Small Product Sets for Complex Numbers
Berner, M.

Leiden University

Master Thesis

Small Product Sets for Complex Numbers

Author:
Mirco Berner

Supervisor:
Dr. Jan Hendrik Evertse

February 6, 2020

Contents

Notation

For a commutative integral domain G and a subset $A \subset G$ with n elements, we define the h-fold sum set

$$hA := \{a_1 + \ldots + a_h,\ a_i \in A\},$$

the h-fold product set

$$A^{(h)} := \{a_1 \cdot \ldots \cdot a_h,\ a_i \in A\},$$

the ratio set

$$A/A := \left\{a_1 \cdot a_2^{-1} = \frac{a_1}{a_2},\ a_1 \in A,\ a_2 \in A \setminus \{0\}\right\}$$

and the difference set

$$A - A := \{a_1 - a_2,\ a_1, a_2 \in A\}.$$

Sometimes we will denote the ratio set by $\frac{A}{A}$, $2A$ by $A + A$ and $A^{(2)}$ by $A \cdot A$ or AA. Moreover, we denote the cardinality of a set A by $|A|$ and we will use $|\cdot|$ for the absolute value on $\mathbb{C}$, although this may conflict with the denotation for the cardinality; if we use it in the sense of the absolute value, we will point it out. Throughout the entire thesis we will stick to use c to denote an absolute constant, but at each occurrence it may be different.

The famous Erdős and Szemerédi Conjecture states that for a finite subset A of the complex numbers, at least one of the product set $A \cdot A$ or the sum set $A + A$ is large, more precisely: for every $\epsilon > 0$ there is $c(\epsilon) > 0$ such that $\max\{|AA|, |A + A|\} \geq c(\epsilon)|A|^{2-\epsilon}$ *for every finite, non-empty subset A of the complex numbers. They assumed this conjecture will even hold in general, i.e. for every $\epsilon > 0$ and every integer $h \geq 2$ there is $c(h, \epsilon) > 0$ such that* $\max(|hA|, |A^{(h)}|) \geq c(h, \epsilon)|A|^{2-\epsilon}$*. With the help of a result of Evertse, Schlickewei, and Schmidt on linear equations with unknowns taking their values from a multiplicative group of finite rank, M.-C. Chang managed to prove the h-fold Erdős-Szemerédi conjecture under the assumptions that A is a finite subset of the integers and the product set of A is small, i.e. if $|AA| \leq K|A|$ then $|hA| \geq c(h, K)|A|^h$. Using ideas of Chang, Granville and Solymosi proved that for every $K > 1$ there is $C' > 0$ such that if A is any finite, non-empty subset of $\mathbb{C}$ which satisfies $|AA| \leq K|A|$, then $|A + A| \geq |A|^2/2 - C'|A|$. We will extend the results of Chang and Granville and Solymosi as follows: for every finite, non-empty subset A of $\mathbb{C}$ with $|AA| \leq K|A|$ and every integer $h \geq 2$ we have $|hA| \geq |A|^h/h! - c(K, h)|A|^{h-1}$. Further, we will give an upper bound for $c(K, h)$ in terms of K, using a result of Sanders [23]. If we replace K by a slowly growing function of $|A|$ we get $|hA| \geq |A|^h/h! - |A|^{h-\epsilon}$ for $|A|$ sufficiently large in terms of h and ϵ.*

The thesis is divided into three chapters. The first chapter gives a short outline of the previous results regarding the Erdős and Szemerédi Conjecture. The second chapter proves three main results for the complex case and the third chapter is entirely devoted to the proof of the extension of the results of Granville, Solymosi and Chang.

1 Introduction

If you retrospect and ponder about your first math lessons in school, probably you will remember that the math teacher introduced to you the operations *addition* and *multiplication*. Presumably, you have already been conversant in a loose way with both terms, at least you knew the terms. Moreover, the brighter students may have already figured out how to multiply and to add, respectively how mental arithmetic works.

Nevertheless, it was still a drudgery since a schematic approach was missing. You learnt how to add by writing one number on top of the other one and then to sum the single digits. Furthermore, you were shown a conceptual approach for the multiplication of two numbers as well, though this was still a tedious process.

Finally, you learnt an efficient way to 'multiply' two small numbers by inculcating the multiplication table or in other words, he showed you are chart with 9×9 entries and each entry corresponds to a number $a \cdot b$, where $a, b \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Yet, for the most savvy students in the class like Paul Erdős, this was still not challenging enough or even a cinch and Erdős started to muse about other properties of the chart [16]. By observing the symmetry of the spreadsheet, he concluded that there exist at most $\sum_{t=1}^{9} t = \frac{9 \cdot 10}{2} = \binom{9+1}{2}$ different entries. However, he noticed that a bunch of entries are equal and was left wondering how many are distinct. After counting all the unique entries and determining there exist 36, he asked himself:

If we extend the chart to $n \times n$ entries, which proportion of the integers $\leq n^2$ appear in the chart?

Notice that if we take $A = \{1, 2, \ldots, n\}$, the question could be rephrased as:

What is the size of $A \cdot A$ and what is $\frac{|A \cdot A|}{n^2}$?

As time went by he matured to a mathematical luminary and started to wonder what will happen if n tends to infinity.
Unsurprisingly (Erdős is considered to be the most productive mathematician ever; he published more than 1300 papers), he found the answer to his question by proving

$$\lim_{n \to \infty} \frac{|A_n \cdot A_n|}{n^2} = 0 \quad \text{where } A_n = \{1, \ldots, n\}.$$

The proof is based on the result from analytic number theory, due to Hardy and Ramanujan, that all positive integers $\leq n$ up to $o(n)$ integers, have $\sim \log \log n$ prime factors (counted with their multiplicity). This implies, that almost all products $a_1 \cdot a_2 \in A_n \cdot A_n$ have $\sim 2 \log \log n$ prime factors, whereas almost all integers $\leq n^2$ have $\sim \log \log n$ prime factors. By the observation $|A_n \cdot A_n| < n^2$ the result follows.

The canny reader may have already wondered himself, what happens if we take A_n to be a subset of $\mathbb{Z}_{>0}$ of cardinality n with multiplicative structure like the first powers of 2. In that case we obtain

$$\lim_{n \to \infty} \frac{|A_n + A_n|}{n^2} = \frac{1}{2} \quad \text{where } A_n = \{1, 2, 2^2, \ldots, 2^{n-1}\}.$$

What does multiplicative structure for a set A of $\mathbb{C}$ mean? Loosely speaking: $a_1, a_2 \in A$ implies $a_1 \cdot a_2 \in A$ with a 'high' probability. By the same concept we obtain the notion for additive structure. In particular, a set A has a lot of additive structure if it contains a large subset C of the following form:

$$C := \{a_0 + a_1 n_1 + a_2 n_2 + \ldots + a_k n_k : \ 0 \leq n_i \leq N_i \text{ for } 1 \leq i \leq k\}$$

where $a_0, ..., a_k$ are integers with $a_1, \ldots, a_k \neq 0$ and $N_1, \ldots, N_k$ are integers ≥ 2. Such a set is called a generalized arithmetic progression of dimension k.

Likewise, a set A has a lot of multiplicative structure if it contains a large subset D of the form:

$$D := \{a_0 \cdot a_1^{n_1} \cdot a_2^{n_2} \cdot \ldots \cdot a_k^{n_k} : \ 0 \leq n_i \leq N_i \text{ for } 1 \leq i \leq k\}$$

where $a_0, \ldots, a_k$ are positive integers and $N_1, N_2, \ldots, N_k$ are integers ≥ 2. Such a set is called a generalized geometric progression of dimension k.

Our intuition tells us that whatever finite subset A of $\mathbb{Z}_{>0}$ we take, it cannot have at the same time a lot of additive structure and a lot of multiplicative structure, that is, at least one of the quantities $|A + A|, |A \cdot A|$ must be 'large'. Nevertheless, we should not rush into the conclusion that

$$\frac{\max\{|A \cdot A|, |A + A|\}}{|A|^2} > c, \tag{1.1}$$

for some absolute constant $c \in (0, 1]$, since Erdős and Szmerédi [11] showed that for some positive number d there are arbitrarily large subsets A of the integers such that

$$\max\{|A \cdot A|, |A + A|\} < |A|^{2 - \frac{d}{\log \log |A|}}. \tag{1.2}$$

Inequality (1.2) is already a good indicator how we could weaken assertion (1.1) to obtain a meaningful conjecture. By observing that $d/\log \log |A|$ can be made arbitrarily small by letting $|A|$ tend to infinity, one is led to the following:

Conjecture 1.1 (Erdős and Szemerédi [11], 1983)**.** *For every $\epsilon > 0$ there exists $c(\epsilon) > 0$ such that for every finite, non-empty subset A of $\mathbb{Z}_{>0}$ one has*

$$\max\{|A \cdot A|, |A + A|\} \geq c(\epsilon)|A|^{2-\epsilon}.$$

The current state of affairs regarding this conjecture is rather dire. To give a feeling of the complexity of this problem, we will outline the major progressions regarding Conjecture 1.1. The first step was done by Erdős and Szemerédi themselves. They showed:

Theorem 1.2 (Erdős and Szemerédi [11], 1983)**.** *There exists $\theta, c > 0$ such that for every finite, non-empty subset A of $\mathbb{Z}_{>0}$ one has*

$$\max\{|A \cdot A|, |A + A|\} \geq c|A|^{1+\theta}.$$

This result is already confirming our 'gut feeling'; no finite subset A of $\mathbb{Z}_{>0}$ can have at the same time too much additive structure and too much multiplicative structure, since the sum set or product set is considerably larger then $|A|$. The next step was done by Nathanson 14 years later. He was the first to state an explicit value for θ.

Theorem 1.3 (Nathanson [20], 1997)**.** *There exists $c > 0$ such that for every finite, non-empty subset A of $\mathbb{Z}_{>0}$ one has*

$$\max\{|A \cdot A|, |A + A|\} \geq c|A|^{1+\frac{1}{31}}.$$

Moreover, together with Tenenbaum, he could prove Conjecture 1.1 under the assumption that $|A + A|$ is very small.

Theorem 1.4 (Nathanson and Tenenbaum [21], 1997)**.** *For every $\epsilon > 0$ there exists $c(\epsilon) > 0$ such that for every finite, non-empty subset A of $\mathbb{Z}_{>0}$ with $|A + A| \leq 3|A| - 4$ one has*

$$|A \cdot A| \geq c(\epsilon)|A|^{2-\epsilon}.$$

Ford [13] improved the bound $\frac{1}{31}$ in Theorem 1.2 to $\frac{1}{15}$ and subsequently Chen [8] to $\frac{1}{5}$. These results were all eclipsed by Elekes' new bound.

Theorem 1.5 (Elekes [10], 1997)**.** *There exists $c > 0$ such that for every finite, non-empty subset A of $\mathbb{R}$ one has*

$$\max\{|A \cdot A|, |A + A|\} \geq c|A|^{1+\frac{1}{4}}.$$

The bound of Elekes is considered to be the greatest contribution regarding Conjecture 1.1 so far. The jump from $\frac{1}{5}$ to $\frac{1}{4}$ may not seem so impressive, but the fact that he transformed the problem from the integers, let alone the natural numbers, to the real numbers is a veritable game changer for several reasons.

