of the linear operators f or g is $\{0\}$, we have

Theorem 3 *Suppose $|\sigma(f) \setminus \{0\}| \geq 1$ and $|\sigma(g) \setminus \{0\}| \geq 1$. Let k_1, k_2 be nonnegative integers such that X^{k_1} is the power of X with maximal degree that divides P_f and X^{k_2} is the power of X with maximal degree that divides P_g. Let H be the stabilizer of $\sigma(f \otimes g) \setminus \{0\}$in the group $\overline{\mathbb{F}}^*$. Then*

$$\begin{aligned}\deg(P_{f\otimes g}) \quad \geq \quad & \min\{p + \max\{k_1, k_2\}, \deg(P_f) + \deg(P_g) + |\sigma(f)\ H| + |\sigma(g)\ H| - \\ & |\sigma(f)| - |\sigma(g)| - |H| - \min\{k_1, k_2\}\}\,.\end{aligned}$$

Proof Let $a_1, a_2, \ldots, a_r \in \overline{\mathbb{F}}^*$ and $b_1, b_2, \ldots, b_s \in \overline{\mathbb{F}}^*$ (where $r, s \geq 1$) be the nonzero distinct eigenvalues of f and g, respectively. For $i = 1, 2, \ldots, r$, let n_i be the maximal degree of the powers of $X - a_i$ in the list of elementary divisors, over $\overline{\mathbb{F}}$, of f. For $j = 1, 2, \ldots, s$, let m_j be the maximal degree of the powers of $X - b_j$ in the list of elementary divisors, over $\overline{\mathbb{F}}$, of g. Suppose that $a_1, a_2, \ldots, a_r$ and $b_1, b_2, \ldots, b_s$ are ordered in such way that $n_1 \geq n_2 \geq \cdots \geq n_r$ and $m_1 \geq m_2 \geq \cdots \geq m_s$.

From Lemma 6, part (a), we conclude that $X^{\max\{k_1,k_2\}}$ divides $P_{f\otimes g}$.

If $p < n_1$ or $p < m_1$ then (Lemma 6, part (a)) $f \otimes g$ has an elementary divisor of the form $(X - a_1 b_1)^t$, where $t > p$. Since $a_1 b_1 \neq 0$, it follows that

$$\deg(P_{f\otimes g}) \geq \max\{k_1, k_2\} + t > \max\{k_1, k_2\} + p\,,$$

which proves the result.

Suppose

$$p \geq n_1 \geq n_2 \geq \cdots \geq n_r$$

and

$$p \geq m_1 \geq m_2 \geq \cdots \geq m_s\,.$$

If $p \leq n_1 + m_1 - 1$, then from Lemma 6, part (a), we have $\deg(P_{f\otimes g}) \geq \max\{k_1, k_2\} + p$.

Suppose $p > n_1 + m_1 - 1$. Then

$$p > n_i + m_j - 1\,, \qquad i = 1, \ldots, r\,, \quad j = 1, \ldots, s\,.$$

Over the field $\overline{\mathbb{F}}$ the minimal polynomials of f and g factorize as

$$P_f = X^{k_1} \prod_{i=1}^{r} (X - a_i)^{n_i} \text{ and } P_g = X^{k_2} \prod_{j=1}^{s} (X - b_j)^{m_j} .$$

Without loss of generality assume that $s \geq r$.

The elements of $\overline{\mathbb{F}}^*$,

$$a_1 b_1, a_1 b_2, \ldots, a_1 b_s$$

are s distinct eigenvalues of $f \otimes g$ and, for $j = 1, 2, \ldots, s$, $(X - a_1 b_j)^{n_1 + m_j - 1}$ is an elementary divisor of $f \otimes g$ over $\overline{\mathbb{F}}$. Since $X^{\max\{k_1, k_2\}}$ divides $P_{f \otimes g}$ we have

$$P_{f \otimes g} = X^{\max\{k_1, k_2\}} \prod_{j=1}^{s} (X - a_1 b_j)^{n_1 + m_j - 1} q(X) ,$$

where $q(X)$ is a polynomial with coefficients in $\overline{\mathbb{F}}$.

