Linear Algebraic Methods in Additive Theory

by J. A. Dias da Silva

Departamento de Matemática - CELC
Universidade de Lisboa

Introduction

Additive Number Theory is the study of subsets of $\mathbb{Z}$ or $\mathbb{Z}_p$ (the set of the integers modulo p). Let $m \geq 2$ and $A_1, \ldots, A_m \subseteq \mathbb{Z}$ (or $\mathbb{Z}_p$). We denote by $A_1 + \cdots + A_m$ the subset of $\mathbb{Z}$ (or $\mathbb{Z}_p$)

$$A_1 + \cdots + A_m := \{a_1 + \cdots + a_m \mid a_i \in A_i,\ i = 1, \ldots, m\}.$$

The set $A_1 + \cdots + A_m$ is called the the *sumset of* $A_1, \ldots, A_m$.

Following Nathanson [16], in a *direct problem in Additive Theory* we establish properties on the sumset $A_1 + \cdots + A_m$ when properties of $A_1, \ldots, A_m$ are known. In an *inverse problem in Additive Theory* we study the structure of sets $A_1, \ldots, A_m$ whose sumset has prescribed properties, for example, the structure of sets whose sumset has small cardinality.

Some direct problems in Additive Theory have recently been approached by using tools of Linear Algebra. This happened after years of using additive results in Linear Algebra (sometimes reproved with this purpose)[12, 13, 14, 15, 18].

The linear algebraic approach of Additive Number Theory is based on the use of the degrees of invariant polynomials of (diagonal) linear operators as estimators for the cardinality of parts of their spectrum. To illustrate it we need to introduce some terminology and notation.

We denote by $\mathbb{N}_0$ the set of nonnegative integers. We use p to mean the characteristic of the field $\mathbb{F}$, in the case $\mathbb{F}$ has finite characteristic, and ∞ if $\mathbb{F}$ has characteristic zero (we assume the usual conventions on the symbol ∞). If A is a set, $|A|$ denotes the cardinality of A. If f is a linear operator on the finite dimensional vector space V over $\mathbb{F}$, we use $\sigma(f)$ for the spectrum of f (meaning either the family or the set of the roots of the characteristic polynomial of f, in the algebraic closure of $\mathbb{F}$). We use P_f to mean the minimal polynomial of f (that is, the monic polynomial of minimal degree satisfied by f). We say that f is *diagonal* or *of simple structure* if, for some basis of V, the matrix of f is diagonal.

Let $v \in V$. The subspace spanned by the images of v under the powers of f is called the f-*cyclic subspace* of v and denoted $\mathcal{C}_f(v)$, i.e.,

$$\mathcal{C}_f(v) = \langle f^j(v) \mid j \in \mathbb{N}_0 \rangle.$$

The identity operator on V is denoted by I_V.

The following theorems are basic tools for the next sections.

Theorem 1 *If f is a diagonal linear operator on V, the degree of the minimal polynomial of f is equal to the cardinality of its spectrum, i.e.*

$$\deg(P_f) = |\sigma(f)|.$$

Theorem 2 *The degree of the minimal polynomial of f is the maximum of the dimensions of the f-cyclic subspaces of the vectors of V, i.e.,*

$$\deg(P_f) = \max_{v \in V} \dim \mathcal{C}_f(v).$$

From the Cauchy-Davenport theorem to the Erdös-Heilbronn conjecture

Let p be a prime number. The following theorem was proved by Cauchy in 1813 [2], and reproved by Davenport in 1935 [5].

Theorem 1 *Let A and B be nonempty subsets of $\mathbb{Z}_p$. Then*

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

A new proof for the Cauchy-Davenport theorem was obtained [7] using Linear Algebra. The first step needed to get this proof is to obtain the linear algebraic translation of the notion of sumset, i.e., given linear operators f and g to find a linear operator H such that

$$\sigma(H) = \sigma(f) + \sigma(g).$$

Basic Linear Algebra provides that operator, as we can see in the following theorem.

Theorem 2 *Let V and W be nonzero finite dimensional vector spaces over the field $\mathbb{F}$. Let f be a linear operator on V and g be a linear operator on W. The spectrum of the Kronecker sum of f and g,*

$$f \otimes I_W + I_V \otimes g,$$

is equal to the sumset of the spectra of f and g, i.e.,

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

We are now able to state the linear counterpart of the Cauchy-Davenport theorem.