Elekes approached the problem of estimating $\max\{|A \cdot A|, |A + A|\}$ from below by translating it into discrete geometry, which extended the opportunities to tackle this problem immensely. Moreover, Elekes' geometric approach allowed an extension of his result to subsets A of the complex numbers, which suggests that Conjecture 1.1 is also true for complex numbers. And last but not least, Elekes' bound could be further improved based on his ingenious idea.

The year 1997 was extremely fruitful regarding Conjecture 1.1, which explains in a way the stagnation of contributions in the following years. However, the year 2003 was again quite successful. Chang could prove the counterpart of Theorem 1.4 and even a little bit more.

Theorem 1.6 (Chang [6], 2003)**.** *Let $K > 1$. Then for every finite, non-empty subset A of $\mathbb{Z}_{>0}$ with $|A \cdot A| \leq K|A|$ one has*

$$|A + A| \geq 36^{-K}|A|^2.$$

Elekes and Rusza could extend Theorem 1.4 to the real numbers and even a little bit further.

Theorem 1.7 (Elekes and Rusza [24], 2003)**.** *For every $K > 1$ there exists $c(K) > 0$ such that for every finite subset A of $\mathbb{R}$ of cardinality at least 2 with $|A + A| \leq K|A|$ one has*

$$|A \cdot A| \geq c(K)\frac{|A|^2}{K^4 \log |A|}.$$

Astonishingly, already 2 years later came the next exceptionally productive year. This year marks the transition from the real numbers to the complex numbers. Chang was the first who managed to give a lower bound for the complex case.

Theorem 1.8 (Chang [7], 2005)**.** *There exists $c > 0$ such that for every finite subset A of $\mathbb{C}$ one has*

$$\max\{|A \cdot A|, |A + A|\} \geq c|A|^{1+\frac{1}{54}}.$$

Shortly after Chang achieved this breakthrough, Solymosi proved Elekes' bound for complex numbers.

Theorem 1.9 (Solymosi [25], 2005)**.** *There exists $c > 0$ such that for every finite subset A of $\mathbb{C}$ one has*

$$\max\{|A \cdot A|, |A + A|\} \geq c|A|^{1+\frac{1}{4}}.$$

This result solidified the belief in the truth of Conjecture 1.1 for complex numbers, since at that time the current bound for real numbers even held for complex numbers; the best bounds for real numbers and complex numbers available nowadays are almost the same. Solymosi went on by proving:

Theorem 1.10 (Solymosi [26], 2005). *There exists a constant $c > 0$ such that for every finite subset A of $\mathbb{C}$ of cardinality at least 2 one has*

$$|A + A|^8 \cdot |A \cdot A|^3 \geq c \frac{|A|^{14}}{\log^3 |A|}.$$

Consequently, there is a constant $c > 0$ such that for every set A as above one has

$$\max\{|A \cdot A|, |A + A|\} \geq c \frac{|A|^{1+3/11}}{\log^{3/11} |A|}.$$

Furthermore, there is a constant $c > 0$ such that for every set A as above satisfying in addition $|A + A| \leq K|A|$ for some $K > 1$ one has

$$|A \cdot A| \geq cK^{-8/3} \frac{|A|^2}{\log |A|}.$$

Finally, in 2009 Solymosi presented the foundation of the current state-of-the-art bound for real numbers.

Theorem 1.11 (Solymosi [27], 2009). *There exists $c > 0$ such that for every finite subset A of $\mathbb{R}$ of cardinality at least 2 one has*

$$\max\{|A \cdot A|, |A + A|\} \geq c \frac{|A|^{1+\frac{1}{3}}}{\log^{\frac{1}{3}} |A|}.$$

We called this result a foundation, since the subsequent improvements of this bound are of the form $(|A|^{1+\frac{1}{3}+c})/\log^{\frac{1}{3}} |A|$, for some tiny c. The current value for c is $\frac{1}{1509}$, which was calculated in 2017 in a rather agonizing way [15].

Shortly after Solymosi published Theorem 1.11, Rudnev extended his result to the complex numbers. Unfortunately, his proof turned out to be inaccurate. Luckily, four years later in 2013, together with Konyagin he managed to prove an analogue of Solymosi's result for complex numbers.

Theorem 1.12 (Konyagin and Rudnev [18], 2013). *There exists $c > 0$ such that for every finite subset A of $\mathbb{C}$ of cardinality at least 2 one has*

$$\max\{|A \cdot A|, |A + A|\} \geq c \frac{|A|^{1+\frac{1}{3}}}{\log^{\frac{1}{3}} |A|}.$$

To some of the readers, the question about extending Conjecture 1.1 to h-fold sum sets and product sets may have arisen. Indeed, Erdős and Szemerédi conjectured the following as well.

Conjecture 1.13 (Erdős and Szemerédi [11], 1983). *For every $\epsilon > 0$ and every positive integer h, there exists $c := c(\epsilon, h) > 0$ such that for every finite subset A of the positive integers we have*

$$\max\{|A^{(h)}|, |hA|\} \geq c|A|^{h-\epsilon}.$$

Unfortunately, since its formulation, very little progress has been made towards a proof of Conjecture 1.13, and the partial results that have been obtained are much weaker than those related to Conjecture 1.1. The reason for this may be that Elekes' approach, to view Conjecture 1.1 as a geometric problem on the real line or complex plane, could not be generalized to Conjecture 1.13.

Besides Solymosi, Mei-Chu Chang is one of the leading contributors to sum- and product set problems. Solymosi considered mostly the problems related to double sum- and product sets, while Chang focused mostly on h-fold sum- and product sets. Together with Bourgain she obtained the following partial result.

Theorem 1.14 (Bourgain and Chang [2], 2003). *For every $b > 0$ there exists a positive integer h such that for every finite subset A of $\mathbb{Z}$ one has*

$$|hA| + |A^{(h)}| \geq |A|^b.$$

As mentioned by Bourgain and Chang, one may take $h = \exp O(b^4)$. Chang managed to prove some further partial results towards Conjecture 1.13, where either $|A + A|$ or $|A \cdot A|$ is small.

Theorem 1.15 (Chang [5], 2002). *For every $\epsilon > 0, K > 1, h \in \mathbb{Z}_{>0}$ there exists $c = c(\epsilon, h, K) > 0$ such that for every finite subset A of $\mathbb{Z}$ of cardinality $\geq n_0$ with $|A + A| \leq K|A|$ one has*

$$|A^{(h)}| \geq c|A|^{h-\epsilon}.$$

Shortly after, Chang could prove the following counterpart:

Theorem 1.16 (Chang [6], 2003). *Let $K > 1, h \in \mathbb{Z}_{>0}$. Then for every finite, non-empty subset A of $\mathbb{Z}_{>0}$ with $|A \cdot A| \leq K|A|$ one has*

$$|hA| \geq c_h(K)|A|^h,$$

where $c_h(K) = (2h^2 - h)^{-hK}$.

These results were the first of their kind. The latter one was considerably generalized later. In 2009 Chipeniuk refined Chang's proof by giving a bound for the complex case:

Theorem 1.17 (Chipeniuk [9], 2009). *Let A be a finite, non-empty subset of $\mathbb{C}$ with $|A \cdot A| \leq K|A|$ for some $K > 1$. Then for every integer $h \geq 2$ one has*

$$|hA| \geq e^{-h^{65h}(K+1)}|A|^h.$$

In the same paper, he also provided the following qualitative bound:

Theorem 1.18 (Chipeniuk [9], 2009). *Let h be an integer ≥ 2. Then there exists $c_h > 0$ such that for every finite, non-empty subset A of $\mathbb{C}$ with $|A \cdot A| < K|A|$ for some K with $1 < K < \log|A|/h^{65h}$ one has*

$$|hA| \geq c_h|A|^h.$$

For large K and large $|A|$ in terms of K, h Theorem 1.18 yields a much better bound than Theorem 1.17. However, both Theorems 1.17 and 1.18 are unsatisfactory, since the desired lower bound for a small K is

$$|hA| \geq \frac{1}{h!}|A|^h + O(|A|^{h-1}). \tag{1.3}$$

Why is this our desired lower bound? Clearly, for any set B we obtain the trivial upper bound

$$|hB| \leq \binom{|B| + h - 1}{h} = \frac{|B|^h}{h!} + O(|B|^{h-1}), \tag{1.4}$$

and for a small K, we would expect hardly any additive structure, which implies the lower bound of (1.3). Granville and Solymosi were the first to prove (1.3) for $h = 2$ by showing the following result:

Theorem 1.19 (Granville and Solymosi [16], 2010). *Let $A \subset \mathbb{C}$ with $|A| = n$ and suppose $|AA| \leq Kn$, then there is a constant C' depending only on K such that*

$$|A + A| \geq \frac{n^2}{2} - C'n.$$

The fundamental important observation (1.4) brings this thesis into play. The core of the thesis consists of the following extension and refinement of Theorem 1.19 and its corollary.

Theorem 1.20. *For every $\epsilon > 0$ there are $K_0(\epsilon) > 1, C(\epsilon) > 0$ with the following property: Let A be any finite, non-empty subset of $\mathbb{C}$ with $|A \cdot A| \leq K|A|$ for some $K > K_0(\epsilon)$. Then*

$$|hA| \geq \frac{|A|^h}{h!} - f(K, h, \epsilon)|A|^{h-1}$$

where

$$f(K, h, \epsilon) = \exp\left(C(\epsilon)h^7 \log h(\log K)^{3+\epsilon}\right).$$

Corollary 1.21. *For every $\epsilon > 0$ and every integer $h \geq 2$, there exists $c(h, \epsilon) > 0, n(h, \epsilon) > 0$ such that for every finite, non-empty subset A of $\mathbb{C}$ with*

$$|A| > n(h, \epsilon), \quad |A \cdot A| \leq |A| \exp\left(c(h, \epsilon)(\log |A|)^{\frac{1-\epsilon}{3+\epsilon}}\right)$$

one has

$$|hA| \geq \frac{|A|^h}{h!} - |A|^{h-\epsilon}.$$

In chapter 2 we will show some proofs of theorems which were formulated in chapter 1. We will restrict ourselves to theorems concerning sum sets and product sets for subsets of the complex numbers, since the real case was treated extensively in numerous papers and the complex case was mostly regarded as a nice 'byproduct' or at best, people tried to extend the theorems to the complex numbers. Nevertheless, the theorems regarding the complex case never got their deserved attention. With this thesis we are aiming at partly changing this sentiment.

The next chapter shows the proofs (taken from [18], [25] and [26]) of the Theorems 1.9, 1.10 and 1.12 which are dealing with double sum sets and product sets. We have decided not to consider the h-fold case since the proofs of the theorems related to that are too long and complicated to be included in this thesis. In chapter 3 we have included the only proof concerning the h-fold case, namely that of Theorem 1.20 and Corollary 1.21; this is the pinnacle of our thesis. There you will observe the clear distinction of the complexity between the two-fold case and the h-fold case.