From Corollary 1 of Kneser's Theorem, applied to $\sigma(f) \setminus \{0\}$ and $\sigma(g) \setminus \{0\}$ we obtain

$$|\sigma(f \otimes g) \setminus \{0\}| = |(\sigma(f) \setminus \{0\})(\sigma(g) \setminus \{0\})| \geq |(\sigma(f) \setminus \{0\})\, H| + |(\sigma(g) \setminus \{0\})\, H| - |H| ,$$

where H is the stabilizer of $\sigma(f \otimes g) \setminus \{0\}$ in $\overline{\mathbb{F}}^*$. Therefore $q(X)$ has, at least, $|(\sigma(f) \setminus \{0\})\, H| + |(\sigma(g) \setminus \{0\})\, H| - |H| - s$ distinct roots in $\overline{\mathbb{F}}^*$ and

$$\begin{aligned}
\deg(P_{f \otimes g}) &= \max\{k_1, k_2\} + \sum_{j=1}^{s} (n_1 + m_j - 1) + \deg(q(X)) \\
&\geq \max\{k_1, k_2\} - k_2 + s n_1 + \deg(P_g) - 2s + |(\sigma(f) \setminus \{0\})\, H| + \\
&\qquad\qquad |(\sigma(g) \setminus \{0\})\, H| - |H| \\
&\geq \max\{k_1, k_2\} - k_2 + r n_1 + \deg(P_g) + |(\sigma(f) \setminus \{0\})\, H| + \\
&\qquad\qquad |(\sigma(g) \setminus \{0\})\, H| - |H| - r - s + (s - r)(n_1 - 1) \\
&\geq \max\{k_1, k_2\} - k_1 - k_2 + \deg(P_f) + \deg(P_g) + |(\sigma(f) \setminus \{0\})\, H| + \\
&\qquad\qquad |(\sigma(g) \setminus \{0\})\, H| - |\sigma(f) \setminus \{0\}| - |\sigma(g) \setminus \{0\}| - |H| .
\end{aligned}$$

Since

$$\begin{aligned}
|(\sigma(f) \setminus \{0\})\, H| - |\sigma(f) \setminus \{0\}| &= |\sigma(f)\, H| - |\sigma(f)| , \\
|(\sigma(g) \setminus \{0\})\, H| - |\sigma(g) \setminus \{0\}| &= |\sigma(g)\, H| - |\sigma(g)|
\end{aligned}$$

and $\max\{k_1, k_2\} - k_1 - k_2 = -\min\{k_1, k_2\}$, the result follows. ∎

In case that $0 \notin \sigma(f)$, $0 \notin \sigma(g)$ and $\sigma(f \otimes g) = \sigma(f)\sigma(g)$ is not a periodic set in the group $\overline{\mathbb{F}}^*$, the lower bound obtained from Theorem 3 is equal to the lower bound established in [5] for the Kronecker sum $f \otimes I_W + I_V \otimes g$:

Corollary 5 *Suppose $0 \notin \sigma(f)$, $0 \notin \sigma(g)$ and $\sigma(f \otimes g) = \sigma(f)\sigma(g)$ is not a periodic set in the group $\overline{\mathbb{F}}^*$. Then*

$$\deg(P_{f \otimes g}) \geq \min\{p, \deg(P_f) + \deg(P_g) - 1\} .$$

If one of the minimal polynomials P_f or P_g is a power of X then the minimal polynomial of $f \otimes g$ can be easily evaluated. Suppose both P_f and P_g are powers of X. If $P_f = X^k$ and $P_g = X^q$ then (Lemma 6) $X^{\min\{k,q\}}$ divides $P_{f\otimes g}$. But

$$(f \otimes g)^{\min\{k,q\}}(v \otimes w) = f^{\min\{k,q\}}(v) \otimes g^{\min\{k,q\}}(w) = 0\,, \quad \forall v \in V\,,\ \forall w \in W\,.$$

Therefore $P_{f\otimes g} = X^{\min\{k,q\}}$.