Theorem 3 (Linear Cauchy-Davenport [7]) *Let V and W be nonzero finite dimensional vector spaces over $\mathbb{F}$. Let f be a linear operator on V and g a linear operator on W. Then*

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

The proof of this theorem was obtained by showing that for $v \in V$ and $w \in W$ the set

$$\{f \otimes I_W + I_V \otimes g)^k (v \otimes w) \mid \\ k = 0, \ldots, \min\{p, \dim \mathcal{C}_f(v) + \dim \mathcal{C}_g(w) - 1\} - 1\}$$

is linearly independent. From this fact we get the inequality

$$\dim \mathcal{C}_{f\otimes I_W + I_V \otimes g}(v \otimes w) \geq \\ \min\{p, \dim \mathcal{C}_f(v) + \dim \mathcal{C}_g(w) - 1\}. \quad (2)$$

Choosing $v \in V$ such that $\dim \mathcal{C}_f(v) = \deg P_f$ and $w \in W$ such that $\mathcal{C}_g(w) = \deg P_g$ (recall Theorem 2) we have

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

The Cauchy-Davenport Theorem can now be easily derived. Let A and B be subsets of $\mathbb{Z}_p$ of cardinalities r and s respectively. Let f be a diagonal linear operator on an r-dimensional vector space, V, over $\mathbb{Z}_p$, whose spectrum is A. Let g be a diagonal linear operator on an s-dimensional vector space, W, over $\mathbb{Z}_p$, whose spectrum is B. Using Theorem 3 and replacing in (1) the degrees of the minimal polynomials of f, g and $f \otimes I_W + I_V \otimes g$ (recall Theorems 1 and 2) by the cardinality of their spectra we get the Cauchy-Davenport Theorem.

The Erdös-Heilbronn conjecture was another (direct) additive problem that has been successively fitted in the linear algebraic approach. In order to state this conjecture let us introduce some more terminology and notation. We say *m-set* to mean a set of cardinality m. Let A be a nonempty subset of $\mathbb{F}$. We denote by $\wedge^m A$ the set of the sums of the elements of the m-subsets of A (we refer to these sums as "sums of the m-subsets"or "m-restricted sums"). For instance, if $A = \{a_1, \ldots, a_n\} \subseteq \mathbb{F}$

$$\wedge^2 A = \{a_i + a_j \mid 1 \leq i < j \leq n\}.$$

In 1964 Erdös and Heilbronn [10] made the following conjecture:

Conjecture *Let p be a prime number and let A be a nonempty subset of $\mathbb{Z}_p$. The set of the sums of the 2-subsets of A has cardinality at least $\min\{p, 2|A|-3\}$, i.e.,*

$$|\wedge^2 A| \geq \min\{p, 2|A|-3\}.$$

In the linear algebraic approach to this conjecture the following more general problem was considered: "Let n be a positive integer. Find a lower bound for the set of cardinalities of $\wedge^m A$ when A runs over the set of finite subsets of $\mathbb{F}$ of cardinality n, i.e. find a lower bound for the set

$$\{|\wedge^m A| \quad | \quad A \subseteq \mathbb{F} \text{ and } |A| = n\}".$$

Given a linear operator f we have, now, to find a linear operator H such that the spectrum of H is the set of the sums of the m-subsets of the spectrum of f. As before, this linear operator has already been considered in Linear Algebra. Let f be a linear operator on V. Consider the linear operator $D(f)$ on $\wedge^m V$, the mth exterior power of V, defined by the equalities [1, Ch. III, p. 129],

$$\begin{aligned} D(f)(v_1 \wedge \cdots \wedge v_m) \quad = \quad & f(v_1) \wedge v_2 \wedge \cdots \wedge v_m + \\ & + v_1 \wedge f(v_2) \wedge \cdots \wedge v_m + \\ & + \cdots + v_1 \wedge v_2 \wedge \cdots \wedge f(v_m), \\ & v_1, \ldots, v_m \in V. \end{aligned}$$

The following theorem is a consequence of the definition of $D(f)$.

Theorem 4 *Let f be a diagonal linear operator on the finite dimensional vector space V. Then $D(f)$ is diagonal and the spectrum of $D(f)$ is the set of the sums of the m-subsets of $\sigma(f)$, i.e.,*

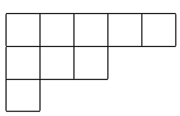
$$\sigma(D(f)) = \wedge^m \sigma(f).$$

To go on with the announced approach to the Erdös-Heilbronn conjecture, we need to express the image of the powers of $D(f)$, on certain decomposable exterior tensors, as linear combinations of a basis of $\wedge^m V$ (designed to fit in this problem). For this we introduce some combinatorial terminology and notation.

