A presentation of the discretized sum-product in division algebras

Nicolas de Saxcé

February 2, 2024

Abstract

We explain how the method introduced by Guth, Katz and Zahl for the real line $\mathbb{R}$, can be used to prove a sum-product theorem for division algebras over a local field K of zero characteristic.

Introduction

In the ring of integers $\mathbb{Z}$, one observes a form of independence between addition and multiplication, which translates in particular as follows: If A is a finite subset in $\mathbb{Z}$, the cardinality of the set $(A+A)\cup(A\cdot A)$ of sums and products of two elements of A is not controlled by that of A. This *sum-product* phenomenon seems to have been first studied by Erdős and Szemerédi [9], who proved in 1983 the following remarkable combinatorial result.

Theorem 1 (Erdős-Szemerédi)**.** *There exists $\tau > 0$ such that for any finite subset $A \subset \mathbb{Z}$,*

$$|A+A| + |A\cdot A| \geq |A|^{1+\tau}.$$

Erdős and Szemerédi also conjectured that for all $\varepsilon > 0$, the inequality $|A+A|+|A\cdot A| \geq |A|^{2-\varepsilon}$ would be valid as soon as the cardinality of A is large enough. Solymosi [19] showed that one could take $\tau = \frac{1}{3}$ in the above theorem, and at present, the best result in the direction of the conjecture of Erdős and Szemerédi, due to Rudnev and Stevens [18], gives $\tau = \frac{1}{3} + \frac{2}{1167}$. The present article deals with statements analogous to the sum-product theorem of Erdős and Szemerédi, but which apply in other rings, and to infinite sets whose size is measured by a covering number at some small scale.

The sum-product phenomenon goes well beyond the framework of finite sets of integers. We now know that the inequality of the above theorem is valid for any finite subset of any field which is not too close to a subfield, and Tao [20] even obtained a version which applies in any ring without zero divisors. Furthermore, Katz and Tao [14] also suggested in 2001 to study the sum-product phenomenon for subsets of $\mathbb{R}$ whose size would be measured using a covering number at one small positive scale δ. Their goal was to address a conjecture of Erdős and Volkmann [21, 8] according to which there does not exist a Borel subring of $\mathbb{R}$ with Hausdorff dimension strictly between 0 and 1. That conjecture was solved shortly afterwards by Edgar and Miller [7] using an elegant method which

allowed them more generally to study the Borel subrings of a local field of zero characteristic.

Theorem 2 (Edgar-Miller). *1. Any Borel subring of $\mathbb{C}$ of strictly positive dimension is equal to $\mathbb{R}$ or $\mathbb{C}$.*

2. Let K be a finite extension of $\mathbb{Q}_p$. Any Borel subring of K of strictly positive dimension is closed.

Note that the first point implies that a Borel subring of $\mathbb{R}$ of strictly positive dimension is equal to $\mathbb{R}$, while the second shows that a Borel subring of $\mathbb{Q}_p$ of strictly positive dimension positive is equal to $\mathbb{Z}_p$ or $\mathbb{Q}_p$. Independently of Edgar and Miller, and almost at the same time, Bourgain [2] managed to carry out, in the case of $\mathbb{R}$, the method envisaged by Katz and Tao [14] and he thus obtained the following more precise result.

Proposition 1 (Bourgain). *If A is a Borel subset of $\mathbb{R}$ such that $0 < \dim_{\mathrm{H}} A < 1$, then $\dim_{\mathrm{H}} A + AA > \dim_{\mathrm{H}} A$.*

A central element of Bourgain's proof is a *discretized* sum-product theorem, in which the cardinality is replaced by a covering number. Given $\delta > 0$, the covering number at scale δ of a subset A of a metric space X is defined by

$$N(A,\delta) = \min\{N \mid \exists x_1,\dots,x_N \in X :\ A \subset \bigcup_{i=1}^{N} B(x_i,\delta)\}.$$

The discretized sum-product theorem, conjectured by Katz and Tao [14] and later proved by Bourgain [2, 3] states as follows.

Theorem 3 (Discretized sum-product in $\mathbb{R}$). *Given $\sigma > 0$, there exists $\varepsilon > 0$ such that the following statement holds for any sufficiently small $\delta > 0$.*

Let $A \subset [0,1]$ be such that

1. $N(A,\delta) \leq \delta^{-\sigma-\varepsilon}$;

2. $\forall \rho \geq \delta$, $\forall x \in E$, $N(A \cap B(x,\rho),\delta) \leq \rho^{\sigma}\delta^{-\varepsilon}N(A,\delta)$;

Then

$$N(A+A,\delta) + N(AA,\delta) \geq \delta^{-\varepsilon}N(A,\delta).$$

The first proofs of this result by Bourgain [2, 3] were based on a fine multi-scale analysis of the subsets A in $\mathbb{R}$ which satisfy $N(A+A,\delta) \leq \ delta^{-\varepsilon}N(A,\delta)$. Recently, Guth, Katz and Zahl [10] found a new, more direct proof. The aim of this article is to present a slightly modified version of their proof, valid more generally in any local division algebra of zero characteristic. We shall obtain the following general statement.

Theorem 4 (Sum-product in a local division algebra). *Let E be a finite-dimensional division algebra on $\mathbb{R}$ or $\mathbb{Q}_p$. Given $\sigma \in (0, \dim E)$, there exists $\varepsilon > 0$ such that the following statement holds for any sufficiently small $\delta > 0$.*

Let $A \subset B_E(0,1)$ be such that

1. $N(A,\delta) \leq \delta^{-\sigma-\varepsilon}$;

2. $\forall \rho \geq \delta$, $\forall x \in E$, $N(A \cap B(x,\rho),\delta) \leq \rho^{\sigma}\delta^{-\varepsilon}N(A,\delta)$;

3. $\forall F \subset E$ subalgebra, $\exists a \in A :\ d(a,F) \geq \delta^{\varepsilon}$.

Then,

$$N(A + AA, \delta) \geq \delta^{-\varepsilon} N(A, \delta).$$

For real algebras, Weikun He [11] proved a version of this result that holds more generally in any simple algebra, using the sum-product results in $\mathbb{C}$ that appear in [4]. With an additional hypothesis of non-concentration in the neighborhood of ideals, one can even show that this type of statement is still valid in any real semi-simple algebra [12, Theorem 2.2], and also for certain representations of real Lie groups [13]. The proof presented here does not apply to this general framework, but it is more elementary, does not use the variants of the sum-product in $\mathbb{C}$ of Bourgain and Gamburd, and moreover, remains valid for division algebras over $\mathbb{Q}_p$. The attentive reader will have noticed that the conclusion of the sum-product theorem in a local division algebra is a little weaker than in the case of $\mathbb{R}$, since we only obtain a bound on the set $A + AA$, which allows to control both $A + A$ and AA. If we want to keep our assumptions, this is inevitable, as shown by the example of the pure imaginary segment $A = [0, i]$ in $\mathbb{C}$. However, a lemma of Katz and Tao ensures that if A satisfies $N(A + A, \delta) + N(AA, \delta) \leq \delta^{-\varepsilon} N(A, \delta)$, then there exists a part A' in A such that $N(A'A' + A'A', \delta) \leq \delta^{-O(\varepsilon)} N(A, \delta)$, and this makes it possible to improve the conclusion of Theorem to find a statement close to that of Bourgain, if one replaces the third assumption by a condition ensuring that A is not concentrated near sets of the form aF, where F is a subalgebra of E and $a \in E$. In the case of $\mathbb{R}$ or $\mathbb{Q}_p$, there are no proper subalgebras, and this condition is automatically implied by (ii).

In a follow-up paper [6], we shall use Theorem 4 to show that in a finite-dimensional division algebra over $\mathbb{R}$ or $\mathbb{Q}_p$, every Borel subring of positive dimension is closed, which answers a Miller [1] about the generalization of the conjecture of Erdős and Volkmann to non-commutative local division algebras. We shall even obtain a dimensional inequality analogous to Proposition 1 above.

In the following, we shall state and prove Theorem 4 in several particular cases before dealing with the general case. The reader will undoubtedly find this approach a little repetitive, but it will allow us to study precisely how the growth rate ε depends on the ambient algebra E, and perhaps also to bring up more clearly the main ideas of the proof in the simplest cases.