Suppose now that P_f is a power of X and P_g is not. Then (Lemma 6) P_f divides $P_{f\otimes g}$. Since

$$(f \otimes g)^{\deg(P_f)}(v \otimes w) = f^{\deg(P_f)}(v) \otimes g^{\deg(P_f)}(w) = 0\,, \quad \forall v \in V\,,\ \forall w \in W\,,$$

we have $P_{f\otimes g} = P_f$.

5 Equality cases

Next we use Kemperman's Theorem to characterize equality cases in Corollary 5.

In next Theorem we assume that $0 \notin \sigma(f)$ and $0 \notin \sigma(g)$. By $a_1, a_2, \ldots, a_r \in \overline{\mathbb{F}}^*$ and $b_1, b_2, \ldots, b_s \in \overline{\mathbb{F}}^*$ (where $r, s \geq 1$) we denote the distinct eigenvalues of f and g, respectively. For $i = 1, 2, \ldots, r$, n_i is the maximal degree of the powers of $X - a_i$ in the list of elementary divisors, over $\overline{\mathbb{F}}$, of f. For $j = 1, 2, \ldots, s$, m_j is the maximal degree of the powers of $X - b_j$ in the list of elementary divisors, over $\overline{\mathbb{F}}$, of g. We suppose that $a_1, a_2, \ldots, a_r$ and $b_1, b_2, \ldots, b_s$ are ordered in such way that $n_1 \geq n_2 \geq \cdots \geq n_r$ and $m_1 \geq m_2 \geq \cdots \geq m_s$. Over $\overline{\mathbb{F}}$ we can factorize P_f and P_g as

$$P_f = \prod_{i=1}^{r}(X - a_i)^{n_i} \text{ and } P_g = \prod_{j=1}^{s}(X - b_j)^{m_j}\,.$$

Theorem 4 *Suppose $\sigma(f \otimes g) = \sigma(f)\sigma(g)$ is not a periodic set in the group $\overline{\mathbb{F}}^*$ and $s = |\sigma(g)| \geq |\sigma(f)| = r$. Then*

$$\deg(P_{f\otimes g}) = \min\{p, \deg(P_f) + \deg(P_g) - 1\} \tag{4}$$

if and only if all the elementary divisors, over $\overline{\mathbb{F}}$, of f and g have degrees less than or equal to p, and one of the following conditions holds:

(a) $|\sigma(f)| = |\sigma(g)| = 1$*;*

(b) $p \geq \deg(P_g)$ *and f is a scalar linear operator;*

(c) $p \geq \deg(P_f) + \deg(P_g) - 1$*, f and g are linear operators of simple structure over $\overline{\mathbb{F}}$ and* *the pair $(\sigma(f), \sigma(g))$ is elementary, in $\overline{\mathbb{F}}^*$, of one of the types (I), (II) or (III) (described in Lemma 3)*

or

there exist a positive integer $n \geq 2$, such that $n \not\equiv 0 \pmod p$, $d \in \overline{\mathbb{F}}^*$ with order n, $\lambda_1, \lambda_2, \ldots, \lambda_k \in \sigma(f)$, and $\mu_1, \mu_2, \ldots, \mu_\ell \in \sigma(g)$ such that

(i) $\sigma(f) = A_1 \dot{\bigcup} \left(\dot{\bigcup}_{i=2}^{k} \lambda_i \langle d \rangle \right)$, $A_1 \subseteq \lambda_1 \langle d \rangle$,

$\sigma(g) = B_1 \dot{\bigcup} \left(\dot{\bigcup}_{j=2}^{\ell} \mu_j \langle d \rangle \right)$, $B_1 \subseteq \mu_1 \langle d \rangle$,

where (A_1, B_1) is elementary;

(ii) $\left(\lambda_1 \mu_1 \lambda_i^{-1} \mu_j^{-1}\right)^n \neq 1$ *if* $(i,j) \neq (1,1)$;

(iii) $|\{\lambda_i^n \mu_j^n : i = 1, 2, \ldots, k\,,\ j = 1, 2, \ldots \ell\}| = k + \ell - 1$.