A *partition* of m is a decreasing sequence of nonnegative integers whose sum is equal to m. We say that a partition λ has *length* s (and write $s = \ell(\lambda)$) if the number of positive terms of λ is s. We denote by $\mathcal{P}_{m,s}$ the set of partitions of m of length at most s, and by $\mathcal{P}_s$ the set of partitions of length at most s, i.e.,

$$\mathcal{P}_s = \bigcup_{i \in \mathbb{N}} \mathcal{P}_{i,s}.$$

To each partition of m, $\lambda = (\lambda_1, \ldots, \lambda_t)$, we associate the Young tableau $[\lambda]$ which consists of m boxes placed in t rows, all starting in the same column, where the i-th row of $[\lambda]$ has λ_i boxes, $i = 1, \ldots, t$. For instance, the Young tableau associated with the partition $(5, 3, 1)$ is



Let λ be a partition of m. The (i, j)-*hook* of $[\lambda]$ is the subset of boxes of $[\lambda]$ consisting of the (i, j)-box of $[\lambda]$ (the box in the ith row and jth column of $[\lambda]$) together with the boxes in the same row to the right and the boxes in the same column under it. We denote by H_{ij}^{λ} the (i, j)-hook of $[\lambda]$ and by h_{ij}^{λ} the cardinality of H_{ij}^{λ}.

Let $v \in V$. The set

$$\begin{gathered}\{f^{\lambda_m}(v) \wedge f^{\lambda_{m-1}+1}(v) \wedge \cdots \wedge f^{\lambda_1+m-1}(v) \mid \\ \lambda \in \mathcal{P}_m, \lambda_1 \leq \dim \mathcal{C}_f(v) - m\}\end{gathered} \tag{3}$$

is a basis for the mth exterior power of $\mathcal{C}_f(v)$. Then it is possible to express the image of powers of $D(f)$ on $v \wedge f(v) \wedge \cdots \wedge f^{m-1}(v)$ as a linear combination of this basis. The following theorem gives us that linear combination.

Theorem 5 ([8])

$$D(f)^t(v \wedge f(v) \wedge \cdots \wedge f^{m-1}(v)) =$$

$$= \sum_{\lambda \in \mathcal{P}_{t,m}} \frac{t!}{\prod_{i,j} h_{ij}^{\lambda}} f^{\lambda_m}(v) \wedge f^{\lambda_{m-1}+1}(v) \wedge \cdots \wedge f^{\lambda_1+m-1}(v).$$

With this expansion of $D(f)^t(v \wedge f(v) \wedge \cdots \wedge f^{m-1}(v))$ as a linear combination of the elements of the basis (3) it is possible to prove that, if $v \in V$,

$$\begin{gathered}\{D(f)^t(v \wedge f(v) \wedge \cdots \wedge f^{m-1}(v)) \mid \\ t = 0, \ldots, \min\{p, m(\dim \mathcal{C}_f(v) - m) + 1\} - 1\}\end{gathered}$$

is a linearly independent set: Using arguments similar to the ones which have been used to prove the linear Cauchy-Davenport Theorem, we get what we can call the Linear Erdös-Heilbronn Theorem.

Theorem 6 ([8]) *Let V be a nonzero finite dimensional vector space over $\mathbb{F}$. Let f be a linear operator on V. Then*

$$\deg(P_{D(f)}) \geq \min\{p, m(\deg P_f - m) + 1\}.$$

Let A be a finite nonempty subset of $\mathbb{F}$. Taking f diagonal with spectrum A, and using the line of argument presented after the proof of the Linear Cauchy-Davenport Theorem, we obtain the following theorem :

Theorem 7 ([8]) *Let A be a finite nonempty subset of $\mathbb{F}$. Then*

$$| \wedge^m A| \geq \min\{p, m(|A| - m) + 1\}.$$

This theorem gave an affirmative answer to the Erdös-Heilbronn conjecture. In fact, taking $m = 2$ and $\mathbb{F}$ the field $\mathbb{Z}_p$ in the previous theorem, we conclude that the Erdös-Heilbronn conjecture is true.