2 Small sum sets

We will start with Theorem 1.9, which extends Elekes' bound to the complex case. You can consider this proof as a nice warming up for the subsequent proofs. We point out, that the complexity of the argumentations will increase throughout the thesis.

2.1 Proof of Theorem 1.9

We will follow the proof of Solymosi [25]. Before we can dive into the proof, we need a definition. Let A be a finite, non-empty subset of $\mathbb{C}$. For each $a_i \in A$, take an element a_i' from A which is different from a_i and which has distance closest to a_i. Thus we have $|A|$ ordered pairs (a_i, a_i'). Let's call them *neighboring pairs*.

Definition 2.1. *Let A, B, C be finite subsets of $\mathbb{C}$. We say that a quadruple (a, a', b, c) is good if (a, a') is a neighboring pair in $A \times A, b \in B, c \in C$ and*

$$\big|\{u \in A + B : |a + b - u| \leq |a - a'|\}\big| \leq \frac{28|A + B|}{|A|}$$

together with

$$\big|\{v \in A \cdot C : |a \cdot c - v| \leq |a \cdot c - a' \cdot c|\}\big| \leq \frac{28|A \cdot C|}{|A|}$$

hold.

This means more or less that a quadruple (a, a', b, c) is good if there are not too many elements in $A + B, A \cdot C$ that are close to $a + b, a \cdot c$.

Lemma 2.2. *Let A,B,C be finite subsets of $\mathbb{C}$. For each $b \in B, c \in C$, the number of neighboring pairs $(a, a') \in A \times A$ such that (a, a', b, c) is good is at least $|A|/2$.*

Proof. Let us consider the set of disks around the elements of A with radius $|a - a'|$ (i.e. for every $a \in A$ we take the largest disk with center a, which contains no other elements of A in its interior). We show that no more than seven among these disks can have a point in common. Let $A := \{z_0, z_1, \ldots, z_m\} \subset \mathbb{C}$ and assume that there exists $z \in \mathbb{C}$ with $|z - z_j| \leq \min_{i \neq j} |z_j - z_i|$ for $j = 0, \ldots, m$. We will show that $m \leq 6$. Assume, without loss of generality, that $z = 0$ and $z_1, \ldots, z_m \neq 0$. Pick any two distinct indices i, j from $\{1, ..., m\}$ and suppose $|z_i| \leq |z_j|$. Then $1 \leq |1 - z_i/z_j|$ and $|z_i/z_j| \leq 1$ and therefore $|\arg(z_i/z_j)| \geq \pi/3$ since z_i/z_j lies on or inside the closed unit disk with center 0 but not inside the closed unit disk with center 1 and the unit circles around the points 0,1 intersect at $e^{\pm\pi\sqrt{-1}/3}$. Now assume $0 \leq \arg z_i < 2\pi$ for $1 \leq i \leq m$. Since $|\arg z_i - \arg z_j| \geq \pi/3$ for $i \neq j$ we have indeed $m \leq 6$. Hence we obtain the following two inequalities

$$\sum_{a \in A} \big|\{u \in A + B : |a + b - u| \leq |a - a'|\}\big| \leq 7|A + B|,$$
$$\sum_{a \in A} \big|\{v \in A \cdot C : |ac - v| \leq |ac - a'c|\}\big| \leq 7|A \cdot C|.$$

We show that for each $b \in B, c \in C$, at least half of the neighboring pairs $(a, a') \in A \times A$ make a good quadruple (a, a', b, c). Assume that for some b, c the contrary were true. Then there would be more than $|A|/4$ neighboring pairs (a, a') that fulfill at least one of the following inequalities:

$$\big|\{u \in A + B : |a + b - u| \leq |a - a'|\}\big| > \frac{28|A + B|}{|A|},$$
$$\big|\{v \in A \cdot C : |a \cdot c - v| \leq |a \cdot c - a' \cdot c|\}\big| > \frac{28|A \cdot C|}{|A|}.$$

The first inequality implies

$$7|A+B| \geq \frac{|A|}{4} \left|\{u \in A+B : |a+b-u| \leq |a-a'|\}\right| > 7|A+B|,$$

and similarly, the second inequality has as a consequence

$$7|A \cdot C| \geq \frac{|A|}{4} \left|\{v \in A \cdot C : |a \cdot c - v| \leq |ac - a'c|\}\right| > 7|A \cdot C|.$$

□

Proposition 2.3. *Let A, B, C be finite, non-empty subsets of $\mathbb{C}$, with $0 \notin C$. Then*

$$|A+B| \cdot |A \cdot C| \geq \frac{1}{28\sqrt{2}} |A|^{3/2} |B|^{1/2} |C|^{1/2}.$$

Proof. Our goal is to find a suitable upper bound for the number of good quadruples (a, a', b, c). Instead of finding an upper bound for the quadruples (a, a', b, c), we will calculate an upper bound for the quadruples of the form $(a+b, a'+b, ac, a'c)$. This approach is justified by the fact that there is a map

$$\begin{aligned} \phi : A \times A \times B \times C &\to (A+B) \times (A+B) \times (AC) \times (AC) \\ (a, a', b, c) &\mapsto (a+b, a'+b, ac, a'c) \end{aligned}$$

that is injective on the subset U of good quadruples in the domain, so the image of U has the same cardinality as U. Let denote by ϕ_i the i-th component of $\phi(a, a', b, c)$. The injectivity follows from the observation, that $\phi_3 - \phi_4 = ac - a'c = c(a - a')$, $\quad \phi_1 - \phi_2 = a + b - (a' + b) = a - a'$ and $(\phi_3 - \phi_4)/(\phi_1 - \phi_2) = c(a - a')/(a - a') = c \neq 0$ and this in turn gives $\phi_3/c = ca/c = a$, $\quad \phi_4/c = ca'/c = a'$ together with $\phi_1 - \phi_3/c = \phi_1 - a = (a+b) - a = b$.

For the first component $a+b$ there exist $|A+B|$ choices and for the second element $a'+b$ we can choose at most $\frac{28|A+B|}{|A|}$ elements closest to $a+b$. For the third element $a \cdot c$ there exist $|A \cdot C|$ possibilities and consequently the fourth component has at most $\frac{28|AC|}{|A|}$ possibilities. By Lemma 2.2 we can bound the number of good quadruples (a, a', b, c) from below by $|(A|/2) \cdot |B||C|$. These two observations yield

$$|A+B| \frac{28|A+B|}{|A|} |A \cdot C| \frac{28|A \cdot C|}{|A|} \geq \frac{|A|}{2} \cdot |B| \cdot |C|$$

which is equivalent to Proposition 2.3. □

Theorem 1.9 is clearly true if A is a singleton. If $|A| \geq 2$ then Theorem 1.9 follows by applying Proposition 2.3 with $A' := A \setminus \{0\}$ instead of A, and $B = C = A'$.
From Proposition 2.3, applied with $A' = A \setminus \{0\}$ and $B = C = A'$, one obtains at once the following corollary, which is the first decent step into the direction of Conjecture 1.1, although it is still not entirely confirming our gut instinct, which tells us that the product set or the sum set should be large if the other set is 'small'.

Corollary 2.4. *Let A be a finite, non-empty subset of $\mathbb{C}$. If $|A+A| \leq K|A|$, then*

$$|A \cdot A| \geq \frac{1}{28\sqrt{2}} K^{-1} (|A| - 1)^{3/2},$$

and likewise if $|A \cdot A| \leq K|A|$,

$$|A+A| \geq \frac{1}{28\sqrt{2}} K^{-1} (|A| - 1)^{3/2}.$$

2.2 Proof of Theorem 1.10

The proof of Solymosi's Theorem 1.10 has been greatly influenced by Elekes' idea to use the Szemerédi-Trotter Theorem from discrete geometry. Solymosi used the generalization of their theorem to the complex numbers, due to Toth. By refining some of Elekes' techniques, Solymosi could further improve the lower bound.

Theorem 2.5 (Szemerédi and Trotter, version Toth [28])**.** *There is $C > 0$ such that if P is any collection of points in $\mathbb{C}^2$ of cardinality n and $\mathcal{L}$ any collection of lines (one-dimensional linear subvarieties) in $\mathbb{C}^2$ of cardinality l, then the number of point-line incidences (a, L) with $a \in P, L \in \mathcal{L}$ and $a \in L$ is at most $I(n, l) := C \cdot (n \cdot l)^{2/3} + 3n + 3l$.*

Corollary 2.6. *There is $C > 0$ such that for any set P of n points in $\mathbb{C}^2$ and any $k \geq 2$, the number of k-rich lines with respect to P (lines from $\mathbb{C}^2$ with at least k points from P) is at most $C(\frac{n^2}{k^3} + \frac{n}{k})$.*

Proof. Let $\mathcal{L}$ be any set of lines of cardinality l with at least k points of P. Notice that the number of 2-rich lines in P is at most $\binom{n}{2} = n(n-1)/2$, hence for any $k \geq 2$ the number of k-rich lines is at most $n(n-1)/2$. This certainly implies Corollary 2.6 if one imposes some upper bound on k. Hence there is no loss of generality to assume that $k > 12$. Further, there is no loss of generality to assume $l \geq 12n/k$. Then by Theorem 2.5, with the constant C from that theorem, we have

$$k \cdot l \leq I(n, l) := C \cdot (n \cdot l)^{2/3} + 3n + 3l \leq C(nl)^{2/3} + k \cdot l/2,$$

implying

$$k \cdot l \leq 2C(nl)^{2/3},$$

and thus, $l \leq 8C^3 n^2/k^3$. This proves Corollary 2.6 with C from Theorem 2.5 replaced by another constant C. □

Proof of Theorem 1.10. Again, we will follow the proof of Solymosi [26]. By c we will denote constants which at each occurrence may have different values. We set $|A| = n$, $|A^{(2)}| = t$ and

$$E_A^{\times} = \left|\{(a_1, \ldots, a_4) \in A^4 : a_1 \cdot a_2 = a_3 \cdot a_4\}\right|,$$
$$r_A^{\times}(a) = \left|\{(a_1, a_2) \in A^2 : a_1 \cdot a_2 = a,\ a \in A^{(2)}\}\right|.$$

In order to prove Theorem 1.10, we will find in a canny way an upper bound for the number of point-line incidences of particular point and line sets. Let us start by determining a lower bound for the number of unordered double pairs $\{(a_i, a_j), (a_u, a_v)\}$ with $(a_i, a_j), (a_u, a_v) \in A \times A$ which satisfy $a_i \cdot a_j = a_u \cdot a_v$. By the Cauchy-Schwartz inequality we calculate a lower bound for the number $E_A^{\times}$ of ordered double pairs:

$$E_A^{\times} = \sum_{a \in A^{(2)}} r_A^{\times}(a)^2 \geq \frac{1}{|A^{(2)}|} \cdot \left(\sum_{a \in A^{(2)}} r_A^{\times}(a) \right)^2 = \frac{n^4}{t}. \tag{2.1}$$

Hence, the number of unordered double pairs is bounded below by $c\frac{n^4}{t}$ for some constant c with $0 < c \leq 1$. This in turn implies the lower bound $c\frac{n^4}{t}$ for the number of unordered double pairs $(a_i, a_v), (a_u, a_j) \in A^2$, fullfiling $a_i \cdot a_j = a_u \cdot a_v$. Now we partition the set A^2 into classes $L_1, \ldots, L_k$ such that (a_i, a_j) and (a_u, a_v) are in the same class if and only if $a_i \cdot a_v = a_u \cdot a_j$.