(d) *$p \geq \deg(P_f) + \deg(P_g) - 1$, f is a linear operator of simple structure over $\overline{\mathbb{F}}$, $r = |\sigma(f)| < |\sigma(g)| = s$ and there exist $t \in \{r, r+1, \ldots, s-1\}$, an integer $m \geq 2$, such that $m \not\equiv 0 \pmod p$, $d_1 \in \overline{\mathbb{F}}^*$ with order m, satisfying*

(d1) $\begin{cases} m_1 = m_2 = \cdots = m_r \geq m_{r+1} \geq \cdots \geq m_t > 1 = m_{t+1} = \cdots = m_s\,, \\ \sigma(f) \subseteq a \langle d_1 \rangle\,, \forall a \in \sigma(f)\,, \\ \{b_1, b_2, \ldots, b_t\} \text{ is the union of } \langle d_1 \rangle \text{-cosets} \end{cases}$

and

(d2) *the pair $(\sigma(f), \{b_{t+1}, \ldots, b_s\})$ is elementary, in $\overline{\mathbb{F}}^*$, of one of the types (I), (II) or (III)*

or

there exist a positive integer $n \geq 2$, such that $n \not\equiv 0$, $d \in \overline{\mathbb{F}}^*$ with order n, $\lambda_1, \lambda_2, \ldots, \lambda_k \in \sigma(f)$, and $\mu_1, \mu_2, \ldots, \mu_\ell \in \{b_{t+1}, \ldots, b_s\}$ such that

(i) $\sigma(f) = A_1 \dot{\bigcup} \left(\dot{\bigcup}_{i=2}^{k} \lambda_i \langle d \rangle \right)$, $A_1 \subseteq \lambda_1 \langle d \rangle$,

$\{b_{t+1}, \ldots, b_s\} = B_1 \dot{\bigcup} \left(\dot{\bigcup}_{j=2}^{\ell} \mu_j \langle d \rangle \right)$, $B_1 \subseteq \mu_1 \langle d \rangle$,

where (A_1, B_1) is elementary;

(ii) $\left(\lambda_1\mu_1\lambda_i^{-1}\mu_j^{-1}\right)^n \neq 1 \quad$ *if* $\quad (i,j)\neq(1,1)$*;*

(iii) $|\{\lambda_i^n\mu_j^n : i=1,2,\ldots,k\,,\ j=1,2,\ldots\ell\}| = k+\ell-1$.

Remark 7 From Lemma 7 we have $P_{f\otimes g} = P_{g\otimes f}$. Then in case $s = |\sigma(g)| \leq |\sigma(f)| = r$ we have a similar result, obtained from Theorem 4 by exchanging the roles of f and g.

Proof

Sufficient condition

(a) $P_f = (X-a_1)^{n_1}$ and $P_g = (X-b_1)^{m_1}$. There exists $t\in\mathbb{N}$ such that $P_{f\otimes g} = (X-a_1b_1)^t$. From Lemma 6, part (b), there exist $(X-a_1)^k$ and $(X-b_1)^q$ elementary divisors of f and g, respectively, such that $t=\min\{p,k+q-1\}$. But $(X-a_1)^{n_1}$ and $(X-b_1)^{m_1}$ are elementary divisors of f and g, respectively. Then (Lemma 6, part (a)) $(X-a_1b_1)^{\min\{p,n_1+m_1-1\}}$ is an elementary divisor of $f\otimes g$. Since $k\leq n_1$ and $q\leq m_1$, then $t=\min\{p,n_1+m_1-1\}$ and (4) holds.

