LINEAR ALGEBRAIC TECHNIQUES IN ADDITIVE THEORY AND A GENERALIZATION OF THE CAUCHY-DAVENPORT THEOREM

Hemar Godinho*

1. Introduction

A classical example of the theory of addition of sets is the well known Cauchy-Davenport theorem that says:

" *If A, B are sets of residues modulo a prime p, and*

$$A + B = \{a + b \mid a \in A \ , \ b \in B\}$$

then

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

This result has an interesting story. In 1935, Davenport[3] proved this theorem. And in 1947, he discovered[4] that this was first proved by Cauchy in 1813. This simple but elegant result has had many applications and extensions for abelian groups. For more details one may report to the results of Chowla[1], Mann[9], Scherk and Kemperman[11], and Pollard[10].

The *critical sets* (i.e., the sets for which equality holds on the theorem above) were given by Vosper[12]. He proved:

Theorem *The sets A, B are critical sets if*

1. $|A| + |B| > p$;

2. $\min(|A|, |B|) = 1$;

*supported by CNPq/Brazil and FAP-DF/Brazil.

3. *A, B are representable in arithmetical progressions with the same common difference*;

4. $A = (\mathbb{Z}_p - (c - B))$ for some $c \in \mathbb{Z}_p$

One of the applications of the Cauchy-Davenport Theorem (see Mann, Chowla and Strauss[2]) is related to expressions of the type

$$a_1 x_1^{k_1} + \cdots + a_s x_s^{k_s} \equiv d \pmod{p^m}.$$

And it is interesting to observe that Cauchy had a similar motivation for his result. He was interested in proving that the binary quadratic form $ax^2 + by^2$ represents all residue classes modulo p.

I would like to present a further extension of the Cauchy-Davenport Theorem, now related to symmetric polynomials, together with results on critical sets. Here I will give the main highlighs of the proofs and techniques, were the main features are the Linear Algebraic techniques. The results presented are a consequence of a colaboration with Dias da Silva[5,6], from the Universidade de Lisboa.

2. The Problem

Let

$$s_{k,m}(X_1, \cdots, X_m) = \sum_{\omega \in Q_{k,m}} X_{\omega(1)} \cdot X_{\omega(2)} \cdots X_{\omega(k)}$$

where the set $Q_{r,s}$ is the set of the strictly increasing mappings from $\{1, \ldots, k\}$ into $\{1, \ldots, m\}$, the kth symmetric polynomial on the indeterminates $X_1, \cdots, X_m$.

Define the set

$$s_{k,m}(A_1, \ldots, A_m) :=$$

$$\{s_{k,m}(a_1, \ldots, a_m) \mid (a_1, \ldots, a_m) \in A_1 \times \cdots \times A_m\}.$$

Our purpose is to find lower bounds for $|s_{k,m}(A_1, \ldots, A_m)|$, the cardinality of the set.

The theorem of Cauchy-Davenport can be easily generalized to addition of n sets of residues, giving

$$|A_1 + A_2 + \cdots + A_m| \geq \min\{p\ ,\ |A_1| + \cdots + |A_m| - m + 1\},$$

which in our notation is equivalent to

$$|s_{1,m}(A_1, \ldots , A_m)| \geq \min\{p\ ,\ |A_1| + \cdots + |A_m| - m + 1\}.$$

We would like to find similar bounds for all other powers k.

3. Linear Algebraic Techniques

Dias da Silva and Hamidoune[8] were the first to apply linear algebraic techniques to number theory, proving a longstanding conjecture of Erdös and Heilbronn. And the starting point was to present a new proof[7] for the Cauchy-Davenport Theorem, as a consequence of a result on lower bounds for the degree of the minimal polynomial of the linear operator (a *Kronecker sum*)

$$f \otimes I_W + I_V \otimes g \ \in\ L(V \otimes W, V \otimes W),$$

where V and W are vector spaces of finite dimension over a field.

Let us start with all the necessary definitions and notations. Let V_i be a vector space of finite dimension over $\mathbb{F}$ (an arbitrary field of characteristic p, a prime number, if it is of finite characteristic, or $p = \infty$ otherwise). Let $L(V_i, V_i)$ be the $\mathbb{F}$-algebra of linear operators on V_i. We denote by $V_1 \otimes \cdots \otimes V_m$ the tensor product of $V_1, \ldots , V_m$. If T is a linear operator, we denote by P_T the minimal polynomial of T, by $\sigma(T)$ the spectrum of T (the n-tuple of characteristic roots of T in $\overline{\mathbb{F}}$, the algebraic closure of $\mathbb{F}$) and by I the identity linear operator.