The plan of the article is as follows: after some preliminary reminders from additive combinatorics, we study in Section 1 the algebras defined on $\mathbb{Q}_p$, by first treating the case $E = \mathbb{Q}_p$, where the proof is the most transparent, then we explain in Section 2 the necessary modifications to adapt the proofs to cover the case of real algebras. We conclude the paper with some remarks on possible extensions of the results presented here.

Notation and preliminary results

Throughout this article, we consider a local field k with zero characteristic. By Ostrowski's theorem, k is equal to $\mathbb{R}$, $\mathbb{C}$, or a finite extension of $\mathbb{Q}_p$, for some prime number p. We are interested in the combinatorial properties of sum and product in a finite-dimensional division algebra E over k. The usual absolute value on $\mathbb{R}$ or $\mathbb{Q}_p$ extends uniquely to E, and this endows E with a natural

1. We thank Emmanuel Breuillard for mentioning this question to us.

structure of normed algebra, Euclidean if k is Archimedean, and ultrametric if k is ultrametric. Recall that if A and B are two subsets of E, we note

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

and

$$AB=\{ab\ ;\ a\in A,\ b\in B\}.$$

Additionally, if n is a natural number,

$$nA=\{a_1+\cdots+a_n\ ;\ a_i\in A\}$$

and

$$A^n=\{a_1\dots a_n\ ;\ a_i\in A\}.$$

Finally, we denote

$$\langle A\rangle_s=sA^s-sA^s.$$

Many of the elementary results from additive combinatorics usually stated for finite sets and cardinality adapt naturally to covering numbers. In particular, we shall use the Plünnecke inequality for covering numbers, which can be deduced from the usual Plünnecke inequality by an approximation argument. Below, and throughout, we write $X\lesssim Y$ if there exists a constant C such that $X\leq CY$; the constant C may depend on the ambient algebra E.

Proposition 2 (Plünnecke's inequality)**.** *Let A and B be two subsets of E such that $N(A+B,\delta)\leq KN(A,\delta)$. For all natural numbers m and n,*

$$N(mA-nA,\delta)\lesssim K^{m+n}N(A,\delta).$$

If A is a subset of a metric space, we denote $A^{(\delta)}$ the neighborhood of A of size δ in X, i.e.

$$A^{(\delta)}=\{x\mid d(x,A)\leq\delta\}.$$

We shall also use Ruzsa's covering lemma for the quantities $N(\cdot,\delta)$, the proof of which is left as an exercise.

Lemma 1 (Ruzsa's covering lemma)**.** *Let A and B be two subsets of E such that $N(A+B,\delta)\leq KN(A,\delta)$. There exists a subset $X\subset B^{(\delta)}$ such that $N(X,\delta)\lesssim K$ and $B\subset A-A+X$.*

Sometimes, we shall use the Landau notation $X=O(Y)$ to mean $X\lesssim Y$. In particular, the notation $O(1)$ denotes a constant which may depend on the ambient algebra E.

1 Division algebras over $\mathbb{Q}_p$

The proof of Theorem 4 is a little simpler when $E=\mathbb{Q}_p$, and we shall therefore start with this particular case. Then, we shall treat the case of a finite extension k of $\mathbb{Q}_p$, for which it suffices to introduce a lemma of "escape out of subspaces"; we shall see that the growth exponent obtained in this case is relatively independent of k. Finally, we shall indicate the few modifications necessary to adapt the proof to the case of a non-commutative division algebra E over $\mathbb{Q}_p$; unfortunately, in this non-commutative framework, our proof gives a growth exponent which depends on the dimension of E on $\mathbb{Q}_p$.

1.1 Sum-product in $\mathbb{Z}_p$

The p-adic valuation of a rational number x is the unique integer $v_p(x)$ such that

$$x = p^{v_p(x)} \cdot \frac{a}{b}, \quad \text{with } a \text{ and } b \text{ not divisible by } p.$$

One defines an absolute value on $\mathbb{Q}$ by the formula $|x|_p = p^{-v_p(x)}$, and the associated distance is given by $d_p(x,y) = |x-y|_p$. The field $\mathbb{Q}_p$ of the p-adic numbers is equal to the complement of $\mathbb{Q}$ for this distance. We also note $\mathbb{Z}_p$ the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$; it is an open and closed neighborhood of 0 in $\mathbb{Q}_p$. Recall that the distance d_p on $\mathbb{Q}_p$ is *ultrametric*, i.e.

$$\forall x, y, z \in \mathbb{Q}_p, \quad d_p(x,z) \leq \max\{d_p(x,y), d_p(y,z)\}.$$

It is this inequality, stronger than the triangular inequality, which makes the proof of the discretized sum-product theorem a little more transparent in $\mathbb{Q}_p$ than in $\mathbb{R}$. Throughout the rest of this section, the prime number p is fixed, and we simply write $d(x,y) = d_p(x,y)$.

The algebra $E = \mathbb{Q}_p$ does not contain any non-trivial subalgebra, so Theorem 4 is a little simpler in this particular case.

Theorem 5 (Discretized sum-product in $\mathbb{Z}_p$)**.** *Given $\sigma \in (0,1)$, let $\varepsilon = \frac{\sigma(1-\sigma)}{21+2\sigma} > 0$. The following statement holds for any small enough $\delta > 0$.*
Let $A \subset \mathbb{Z}_p$ be such that

1. $N(A,\delta) = \delta^{-\sigma}$;
2. $\forall \rho \geq \delta$, $\forall x \in E$, $N(A \cap B(x,\rho),\delta) \leq C\rho^\sigma N(A,\delta)$.

Then,

$$N(AA - AA, \delta) \geq C^{-O(1)}\delta^{-\varepsilon} N(A,\delta).$$

Proof. Let $\gamma > 0$ be a parameter. We consider the set

$$B = \left\{ \frac{a_1 - a_2}{a_3 - a_4} \ ; \ a_1, a_2, a_3, a_4 \in A, \ |a_3 - a_4| \geq \delta^\gamma \right\} \cap \mathbb{Z}_p$$

and the scale

$$\delta_1 = \delta^{1-2\gamma}.$$

Note that the set B always contains 0 and 1. We distinguish two cases.
First case: $\forall x \in B$, $d(x+1, B) \leq \delta_1$.
If $d(y,B) \leq \delta_1$, there exists x in B such that $d(y,x) \leq \delta_1$, and then

$$d(y+1, B) \leq \max\{d(y+1, x+1), d(x+1, B)\} \leq \delta_1.$$

This shows that $B^{(\delta_1)}$ is stable under $x \mapsto x+1$. Therefore $B^{(\delta_1)}$ contains $\mathbb{Z}$, and also $\mathbb{Z}_p$, by density. In particular,

$$N(B, \delta_1) \geq \delta_1^{-1} = \delta^{-1+2\gamma}.$$

Let B' be a maximal $2\delta_1$-separated subset in B, and for each x in B', fix a representation

$$x = \frac{a_x}{b_x} \quad \text{where} \quad a_x \in A - A \text{ and } b_x \in (A-A) \setminus B(0, \delta^\gamma).$$

If A' is a maximal $2\delta^{1-\gamma}$-separated part in $A \setminus B(0,\delta^\gamma)$, the map

$$\begin{array}{ccc} A' \times B' & \to & A(A-A) \times (A-A)A \\ (a,x) & \mapsto & (aa_x, b_x a) \end{array}$$

is injective at the δ scale. Indeed, suppose

$$\begin{cases} aa_x = u + \underline{O}(\delta) \\ b_x a = v + \underline{O}(\delta) \end{cases}$$

where $\underline{O}(\delta)$ denotes an element of norm at most δ. Then,

$$x = \frac{a_x}{b_x} = \frac{u}{v} + \underline{O}\left(\frac{\delta}{|ab_x|}\right) = \frac{u}{v} + \underline{O}(\delta_1)$$

so $x \in B'$ is uniquely determined, and

$$a = \frac{v}{b_x} + \underline{O}\left(\frac{\delta}{|b_x|}\right) = \frac{v}{b_x} + \underline{O}(\delta^{1-\gamma})$$

is also determined in A'. Therefore,

$$N(AA-AA,\delta)^2 \geq N(B,\delta_1)|A'| \gtrsim \delta^{-1+2\gamma}|A'|.$$

As $|A'| \simeq N(A,\delta^{1-\gamma}) \gtrsim \delta^\gamma N(A,\delta)$ and $N(A,\delta) = \delta^{-\sigma}$, we obtain

$$N(AA-AA,\delta) \geq \delta^{-\frac{1}{2}+\gamma}|A'|^{\frac{1}{2}} \gtrsim \delta^{-\frac{1-\sigma-3\gamma}{2}} N(A,\delta).$$