Notice that the points of a class L_i lie on a line of $\mathbb{C}^2$ through the origin, which we denote by

L_i'. In the following we denote the cardinality of L_i by l_i. Additionally, another way to count all the possible unordered double pairs is by taking two elements from each class. This idea yields

$$\sum_{i=1}^{k} \binom{l_i}{2} \geq c \cdot \frac{n^4}{t}.$$

We divide these classes into sets $C_1, \ldots, C_s$ such that $L_i \in C_j$ if and only if $2^{2(j-1)} < \binom{l_i}{2} \leq 2^{2j}$. Each L_i contains at most n pairs since if one fixes (a_i, a_j), then a_v is determined by a_u. So $2^{2(s-1)} < \binom{n}{2}$, which shows $s < \frac{1}{2} \log 2n(n-1)/\log 2$. We choose the set C_m such that the number of pairs of the union of the classes L_i in C_m is maximal. We denote by Y_i the collection of all unordered double pairs of a class L_i and by X_m the union of those Y_i with $L_i \in C_m$. Thus the number of elements of X_m is bounded below by:

$$|X_m| = \left|\left\{ \{(a_\alpha, a_\beta), (a_\gamma, a_\delta)\} : (a_\alpha, a_\beta) \in L_i, (a_\gamma, a_\delta) \in L_i, L_i \in C_m \right\}\right| \geq c \cdot \frac{n^4}{t \cdot \log n}.$$

Moreover, $|X_m|$ is bounded above by $2^{2m}|C_m|$. If we combine the upper and lower bound, we obtain

$$2^{2m-2} \geq c \frac{n^4}{t|C_m| \log n}. \tag{2.2}$$

Now comes the trick with the special point and line set. We introduce a new collection of translated lines

$$\mathcal{L} = \{(a_u, a_v) + L_i' : L_i \in C_m, (a_u, a_v) \in A \times A\}.$$

where L_i' is the line of $\mathbb{C}^2$ through the origin containing L_i. Notice that each translated line is incident to at least 2^{m-1} points of $(A+A) \times (A+A)$. More precisely, every translated line has a 'starting point' $(a_u, a_v) \in A^2$ and to this point we add the points from the sets $L_i \in C_m$ with at least 2^{m-1} points/elements of A^2 .

Short remark: Probably, the starting point is not in $(A+A) \times (A+A)$. Be attentive; it is important to distinguish between the sets $(A+A) \times (A+A)$ and $A \times A$ in the following part of the proof. For visualization, see Figure 1.

By Corollary 2.6 the number of 2^{m-1}-rich lines on $(A+A) \times (A+A)$ is bounded above by

$$c \left(\frac{|A+A|^4}{(2^{m-1})^3} + \frac{|A+A|^2}{2^{m-1}} \right).$$

Clearly $|A+A| > |A|$ and $|A| \geq 2^{m-1}$, since each L_i contains at least 2^{m-1} and at most $n = |A|$ points. This implies

$$\frac{|A+A|^4}{(2^{m-1})^3} = \left(\frac{|A+A|}{2^{m-1}} \right)^2 \cdot \frac{|A+A|^2}{2^{m-1}} > \frac{|A+A|^2}{2^{m-1}},$$

whence

$$|\mathcal{L}| \leq c \cdot \frac{|A+A|^4}{(2^{m-1})^3}. \tag{2.3}$$

We now apply Theorem 2.5 to the configuration where $P = A \times A$, and $\mathcal{L}$ is the same set of lines as before, so we disregard the points in $(A+A) \times (A+A)$. Theorem 2.5 shows, that the number of point-line incidences is bounded above by

$$O(|\mathcal{L}|^{\frac{2}{3}} \cdot (n^2)^{\frac{2}{3}} + |\mathcal{L}| + n^2).$$

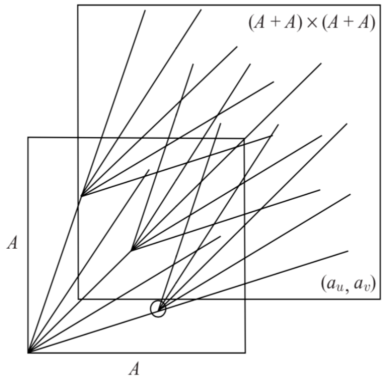

Figure 1: Translates of the lines of C_m

We already know the lower bound $n^2|C_m|$ for the number of point-line incidences, since we have n^2 'starting points' and to each 'starting point' we attach $|C_m|$ lines. Hence one of the following three cases holds.

$$\mathbf{1.}\ n^2|C_m| \le c|\mathcal{L}|^{\frac{2}{3}} \cdot n^{\frac{4}{3}},$$

or

$$\mathbf{2.}\ \ n^2|C_m| \le c|\mathcal{L}|,$$

or

$$\mathbf{3.}\ n^2|C_m| \le cn^2.$$

We observe that the first case includes the third case, since $|\mathcal{L}| \ge n$ because each point of $A \times A$ is cointained in $\mathcal{L}$. The second case is also included in the first case, because $\mathcal{L}$ has n^2 translates with fewer than n^2 lines and this means that

$$|\mathcal{L}|^{\frac{1}{3}} \le n^{\frac{4}{3}}$$

or equivalently

$$|\mathcal{L}| \le n^4$$

is satisfied. Finally we can conclude

$$n^2|C_m| \le c|\mathcal{L}|^{\frac{2}{3}} n^{\frac{4}{3}}. \tag{2.4}$$

Now we will see how nicely our previous observations of (2.2), (2.3) and (2.4) are working together. In the first step we use (2.4), in the second step (2.3) and in the last step (2.2):

$$n^2|C_m| \le c|\mathcal{L}|^{\frac{2}{3}} n^{\frac{4}{3}} \le c\left(\frac{|A+A|^4}{(2^{m-1})^3}\right)^{\frac{2}{3}} n^{\frac{4}{3}} \le c\frac{|A+A|^{\frac{8}{3}}}{2^{2m-2}} n^{\frac{4}{3}} \le c\frac{|A+A|^{\frac{8}{3}}}{\left(\frac{n^4}{t\cdot|C_m|\log n}\right)} n^{\frac{4}{3}}$$

and this in turn shows

$$c\frac{n^{14}}{\log^3|A|} \le |A+A|^8 \cdot t^3 = |A+A|^8 \cdot |A \cdot A|^3, \tag{2.5}$$

which concludes the proof. □

A nice ancillary effect of Theorem 1.10 is the extension of Theorem 1.7 to the complex numbers.

Corollary 2.7. *Let A be a finite subset of $\mathbb{C}$ of cardinality at least 2 and $K > 1$. If $|A + A| \leq K|A|$, then*

$$|A \cdot A| \geq c\frac{|A|^2}{\log |A|}$$

for some absolute constant c.

By combining Corollary 2.7 with Theorem 1.20 we observe a wonderful fact: Conjecture 1.1 holds on the condition $|A \cdot A| < K|A|$ or $|A + A| < K|A|$ for some absolute constant K.

2.3 Proof of Theorem 1.12

For the proof of Theorem 1.12 we will follow the proof of Konyagin and Rudnev [18]. Since the proof is a little bit more tricky than the previous two we will structure the argumentation in a clear way, starting with some preliminaries. Afterwards, we will prove the theorem on the condition, that we have already proven some intermediary results. This approach will facilitate the understanding of the argumentations of those claims/intermediary results, since the reader is already fully aware of the purpose of those results. Furthermore, the problem will be tackled by considering $\mathbb{C}$ as isomorphic to $\mathbb{R}^2$, i.e. each point $d \in \mathbb{C}$ will be regarded as a point $d \in \mathbb{R}^2$.

Preliminaries:
Since the proof relies heavily on geometric properties, we will be concerned with the quantity $E_A^\times$. By introducing a new quantity

$$r_A^/(l) = \left|\{(a_1, a_2) \in A^2 : \frac{a_1}{a_2} = l,\ l \in \frac{A}{A}\}\right|,$$

and observing that $E_A^\times$ has also the alternative representation

$$E_A^\times = \left|\{(a_1, a_2, a_3, a_4) \in A^4 : (a_1, a_2) = (la_3, la_4),\ l \in \frac{A}{A}\}\right|$$

we can give a new description of $E_A^\times$ by

$$E_A^\times = \sum_{l \in \frac{A}{A}} r_A^/(l)^2. \tag{2.6}$$

This description is more convenient from the geometrical perspective, since for each l, the corresponding pairs $(a_i, a_j) \in A^2$ with $\frac{a_i}{a_j} = l$ are collinear points on a line through the origin with slope l. We will make use of this notion in the following. By the observation that $r_A^/(l) \leq |A|$, we can subdivide the sum $E_A^\times$ into at most $\lceil \log_2(|A|) \rceil$ dyadic subsums:

$$E_A^\times = \sum_{j=0}^{\lceil \log_2 |A| \rceil} \left(\sum_{\substack{l \in \frac{A}{A} \\ 2^j \leq r_A^/(l) < 2^{j+1}}} r_A^/(l)^2 \right).$$

This implies there exists m with $0 \leq m \leq \lceil \log_2(|A|) \rceil$ such that

$$\sum_{\substack{l \in \frac{A}{A} \\ 2^m \leq r_A^/(l) < 2^{m+1}}} r_A^/(l)^2 \geq \frac{E_A^\times}{\lceil \log_2 |A| \rceil} \geq c\frac{E_A^\times}{\log_2 |A|} \tag{2.7}$$

and by combining (2.1) with (2.7), we obtain

$$\sum_{\substack{l\in\frac{A}{A}\\ 2^m\leq r^{/}_{A}(l)<2^{m+1}}} r^{/}_{A}(l)^2 \geq c\frac{|A|^4}{|AA|\log_2|A|}. \tag{2.8}$$

For the sake of conciseness in the remaining parts, we will abbreviate (2.8) a little bit. Let us denote $N = 2^{m+1}, n(l) = r^{/}_{A}(l)$ and $L = \{l \in \frac{A}{A} : 2^m \leq r^{/}_{A}(l) < 2^{m+1}\}$. Then

$$|L|N^2 \geq c\frac{|A|^4}{|AA|\log_2|A|}. \tag{2.9}$$

Lastly, let P denote the set of all points in $A \times A$, lying on the lines through the origin with slope in L.