Let $A_1, \cdots , A_m$ be algebras, and define, for $\omega \in Q_{k,m}$, the map δ_ω from $A_1 \times \cdots \times A_m$ to $A_1 \otimes \cdots \otimes A_m$, as

$$\delta_\omega(a_1, \cdots , a_m) = u_1 \otimes \cdots \otimes u_m,$$

where $u_j = a_j$ if $j \in \mathrm{Im}\,(\omega)$, or $u_j = 1_{A_j}$ otherwise.

Consider $T_i \in L(V_i, V_i)$ $(1 \leq i \leq m)$ linear operators and denote by $s_{k,m}(T_1, \ldots, T_m)$ the linear operator on $V_1 \otimes \cdots \otimes V_m$ defined as:

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

For example, in the case of $s_{2,3}(X_1, X_2, X_3) = X_1X_2 + X_1X_3 + X_2X_3$, we will have

$$s_{2,3}(T_1, T_2, T_3) = T_1 \otimes T_2 \otimes I + T_1 \otimes I \otimes T_3 + I \otimes T_2 \otimes T_3.$$

The next theorem will be stated with no proof.

Theorem 1. *Let T_i be a diagonal linear operator such that $\sigma(T_i) = A_i$, for $i = 1, \cdots, m$. Then $s_{k,m}(\mathbb{T}) := s_{k,m}(T_1, \ldots, T_m)$ is also diagonal and $\sigma(s_{k,m}(\mathbb{T})) = s_{k,m}(A_1, \ldots, A_m)$. Thus $\deg P_{s_{k,m}(\mathbb{T})} = |s_k(A_1, \ldots, A_m)|$.*

This result gives a linear algebraic interpretation to our problem. We want now to find lower bounds for the degree of the minimal polynomial of the linear operator $s_{k,m}(T_1, \ldots, T_m)$.

4. The degree of $P_{s_{k,m}(\mathbb{T})}$

The result we are aiming to prove is

Theorem 2. *For p large enough, the degree of the minimal polynomial of $s_{k,m}(T_1, \ldots, T_m)$ is greater than or equal to $\ell + 1$, where*

$$\ell = \left\lfloor \frac{\deg P_{T_1} + \deg P_{T_2} + \cdots + \deg P_{T_m} - m}{k} \right\rfloor. \tag{1}$$

The proof of this theorem will be complete once we prove that, for the ℓ given above, the set

$$\{I, s_{k,m}(\mathbb{T}), s_{k,m}(\mathbb{T})^2, \cdots, s_{k,m}(\mathbb{T})^\ell\}$$

is linearly independent.

Hence the first step is to understand the expression of powers $s_{k,m}(\mathbb{T})^\tau$. Clearly the powers of $s_{k,m}(T_1, \ldots, T_m)^\tau$ will be related to the powers of the single operators T_i multiplied by coefficients. Hence two problems appears immediatly: the characteristic of $\mathbb{F}$, and to realize that the powers of T_i are *modulo* deg P_{T_i}.

Let us avoid these considerations for the moment, looking at the "*tensorial polynomial*"

$$s_{k,m}(\mathbb{X}) = \sum_{\omega \in Q_{k,m}} \delta_\omega(X_1, \cdots, X_m),$$

where

$$s_{k,m}(\mathbb{X}) \in \mathbb{Z}[X_1] \otimes \cdots \otimes \mathbb{Z}[X_m].$$

In $\mathbb{Z}$, denoting by $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$,

$$(a_1 + a_2 + \cdots + a_b)^\tau = \sum_{\substack{(m_1,\ldots,m_b)\in\mathbb{N}_0^b \\ m_1+m_2+\cdots+m_b=\tau}} \frac{\tau!}{m_1!m_2!\cdots m_b!} a_1^{m_1} \cdot a_2^{m_2} \cdots a_b^{m_b}.$$

Now, writing $b = |Q_{k,m}| = \left(\begin{array}{c} m \\ k \end{array} \right)$, we have

$$s_{k,m}(\mathbb{X}) = \delta_{\omega_1}(\mathbb{X}) + \cdots + \delta_{\omega_b}(\mathbb{X}).$$

So

$$s_{k,m}(\mathbb{X})^\tau = \sum_{\substack{(n_{\omega_1},\ldots,n_{\omega_b})\in\mathbb{N}_0^b \\ n_{\omega_1}+n_{\omega_2}+\cdots+n_{\omega_b}=\tau}} \frac{\tau!}{n_{\omega_1}!n_{\omega_2}!\cdots n_{\omega_b}!} \delta_{\omega_1}(\mathbb{X})^{n_{\omega_1}} \cdots \delta_{\omega_b}(\mathbb{X})^{n_{\omega_b}}.$$