Second case: There exists x in B such that $d(x+1,B) > \delta_1$.
Let us write $x+1 = \frac{e_1}{e_2}$, with $e_1 \in 2A-2A$ and $e_2 \in A-A$ such that $|e_1| \leq |e_2|$ and $|e_2| \geq \delta^\gamma$. We first want to get a lower bound on $N(e_1A + e_2A, \delta)$. Let

$$Q = \{(a_1,a_2,a_3,a_4) \in A^{\times 4} \mid e_2a_1 + e_1a_4 = e_2a_2 + e_1a_3 + \underline{O}(\delta)\}.$$

If (a_1,a_2,a_3,a_4) is in Q, then

$$\left|\frac{a_1-a_2}{a_3-a_4} - \frac{e_1}{e_2}\right| \leq \delta|e_2|^{-1}|a_3-a_4|^{-1} \leq \delta^{1-\gamma}|a_3-a_4|^{-1}.$$

Since $d(\frac{e_1}{e_2}, B) \geq \delta^{1-2\gamma}$, we must have $|a_3-a_4| \leq \delta^\gamma$. If a_4 is known up to an error of size δ, by non-concentration, there are at most $C\delta^{\gamma\sigma}N(A,\delta)$ possibilities for a_3. Then, if a_1, a_3, a_4 are known up to δ, the non-concentration assumption and the equality

$$a_2 = a_1 + \frac{e_1}{e_2}a_4 - \frac{e_1}{e_2}a_3 + O(|e_2|^{-1}\delta)$$

show that there are at most $C|e_2|^{-\sigma}\delta^\sigma N(A,\delta)$ possibilities for a_2, and so

$$N(Q,\delta) \lesssim C^2|e_2|^{-\sigma}\delta^{\sigma(1+\gamma)}N(A,\delta)^4.$$

With the Cauchy-Schwarz inequality this gives

$$N(e_1A + e_2A, \delta) \geq \frac{N(A,\delta)^4}{N(Q,\delta)} \gtrsim C^{-2}|e_2|^\sigma\delta^{-\sigma(1+\gamma)}.$$

On the other hand, as

$$e_1A + e_2A \subset B(0, |e_2|),$$

we can also bound

$$\begin{aligned} N(e_1A + e_2A, \delta) &\lesssim \frac{1}{N(AA, |e_2|)} N(AA + e_1A + e_2A, \delta) \\ &\lesssim C^{\frac{1}{\sigma}} \frac{1}{N(A, |e_2|)} N(AA + e_1A + e_2A, \delta) \\ &\lesssim C^{\frac{1}{\sigma}+1} |e_2|^{\sigma} N(4AA - 3AA, \delta) \end{aligned}$$

and with the Plünnecke inequality,

$$\left(\frac{N(AA - AA, \delta)}{N(A, \delta)} \right)^7 \lesssim C^{-O(1)} |e_2|^{-\sigma} \frac{N(e_1A + e_2A, \delta)}{N(A, \delta)} \lesssim C^{-O(1)} \delta^{-\sigma\gamma}.$$

To conclude, we set $\gamma = \frac{1-\sigma}{3+\frac{2\sigma}{7}}$, so that $\epsilon = \frac{\sigma\gamma}{7} = \frac{1-\sigma-3\gamma}{2} = \frac{\sigma(1-\sigma)}{2\sigma+21}$, and the case disjunction above therefore shows that one always has

$$N(AA - AA, \delta) \geq C^{-O(1)} \delta^{-\varepsilon} N(A, \delta).$$

□

1.2 Finite extensions of $\mathbb{Q}_p$

In this paragraph, we consider a finite extension k of $\mathbb{Q}_p$. The absolute value $|\cdot|_p$ on $\mathbb{Q}_p$ admits a unique extension to k, and for x, y in k, we again write $d(x, y) = |x - y|_p$. This distance on k satisfies the ultrametric inequality. We refer to [1] for the elementary properties of finite extensions of $\mathbb{Q}_p$.

Theorem 6 (Discretized sum-product in k)**.** *Let k be a finite extension of $\mathbb{Q}_p$, and $d = [k : \mathbb{Q}_p]$. Given $\sigma \in (0, 1)$, we set $\varepsilon = \frac{d\sigma(1-\sigma)}{4(40+\sigma)}$. The following statement holds for any sufficiently small $\delta > 0$.*

Let $A \subset B_k(0, 1)$ be such that

1. *$N(A, \delta) = \delta^{-d\sigma}$;*
2. *$\forall \rho \geq \delta$, $\forall x \in k$, $N(A \cap B(x, \rho), \delta) \leq C\rho^{d\sigma} N(A, \delta)$;*
3. *$\forall F \subset k$ subalgebra over $\mathbb{Q}_p$, $\exists a \in A : \ d(a, F) \geq c$.*

Then,

$$N(A + AA, \delta) \geq c^{O(1)} C^{-O(1)} \delta^{-\varepsilon} N(A, \delta).$$

Remark. The quantity σ corresponds to the renormalized dimension of A:

$$\sigma = \dim' A := \frac{\dim A}{d}.$$

And the lower bound on ε given by the above theorem shows that the growth rate for the renormalized dimension is independent of the field k. Indeed, setting $\varepsilon' = \frac{\varepsilon}{d} \geq \frac{\sigma(1-\sigma)}{164}$, we have

$$\dim'(A + AA) \geq \dim' A + \varepsilon'.$$

Proof of Theorem 6. The proof is similar to that of theorem 5, but we use the two operations $(x,y) \mapsto x+y$ and $(x,y) \mapsto xy$ instead of $x \mapsto x+1$, to obtain a growth rate that is independent of k. As above, for $\gamma > 0$, we consider the set

$$B = \left\{ \frac{a_1 - a_2}{a_3 - a_4} \ ; \ a_1, a_2, a_3, a_4 \in A, \ |a_3 - a_4| \geq \delta^\gamma \right\} \cap B_k(0,1)$$

and the scale

$$\delta_1 = \delta^{1-3\gamma}.$$

Note that the set B always contains 0 and 1. We make two cases.
First case: $\forall x, y \in B$, $d(x+y, B) \leq \delta_1$ and $d(xy, B) \leq \delta_1$.
Let us show that $B^{(\delta_1)}$ is stable under $+$ and $\times$. If $d(x', B), d(y', B) \leq \delta_1$, we choose $x, y \in B$, such that $d(x', x), d(y', y) \leq \delta_1$, and then

$$d(x'+y', B) \leq \max\{d(x'+y', x+y'), d(x+y', x+y), d(x+y, B)\} \leq \delta_1.$$

Similarly, as $A \subset B_k(0,1)$,

$$d(x'y', B) \leq \max\{d(x'y', xy'), d(xy', xy), d(xy, B)\} \leq \delta_1.$$

Since B contains 0 and 1, the stability under addition shows that $B^{(\delta_1)} \supset \mathbb{Z}_p$, then the stability under multiplication, with the proposition 4 below below, shows that there exists a subalgebra F of E such that

$$B_F(0, c^{O(1)}) \subset B^{(\delta_1)} \subset B_F(0, O(1)). \tag{1}$$

First suppose $F \subsetneq E$. If a_0 is a fixed element of maximum norm in A, the inclusion $B \subset F$ implies that $a_0^{-1}(A-A) \subset F$. Since A is far from any subalgebra, we can find a in A such that $d(a, F) \geq c$, and then F and aF are in direct sum, so that

$$\begin{aligned} N(A - A + AA - AA, \delta) &\gtrsim C^{-O(1)} N(a_0^{-1}(A-A) + a a_0^{-1}(A-A), \delta) \\ &\gtrsim c^{O(1)} C^{-O(1)} N(A-A, \delta)^2 \\ &\gtrsim c^{O(1)} C^{-O(1)} \delta^{-d\sigma} N(A, \delta). \end{aligned}$$