In order to simplify the calculations a little bit, we will impose some restrictions on the set A, since we are not aiming for the optimal value of c. Let A be a subset of $\mathbb{C}^*$ with the property, that each $a \in A$ lies in the angular sector with angular half-width $|\tan(2\arg a)| < \epsilon$ around the real axis with vertex at 0. The constant ϵ should be reasonable small, say $\epsilon = \frac{1}{100}$. This feature is only of importance in the final geometric argument in the proof.

This restriction is justified by the fact that our calculations hold in generality, i.e. we could partition $\mathbb{C}^*$ by angular sectors with half-width $< \frac{1}{100}$. Then $\mathbb{C}^*$ is partitioned by less than 1500 angular sectors and we pick the angular sector S_m which covers most elements of A. Notice, that S_m covers more than $\frac{1}{1500}|A|$ points. Afterwards, we could repeat the calculations in the proof of Theorem 1.12 and divide the constant c by 1500, which yields certainly a lower bound for the product set or sum set.

Given distinct $\alpha, \beta \in \mathbb{C}$, we denote by $\langle\alpha, \beta\rangle$ the open line segment between them, i.e.
$\{t\alpha + (1-t)\beta t \in \mathbb{R}, 0 < t < 1\}$. A tree on a finite subset V of $\mathbb{C}$ is a tree, i.e., connected undirected graph without loops, with vertex set V, of which each edge is an open line segment $\langle\alpha, \beta\rangle$ connecting two distinct elements α, β of V. A minimal tree on V is a tree on V of which the sum of the Euclidean lengths of its edges is minimal among all trees on V.

The core of the proof is Claim 1.12 below, which enables us to connect $|A + A|^2$ with the lower bound in (2.9). This will complete the proof of Theorem 1.12 on the condition that the claim is true.

Claim 1.12:
Let V be a subset of A/A with at least two elements, and let T be a minimal tree on V. For each edge $e = \langle l_1, l_2\rangle$ of T, let H_e denote the set of numbers $\frac{y_1+y_2}{x_1+x_2}$ with $x_1, y_1, x_2, y_2 \in A$ and $\frac{y_1}{x_1} = l_1, \frac{y_2}{x_2} = l_2$. Then $H_e \cap H_{e'} = \emptyset$ for each distinct pair of edges e, e' of T.

Proof of Theorem 1.12. Notice that $x_1 \neq -x_2$, since each $a \in A$ lies in the angular sector. For $l \in V$, let us denote by $n(l)$ the number representations of l, this is the number of pairs $(x, y) \in A \times A$ with $\frac{y}{x} = l$. Denote by E the set of edges of T, where T is a tree as in Claim 1.12, with $V = L$. Then linear algebra tells us that for any edge $e = (l_1, l_2) \in E$, the vector $(x_1 + y_1, x_2 + y_2) \in \mathbb{C}^2$ with $x_1, y_1, x_2, y_2 \in A, \frac{x_1}{y_1} = l_1, \frac{x_2}{y_2} = l_2$ attains precisely $n(l_1) \cdot n(l_2)$ distinct values. Claim 1.12 implies that for each edge $e = \langle l_1, l_2\rangle \in E$ there is an injective map $\phi : (x_1, y_1, x_2, y_2) \mapsto (x_1 + x_2, y_1 + y_2)$, from the set S of quadruples $(x_1, y_1, x_2, y_2) \in A^4$ such that $\langle\frac{y_1}{x_1}, \frac{y_2}{x_2}\rangle \in E$ to $(A + A) \times (A + A)$.

To see this, assume the contrary were true. Then there is a pair of different edges $e = \langle l_1, l_2\rangle, e' = \langle l'_1, l'_2\rangle$ of the tree T, such that

$$(x_1 + x_2, y_1 + y_2) = (x'_1 + x'_2, y'_1 + y'_2),$$

where $l_1 = \frac{y_1}{x_1}, l_2 = \frac{y_2}{x_2}, l'_1 = \frac{y'_1}{x'_1}, l'_2 = \frac{y'_2}{x'_2}$ and this in turn implies

$$\frac{y_1 + y_2}{x_1 + x_2} = \frac{y'_1 + y'_2}{x'_1 + x'_2}$$

which is a contradiction to Claim 1.12, which asserts that these two numbers belong to disjoint sets $H_e, H_{e'}$. By the injectivity of ϕ we obtain the following inequality:

$$|A + A|^2 \geq \sum_{(l_1,l_2)\in E} n(l_1)n(l_2) \geq \frac{1}{2} \sum_{(l_1,l_2)\in E} (n(l_1) + n(l_2)) \min(n(l_1), n(l_2)). \tag{2.10}$$

By (2.9) and (2.10) together with the observation that T has $|L| - 1$ edges, since T is a minimal spanning tree with $|L|$ vertices, and $\frac{N}{2} \leq n(l) \leq N$ because $N = 2^{m+1}, n(l) = r^{/}_{A}(l)$ for $l \in L$, we have

$$|A + A|^2 \geq (|L| - 1)\frac{N^2}{4} \geq c\frac{|A|^4}{|AA| \log |A|},$$

which concludes the proof. □

Now comes the complex part of the proof. The argumentation of Claim 1.12 is quite intricate.

Proof of Claim 1.12. For each edge e of T, we construct an open set M_e which contains H_e, which contains the open line segment e and which is symmetric about e (i.e., invariant under the orthogonal reflection in the line through e), in such a way that M_e, M'_e are disjoint for any two distinct edges e, e' of T . This clearly implies Claim 1.12. Let $x_1, y_1, x_2, y_2 \in A$ and assume that $y_1/x_1 = l_1$ and $y_2/x_2 = l_2 \in V$. Let $u = x_2/x_1$. Then

$$\frac{y_1 + y_2}{x_1 + x_2} = \frac{y_1 + y_2}{(u + 1)x_1} = \frac{l_1}{1 + u} + l_2\frac{u}{1 + u} = l_1 + (l_2 - l_1)\frac{u}{1 + u}. \tag{2.11}$$

By our restriction $\tan |2 \arg x_i| < \epsilon$ for $i = 1, 2$, the number u lies in the open angular wedge $W_\epsilon = \{z : \tan |\arg z| < \epsilon\}$. We denote by M_ϵ the image of W_ϵ under the Möbius map $z' = \frac{z}{z+1}$. Hence $\frac{u}{u+1} \in M_\epsilon$. The set M_ϵ is the intersection of two open discs centred at $z_\pm = \frac{1}{2} \pm \frac{i}{2\epsilon}$ with equal radius $|z_\pm|$. M_ϵ is contained in the open rhombus, whose major diagonal is the open line segment $(0, 1)$ and the minor diagonal has length ϵ. Now comes the construction of our set M_e where $e = \langle l_1, l_2\rangle$. By (2.11) we have

$$\frac{y_1 + y_2}{x_1 + x_2} \in M_e := l_1 + (l_2 - l_1)M_\epsilon.$$

Hence the set M_e is contained in the open rhombus R_e, whose main diagonal is $e = \langle l_1, l_2\rangle$ and whose minor diagonal has length $\epsilon|l_2 - l_1|$.

To follow what is usual in geometry, we will denote the vertices of T by $A, B, C, D, \ldots$, although this may conflict with the denotation for the set A. In such a case we will point out what we mean. Furthermore, we assume the reader is already familiar with the basic properties of minimal trees. In the following we will list two of them (for the unfamiliar reader, the proofs of the following two properties is well explained in [16] on page 6):

1. No edge is crossing another edge.
2. The angle between two adjacent edges is at least $\frac{\pi}{3}$.

Hence, the rhombi around adjacent edges cannot intersect. This fact emanates from the restriction, that ϵ has to be 'small'.
In order to finish the proof we will show for any two non-adjacent edges $\langle AB\rangle$ and $\langle CD\rangle$ of T that $R_{\langle AB\rangle} \cap R_{\langle CD\rangle} = \emptyset$. The key element in the argumentation is the following observation.

Lemma 2.8. *The vertices C, D cannot lie in the open disk with diameter $\langle AB\rangle$.*

Proof. We will show the lemma by contradiction. Assume that C lies inside the open disk, then the angle ACB is obtuse. Hence the edge (AB) can be deleted and replaced in the tree T by one of the shorter line segments $\langle AC\rangle$ or $\langle BC\rangle$, without violating connectivity or creating loops. This contradicts the minimality of T. □

Now we use the previous lemma together with the fact that $(AB) \cap (CD) = \emptyset$ to prove the following lemma, which will enable us to finish the proof of Claim 1.12.

Lemma 2.9. *If $R_{\langle AB\rangle} \cap R_{\langle CD\rangle} \neq \emptyset$ and α is the angle between $\langle AB\rangle$ and $\langle CD\rangle$ with $0 < \alpha < \pi/2$, then*

$$\tan\alpha \leq \frac{2\epsilon}{1-\epsilon^2}.$$

Proof. Assume the edge $\langle CD\rangle$ intersects the rhombus $R_{\langle AB\rangle}$. According to Lemma 2.8, neither C nor D is included in the closure of $R_{\langle AB\rangle}$. Thus, $\langle CD\rangle$ intersects the boundary of the rhombus $R_{\langle AB\rangle}$ at two points, say E and F. Since the close line segment connecting E and F, which we denote by $[EF]$ is a subset of $\langle CD\rangle$, we have $[EF] \cap \langle AB\rangle \neq \emptyset$. By this observation, we infer that for the angle α between $[EF]$ and $\langle AB\rangle$ we have $\tan\alpha < \epsilon$. A similar argumentation shows the statement for $\langle AB\rangle$ intersects $R_{\langle CD\rangle}$.

Now, suppose (CD) does not intersect $R_{\langle AB\rangle}$ and (AB) does not intersect $R_{\langle CD\rangle}$. This implies that the boundaries of the rhombi $R_{\langle AB\rangle}$ and $R_{\langle CD\rangle}$ have two intersections, say, E and F. Notice that the segment $[EF]$ does not intersect the edges $\langle AB\rangle$ and $\langle CD\rangle$.

Consequently, the angles α_1 between $[EF]$ and $\langle AB\rangle$ and α_2 between $[EF]$ and $\langle CD\rangle$ satisfy the inequalities $\tan\alpha_1 < \epsilon$ and $\tan\alpha_2 < \epsilon$ and for the angle α between $\langle AB\rangle$ and $\langle CD\rangle$ is $\alpha \leq \alpha_1 + \alpha_2$. This observation yields

$$\tan\alpha \leq \tan(\alpha_1+\alpha_2) = \frac{\tan\alpha_1 + \tan\alpha_2}{1-\tan\alpha_1\cdot\tan\alpha_2} \leq \frac{2\epsilon}{1-\epsilon^2}.$$

□

Finally, we are left to disprove the assumption $R_{\langle AB\rangle} \cap R_{\langle CD\rangle} \neq \emptyset$. Assume, without loss of generality, that $|AB| = 1, |AB| \geq |CD|, A = 0$ and $B = 1$. If $R_{\langle AB\rangle} \cap R_{\langle CD\rangle} \neq \emptyset$, then $\langle AB\rangle$ and $\langle CD\rangle$ are close to being parallel and we use this observation together with Lemma 2.8 for an estimation of the presumable location of the vertices C, D.