(b) Suppose $f = a_1 I_V$.
Then $P_f = X-a_1$, $\sigma(f\otimes g) = \{a_1b_j : j=1,\ldots,s\}$ and (Lemma 6, part (a))

$$\prod_{j=1}^{s}(X-a_1b_j)^{\min\{p,m_j\}} = \prod_{j=1}^{s}(X-a_1b_j)^{m_j}$$

divides $P_{f\otimes g}$. For $j=1,\ldots,s$ let t_j be the maximal degree of the powers of $X-a_1b_j$ that divide $P_{f\otimes g}$. From Lemma 6, part (b), it follows that, for $j=1,\ldots,s$, there exists $q_j\leq m_j$ such that $(X-b_j)^{q_j}$ is an elementary divisor of g and $t_j=\min\{p,q_j\}\leq m_j$. Then $t_j=m_j$ for all j and

$$\deg(P_{f\otimes g}) = \deg(P_g) = \min\{p, \deg(P_f)+\deg(P_g)-1\}\,.$$

(c) The result follows directly from Corollary 4 since if f and g are of simple structure over $\overline{\mathbb{F}}$ then $f\otimes g$ is also of simple structure.

(d) From (d2), Corollary 4 and Remark 6 we have that

$$|\sigma(f)\{b_{t+1},\ldots,b_s\}| = |\sigma(f)| + |\{b_{t+1},\ldots,b_s\}| - 1 = r+s-t-1\,.$$

From (d1) we have $\{b_1,\ldots,b_t\}\,\langle d_1\rangle = \{b_1,\ldots,b_t\}$ and therefore

$$t\leq |\sigma(f)\{b_1,\ldots,b_t\}| \leq |a_i\{b_1,\ldots,b_t\}\,\langle d_1\rangle\,| = t\,,\quad i=1,\ldots,r.$$

Then $\sigma(f)\{b_1,\ldots,b_t\} = a_i\{b_1,\ldots,b_t\}$, for $i=1,\ldots,r$.

Suppose $\sigma(f)\{b_1,\ldots,b_t\}\cap\sigma(f)\{b_{t+1},\ldots,b_s\}\neq\emptyset$. Then, for some $i\in\{1,2,\ldots,r\}$ and some $j\in\{t+1,\ldots,s\}$

$$a_ib_j\in\sigma(f)\{b_1,\ldots,b_t\} = a_i\{b_1,\ldots,b_t\}\,.$$

It follows that $b_j \in \{b_1, \dots, b_t\}$ and this is a contradiction.

Then $\sigma(f)\{b_1, \dots, b_t\} \cap \sigma(f)\{b_{t+1}, \dots, b_s\} = \emptyset$ and

$$\sigma(f)\sigma(g) = \sigma(f)\{b_1, \dots, b_t\}\dot{\cup}\sigma(f)\{b_{t+1}, \dots, b_s\} = a_1\{b_1, \dots, b_t\}\dot{\cup}\sigma(f)\{b_{t+1}, \dots, b_s\}\,. \tag{5}$$

From (d1) we have that $n_i + m_j - 1 = 1$, for $i = 1, \dots, r$ and $j = t+1, \dots, s$.

Then ((5) and Lemma 6, part (b))

$$P_{f\otimes g} = \prod_{j=1}^{t}(X - a_1 b_j)^{m_j}\, q(X)\,,$$

where $\deg(q(X)) = |\sigma(f)\{b_{t+1}, \dots, b_s\}| = r+s-t-1$. Then $\deg(P_{f\otimes g}) = \sum_{j=1}^{t} m_j + s - t + r - 1 = \deg(P_g) + \deg(P_f) - 1$.