With the Plünnecke inequality, this implies

$$N(A + AA, \delta) \gtrsim c^{O(1)} C^{-O(1)} \delta^{-\frac{d\sigma}{14}} N(A, \delta). \tag{2}$$

Now suppose $F = E$. The left inclusion in the formula (1) above implies

$$N(B, \delta_1) \geq c^{O(1)} \delta_1^{-d} = c^{O(1)} \delta^{-d+3d\gamma}.$$

Let us then consider B' a maximal $2\delta_1$-separated subset in B, and for each x in B', let us fix a representation

$$x = \frac{a_x}{b_x} \quad \text{where} \quad a_x \in A - A \text{ and } b_x \in (A-A) \setminus B(0, \delta^\gamma).$$

If A' is a maximal $2\delta^{1-\gamma}$-separated subset in $A \setminus B(0, \delta^\gamma)$, then the map

$$\begin{array}{ccc} A' \times B' & \to & A(A-A) \times (A-A)A \\ (a, x) & \mapsto & (a_x a, b_x a) \end{array}$$

is injective at scale δ. Therefore,

$$N(B,\delta_1) \leq \frac{N(AA-AA,\delta)^2}{|A'|}.$$

Since $|A'| \simeq N(A,\delta^{1-\gamma}) \gtrsim \delta^{d\gamma} N(A,\delta)$, we find

$$N(AA-AA,\delta) \geq c^{O(1)}\delta^{-\frac{(1-\sigma-4\gamma)d}{2}} N(A,\delta),$$

which by the Plünnecke inequality implies

$$N(A+AA,\delta) \geq c^{O(1)}\delta^{-\frac{(1-\sigma-4\gamma)d}{4}} N(A,\delta). \tag{3}$$

Second case: There exists x and y in B such that $d(x+y,B) > \delta_1$ or $d(xy,B) > \delta_1$.
Depending on the case, write $x+y = \frac{e_1}{e_2}$ with $e_1 \in 2(A-A)(A-A)$ and $e_2 \in (A-A)(A-A)$, or $xy = frace_1e_2$ with $e_1 \in (A-A)(A-A)$ and $e_2 \in (A-A)(A-A)$. Note that in any case $|e_1| \leq |e_2|$ and $|e_2| \geq \delta^{2\gamma}$.

We first want to get a lower bound on $N(e_1A+e_2A,\delta)$. Let

$$Q = \{(a_1,a_2,a_3,a_4) \in A^{\times 4} \mid e_2a_1 + e_1a_4 = e_2a_2 + e_1a_3 + \underline{O}(\delta)\}.$$

If (a_1,a_2,a_3,a_4) belongs to Q, then

$$\left|\frac{a_1-a_2}{a_3-a_4} - \frac{e_1}{e_2}\right| \leq \frac{\delta}{|e_2(a_3-a_4)|} \leq \frac{\delta^{1-2\gamma}}{|a_3-a_4|}.$$

Since $d(\frac{e_1}{e_2},B) \geq \delta^{1-3\gamma}$, we must have $|a_3-a_4| \leq \delta^\gamma$. If a_4 is known up to δ, by non-concentration, there are at most $C\delta^{\gamma d\sigma}N(A,\delta)$ choices for a_3. Then, if a_1,a_3,a_4 are known up to δ, as

$$a_2 = a_1 + \frac{e_1a_4}{e_2} - \frac{e_1a_3}{e_2} + \underline{O}(\frac{\delta}{|e_2|})$$

the non-concentration hypothesis shows that there are at most $C|e_2|^{-d\sigma}\delta^{d\sigma}N(A,\delta)$ possibilities for a_2, and so

$$N(Q,\delta) \leq C^2|e_2|^{-d\sigma}\delta^{d\sigma(1+\gamma)}N(A,\delta)^4.$$

Consequently,

$$N(e_1A+e_2A,\delta) \geq \frac{N(A,\delta)^4}{N(Q,\delta)} \geq C^{-2}|e_2|^{d\sigma}\delta^{-d\sigma(1+\gamma)}.$$

Since $e_1A+e_2A \subset B_k(0,|e_2|)$, this implies

$$\begin{aligned} N(A+e_1A+e_2A,\delta) &\gtrsim N(A,|e_2|)N(e_1A+e_2A,\delta) \\ &\gtrsim C^{-O(1)}|e_2|^{-d\sigma}|e_2|^{d\sigma}\delta^{-d\sigma(1+\gamma)} \\ &= C^{O(1)}\delta^{-d\gamma}N(A,\delta). \end{aligned}$$

Now, according to Proposition 3 below and the remark that follows it,

$$\frac{N(A+e_1A+e_2A,\delta)}{N(A,\delta)} \lesssim \left(\frac{N(A+AA,\delta)}{N(A,\delta)}\right)^{40}$$

and so,

$$N(A+AA,\delta) \gtrsim C^{-O(1)}\delta^{-\frac{d\gamma}{38}}N(A,\delta). \tag{4}$$

With $\gamma = \frac{1-\sigma}{4(1+\frac{\sigma}{38})}$, we find

$$\varepsilon = \frac{(1-\sigma-4\gamma)d}{4} = \frac{d\sigma\gamma}{38} = \frac{\sigma(1-\sigma)}{4(38+\sigma)} < \frac{\sigma d}{14}$$

and the inequalities (2), (3) and (4) together allow us to conclude:

$$N(A+AA,\delta) \gtrsim c^{O(1)}C^{-O(1)}\delta^{-\varepsilon}N(A,\delta).$$

□

It remains to prove the two results that we used. The first is a standard additive combinatorics result, which shows that the growth of the set $A+AA$ makes it possible to control that of any set

$$\langle A\rangle_s = sA^s - sA^s.$$

The proof is based on Plünnecke's inequality and Ruzsa's covering lemma.

Proposition 3. *Let E be a finite-dimensional algebra on $\mathbb{R}$ or $\mathbb{Q}_p$. If $A \subset B_E(0,1)$ satisfies $N(A+AA,\delta) \leq KN(A,\delta)$, then, for every integer $s \geq 1$,*

$$N(\langle A\rangle_s,\delta) \leq K^{O_s(1)}N(A,\delta).$$

Remark. If A satisfies $N(A+AA,\delta) \leq KN(A,\delta)$, and if e_1, e_1' and e_2 are three elements of $(A-A)(A-A)$, we leave it to the reader to check that the proof of this proposition yields

$$N(A+e_1A+e_1'A-e_2A,\delta) \lesssim K^{38}N(A,\delta).$$

Proof of Proposition 3. Let us first show that for all $x \in \langle A\rangle_s$, there exists a finite set $X_{x,s}$ such that

$$N(X_{x,s},\delta) \leq K^{O_s(1)} \quad \text{et} \quad xA \subset A-A+X_{x,s}.$$

This can be seen by induction on s. For $s=1$, by Ruzsa's covering lemma, there exists a set X such that $N(X,\delta) \lesssim K$ and $AA \subset A-A+X$, so the result is clear. Then, we notice that if $xA \subset A-A+X_{x,s}$ and $yA \subset A-A+X_{y,s}$, then thanks to Ruzsa's covering lemma again, we can write

$$\begin{aligned}(x+y)A &\subset xA+yA\\ &\subset A-A+A-A+X_{x,s}+X_{y,s}\\ &\subset A-A+X_{x+y,s+1}\end{aligned}$$

for a set $X_{x+y,s+1}$ such that $N(X_{x+y,s+1},\delta) \lesssim K^{O_s(1)}$. Likewise,

$$(x-y)A \subset A-A+X_{x-y,s+1},$$

and also,

$$\begin{aligned}xyA &\subset xA-xA+xX_{y,s}\\ &\subset A-A+A-A+X_{x,s}-X_{x,s}+xX_{y,s}\\ &\subset A-A+X_{xy,s+1}.\end{aligned}$$

Naturally, this property still holds for all x in a δ-neighborhood of $\langle A\rangle_s$.