Assume that both C, D are not lying inside the open disc with the diameter $\langle AB\rangle$. By the assumption $R_{\langle AB\rangle} \cap R_{\langle CD\rangle} \neq \emptyset$, $|CD| \leq |AB|$ and the fact that $\tan\alpha \leq \frac{2\epsilon}{1-\epsilon^2}$, where α is the angle between $\langle AB\rangle$ and $\langle CD\rangle$, a short calculation yields that for the imaginary parts we have $|\Im(C)|, |\Im(D)| \leq 4\epsilon$. Furthermore, we observe for ϵ small enough, the real part of the leftmost point, where the horizontal line with $|\Im(z)| = 4\epsilon$ intersects the circle with the diameter $|AB| = 1$ is at most $c\epsilon^2$ for $|c|$ reasonable small. By the condition $|CD| \leq |AB|$, we conclude that one of the endpoints of $\langle CD\rangle$, say C, must lie inside the open square box $\{\max(|\Re(z)|, |\Im(z)|) < 4\epsilon\}$ around A, whereas D lies inside the same box translated by 1, i.e. its centre is now B.

This implies that we get a contradiction of the minimality of T, since for ϵ small enough, the edge $\langle AB\rangle$ with length 1 can be deleted in T and replaced by a shorter edge $\langle AC\rangle$ or $\langle BD\rangle$, without violating connectivity or creating loops. This completes the proof of Claim 1.12, since for any two distinct edges $e_1, e_2 \in T$, the open rhombi R_{e_1} and R_{e_2} are disjoint. □

2.4 Plünnecke-type results

As we have already mentioned the trivial upper bound $\binom{|A|+h-1}{h}$ for $|hA|$ in the introduction, we will give two improvements of this bound in particular circumstances. The first one is concerned with the problem, what one can infer about the size of the difference set $(nA - mA)$ on the condition $|A + A| \leq K|A|$.

Theorem 2.10 (Plünnecke-Rusza inequality [19])**.** *Let A be a finite subset of $\mathbb{C}$ with $|A+A| \leq K|A|$ for some $K > 1$. Then for all non-negative integers m, n one has*

$$|nA - mA| \leq K^{n+m}|A|.$$

Before we can prove Theorem 2.10, we need the following two lemmas.

Lemma 2.11 (Rusza's triangle inequality [19])**.** *For any three finite subsets U, V, W of $\mathbb{C}$ one has*

$$|U||V - W| \leq |U + V||U + W|.$$

Proof. For each $d \in V - W$, we choose one representative $(v_d, w_d) \in V \times W$ such that $v_d - w_d = d$. We define the map

$$f : U \times (V - W) \to (U + V) \times (U + W) : \ (u, d) \mapsto (u + v_d, u + w_d).$$

We show that f is injective, which clearly implies Lemma 2.11. Assume that for any two pairs $(u, d), (u', d') \in U \times (V - W)$ we have $f(u, d) = f(u', d')$. This means that $(u + v_d, u + w_d) = (u' + v_{d'}, u' + w_{d'})$. Subtraction of the second element from the first element on both sides yields $d = v_d - w_d = v_{d'} - w_{d'} = d'$ and this in turn shows $u = u'$ and thus $(u, d) = (u', d')$ as required. This proves the lemma. □

Lemma 2.12 (Petridis [19])**.** *Let A, X be finite, non-empty subsets of $\mathbb{C}$ with $|A + X| = K|X|$ and $\frac{|A+Y|}{|Y|} \geq K$ for each non-empty subset Y of X. Then for every finite subset S of $\mathbb{C}$ one has*

$$|S + X + A| \leq K|S + X|.$$

Proof. At first we will partition the sets $X+A+S$ and $S+X$ into $|S|$ distinct subsets. Afterwards we will compare the size of those subsets against each other. This approach facilitates the comparison of $|S + X + A|$ and $|S + X|$.
We set $X_1 := X$ and then define $X_2, \ldots, X_m$ inductively by

$$s_j + X_j = (s_j + X) \setminus \left(\bigcup_{i<j} (s_i + X) \right)$$

for $j = 2, \ldots, m$. Thus we have subdivided $S + X$ into a disjoint union

$$S + X = \bigcup_j (s_j + X_j).$$

where here and below, j is ranging from 1 to s. By this description of $S + X$, we obtain for the cardinality

$$|S + X| = \sum_j |s_j + X_j| = \sum_j |X_j|.$$

Now we repeat the same process for $S+X+A = S+M$, where $M := X+A$. Similarly to the previous partition, we define $M_j \subset M$ by $M_1 := M$ and

$$s_j + M_j = (s_j + M) \setminus \left(\bigcup_{i<j} (s_i + M) \right)$$

for $j = 2, \ldots, s$, and likewise for the partition of $S+M$ we find

$$S + M = \bigcup_j (s_j + M_j).$$

This implies for the cardinality:

$$|S+M| = \sum_j |s_j + M_j| = \sum_j |M_j|.$$

Now we begin to compare $|X_j|$ with $|M_j|$. Notice that for $x \notin X_j$, i.e. $x \in X \setminus X_j$, one has

$$s_j + x \in \bigcup_{i<j} (s_i + X),$$

which implies

$$s_j + x + A \subset \bigcup_{i<j} (s_i + X + A) = \bigcup_{i<j} (s_i + M).$$

Additionally, $x + A \subset M \setminus M_j$ for each $x \in X \setminus X_j$ and as a consequence,

$$(X \setminus X_j) + A \subset M \setminus M_j.$$

By this observation we conclude that

$$|M_j| \le |M| - |(X \setminus X_j) + A| = |X+A| - |(X \setminus X_j) + A|. \tag{2.12}$$

Remember that X minimizes the ratio $\frac{|A+Y|}{|Y|}$, so suppose $\frac{|A+X|}{|X|} = K'$. Clearly is $K' \le \frac{|A+B|}{|B|} \le K$ and by the property of minimality is

$$K' \le \frac{|(X \setminus X_j) + A|}{|X \setminus X_j|} \quad \text{or} \quad |(X \setminus X_j) + A| \ge K' |X \setminus X_j|. \tag{2.13}$$

By inserting estimation (2.13) into inequality (2.12) we obtain

$$|M_j| \le |X+A| - |(X \setminus X_j) + A| \le K'|X| - K'|X \setminus X_j| = K'|X_j| \le K|X_j|.$$

Finally, with this rationale in mind, we can easily match the size of $S+X+A$ with the size of $S+X$ by also using our initial partition of both sets. Consequently,

$$|S+X+A| = \sum_j |M_j| \le \sum_j K|X_j| = K|S+X|,$$

which shows the desired result. □

Proof of Theorem 2.10. We will follow the proof of Petridis. Pick a non-empty subset X of A for which $K' := \frac{|X+A|}{|X|}$ is minimal. Then $K' \le K$.

$$|S+X+A| \le K'|S+X|$$

for any finite subset S of $\mathbb{C}$. Now comes the initial trick: we apply the above inequality subsequently with $S = (m-1)A, (m-2)A, \ldots, \emptyset$, and obtain

$$|mA + X| = |(m-1)A + A + X| \leq K'|(m-1)A + X| \leq \ldots \leq K'^{m-1}|A + X| = K'^{m-1}K'|X| = K'^{m}|X|.$$

The second step follows by Rusza's triangle inequality with $U = X, V = mA$ and $W = nA$. We find

$$|X||mA - nA| \leq |mA + X||nA + X| \leq K'^{m+n}|X|^2,$$

leading to

$$|mA - nA| \leq K'^{m+n}|X| \leq K'^{m+n}|A|.$$

□

The following bound improves the previous bound a little bit if you restrict yourself to the sumset.

Theorem 2.13 (Strict Plünnecke inequality)**.** *Let A be a finite subset of $\mathbb{C}$ with $|A+A| \leq K|A|$ for some $K > 1$. Then for $h \in \mathbb{Z}_{>0}$ one has*

$$|hA| < K^h|A|$$

Proof of Theorem 2.13. Let X be a non-empty subset of A for which $K_X := \frac{|A+X|}{|X|}$ is minimal. So $K_X \leq K$. By applying Lemma 2.12 subsequently with $S = (h-1) \cdot A, (h-2) \cdot A, \ldots, \emptyset$ one obtains

$$|hA| \leq |hA + X| \leq K_X \cdot |(h-1)A + X| \leq \cdots \leq K_X^h \cdot |X| \leq K_X^h \cdot |A| \leq K^h \cdot |A|.$$

Suppose that $|hA| = K^h \cdot |A|$. Then in the above chain of inequalities, all $\leq$ signs become $=$ signs, so in particular $K_X = K, X = A, |hA| = |(h+1)A| = K|hA|$, implying $K = 1$, against our assumption. □

3 Small product sets

The following part is the centerpiece of this thesis. As already broadly laid out in the introduction, Theorem 1.20 is 'almost' optimal in the sense that the leading term $|A|^h/h!$ in the lower bound for $|hA|$ is optimal. Unfortunately, the proof of the theorem is not a straightforward affair, and it depends on a couple of deep theorems from the literature, which we will state below without proof. Nevertheless, we have tried to present our arguments as concisely as possible, while including the relevant details.

Our proof is based on Chang's proof for integers [4] and her ingenious idea to use a result of Evertse, Schlickewei, and Schmidt (abbreviated as ESS) on linear equations with unknowns taking values from a multiplicative group of finite rank [12]. We will apply her idea with an improved version of the result of ESS, due to Amoroso and Viada [1], together with a theorem of Sanders [23] to extend Theorem 1.19 [16] to the h-fold case.

Although the following theorems hold only on the condition $A \subset \mathbb{C}^*$, this distinction turns out to be marginal regarding the lower bound for $|hA|$. Thus, we will treat the case $A \subset \mathbb{C}^*$ at first and on the basis of this result, we will prove the theorem for $A \subset \mathbb{C}$.
A subgroup Γ of K^* is said to have rank r, if it has a free subgroup Γ_0 of rank r such that for every $a \in \Gamma$ there is a positive integer l (which may depend on a) such that $a^l \in \Gamma_0$. For instance, the group of all roots of unity in $\mathbb{C}^*$ has rank 0.

The next theorem was first proved in a weaker form by Evertse, Schlickewei and Schmidt [12] and later improved by Amoroso and Viada.

Theorem 3.1 (Amoroso, Viada [1]). *Let K be a field of characteristic 0, $\Gamma \subset K^*$ a multiplicative subgroup of finite rank r and $b_1, \ldots, b_d \in K^*$. Then the number of solutions of the equation*

$$b_1x_1 + \ldots + b_dx_d = 1$$

in $x_1, \ldots, x_d \in \Gamma$ with no subsum on the left-hand side vanishing is at most

$$A(d, r) = (8d)^{4d^4(d+rd+1)}.$$

Sometimes we will refer to the solutions for which all subsums of $b_1x_1 + \cdots + b_dx_d$ are non-zero as non-degenerate solutions. In order to apply Theorem 3.1, we need a 'good' estimation for the rank of Γ.
For any additive abelian group G we define a m-dimensional centred convex progression $P \subset G$ as an image of a symmetric convex body $Q \subset \mathbb{R}^m$ under a homomorphism $\phi : \mathbb{Z}^m \to G$, so that $\phi(\mathbb{Z}^m \cap Q) = P$.