Multiplicities and generalized sums

Let $A = \{a_1, \ldots, a_n\}$ and B be finite nonempty subsets of $\mathbb{F}$. For $c \in A+B$ define $\nu_c(A,B)$, the *multiplicity* of c in $A+B$, as the cardinality

$$\nu_c(A,B) = |\{(a,b) \mid a \in A,\ b \in B,\ \text{and } a+b=c\}|.$$

We write $\mu_i(A,B)$ (or simply μ_i) to mean the cardinality of the set of the $c \in A+B$ that have multiplicity greater than or equal to i, i.e.,

$$\mu_i(A,B) = |\{c \in A+B \mid \nu_c(A,B) \geq i\}|.$$

Similarly, if $c \in \wedge^2 A$ we denote by $\nu_c^{(R)}(A)$, the *multiplicity* of c in $\wedge^2 A$, as the cardinality

$$\nu_c^{(R)}(A) = |\{(r,s) \mid 1 \leq r < s \leq n,\ \text{and } a_r + a_s = c\}|.$$

The symbol $\mu_i^{(R)}(A)$ (or simply $\mu_i^{(R)}$) indicates the set of the elements c of $\wedge^2 A$ whose multiplicity is greater than or equal to i, i.e.,

$$\mu_i^{(R)}(A) = |\{c \in A+B \mid \nu_c^{(R)}(A) \geq i\}|.$$

In 1974, J. M. Pollard [17] established an average theorem for the multiplicities in $A+B$ proving that, if $A, B \subseteq \mathbb{Z}_p$, then, for $t = 1, 2, \ldots, \min\{|A|, |B|\}$, we have

$$\sum_{i=1}^{t} \mu_i \geq t \min\{p, |A|+|B|-t\}. \tag{1}$$

Extending the arguments used to prove the Cauchy-Davenport and Erdös-Heilbronn theorems, and using some recent results on Linear Algebraic Control Theory [19], it was possible to generalize Pollard's theorem in the following two different ways:

Theorem 1 *Let A and B be finite nonempty subsets of $\mathbb{F}$. Then, for $t = 1, 2, \ldots, \min\{|A|, |B|\}$, we have*

$$\sum_{i=1}^{t} \mu_i \geq t \min\{p, |A|+|B|-t\}.$$

Theorem 2 *Let $A \subseteq \mathbb{F}$ and $1 \leq t \leq \lfloor \frac{|A|}{2} \rfloor$. Assume that $|A| \geq 2$. Then we have*

$$\sum_{i=1}^{t} \mu_i^{(R)} \geq t \min\{p, 2(|A|-t)-1\}.$$

Consider, now, the elementary symmetric polynomial of degree k in the indeterminates $X_1, \ldots, X_m$,

$$s_k(X_1, \ldots, X_m) = \sum_{\alpha \in Q_{k,m}} X_{\alpha(1)} \cdots X_{\alpha(m)},$$

where $Q_{k,m}$ denotes the set of strictly increasing maps from $\{1, \ldots, k\}$ into $\{1, \ldots, m\}$. Let $A_1, \ldots, A_m$ be subsets of $\mathbb{F}$. We denote by $s_k(A_1, \ldots, A_m)$ the subset of $\mathbb{F}$

$$s_k(A_1, \ldots, A_m) = \{s_k(a_1, \ldots, a_m) \mid a_i \in A_i,\ i = 1, \ldots, m\}.$$

This concept generalizes the notion of sumset of $A_1, \ldots, A_m$. In fact, $s_1(A_1, \ldots, A_m)$ is the sumset of $A_1, \ldots, A_m$, i.e.

$$s_1(A_1, \ldots, A_m) = A_1 + \cdots + A_m.$$

It is natural to search additive results for these generalized sumsets. Again, the linear algebraic approach worked for this generalization.