Let us now show by induction that there exists X_s in a δ-neighborhood of $\langle A\rangle_s$ such that $N(X_s,\delta)\leq K^{O_s(1)}$ and $A^s\subset A-A+X_s$. This has already been seen for $s=2$. Let us therefore assume the result is known for some $s\geq 2$. Then,

$$A+A^{s+1}\subset A+A(A-A+X_s)\subset A+AA-AA+AX_s.$$

By the first part of the proof, $AX_s\subset A-A+X'$, where $X'=\cup_{x\in X_s}X_{x,s}$, so

$$\begin{aligned}N(A+A^{s+1},\delta)&\leq N(A+AA-AA+A-A+X',\delta)\\&\leq K^{O_s(1)}N(A,\delta)\end{aligned}$$

Then

$$A^{s+1}\subset A-A+X_{s+1},$$

by Ruzsa's covering lemma.

To conclude, it suffices to observe that we have

$$\begin{aligned}\langle A\rangle_s&=A^s\pm\cdots\pm A^s\\&\subset A-A+\cdots+A-A+X_s\pm\cdots\pm X_s\end{aligned}$$

which indeed implies $N(\langle A\rangle_s,\delta)\leq K^{O_s(1)}N(A,\delta)$, by the Plünnecke inequality. □

The second proposition gives a bound on the number of products necessary to generate an algebra E from a generating subset A. In the real case, this statement is proven in He [11, Proposition 16] using the Łojasiewicz inequality. We give here a slightly different proof, which also applies to the p-adic case.

Proposition 4 (Escape from subspaces)**.** *Let E be a normed division algebra over $\mathbb{R}$ or $\mathbb{Q}_p$, and let $A\subset B_E(0,1)$ be a subset at distance $\rho>0$ of any subalgebra. There exists $a_1,\dots,a_d$ in A^d such that $\det(a_1,\dots,a_d)\geq\rho^{O(1)}$.*

Proof. Replacing A by $A\setminus B_E(0,\rho)$ if necessary, we may assume that every element a in A satisfies $|a|\geq\rho$.

We construct the basis $(a_k)_{k\geq 1}$ by induction. Let $k\geq 0$, and suppose that the elements a_i, $i\leq k$ have been constructed in A^k so that for all $i\leq k$, $d(a_i,V_i)\geq\rho^{O(1)}$, where $V_i=\mathrm{Span}(a_j;j<i)$. Let G denote the compact group of elements of norm 1 in E, and

$$A'=\{\frac{a}{|a|}\ ;\ a\in A\}.$$

The group G naturally acts from the left on E, and A' is at distance ρ from any subgroup of the form $\mathrm{Stab}_G W$, where $W<E$ is a subgroup vector space, because by assumption, A is at distance ρ from any subalgebra. The second point of Lemma 2 below applied to the set

$$F=\{\mathbf{w}=v_1\wedge\cdots\wedge v_k\in\wedge^k E\ ;\ |\mathbf{w}|=1\}$$

therefore shows that there exists a in A such that

$$d(\frac{a}{|a|}V_{k+1},V_{k+1})=d(aV_{k+1},V_{k+1})\geq\rho^{O(1)}.$$

Now, given the condition $d(a_i, V_i) \geq \rho^{O(1)}$ for $i = 1, \ldots, k$, we have

$$d(aV_{k+1}, V_{k+1}) \leq \rho^{-O(1)} \max_{1 \leq i \leq k} d(aa_i, V_{k+1}).$$

Therefore, there exists a in A and $i \in \{1, \ldots, k\}$ such that $d(aa_i, V_{k+1}) \geq \rho^{O(1)}$. We then set $a_{k+1} = aa_i \in A^{k+1}$.

The family $(a_i)_{1 \leq i \leq d}$ is a family of elements of A^d, and the inequalities $d(a_i, V_i) \geq \rho^{O(1)}$ and $|a_i| = O(1)$ for $i = 1, \ldots, d$ show that we also have

$$\det(a_1, \ldots, a_d) \geq \rho^{O(1)}.$$

□

Lemma 2 (Distance to stabilizer)**.** *Let G be a compact Lie group on $k = \mathbb{R}$ or $\mathbb{Q}_p$, and V be a linear representation of G on k.*

1. *For all $v \in V$, there exists a constant $c > 0$ such that for all $g \in G$, $d(gv, v) \geq c \cdot d(g, \mathrm{Stab}_G\, v)$.*
2. *If F is a compact subset invariant under the action of G, there exists $C > 0$ such that for all $v \in F$, there exists $v_1 \in F$ such that for all $g \in G$, $d(g, \mathrm{Stab}_G\, v_1) \leq C d(gv, v)$.*

Proof. Let us denote $H = \mathrm{Stab}_G\, v$ and $\mathfrak{h} = \mathrm{Lie}(H)$. Let W be a complement of $\mathfrak{h}$ in $\mathfrak{g} = \mathrm{Lie}(V)$ and U be a neighborhood of 0 in W such that $Y \mapsto e^Y \cdot v$ be a diffeomorphism of U on its image. There exists $c_0 > 0$ such that if $d(g, H) < c_0$, we can write $g = e^Y h$, with $h \in H$ and $Y \in U$, hence

$$d(gv, v) = d(e^Y v, v) \simeq \|Y\| \simeq d(g, H).$$

Since moreover, the continuous function $g \mapsto \frac{d(gv,v)}{d(g,H)}$ is strictly positive on the compact set $d(g, H) \geq c_0$, we indeed find that there exists $c > 0$ such that for all $g \in G$, $d(gv, v) \geq c d(g, H)$. This shows the first part of the lemma.

For the second, let v_0 be a unit vector in V. Let T_0 be the tangent space to Gv_0 at the point v_0 and $T_0^\perp$ be a $(\mathrm{Stab}_G\, v_0)$-invariant complement in V. In a neighborhood U_{v_0} of Gv_0, any vector v can be written uniquely

$$v = x + t,$$

with $x = \sigma(x)v_0 \in Gv_0$ and $t \in \sigma(x)T_0^\perp$ for a certain $\sigma(x) \in G$, and the map $v\ mapsto(x, t)$ is a diffeomorphism of U_{v_0} onto $Gv_0 \times B_{T_0^\perp}(0, r_0)$. Now, for g in G,

$$gv = gx + gt \quad \text{et} \quad gt \in g\sigma(x)T_0^\perp = \sigma(gx)T_0^\perp,$$

Therefore,

$$\begin{aligned} d(gv, v) &\gtrsim d(gx, x) \\ &= d(g\sigma(x)v_0, \sigma(x)v_0) \\ &= d(\sigma(x)^{-1}g\sigma(x)v_0, v_0) \\ &\geq \frac{1}{C_0} d(g, \mathrm{Stab}_G\, \sigma(x)v_0) \end{aligned}$$

according to the first point of the lemma. This shows the desired property for all v in the neighborhood of an arbitrary point v_0, taking $v_1 = \sigma(x)v_0$. We conclude by taking a finite covering of F by open sets of the form U_{v_0}. □

1.3 Non-commutative division algebras

In this paragraph, E denotes a division algebra over $\mathbb{Q}_p$, not necessarily commutative. The usual absolute value $|\cdot|_p$ on $\mathbb{Q}_p$ again extends uniquely to E.

Theorem 7 (Sum-product in division algebras over $\mathbb{Q}_p$)**.** *Let E be a division algebra of dimension d over $\mathbb{Q}_p$. Given $\sigma \in (0,1)$, there exists $\varepsilon = \varepsilon(d) > 0$ such that the following statement holds for any sufficiently small $\delta > 0$.*

Let $A \subset B_E(0,1)$ be such that

1. $N(A,\delta) = \delta^{-d\sigma}$;
2. $\forall \rho \geq \delta$, $\forall x \in E$, $N(A \cap B(x,\rho),\delta) \leq C\rho^{d\sigma} N(A,\delta)$;
3. $\forall F \subset E$ *subalgebra*, $\exists a \in A :\ d(a,F) \geq c$.