The following theorem of Sanders is a quantitative version of Freiman's theorem for general abelian groups (Lemma 1.14 in [14]).

Theorem 3.2 (Sanders [23]). *Let G be any additive abelian group. Then for every $\epsilon > 0$ there exist $K_0(\epsilon), C(\epsilon) > 0$ with the following property. Let A be any finite, non-empty subset of G with $|A + A| \leq K|A|$ for some $K > K_0(\epsilon)$. Then there are a set $X' \subset G$, an $m-$dimensional centred convex progression $P \subset G$ and finite subgroup H of G such that*

$$A \subset X' + P + H, \quad |X'| \leq e^{C(\epsilon)\log^{3+\epsilon}(K)}, \quad m \leq C(\epsilon)\log^{3+\epsilon}(K).$$

By combining Theorem 3.1 and 3.2, we can derive the following corollary.

Corollary 3.3. *For every $\epsilon > 0$ there exist $K_0(\epsilon), C(\epsilon) > 0$ with the following property. Let A be any finite, non-empty subset of $\mathbb{C}^*$ satisfying $|A \cdot A| \leq K|A|$ for some $K > K_0(\epsilon)$. Then there exist a finite subset X of $\mathbb{C}^*$ and a finitely generated subgroup Γ of $\mathbb{C}^*$ with*

$$|X| \leq e^{C(\epsilon)\log^{3+\epsilon}(K)}, \quad \mathrm{rank}(\Gamma) \leq C(\epsilon)\log^{3+\epsilon}(K),$$

such that $A \subset X \cdot \Gamma = \{yz \ : \ y \in X, z \in \Gamma\}$. *Furthermore, for* $b_1, \ldots, b_d \in \mathbb{C}^*$, *the number of non-degenerate solutions of*

$$b_1 x_1 + \ldots + b_d x_d = 1, \quad x_1, \ldots, x_d \in A \tag{3.1}$$

is at most $|X|^d \cdot (8d)^{4d^4(d+d\cdot\mathrm{rank}(\Gamma)+1)}$.

Proof. Consider the group isomorphism

$$\begin{aligned} \log : \mathbb{C}^* &\to G' := \mathbb{C}/2\pi i\mathbb{Z} \\ z &\mapsto \log|z| + i\arg z \mod (2\pi i\mathbb{Z}). \end{aligned}$$

This function maps A to a finite subset $A' := \log(A)$ of G' of the same cardinality and by the property $\log(a \cdot a') = \log(a) + \log(a')$ we conclude

$$|A' + A'| = |\log(A) + \log(A)| = |\log(A \cdot A)| = |A \cdot A| \leq K|A| = K|\log(A)| = K|A'|.$$

Let $\epsilon > 0$, and $K_0(\epsilon), C(\epsilon)$ the quantities from Theorem 3.2. Let $K > K_0(\epsilon)$. By Theorem 3.2, we have $A' \subset X' + P + H$, where $|X'| \leq e^{C(\epsilon)\log^{3+\epsilon}(K)}$, H is a finite subgroup of G', and $P \subset \{\sum_{i=1}^m n_i\phi(e_i),\ n_i \in \mathbb{Z}\}$, with e_i the i-th standard basis vector of $\mathbb{Z}^m$, ϕ the homomorphism from the definition of centred convex progression, and $m \leq C(\epsilon)\log^{3+\epsilon}(K)$. Thus, $H + P$ is contained in a subgroup Γ' of G' of rank at most $C(\epsilon)\log^{3+\epsilon}(K)$. Applying the inverse of log, i.e. exp, we see that $A \subset \exp(X' + \Gamma') = e^{X'} \cdot e^{\Gamma'} = X \cdot \Gamma$.

Let us express $x_i \in A$ as $y_i \cdot z_i$, where $y_i \in X$ and $z_i \in \Gamma$. Hence, equation (3.1) becomes

$$(b_1 y_1)z_1 + \ldots + (b_d y_d)z_d = 1. \tag{3.2}$$

By fixing $y_1, \ldots, y_d$ there exist according to Theorem 3.1 at most $(8d)^{4d^4(d+d\,\mathrm{rank}(\Gamma)+1)}$ non-degenerate solutions $z_1, \ldots, z_d \in \Gamma$ to (3.2). Moreover, there exist $|X|^d$ different tuples $(y_1, \ldots, y_d)$. It follows that there exist at most $|X|^d \cdot (8d)^{4d^4(d+d\cdot\mathrm{rank}(\Gamma)+1)}$ non-degenerate solutions of (3.1). □

Let $\epsilon > 0$, $K > 1$ and write $K' := \max\{K, K_0(\epsilon)\}$. Let A be a finite subset of $\mathbb{C}^*$ with $|AA| < K|A|$. Suppose A has cardinality n. By Corollary 3.3 we have $A \subset X \cdot \Gamma$, where X is a finite subset of $\mathbb{C}^*$ of cardinality at most $f := e^{C(\epsilon)\log^{3+\epsilon}(K')}$ and Γ a finitely generated subgroup of $\mathbb{C}^*$ of rank at most $r := C(\epsilon)\log^{3+\epsilon}(K')$ and therefore $|X|^d \cdot (8d)^{4d^4(d+d\cdot\mathrm{rank}(\Gamma)+1)} \leq f^d \cdot (8d)^{4d^4(d+rd+1)}$.
To structure the proof of Theorem 1.20 and Lemma 3.4 concisely, we now introduce some notation.

$$\begin{aligned} E_A^+(t) := \Bigg| \Bigg\{ &(a_1, \ldots, a_{2t}) \in A^{2t} : \\ &a_1 + \ldots + a_t = a_{t+1} + \ldots + a_{2t}, \\ &a_i + a_j \neq 0 \text{ for all } i,j \text{ with } 1 \leq i < j \leq t \text{ or } t+1 \leq i < j \leq 2t \Bigg\} \Bigg|, \end{aligned}$$

and for $a \in tA$

$$r_A^+(t,a) := \left| \left\{ (a_1, \ldots, a_t) \in A^t : a_1 + \ldots + a_t = a, a_i + a_j \neq 0 \text{ for all } i,j \text{ with } 1 \leq i < j \leq t \right\} \right|.$$

Further, define

$$
\begin{aligned}
D_0(t) &:= \sup_{b_1,\ldots,b_t\in\mathbb{C}^*} \Big|\{(a_1,\ldots,a_t)\in A^t : b_1a_1+\ldots+b_ta_t=0\}\Big|,\\
D_1(t) &:= \sup_{b_1,\ldots,b_t\in\mathbb{C}^*} \Big|\{(a_1,\ldots,a_t)\in A^t : b_1a_1+\ldots+b_ta_t=1\}\Big|,\\
A(t,f,r) &:= f^t(8t)^{4t^4(t+rt+1)},\\
B(t,f,r) &:= f^t(8t)^{t^6(t+rt+1)}.
\end{aligned}
$$

The next lemma together with Corollary 3.3 are the foundation of the proof of Theorem 1.20.

Lemma 3.4. *Let A, K, n, f, r be as above. Then for every $t \geq 2$ one has*

$$
\begin{aligned}
D_0(t) &\leq B(t,f,r)\cdot n^{\lfloor \frac{t}{2}\rfloor},\\
D_1(t) &\leq B(t,f,r)\cdot n^{\lfloor \frac{t-1}{2}\rfloor}.
\end{aligned}
$$

Proof. Let us start with $t=2$. We observe that the equation

$$b_1a_1+b_2a_2=0$$

has at most n solutions while the equality

$$b_1a_1+b_2a_2=1$$

has according to Corollary 3.3 at most $A(2,f,r)=B(2,f,r)$ solutions. Hence, for $t=2$ the bound holds. The case $t\geq 3$ will be treated by induction, i.e. we assume the bound was proven for each $t'\leq t-1$.
We will first estimate $D_1(t)$. By inspecting the definition of $D_1(t)$, we find the upper bound:

$$D_1(t)\leq A(t,f,r)+\sum_{j=2}^{t-1}\binom{t}{j}D_0(j)D_1(t-j)\leq 2\sum_{j=2}^{t-1}\binom{t}{j}B(j,f,r)B(t-j,f,r)\cdot n^{\lfloor\frac{t-j-1}{2}\rfloor+\lfloor\frac{j}{2}\rfloor}.$$

The second inequality follows from $A(t,f,r)\leq B(t-1,f,r)$. The next step consists of estimating from above the maxima of $B(j,f,r)\cdot B(t-j,f,r)$ and $\lfloor\frac{t-j-1}{2}\rfloor+\lfloor\frac{j}{2}\rfloor$ over $j=2,\ldots t-1$. The remaining terms can easily bounded by

$$2\sum_{j=2}^{t-1}\binom{t}{j}\leq 2^{t+1}. \tag{3.3}$$

By the condition $j\leq t-1$ we can bound $B(j,f,r)B(t-j,f,r)$ by

$$B(j,f,r)B(t-j,f,r)\leq f^t(8(t-1))^{(t-1)^6(t+rt+2)}. \tag{3.4}$$

The general observation$\lfloor a\rfloor+\lfloor b\rfloor\leq\lfloor a+b\rfloor$ for any two reals a,b yields the upper bound

$$\lfloor\frac{t-j-1}{2}\rfloor+\lfloor\frac{j}{2}\rfloor\leq\lfloor\frac{t-1}{2}\rfloor \tag{3.5}$$

for the exponent of n.
By combining (3.3),(3.4) and (3.5) we obtain the desired upper bound

$$D_1(t)\leq 2^{t+1}\cdot f^t(8(t-1))^{(t-1)^6(t+rt+2)}\cdot n^{\lfloor\frac{t-1}{2}\rfloor}\leq B(t,f,r)\cdot n^{\lfloor\frac{t-1}{2}\rfloor}. \tag{3.6}$$

Let us now estimate $D_0(t)$. We will transform this problem into a problem of finding an upper bound for $D_1(t-1)$. The equation

$$b_1 a_1 + \ldots + b_t a_t = 0$$

can be rewritten as

$$\frac{b_1 a_1 + \ldots + b_{t-1} a_{t-1}}{-b_t a_t} = 1. \tag{3.7}$$

Notice that there exist n possibilities for $-b_t a_t$. This observation together with (3.7) yields the upper bound

$$D_0(t) \leq n \cdot D_1(t-1). \tag{3.8}$$

By (3.6) and (3.8) we conclude

$$D_0(t) \leq n \cdot D_1(t-1) \leq B(t-1, f, r) \cdot n^{\lfloor \frac{t-1-1}{2} \rfloor + 1} \leq B(t-1, f, r) \cdot n^{\lfloor \frac{t}{2} \rfloor}.$$

Hence,

$$D_0(t) \leq B(t, f, r) \cdot n^{\lfloor \frac{t}{2} \rfloor}$$

and

$$D_1(t) \leq B(t, f, r) \cdot n^{\lfloor \frac{t-1}{2} \rfloor}.$$

□

Proof of Theorem 1.20. In what follows we put $n := |A|$. The proof consists of the following steps:

1. For the moment we will assume $A \subset \mathbb{C}^*$.
2. We find a 'nice connection' between $|hA|, E_A^+(h)$ and $\sum_{a \in hA} r_A^+(h, a)$.
3. We bound $E_A^+(h)$ from above in terms of n and $B(h, f, r)$.
4. We bound $\sum_{a \in hA} r_A^+(h, a)$ from below in terms of n.
5. We obtain a lower bound for $|hA|$.
6. We consider the case that $0 \in A$.
7. We calculate a rough bound for $D_0(2h)$.
8. We insert this bound in the lower bound obtained in step 5 and obtain a lower bound of $|hA|$ for $A \subset \mathbb{C}$, i.e. $0 \in A$.