Let $\Delta_i = \{\omega \in Q_{k,m} | i \in \mathrm{Im}\,(\omega)\}$. Since $X_i^{n_{\omega_i}}$ is present in $\delta_{\omega_i}^{n_{\omega_i}}$ if $\omega_i \in \Delta_i$, we must have

$$s_{k,m}(\mathbb{X})^\tau = \sum \frac{\tau!}{n_{\omega_1}!n_{\omega_2}!\cdots n_{\omega_b}!} X_1^{\sigma_1} \otimes \cdots \otimes X_m^{\sigma_m}, \tag{2}$$

where

$$\sigma_j = \sum_{\omega\in\Delta_j} n_\omega. \tag{3}$$

Membership Condition

Given any $(\sigma_1, \cdots, \sigma_m) \in (\mathbb{N} \cup \{0\})^m$, how can we decide if the monomial $X_1^{\sigma_1} \otimes \cdots \otimes X_m^{\sigma_m}$ appears in the expansion of $s_{k,m}(\mathbb{X})^\tau$? There are two conditions:

1) $\sum_{i=1}^m \sigma_i = k\tau$ ($s_{k,m}(\mathbb{X})$ homogeneous of degree $k \Longrightarrow s_{k,m}(\mathbb{X})^\tau$ homogeneous of degree $k\tau$)

2) For this given $(\sigma_1, \cdots, \sigma_m)$, there must be a positive integer solution for the system (3).

Let us write the system (3) above in its matricial form as

$$[C_1 C_2 \cdots C_b]\ {}^t[n_{\omega_1} \ldots n_{\omega_b}] = {}^t[\sigma_1 \cdots \sigma_m],$$

observing that the columns C_j's, of coefficient matrix, have only entries 0's and 1's. Since each variable X_i appears k times in $s_{k,m}(\mathbb{X})$, each column C_i has exactly k 1's. This matricial equation can also be written as

$$n_{\omega_1} C_1 + \ldots + n_{\omega_b} C_b = {}^t[\sigma_1 \cdots \sigma_m],$$

which is equivalent to

$$\left[\underbrace{C_1 \cdots C_1}_{n_{\omega_1}} \underbrace{C_2 \cdots C_2}_{n_{\omega_2}} \cdots \underbrace{C_b \cdots C_b}_{n_{\omega_b}} \right] = {}^t[\sigma_1 \cdots \sigma_m].$$

Hence the problem is to find a $(0,1)$-matrix as above with row sum vector $(\sigma_1, \sigma_2, \cdots, \sigma_m)$ and column sum vector $(k, \cdots, k)$. And using some results from matrix theory we proved

Theorem. The monomial $X_1^{\sigma_1} \otimes \cdots \otimes X_m^{\sigma_m}$ *appears in the expansion of* $s_{k,m}(\mathbb{X})^\tau$ *if only if* $\sigma_i \leq \tau$ *and* $\sum \sigma_i = k\tau$.

Linear Combination

We now return to the operator $s_{k,m}(\mathbb{T})$, translating the results from $s_{k,m}(\mathbb{X})$, through a map from

$$\mathbb{Z}[X_1] \otimes \cdots \otimes \mathbb{Z}[X_m] \longrightarrow \langle T_1 \rangle \otimes \cdots \otimes \langle T_m \rangle,$$

where $\langle T_1 \rangle \otimes \cdots \otimes \langle T_m \rangle$ is the commutative $\mathbb{F}$- subalgebra of $L(V_1, V_1) \otimes \cdots \otimes L(V_m, V_m)$. This map "*substitutes*" X_i by T_i, and consider its coefficients modulo p, the characteristic of $\mathbb{F}$.

A basis for the commutative subalgebra $\langle T_1 \rangle \otimes \cdots \otimes \langle T_m \rangle$ is

$$\mathcal{B} = \{T_1^{e_1} \otimes \cdots \otimes T_m^{e_m} \mid 0 \leq e_j \leq n_i - 1 \quad \text{for} \quad i = 1, 2, \cdots, m \ \}$$

where $n_i = \deg P_{T_i}$. Using the map above to *translate* (2), we would have the *polynomial expansion* of $s_{k,m}(\mathbb{T})^\tau$, but we are now interested in its expression as a linear combination of the elements of the basis $\mathcal{B}$. And this can be achieved by considering for every monomial $T_1^{\sigma_1} \otimes \cdots \otimes T_m^{\sigma_m}$, its powers σ_i *modulo* n_i. For example, suppose $T_1^{\sigma_1} = \sum_{j=0}^{n_1-1} a_j T_1^j$. Then, by multilinearity,

$$T_1^{\sigma_1} \otimes T_2^{\sigma_2} \otimes \cdots \otimes T_m^{\sigma_m} = \sum_{j=0}^{n_1-1} a_j T_1^j \otimes T_2^{\sigma_2} \otimes \cdots \otimes T_m^{\sigma_m}.$$