Necessary condition

Since $\deg(P_{f\otimes g}) \leq p$, from Lemma 6 we conclude that $p \geq n_1 \geq \cdots \geq n_r$, $p \geq m_1 \geq \cdots \geq m_s$ and $p \geq n_i + m_j - 1$, for $i = 1, \dots, r$, $j = 1, \dots, s$.

- Suppose $|\sigma(f)| = r = 1$ and (4) holds. In this case $P_f = (X - a_1)^{n_1}$ and $\sigma(f \otimes g) = \{a_1 b_j : j = 1, \dots, s\}$. From Lemma 6 it follows that

$$\prod_{j=1}^{s}(X - a_1 b_j)^{\min\{p, n_1+m_j-1\}} \text{ divides } P_{f\otimes g}\,. \tag{6}$$

If $n_1+m_j-1 = p$, for some $j \in \{1, \dots, s\}$, from (4) it follows that $P_{f\otimes g} = (X - a_1 b_j)^p$ and (a) holds.

If $n_1 + m_j - 1 < p$ for $j = 1, \dots, s$ then, from (6), we have

$$p \geq \min\{p, \deg(P_f) + \deg(P_g) - 1\} \geq \sum_{j=1}^{s}(n_1 + m_j - 1)\,, \tag{7}$$

and $p \geq s(n_1 - 1) + \deg(P_g) \geq \deg(P_f) + \deg(P_g) - 1$. From (7) we have also that

$$\begin{aligned} & \deg(P_f) + \deg(P_g) - 1 \geq s n_1 + \deg(P_g) - s \\ \Rightarrow\ & (s-1)(n_1 - 1) \leq 0 \\ \Rightarrow\ & s = 1 \vee n_1 = 1\,. \end{aligned}$$

If $s = 1$ (a) holds. If $n_1 = 1$ (b) holds.

- Suppose $r \geq 2$. From Corollary 1 it follows that $|\sigma(f\otimes g)| \geq r+s-1$. From Lemma 6 (part (a)) and from $\deg(P_{f\otimes g}) \leq p$ we have that

$$p > n_i + m_j - 1\,, \quad i = 1, \dots, r\,,\ j = 1, \dots, s\,.$$

Then

$$P_{f\otimes g}=\prod_{j=1}^{s}(X-a_1b_j)^{n_1+m_j-1}q_1(X)\,, \tag{8}$$

where $q_1(X)$ is a polynomial with coefficients in $\overline{\mathbb{F}}$ with, at least, $r-1$ distinct roots in $\overline{\mathbb{F}}^*$. Therefore $\deg(q_1(X))\geq r-1$ and from (8) we have

$$\deg(P_{f\otimes g})\geq sn_1+\deg(P_g)-s+r-1\,.$$

From the hypothesis it follows that

$$rn_1+\deg(P_g)-1\geq\deg(P_f)+\deg(P_g)-1\geq\deg(P_f\otimes g)\geq sn_1+\deg(P_g)-s+r-1\,. \tag{9}$$

Then $(s-r)(n_1-1)\leq 0$ and, from $s\geq r$, we conclude that $n_1=1$ or $s=r$. In both cases, from (9), we have

$$\deg(P_{f\otimes g})=\deg(P_f)+\deg(P_g)-1$$

and hence, from (4),

$$p\geq\deg(P_f)+\deg(P_g)-1\,.$$

From (8) we have also that

$$\deg(P_f)+\deg(P_g)-1=sn_1-s+\deg(P_g)+\deg(q_1(x))\geq\deg(P_g)+sn_1-s+r-1\,.$$

Then (in both cases $s=r$ or $n_1=1$) we have

$$n_1=n_2=\cdots=n_r \tag{10}$$

and $\deg(q_1(X))=r-1$. Therefore, from (8), it follows that

$$|\sigma(f)\sigma(g)|=|\sigma(f\otimes g)|=|\sigma(f)|+|\sigma(g)|-1\,. \tag{11}$$