Let $V_1, \ldots, V_m$ be nonzero finite dimensional vector spaces over $\mathbb{F}$. Let T_i be a linear operator of V_i, $i = 1, \ldots, m$. If $\alpha \in Q_{k,m}$ let

$$\delta_\alpha(T_1, \ldots, T_m) = S_1 \otimes \cdots \otimes S_m,$$

where $S_i = I_{V_i}$ if $i \notin \operatorname{Im} \alpha$ and $S_i = T_i$ if $i \in \operatorname{Im} \alpha$. Define

$$D_k(T_1, \ldots, T_m) := \sum_{\alpha \in Q_{k,m}} \delta_\alpha(T_1, \ldots, T_m).$$

For instance,

$$D_2(T_1, T_2, T_3) = T_1 \otimes T_2 \otimes I_{V_3} + T_1 \otimes I_{V_2} \otimes T_3 + I_{V_1} \otimes T_2 \otimes T_3.$$

The key result that allows the above mentioned linear algebraic approach is the following theorem:

Theorem 3 *Let $A_1, \ldots, A_m$ be nonempty finite subsets of $\mathbb{F}$. Let T_i be a diagonal linear operator on V_i such that $\sigma(T_i) = A_i$, $i = 1, \ldots, m$. Then $D_k(T_1, \ldots, T_m)$ is diagonal and*

$$\sigma(D_k(T_1, \ldots, T_m)) = s_k(A_1, \ldots, A_m).$$

Using a variation of the arguments already described (for the Linear Cauchy-Davenport Theorem) we can prove:

Theorem 4 ([9]) *For p large enough we have*

$$\deg P_{D_k(T_1, \ldots, T_m)} \geq \left\lfloor \frac{\deg P_{T_1} + \cdots + \deg P_{T_m} - m}{k} \right\rfloor + 1.$$

Considering diagonal linear operators T_i in the conditions of Theorem 3, and the equality (for diagonal linear operators) between the cardinality of the spectrum and the degree of the minimal polynomial (Theorem 1), we obtain, from the previous theorem, the following result:

Theorem 5 ([9]) *Let $A_1, \ldots, A_m$ be finite nonempty subsets of $\mathbb{F}$. For p large enough we have*

$$|s_k(A_1, \ldots, A_m)| \geq \left\lfloor \frac{|A_1| + \cdots + |A_m| - m}{k} \right\rfloor + 1.$$

Bibliografia

[1] N. Bourbaki, *Elements de Mathématique*, Algèbre I, Hermann, Paris, (1970).

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

[3] Cristina Caldeira and J. A. Dias da Silva, The invariant polynomial degrees of the Kronecker sum of two linear operators and Additive Theory, *Linear Algebra and Appl.* 315:125-138 (2000).

[4] Cristina Caldeira and J. A. Dias da Silva, A Pollard type result for restricted sums, *Journal of Number Theory* 72:153-173 (1998).

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

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

[7] 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 and its Applications* 141:283-287 (1990).

[8] J.A. Dias da Silva and Y. O. Hamidoune, Cyclic Spaces for Grassmann derivatives and Additive Theory, *Bull. London Math. Soc.* 26:140-146 (1994).

[9] J. A. Dias da Silva and H. Godinho, Generalized derivations and Additive Theory, preprint.

[10] P. Erdös and R. L. Graham, *Old and new problems and results in combinatorial Additive Theory*, L'Enseignement Mathématique, Genève, 1980.

[11] Serge Lang, *Algebra*, Addison-Wesley, New York, 1993.

[12] M. Marcus, The minimal polynomial of a commutator, *Portugaliae Math.* 25:73-76 (1964).

[13] M. Marcus and M. Shafqat Ali, On the degree of the minimal polynomial of a commutator operator, *Pacific J. Math.* 37:361-565 (1971).

[14] M. Marcus and M. Shafqat Ali, Minimal polynomials of additive commutators and Jordan products, *J. Algebra* 22:12-33 (1972).

[15] M. Marcus and M. Shafqat Ali, On the degree of the minimal polynomial of the Lyapunov Operator. *Monatshefte für Mathematik* 78:229-236 (1974).

[16] Melvyn B. Nathanson, Additive Number Theory: 1. Inverse Problems and the Geometry of Sumsets, Springer Verlag, 1996.

[17] J. M. Pollard, A generalization of a theorem of Cauchy and Davenport, *J. London Math. Soc.* 8:460-462(1974).

[18] Renato Spiegler, An application of group theory to matrices and ordinary differential equations, *Linear Algebra Appl.* 44:143-151 (1982).

[19] I. Zaballa, Controlability and Hermite indices of matrix pairs, *Int. J. Control* 68(1):61-86 (1997).

Great Moments in XXth Century Mathematics

In this issue we present the answers of two researchers, E. C. Zeeman and Thomas J. Laffey, to the question "If you had to mention one or two great moments in XXth century mathematics which one(s) would you pick?".