So, repeating the process for all the other powers, and all monomials in the polynomial expression of $s_{k,m}(\mathbb{T})^\tau$, we will have its *linear* expression in terms of the basis $\mathcal{B}$. The hypothesis of p large guarantees that some of the coefficients are different from zero.

Let τ be an integer less than or equal to $\ell - 1$ (see (1)), and $l_i = \min\{\tau + 1, n_i\}$, $i = 1, \ldots, m$, where $n_i = \deg P_{T_i}$. Let ρ_τ be the integer satisfying

$$(l_1 - 1) + \cdots + (l_{\rho_\tau - 1} - 1) < k\tau \tag{4}$$

and

$$(l_1 - 1) + \cdots + (l_{\rho_\tau - 1}) \geq k\tau. \tag{5}$$

Define $(\theta_{\tau,1}, \ldots, \theta_{\tau,m})$ as a m-tuple of nonnegative integers, such that

$$\theta_{\tau,i} = \begin{cases} l_i - 1 & \text{if } i < \rho_\tau, \\ k\tau - (l_1 + \cdots + l_{\rho_\tau - 1} - (\rho_\tau - 1)) & \text{if } i = \rho_\tau, \\ 0 & \text{if } i > \rho_\tau. \end{cases}$$

Define the element

$$Z_\tau = T_1^{\theta_{\tau,1}} \otimes T_2^{\theta_{\tau,2}} \cdots \otimes T_m^{\theta_{\tau,m}}, \quad \tau = 0, \ldots, \ell - 1.$$

The final step of this proof was to verify that this element Z_τ, belonging to the basis $\mathcal{B}$, also belonged to the expression of $s_{k,m}(T_1, \ldots, T_m)^\tau$ as a linear combination of the elements of this basis. And the important observation is that Z_τ does not appear in the linear expression of any smaller power of $s_{k,m}(T_1, \ldots, T_m)$. Therefore

$$\{I, s_{k,m}(\mathbb{T}), \cdots, s_{k,m}(\mathbb{T})^\ell\}$$

is a linearly independent set, hence

$$\deg P_{s_{k,m}(\mathbb{T})} \geq \ell + 1.$$

For the special cases of degrees $k = 1$ and $k = m - 1$, we could get the following sharper results:

1.) $\deg P_{s_{1,m}(\mathbb{T})} \geq \min\{p, \deg P_{T_1} + \deg P_{T_2} + \cdots + \deg P_{T_m} - m + 1\}$.

2.) $\deg P_{s_{m-1,m}(\mathbb{T})} \geq \min\{p, \lfloor \frac{\deg P_{T_1} + \deg P_{T_2} + \cdots + \deg P_{T_m} - m}{m-1} \rfloor + 1\}$.

5. Additive Results

Let $A_1, \cdots, A_m$ be any subsets of the field $\mathbb{F}$, of cardinality $|A_i| = n_i$. Define T_i to be a diagonal linear operator on a vector space $V_i = \mathbb{F}^{n_i}$ (of dimension n_i) over $\mathbb{F}$, whose set of eigenvalues is $A_i = \{\lambda_{i,1}, \cdots, \lambda_{1,n_i}\}$.

Putting together the results from theorem 1. and the ones above, we have,

$$|s_{k,m}(A_1, \dots, A_m)| = \deg P_{s_{k,m}(\mathbb{T})} \geq \ell + 1,$$

that is, since $\deg P_{T_i} = |A_i|$,

$$|s_{k,m}(A_1, \dots, A_m)| \geq \left\lfloor \frac{|A_1| + |A_2| + \cdots + |A_m| - m}{k} \right\rfloor + 1.$$

And in the particular cases of $k = 1$ and $k = m - 1$ we have

$$|s_{1,m}(A_1, \dots, A_m)| \geq \min\{p, |A_1| + |A_2| + \cdots + |A_m| - m + 1\}$$

which is the **Cauchy-Davenport** Theorem, and

$$|s_{m-1,m}(A_1, \dots, A_m)| \geq \min\{p, \left\lfloor \frac{|A_1| + |A_2| + \cdots + |A_m| - m}{m-1} \right\rfloor + 1\}.$$