Suppose $s=r$. From

$$P_{f\otimes g}=\prod_{i=1}^{r}(X-a_ib_1)^{n_i+m_1-1}q(X)\,,$$

where $\deg(q(X))\geq|\sigma(f\otimes g)|-|\sigma(f)|=s-1$, it follows that

$$\deg(P_f)+\deg(P_g)-1=\deg(P_{f\otimes g})\geq\deg(P_f)+rm_1-1\,.$$

Then $(s=r)$ $\deg(P_g)=sm_1$ and

$$m_1=\cdots=m_r\,. \tag{12}$$

Since we assumed that $r \geq 2$, from (11), we have

$$|\sigma(f)\sigma(g) \setminus a_1\sigma(g)| = |\sigma(f)| - 1 = r - 1 \geq 1\,. \tag{13}$$

Let $a_ib_j \in \sigma(f)\sigma(g) \setminus a_1\sigma(g)$. From $p > n_i + m_j - 1$, and Lemma 6 we conclude that $(X - a_ib_j)^{n_i+m_j-1}$ divides $P_{f\otimes g}$. Then $(X - a_ib_j)^{n_i+m_j-1}$ divides $q_1(X)$. Since $\deg(q_1(X)) = r - 1$, from (8) and (13), it follows that all the roots of $q_1(X)$ are simple and therefore $n_i + m_j - 1 = 1$. Then $n_i = m_j = 1$ and from (10) and (12) we conclude that f and g are of simple structure over $\overline{\mathbb{F}}$.

Then ((11) and Corollary 4) (c) holds.

Suppose $s > r$. Then $n_1 = n_2 = \cdots = n_r = 1$. If $m_1 = 1$ case (c) holds. Suppose $m_1 > 1$. Let $i \in \{1, 2, \ldots, r\}$. Then

$$P_{f\otimes g} = \prod_{j=1}^{s}(X - a_ib_j)^{m_j} q_i(X)\,, \tag{14}$$

where $q_i(X)$ is a polynomial with coefficients in $\overline{\mathbb{F}}$ with, at least, $r - 1$ distinct roots in $\overline{\mathbb{F}}^*$. From (14) it follows that $\deg(q_i(X)) = \deg(P_f)+\deg(P_g)-1-\deg(P_g) = r-1$. Hence all the roots of $q_i(X)$ are simple.

For $\ell = 1, 2, \ldots, r$, $(X-a_\ell b_1)^{m_1}$ divides $P_{f\otimes g}$. Since $m_1 > 1$, there exists one and only one $j_\ell \in \{1, 2, \ldots, s\}$ such that $a_\ell b_1 = a_ib_{j_\ell}$ and $(X - a_\ell b_1)^{m_1}$ divides $(X - a_ib_{j_\ell})^{m_{j_\ell}}$. Since $j_\ell = j_k$ if and only if $\ell = k$, it must be $m_1 = m_2 = \cdots = m_r > 1$. We have also proved that

$$\sigma(f)b_1 \subseteq a_i\sigma(g)\,, \text{ for all } i \in \{1, 2, \ldots, r\}\,. \tag{15}$$

From (14) and since $r \geq 2$ the polynomial $P_{f\otimes g}$ has, at least, one simple root. Then $m_s = 1$. Let $t \in \{r, \ldots, s-1\}$ be such that

$$m_1 = m_2 = \cdots = m_r \geq \cdots \geq m_t > 1 = m_{t+1} = \cdots = m_s\,. \tag{16}$$

Let $\ell \in \{2, \ldots, r\}$ and $j \in \{1, \ldots, t\}$. The polynomial $(X - a_\ell b_j)^{m_j}$ divides $P_{f\otimes g}$. Since $m_j > 1$, from (14) with $i = 1$, we have that $a_\ell b_j \in a_1\{b_1, \ldots, b_t\}$. Then

$$\sigma(f)\{b_1, \ldots, b_t\} = a_1\{b_1, \ldots, b_t\}\,. \tag{17}$$

From (17) we conclude that

$$\sigma(f)\{b_1, \ldots, b_t\} = a_i\{b_1, \ldots, b_t\}\,, \quad i = 1, \ldots, r\,. \tag{18}$$

From Corollary 2 and Remark 1, there exist a positive integer $m \geq 2$ and $d_1 \in \overline{\mathbb{F}}^*$ with order m, such that (d1) holds.