Then,

$$N(A+AA,\delta) \geq c^{O(1)} C^{-O(1)} \delta^{-\varepsilon} N(A,\delta).$$

Proof. Let us denote $K = \frac{N(A+AA,\delta)}{N(A,\delta)}$. We want to show that $K \geq c^{O(1)} C^{-O(1)} \delta^{-\varepsilon}$. Given a parameter $\gamma > 0$, we consider the set

$$B = B_1 \cup B_2,$$

where

$$B_1 = \left\{ (a_1 - a_2)(a_3 - a_4)^{-1} \ ;\ a_1,a_2,a_3,a_4 \in A,\ |a_3 - a_4| \geq \delta^\gamma \right\}$$

and

$$B_2 = \left\{ (a_1 - a_2)^{-1}(a_3 - a_4) \ ;\ a_1,a_2,a_3,a_4 \in A,\ |a_3 - a_4| \geq \delta^\gamma \right\}.$$

We also let

$$\delta_1 = \delta^{1-2\gamma}.$$

Note that the set B always contains 0 and 1. The lack of commutativity makes it difficult to check stability of B under $+$ and $\times$, so we go back to the argument used for $\mathbb{Q}_p$, which only involves the operation $x \mapsto x+1$. It is because of this that the growth exponent obtained will depend on the dimension of E on $\mathbb{Q}_p$.
First case: $\forall x \in B$, $d(x+1,B) \leq \delta_1$.
The set $B^{(\delta_1)}$ is then stable by $x \mapsto x+1$. Therefore, $B^{(\delta_1)} \supset \mathbb{Z}_p$, and so

$$N(B_1^{(\delta_1)} \cap \mathbb{Z}_p, \delta_1) \gtrsim \delta_1^{-1} \quad \text{or} \quad N(B_2^{(\delta_1)} \cap \mathbb{Z}_p, \delta_1) \gtrsim \delta_1^{-1}$$

Suppose to fix ideas that the first inequality holds. According to Proposition 4 above, we can find elements $a_1,\dots,a_d$ in A^d which form a base of E with determinant $c^{O(1)}$. Consequently,

$$N(a_1 B_1^{(\delta_1)} + \cdots + a_d B_1^{(\delta_1)}, \delta_1) \geq c^{O(1)} \delta_1^{-d}. \tag{5}$$

Consider a maximal δ_1-separated subset B in $A + B_1$, and for each x in B', fix a representation

$$x = a_x b_x^{-1} \quad \text{where} \quad \begin{cases} a_x \in A(A-A) + (A-A) \\ b_x \in (A-A) \setminus B(0,\delta^\gamma) \end{cases}.$$

Let also A' be a maximal $\delta^{1-\gamma}$-separated subset in $A \setminus B(0,\delta^\gamma)$. The map

$$\begin{array}{ccc} A' \times B' & \to & (AAA - AAA + AA - AA) \times (AA - AA) \\ (a,x) & \mapsto & (a_x a, b_x a) \end{array}$$

is injective at scale δ. Therefore,

$$N(A+B_1,\delta_1) \leq \frac{N(AAA-AAA+AA-AA,\delta)N(AA-AA,\delta)}{|A'|}$$

and with Proposition 3

$$\begin{aligned} N(A+B_1,\delta_1) &\lesssim K^{32}\frac{N(A,\delta)^2}{|A'|} \\ &\lesssim K^{32}\delta^{-d\gamma}N(A,\delta) \end{aligned}$$

and so

$$N(A+B_1,\delta) \lesssim K^{32}\delta^{-3d\gamma}N(A,\delta).$$

By Ruzsa's covering lemma, this implies that there exists a part X such that $N(X,\delta) \lesssim K^{32}\delta^{-3d\gamma}$ and

$$B_1 \subset A - A +$$

Consequently, for a set X' such that $N(X',\delta) \leq N(X,\delta)^d \leq K^{32d}\delta^{-3d^2\gamma}$,

$$a_1B_1 + \cdots + a_dB_1 \subset dA^{d+1} - dA^{d+1} + X'$$

and therefore, with Proposition 3,

$$\begin{aligned} N(a_1B_1+\cdots+a_dB_1,\delta) &\lesssim K^{32d}\delta^{-3d^2\gamma}N(dA^{d+1}-dA^{d+1},\delta) \\ &\lesssim K^{O_d(1)}\delta^{-3d^2\gamma}N(A,\delta). \end{aligned}$$

This inequality together with (6) gives

$$c^{O(1)}\delta^{-d+2d\gamma} \lesssim N(a_1B_1+\cdots+a_dB_1,\delta_1) \leq N(a_1B_1+\cdots+a_dB_1,\delta) \lesssim K^{O_d(1)}\delta^{-3d^2\gamma}N(A,\delta)$$

whence

$$K^{O_d(1)} \geq c^{O(1)}\delta^{-d(1-\sigma)+2\gamma+3d^2\gamma}.$$

Second case: There exists x in B such that $d(x+1,B) > \delta_1$.
To fix ideas, suppose $x \in B_1$ so that we can write

$$x+1 = e_1e_2^{-1} \quad \text{with} \quad e_1 \in 2A-2A, \quad e_2 \in A-A, \text{ and } |e_2| \geq \delta^\gamma.$$

(If $x \in B_2$, we must instead write $x+1 = e_2^{-1}e_1$ and use the set e_1A+e_2A below, but the rest of the argument adapts without difficulty.)

We first want to bound $N(Ae_2+Ae_1,\delta)$ from below. Let

$$Q = \{(a_1,a_2,a_3,a_4) \in A^{\times 4} \mid a_1e_2 + a_4e_1 = a_2e_2 + a_3e_1 + \underline{O}(\delta)\}.$$

If (a_1,a_2,a_3,a_4) belongs to Q, then

$$\left|(a_3-a_4)^{-1}(a_1-a_2) - e_1e_2^{-1}\right| \leq \delta|e_2|^{-1}|a_3-a_4|^{-1} \leq \delta^{1-\gamma}|a_3-a_4|^{-1}.$$

Since $d(e_1e_2^{-1}, B) \geq \delta^{1-2\gamma}$, we must have $|a_3 - a_4| \leq \delta^\gamma$. If a_4 is known up to δ, then by non-concentration there are at most $C\delta^{d\gamma\sigma}N(A,\delta)$ possibilities for a_3. Then, if a_1, a_3, a_4 are known up to δ, as

$$a_2 + a_3e_1e_2^{-1} = a_1 + a_4e_1e_2^{-1} + \underline{O}(|e_2|^{-1}\delta)$$

the non-concentration assumption shows that there are at most $C|e_2|^{-d\sigma}\delta^{d\sigma}N(A,\delta)$ possibilities for a_2, and so

$$N(Q,\delta) \leq C^2|e_2|^{-d\sigma}\delta^{d\sigma(1+\gamma)}N(A,\delta)^4.$$

Subsequently,

$$N(Ae_1 + Ae_2, \delta) \geq \frac{N(A,\delta)^4}{N(Q,\delta)} \geq C^{-2}|e_2|^{d\sigma}\delta^{-d\sigma(1+\gamma)}$$

and then, as before,

$$N(A + Ae_1 + Ae_2, \delta) \gtrsim C^{-O(1)}\delta^{-d\gamma}N(A,\delta).$$

With Proposition 3, this yields

$$K^{O(1)} \geq C^{-O(1)}\delta^{-d\gamma}.$$

Choosing $\gamma = \frac{d(1-\sigma)}{3d^2+2}$, we find in both cases above $K \geq c^{O(1)}C^{-O(1)}\delta^{-\varepsilon}$, for a certain $\varepsilon > 0$ depending on d. □

2 Division algebras over $\mathbb{R}$

We now briefly explain how the above proof adapts to derive a discretized sum-product theorem in real division algebras. Note that according to Wedderburn's theorem, such an algebra is isomorphic to $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$, the quaternion algebra. The argument is similar to that given for algebra over $\mathbb{Q}_p$, but it is necessary to compensate for the fact that the distance is no longer ultrametric. To do this, we replace the operation $x \mapsto x + 1$ by the two operations $x \mapsto \frac{x}{2}$ and $x \mapsto \frac{x+1}{2}$.

The algebra of quaternions

Recall that the quaternion algebra $\mathbb{H}$ is a four-dimensional algebra over $\mathbb{R}$, a basis of which is given by the elements $(1, i, j, k)$ satisfying the relations $i^2 = j^2 = k^2 = -1$ and $ij = k$. One can identify $\mathbb{H}$ with the subalgebra of $M_2(\mathbb{C})$ generated by the matrices

$$i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{et} \quad k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

The algebra $\mathbb{H}$ is non-commutative, but has no zero divisors, so it is a division algebra. Any proper subalgebra of $\mathbb{H}$ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$. Naturally, the only subalgebra isomorphic to $\mathbb{R}$ is $\mathbb{R} \simeq \mathbb{R}1$, but there exist in $\mathbb{H}$ an infinite number of embeddings of $\mathbb{C}$, among which $\mathbb{C} \simeq \mathbb{R}1 \oplus \mathbb{R}i$, $\mathbb{C} \simeq \mathbb{R}1 \oplus \mathbb{R}j$ and

$\mathbb{C} \simeq \mathbb{R}1 \oplus \mathbb{R}k$. The usual absolute value on $\mathbb{R}$ extends uniquely to an absolute value on $\mathbb{H}$, given by the formula

$$|a + bi + cj + dj| = \sqrt{a^2 + b^2 + c^2 + d^2}.$$

In $\mathbb{H}$, the discretized sum-product theorem states as follows.