6. Critical Sets

Another important aspect of this theory is the search for critical sets. We would like now to make some comments on the structure of a set A, such that

$$|s_{k,m}(A, \dots, A)| = \left\lfloor \frac{m(|A| - 1)}{k} \right\rfloor + 1.$$

The example below shows us that these sets do exist (i.e., the results are best possible). Take

$$p = 7, \quad \mathcal{A} = \{0, 1, 6\} \quad \text{and} \quad s_{2,3}(X_1, X_2, X_3) = X_1X_2 + X_1X_3 + X_2X_3.$$

Then, *modulo* 7, we have

$$s_{2,3}(\mathcal{A}) = \{0, 1, 3, 6\},$$

and

$$\left\lfloor \frac{m(|A| - 1)}{m-1} \right\rfloor + 1 = 4.$$

This example is part of a family of examples described in [6], where the main result is

Theorem 3. *Let m, k be positive integers and $k \leq m$. Assume that $m(n-1) \equiv k-1 \pmod{k}$, and p is sufficiently large. If A is a critical set of cardinality n then*

i) either $n \equiv 0 \pmod{k}$ *or* $n \equiv 1 \pmod{k}$;

ii) $A = \{b_{11}, \cdots, b_{1k}, \cdots, b_{q1}, \cdots, b_{qk}\}$, *if* $n \equiv 0 \pmod{k}$ *and*

$A = \{0, b_{11}, \cdots, b_{1k}, \cdots, b_{q1}, \cdots, b_{qk}\}$, *if* $n \equiv 1 \pmod{k}$,

where, $b_{i1}, \ldots, b_{ik}$ are the roots of an equation of the form $X^k - \alpha_i = 0$, with $\alpha_i \in \mathbb{F}$, $i = 1, \ldots, q$.

For the proof of this theorem we must have a better understanding of the linear expression of $s_{k,m}(\mathbb{T})^\tau$. And for that it is necessary to write explicitly the expression of all powers of $s_{k,m}(\mathbb{T})$ in terms of the basis $\mathcal{B}$.

Then the basic idea is to compare the expression of

$$s_{k,m}(\mathbb{T})^{\ell+1}$$

with all the other expressions of $s_{k,m}(\mathbb{T})^\tau$, and then decide when it can be written as a linear combination of the smaller powers

$$\{I, s_{k,m}(\mathbb{T}), s_{k,m}(\mathbb{T})^2, \cdots, s_{k,m}(\mathbb{T})^\ell\}.$$

Acknowledgments: I would like to express my gratitude to the Organizing Committee of the XVI Escola de Álgebra for the invitation to present this work.

References

[1] Chowla, S., *A theorem on addition of residue classes*, Proc. Indian Acad. Sci. 2, (1935), 242-243.

[2] Chowla, S.; Mann, H. B.; Strauss, E. G., *Some applications of the Cauchy-Davenport Theorem*, Kon. Norske Vidensk. Selsk. Forh. 32 (1959), 74-80.

[3] Davenport, H., *On addition of residue classes*, J. London Math. Soc. 10, (1935), 242-243.

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

[5] Dias da Silva, J. A.; Godinho, H., *Generalized Derivations and Additive Theory*, To appear at J. Linear Algebra and Applications.

[6] Dias da Silva, J. A.; Godinho, H., *A Cauchy-Davenport-type theorem related to Symmetric Polynomials-The Inverse Problem* , (In preparation).

[7] Dias da Silva, J. A.; Hamidoune, Y. O., *A note on minimal polynomials of the kronecker sum of two operators*, Linear Algebra and Appl. 141 (1990), 283-287.

[8] Dias da Silva, J. A.; Hamidoune, Y. O., *Cyclic Spaces for Grasmann Derivatives and Additive Theory*, Bull. London Math. Soc. 26, (1994), 140-146. 22 (1947), 100-101.

[9] Mann, H. B., *Addition Theorems: the addition theorems of Group Theory and Number Theory*, Wiley, New York, (1965).

[10] Pollard, J. M., *A generalization of the theorem of Cauchy and Davenport*, J. London Math. Soc. (2) 8 (1974), 460-462.

[11] Scherk, P.; Kemperman, J. H. B., *Complexes in abelian groups*, Canad. J. Math. 6 (1954), 230-237.

[12] Vosper, A. G., *Critical pairs of subsets of a group of prime order*, J. London Math. Soc. 31 (1956), 200-205.

Departamento de Matemática
Universidade de Brasília
70910-900, Brasília, DF
Brazil