Suppose that

$$\sigma(f)\{b_1, \ldots, b_t\} \cap \sigma(f)\{b_{t+1}, \ldots, b_s\} \neq \emptyset\,.$$

Then, for some $j \in \{1, 2, \ldots, t\}$, $i \in \{1, 2, \ldots, r\}$ and $k \in \{t+1, \ldots, s\}$, we have $a_1 b_j = a_i b_k$. From (17) it follows that $a_1^{-1} a_i \in H(\{b_1, \ldots, b_t\})$. Then $b_k = a_i^{-1} a_1 b_j \in \{b_1, \ldots, b_t\}$ and this is a contradiction. Then

$$\sigma(f)\{b_1, \ldots, b_t\} \cap \sigma(f)\{b_{t+1}, \ldots, b_s\} = \emptyset$$

and

$$\begin{aligned} |\sigma(f)\{b_{t+1}, \ldots, b_s\}| &= |\sigma(f)\,\sigma(g)| - |\sigma(f)\{b_1, \ldots, b_t\}| \\ &= r + s - 1 - t \\ &= |\sigma(f)| + |\{b_{t+1}, \ldots, b_s\}| - 1\,. \end{aligned} \tag{19}$$

Equalities (18) and (19) allow us to apply Corollary 3 with $A = \sigma(f)$, $B = \sigma(g)$, $C = \{b_1, \ldots, b_t\}$ and $D = \{b_{t+1}, \ldots, b_s\}$. Since $\sigma(f)\,\sigma(g)$ is not periodic then also $\sigma(f)\{b_1, \ldots, b_t\}$ is not periodic and (Corollary 4) (d) holds.

$\blacksquare$

References

[1] A. C. Aitken, The normal form of compound and induced matrices, *Proc. London Math. Soc.*, 38(1934), 354-376.

[2] A. Cauchy, Recherches sur les nombres, *J. École Polytech.* 9(1813), 99-116.

[3] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* 10(1935), 30-32.

[4] H. Davenport, A historical note, *J. London Math. Soc.* 22(1947), 100-101.

[5] J. A. Dias da Silva and Y. O. Hamidoune, A Note on the Minimal Polynomial of the Kronecker Sum of Two Linear Operators, *Linear Algebra Appl.*, 141(1990), 283-287.

[6] J. H. B. Kemperman, On small sumsets in an abelian group, *Acta Math.*, 103(1960), 63-88.

[7] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Z.*, 58(1953), 459-484.

[8] M. Kneser, Ein Satz über abelschen Gruppen mit Anwendungen auf die Geometrie der Zahlen *Math. Z.*, 61(1955), 429-434.

[9] M. Marcus, The Minimal Polynomial of a Commutator, *Portugaliae Math.*, 25(1964), 73-76.

[10] M. Marcus, *Finite Dimensional Multilinear Algebra - Parts I and II*, Marcel Dekker, Inc., New York (1973).

[11] M. Marcus e M. Shafqat Ali, On the degree of the minimal polynomial of a commutator operator, *Pacific J. Math.*, 37(1971), 561-565.

[12] M. Marcus e M. Shafqat Ali, Minimal Polynomials of Additive Commutators and Jordan Products, *J. Algebra*, 22(1972), 12-33.

[13] M. B. Nathanson, *Additive Number Theory-Inverse Problems and the Geometry of Sumsets*, Springer-Verlag (1996).

[14] M. Newman, *Integral Matrices*, Academic Press (1972).

[15] W. E. Roth, On direct product matrices, *Bull. Amer. Math. Soc.*, 40(1934), 461-468.