Theorem 8 (Discretized sum-product in $\mathbb{H}$)**.** *Given $\sigma \in (0,1)$, let $\varepsilon = \frac{\sigma(1-\sigma)}{36\sigma + \frac{49}{2}}$. The following statement is valid for any sufficiently small $\delta > 0$.*

Let $A \subset B_{\mathbb{H}}(0,1)$ be such that

1. *$N(A,\delta) = \delta^{-4\sigma}$;*
2. *$\forall \rho \geq \delta$, $\forall x \in \mathbb{H}$, $N(A \cap B(x,\rho),\delta) \leq C\rho^{4\sigma} N(A,\delta)$;*
3. *$\forall F \subset \mathbb{H}$ subalgebra, $\exists a \in A :\ d(a,F) \geq c$.*

Then,

$$N(A + AA, \delta) \geq c^{O(1)} C^{-O(1)} \delta^{-\varepsilon} N(A,\delta).$$

Proof. As in the p-adic case, we use an auxiliary parameter $\gamma > 0$ and we consider

$$B = B_1 \cup B_2,$$

where

$$B_1 = \left\{ (a_1 - a_2)(a_3 - a_4)^{-1} \ ;\ a_1, a_2, a_3, a_4 \in A,\ |a_3 - a_4| \geq \delta^{\gamma} \right\}$$

and

$$B_2 = \left\{ (a_1 - a_2)^{-1}(a_3 - a_4) \ ;\ a_1, a_2, a_3, a_4 \in A,\ |a_3 - a_4| \geq \delta^{\gamma} \right\}.$$

We also put

$$\delta_1 = \delta^{1-2\gamma}.$$

We shall show that

$$K = \frac{N(A + AA, \delta)}{N(A,\delta)} \geq \delta^{-\varepsilon}.$$

<u>First case:</u> $\forall x \in B$, $d(\frac{x}{2}, B) \leq \frac{\delta_1}{2}$ and $d(\frac{x+1}{2}, B) \leq \frac{\delta_1}{2}$.
The set $B^{(\delta_1)}$ is then stable by $x \mapsto \frac{x}{2}$ and $x \mapsto \frac{x+1}{2}$. Therefore, $B^{(\delta_1)} \supset [0,1]$, and so

$$N(B_1^{(\delta_1)} \cap [0,1], \delta_1) \gtrsim \delta_1^{-1} \quad \text{or} \quad N(B_2^{(\delta_1)} \cap [0,1], \delta_1) \gtrsim \delta_1^{-1}$$

Let us assume to fix ideas that the first inequality is satisfied. According to Proposition 4 above, we can find elements $a_1, \ldots, a_4$ in A^2 which form a basis of $\mathbb{H}$ with determinant $c^{O(1)}$. Subsequently,

$$N(a_1 B_1^{(\delta_1)} + \cdots + a_4 B_1^{(\delta_1)}, \delta_1) \geq c^{O(1)} \delta_1^{-4}. \tag{6}$$

Consider B' a maximal δ_1-separated subset in $A + B_1$, and for each x in B', fix a representation

$$x = a_x b_x^{-1} \quad \text{where} \quad \left\{ \begin{array}{l} a_x \in A(A-A) + (A-A) \\ b_x \in (A-A) \setminus B(0,\delta^{\gamma}) \end{array} \right. .$$

If A' is a maximal $\delta^{1-\gamma}$-separated subset in $A \setminus B(0,\delta^\gamma)$, the map

$$\begin{array}{ccc} A' \times B' & \to & (AAA-AAA+AA-AA)\times(AA-AA) \\ (a,x) & \mapsto & (a_x a, b_x a) \end{array}$$

is injective at scale δ Consequently,

$$\begin{aligned} N(A+B_1,\delta_1) &\leq \frac{N(AAA-AAA+AA-AA,\delta)N(AA-AA,\delta)}{|A'|} \\ &\lesssim \delta^{-4\gamma}K^{32}N(A,\delta). \end{aligned}$$

and so

$$N(A+B_1,\delta) \lesssim \delta^{-12\gamma}K^{32}N(A,\delta).$$

By Ruzsa's covering lemma, this implies that there exists a set X such that $N(X,\delta) \lesssim \delta^{-12\gamma}K^{32}$ and

$$B_1 \subset A - A+$$

But Ruzsa's covering lemma also gives $AA \subset Y + A - A$, with $N(Y,\delta) \lesssim K$ and therefore

$$a_1(A-A)+\cdots+a_4(A-A) \subset Y' + 4AA - 4AA$$

for a set Y' such that $N(Y',\delta) \lesssim K^8$ Thus,

$$N(a_1(A-A)+\cdots+a_4(A-A),\delta) \lesssim K^8 N(4AA-4AA,\delta) \lesssim K^{16}N(A,\delta).$$

Therefore,

$$\begin{aligned} N(a_1B_1+\cdots+a_4B_1,\delta) &\lesssim \delta^{-48\gamma}K^{128}N(a_1(A-A)+\cdots+a_4(A-A),\delta) \\ &\lesssim K^{144}\delta^{-48\gamma}N(A,\delta) \end{aligned}$$

This inequality, put in relation with (6), gives

$$\begin{aligned} c^{O(1)}\delta^{-4+8\gamma} &\lesssim N(a_1B_1+\cdots+a_4B_1,\delta) \\ &\lesssim K^{144}\delta^{-48\gamma}N(A,\delta) \\ &= K^{144}\delta^{-48\gamma-4\sigma} \end{aligned}$$

whence

$$K \gtrsim c^{O(1)}\delta^{-\frac{1-\sigma-14\gamma}{36}}.$$

Second case: There exists x in B such that $d(\frac{x}{2},B) > \frac{\delta_1}{2}$ or $d(\ fracx+12,B) > \frac{\delta_1}{2}$.
To fix ideas, assume $x \in B_1$ and $d(\frac{x+1}{2},B) > \frac{\delta_1}{2}$, so that we can write

$$x+1 = e_1e_2^{-1} \quad \text{with} \quad e_1 \in 2A-2A, \quad e_2 \in A-A, \text{ and } |e_2| \geq \delta^\gamma.$$

We first want to get a lower bound for $N(Ae_2+Ae_1,\delta)$. Let

$$Q = \{(a_1,a_2,a_3,a_4) \in A^{\times 4} \mid a_1e_2 + a_4e_1 = a_2e_2 + a_3e_1 + \underline{O}(\delta)\}.$$

If (a_1,a_2,a_3,a_4) belongs to Q, then

$$\left|(a_3-a_4)^{-1}(a_1-a_2) - e_1e_2^{-1}\right| \leq \delta|e_2|^{-1}|a_3-a_4|^{-1} \leq \delta^{1-\gamma}|a_3-a_4|^{-1}.$$

Since $d(e_1e_2^{-1}, B) \geq \delta^{1-2\gamma}/2$, we must have $|a_3 - a_4| \leq 2\delta^\gamma$. If a_4 is known up to an error δ, by non-concentration, there are at most $C2^{4\gamma}\delta^{4\gamma\sigma}N(A,\delta)$ possibilities for a_3. Then, if a_1, a_3, a_4 are known up to δ, as

$$a_2 + a_3e_1e_2^{-1} = a_1 + a_4e_1e_2^{-1} + \underline{O}(|e_2|^{-1}\delta)$$

the non-concentration hypothesis shows that there are at most $C|e_2|^{-4\sigma}\delta^{4\sigma}N(A,\delta)$ possibilities for a_2, and so

$$N(Q,\delta) \lesssim C^2|e_2|^{-4\sigma}\delta^{4\sigma(1+\gamma)}N(A,\delta)^4.$$

Thus,

$$N(Ae_1 + Ae_2, \delta) \geq \frac{N(A,\delta)^4}{N(Q,\delta)} \gtrsim C^{-2}|e_2|^{4\sigma}\delta^{-4\sigma(1+\gamma)}.$$

On the other hand, as $Ae_1 + Ae_2 \subset B_{\mathbb{H}}(0, |e_2|)$, one has

$$\begin{aligned} N(Ae_1 + Ae_2, \delta) &\lesssim \frac{1}{N(A,|e_2|)}N(A + Ae_1 + Ae_2, \delta) \\ &\lesssim C|e_2|^{4\sigma}N(A + Ae_1 + Ae_2, \delta) \\ &\lesssim C|e_2|^{4\sigma}N(A + 3AA - 3AA, \delta) \\ &\lesssim C|e_2|^{4\sigma}K^7N(A,\delta) \end{aligned}$$

where the last inequality follows from the Plünnecke inequality. So,

$$N(A,\delta) \geq C^{-3}K^7\delta^{-4\sigma(1+\gamma)}$$

and therefore

$$K \gtrsim C^{-O(1)}\delta^{\frac{4\sigma\gamma}{7}}.$$

Choosing $\gamma = \frac{1-\sigma}{36}\frac{1}{\frac{4\sigma}{7}+\frac{14}{36}}$ and setting $\varepsilon = \frac{\sigma(1-\sigma)}{36\sigma+\frac{49}{2}}$, we find in both cases

$$K \gtrsim c^{O(1)}C^{-O(1)}\delta^{-\varepsilon}.$$

□

The real line and the complex plane

The methods used in the previous paragraph also apply to prove a discretized sum-product theorem in $\mathbb{R}$ or $\mathbb{C}$, and the argument is even a little simpler, very close to that used for $\mathbb{Q}_p$ in the first part. In the case of $\mathbb{R}$, we obtain a result exactly similar to Theorem 5 obtained for $\mathbb{Q}_p$, but with a constant $\varepsilon = \frac{\sigma(1-\sigma)}{27+2\sigma}$, while for $\mathbb{C}$, the statement is identical to Theorem 6 but with $\varepsilon = \frac{\sigma(1-\sigma)}{72+32\sigma}$. The detailed proofs are left to the interested reader.

Conclusion

For certain applications, it can be interesting to slightly modify the assumptions of the discretized sum-product theorem, or to study the dependence of the growth rate ε as a function of the other parameters. We briefly discuss some of these issues.

Weakening the non-concentration assumption

Bourgain and Gamburd [5] noticed that the discretized sum-product theorem in $\mathbb{R}$ is still valid when the non-concentration condition is given by a parameter $\kappa > 0$ not necessarily equal to the dimension σ. This version of the discretized sum-product is essential for the proof of their spectral gap theorem for subgroups of SU_d generated by elements with algebraic entries.

The argument which makes it possible to weaken the non-concentration assumption is a bit technical, but quite formal, and it applies equally well to algebras with local division. We then obtain the following result, of which we do not include the detailed demonstration.

Theorem 9 (Sum-product in local division algebras)**.** *Let E be a finite-dimensional division algebra on $\mathbb{R}$ or $\mathbb{Q}_p$. Given $\sigma \in (0, \dim E)$ and $\kappa > 0$, there exists $\varepsilon > 0$ such that the following statement holds for all sufficiently small $\delta > 0$.*

Let $A \subset B_E(0,1)$ be such that

1. $N(A,\delta) \leq \delta^{-\sigma-\varepsilon}$;
2. $\forall \rho \geq \delta$, $\forall x \in E$, $N(A,\rho) \geq \delta^{\varepsilon}\rho^{-\kappa}$;
3. $\forall F \subset E$ *sub-algebra*, $\exists a \in A : \ d(a,F) \geq \delta^{\varepsilon}$.

Then,

$$N(A + AA, \delta) \geq \delta^{-\varepsilon} N(A,\delta).$$

Growth exponent

The problem of the dependence of the growth exponent ε as a function of σ has already been much studied in the case of $\mathbb{R}$. Recently, Orponen and Shmerkin [16, Theorem 1.22] managed to obtain for Bourgain's statement the lower bound $\varepsilon > \sigma/6$ when $\sigma \in (0, 2/3)$, which is much better than the bound given by the argument presented above. We note however that their approach does not provide a new proof of the discretized sum-product, since it is based on a discretized radial projection theorem [17], itself based on Bourgain's discretized sum-product theorem.

It would be interesting to also obtain better estimates of the growth rate in the setting of a general local division algebra. We saw in Theorem 6 that this rate is uniform for all local fields with zero characteristic. One may conjecture that this is still the case for any division algebra, not necessarily commutative, and perhaps for any simple associative algebra on $\mathbb{R}$ or $\mathbb{Q}_p$. This could have applications to the study of random walk in compact groups, such as Lubotzky [15, Problem 10.9.1]. Unfortunately, our proof does not seem to adapt to give this result.

References

[1] Yvette Amice. Les nombres p-adiques. Collection SUP. Le mathématicien. 14. Paris: Presses Universitaires de Frances. 189 p. (1975). 1975.

[2] J. Bourgain. On the Erdős-Volkmann and Katz-Tao ring conjectures. *Geom. Funct. Anal.*, 13(2):334–365, 2003.

[3] Jean Bourgain. The discretized sum-product and projection theorems. *J. Anal. Math.*, 112:193–236, 2010.

[4] Jean Bourgain and Alex Gamburd. A spectral gap theorem in SU(d). *J. Eur. Math. Soc. (JEMS)*, 14(5):1455–1511, 2012.

[5] Jean Bourgain and Alex Gamburd. On the spectral gap for finitely-generated subgroups of SU(2). *Invent. Math.*, 171(1):83–121, 2008.

[6] Nicolas de Saxcé. Borel subrings of division algebras. in preparation.

[7] G. A. Edgar and Chris Miller. Borel subrings of the reals. *Proc. Am. Math. Soc.*, 131(4):1121–1129, 2003.

[8] Pál Erdős and B. Volkmann. Additive groups with prescribed Hausdorff dimension. *J. Reine Angew. Math.*, 221:203–208, 1966.

[9] Paul Erdős and E. Szemerédi. On sums and products of integers. Studies in Pure Mathematics, Mem. of P. Turán, 213-218 (1983). 1983.

[10] Larry Guth, Nets Hawk Katz, and Joshua Zahl. On the discretized sum-product problem. *Int. Math. Res. Not.*, 2021(13):9769–9785, 2021.

[11] Weikun He. Discretized sum-product estimates in matrix algebras. *J. Anal. Math.*, 139(2):637–676, 2019.

[12] Weikun He and Nicolas de Saxcé. Semi-simple random walks on the torus. Preprint arXiv:2204.11453.pdf, April 2022.

[13] Weikun He and Nicolas de Saxcé. Sum-product for real Lie groups. *J. Eur. Math. Soc. (JEMS)*, 23(6):2127–2151, 2021.

[14] Nets Hawk Katz and Terence Tao. Some connections between Falconer's distance set conjecture and sets of Furstenburg type. *New York J. Math.*, 7:149–187, 2001.

[15] Alexander Lubotzky. *Discrete groups, expanding graphs and invariant measures. Appendix by Jonathan D. Rogawski*, volume 125 of *Prog. Math.* Basel: Birkhäuser, 1994.

[16] Tuomas Orponen and Pablo Shmerkin. Projections, furstenberg sets, and the *abc* sum-product problem. Preprint, arXiv:2301.10199, January 2023.

[17] Tuomas Orponen, Pablo Shmerkin, and Hong Wang. Kaufman and falconer estimates for radial projections and a continuum version of beck's theorem. Preprint arXiv:2209.00348v1.pdf, September 2022.

[18] Misha Rudnev and Sophie Stevens. An update on the sum-product problem. *Math. Proc. Camb. Philos. Soc.*, 173(2):411–430, 2022.

[19] József Solymosi. Bounding multiplicative energy by the sumset. *Adv. Math.*, 222(2):402–408, 2009.

[20] Terence Tao. The sum-product phenomenon in arbitrary rings. *Contrib. Discrete Math.*, 4(2):59–82, 2009.

[21] B. Volkmann. Eine metrische Eigenschaft reeller Zahlkörper. *Math. Ann.*, 141:237–238, 1960.