Let us start with the second step by finding the 'nice connection'. The connection will be accomplished via the Cauchy-Schwartz inequality:

$$E_A^+(h) = \sum_{a \in hA} r_A^+(h, a)^2 \geq \frac{1}{\sum_{a \in hA} 1^2} \cdot \left(\sum_{a \in hA} r_A^+(h, a) \right)^2 = \frac{\left(\sum_{a \in hA} r_A^+(h, a) \right)^2}{|hA|}. \tag{3.9}$$

We now deal with the third step. Consider the equation

$$a_1 + \ldots + a_h = a_{h+1} + \ldots + a_{2h}, \tag{3.10}$$

which can be rewritten as

$$\sum_{j=1}^{2h-1} b_j a_j = 1 \quad \text{with} \quad b_j = \begin{cases} a_{2h}^{-1} & \text{for } j = 1, \ldots, h, \\ -a_{2h}^{-1} & \text{for } j = h+1, \ldots, 2h-1. \end{cases} \tag{3.11}$$

By the representation as (3.11) we obtain the upper bound

$$E_A^+(h) \leq n\left[\sum_{t=2}^{2h-3} \binom{2h-1}{t} \cdot D_0(t)A(2h-1-t,f,r) + hE_A^+(h-1) + A(2h-1,f,r)\right]. \quad (3.12)$$

This can be seen as follows. Fix a_{2h} and consider the tuples $(a_1,\ldots,a_{2h-1})$ on the condition (3.11) and

$$a_i + a_j \neq 0 \text{ for all with } 1 \leq i < j \leq h \text{ or } h+1 \leq i < j \leq 2h. \quad (3.13)$$

For each such a tuple, we can take from the left-hand side of (3.11) a maximal vanishing subsum, i.e., with a maximal number of terms; then the remaining sum is equal to 1 and has no vanishing subsum. Since we assumed that $A \subset \mathbb{C}^*$ there are no vanishing subsums with one term. The number of tuples with (3.11), (3.13) of which a maximal vanishing subsum has exactly t terms, for some t with $0 \leq t \leq 2h-2$ and $t \neq 1$, is at most $\binom{2h-1}{t} D_0(t)A(2h-1-t,f,r)$, where the term $A(2h-1-t,f,r)$ comes from Corollary 3.3. By adding the terms over these t we would get an upper bound for $E_A^+(h)$ which is to rough for our purpose. Now comes the crucial part: we take the tuples with $t = 2h-2$ apart and deduce an upper bound $hE_A^+(h-1)$ for their number. Notice that for these tuples we have either $a_p + a_{2h} = 0$ for some p with $h+1 \leq p \leq 2h$, which is however excluded by our assumption; or $a_p - a_{2h} = 0$ for some p with $1 \leq p \leq h$. But then we get

$$\sum_{j=1, j\neq p}^{h} a_j = a_{h+1} + \ldots + a_{2h-1}.$$

For fixed p there are at most h possibilities, and for the tuple consisting of the remaining components in $(a_1,\ldots,a_{2h-1})$ at most $E_A^+(h-1)$ possibilities. This provides the bound $hE_A^+(h-1)$. So altogether, we see that the number of tuples with (3.11), (3.13) and with fixed a_{2h} is bounded above by the quantity between the brackets of (3.12). Finally, we have to multiply this quantity by n, since there exist n choices for a_{2h}.

The current recursive formula for the upper bound of $E_A^+(h)$ in (3.12) is a little cumbersome for further calculations, thus we will try to find a closed formula. In order to make life a little bit easier, we will simplify the bound in (3.12) a little bit:

$$\begin{aligned}
E_A^+(h) &\leq n\left[\sum_{t=2}^{2h-3} \binom{2h-1}{t} D_0(t)A(2h-1-t,f,r) + hE_A^+(h-1) + A(2h-1,f,r)\right] \\
&\leq n\left[\sum_{t=2}^{2h-3} \binom{2h-1}{t} B(t,f,r)n^{\lfloor \frac{t}{2} \rfloor}A(2h-1-t,f,r) + hE_A^+(h-1) + A(2h-1,f,r)\right] \\
&\leq n\left[\sum_{t=2}^{2h-3} \binom{2h-1}{t} B(2h-3,f,r)A(2,f,r)n^{h-2} + hE_A^+(h-1) + A(2h-1,f,r)\right] \\
&\leq n\left[2^{2h-1}B(2h-3,f,r)A(2,f,r)n^{h-2} + hE_A^+(h-1) + A(2h-1,f,r)\right]. \quad (3.14)
\end{aligned}$$

Notice that $E_A^+(1) = n$ and observe that for $h = 2$ we have

$$E_A^+(2) \leq 2n^2 + nA(3,f,r). \quad (3.15)$$

To see this, consider the equation

$$a_1 + a_2 = a_3 + a_4$$

which has the alternative representation

$$\frac{a_1 + a_2 - a_3}{a_4} = 1.$$

For fixed a_4, the number of non-degenerate solutions can be bounded by $A(3, f, r)$ and the condition $A \subset \mathbb{C}^*$ allows only 2-element subsums that can vanish. Moreover, conditon (3.13) requires $a_1 + a_2 \neq 0$. Thus, there remain two possible vanishing subsums

$$a_1 - a_3 = 0 \quad \text{or} \quad a_2 - a_3 = 0,$$

and each one has n solutions. Finally, a_4 can attain n different values and this yields the bound in (3.15).
By combining (3.14) and (3.15), we obtain for $h = 3$:

$$\begin{aligned} E_A^+(3) &\leq n \cdot \Big[3E_A^+(2) + 2^5 B(3, f, r)A(2, f, r)n + A(5, f, r) \Big] \\ &\leq n \cdot \Big[3!n^2 + 3A(3, f, r)n + 2^5 B(3, f, r)A(2, f, r)n + A(5, f, r) \Big] \\ &= 3!n^3 + \Big(3A(3, f, r) + 2^5 B(3, f, r)A(2, f, r) \Big) n^2 + A(5, f, r)n \end{aligned}$$

and likewise for $h = 4$:

$$\begin{aligned} E_A^+(4) \leq n \cdot &\Big[4!n^3 + \Big(4 \cdot 3 \cdot A(3, f, r) + 4 \cdot 2^5 \cdot B(3, f, r)A(2, f, r) \Big) n^2 \Big] + \\ &n \Big[4A(5, f, r)n + 2^7 A(2, f, r)B(5, f, r)n + A(7, f, r) \Big] \\ = 4!n^4 + &\Big(4 \cdot 3 \cdot A(3, f, r) + 4 \cdot 2^5 \cdot B(3, f, r)A(2, f, r) + 2^7 A(2, f, r)B(5, f, r) \Big) n^3 + \\ &4A(5, f, r)n^2 + A(7, f, r)n. \end{aligned}$$

Finally, we conclude

$$\begin{aligned} E_A^+(h) \leq\ & h! \cdot n^h + \left(\frac{h!}{2!} A(3, f, r) + A(2, f, r)h! \sum_{t=2}^{h-1} B(2t-1, f, r) \frac{2^{2t+1}}{(t+1)!} \right) \cdot n^{h-1} \\ & \qquad + h! \cdot \left(\sum_{t=1}^{h-2} \frac{A(2(h-t)+1, f, r)}{(h+1-t)!} n^t \right) \\ \leq\ & h! \cdot \left(n^h + A(2, f, r)B(2h-3, f, r) \sum_{t=2}^{h} \frac{2^{2t+1}}{(t+1)!} n^{h-1} \right) \\ & \qquad + h! \cdot \left(A(2h-1, f, r) \sum_{t=1}^{h-2} \frac{1}{(h+1-t)!} n^{h-2} \right) \\ \leq\ & h! \cdot \left(n^h + A(2, f, r)B(2h-3, f, r) \cdot 21 \cdot n^{h-1} + \frac{A(2h-1, f, r)}{3} n^{h-2} \right) \end{aligned} \tag{3.16}$$

by the observations $\sum_{t=2}^{h} \frac{2^{2t+1}}{(t+1)!} \leq 21$ and $\sum_{t=1}^{h-2} \frac{1}{(h+1-t)!} \leq \frac{1}{3}$, which finishes step 3.

We now work out step 4. There exist n^h tuples in A^h and from n^h we have to subtract the number of tuples $(a_1, \ldots, a_h)$ with the property $a_i + a_j = 0$ for some $1 \leq i < j \leq h$. Since

$\sum_{a\in hA} r_A^+(h,a)$ counts all tuples in A^h for which there are no i,j with $a_i + a_j = 0$, we get for the lower bound of $E_A^+(h)$:

$$\sum_{a\in hA} r_A^+(h,a) \geq n^h - \binom{h}{2} n^{h-1} = n^h - \frac{1}{2}h(h-1)n^{h-1}. \tag{3.17}$$

Step 5 is more or less a straightforward affair. By taking the square of the right-hand side from (3.17) we obtain

$$\left(n^h - \frac{1}{2}h(h-1)n^{h-1}\right)^2 = n^{2h} - h(h-1)n^{2h-1} + \frac{1}{4}h^2(h-1)^2 n^{2h-2}, \tag{3.18}$$

and combining (3.9), (3.16) and (3.18) yields

$$\begin{aligned} &h!\left(n^h + A(2,f,r)B(2h-3,f,r)\cdot 21\cdot n^{h-1} + \frac{A(2h-1,f,r)}{3}n^{h-2}\right) \\ \geq &\frac{n^{2h} - h(h-1)n^{2h-1} + \frac{1}{4}h^2(h-1)^2n^{2h-2}}{|hA|}. \end{aligned} \tag{3.19}$$

We infer from (3.19) and $|hA| \leq n^h$ that

$$\begin{aligned} &n^h|hA| + A(2,f,r)B(2h-3,f,r)\cdot 21\cdot n^{2h-1} + \frac{A(2h-1,f,r)}{3}n^{2h-2} \\ \geq \quad &\frac{n^{2h} - h(h-1)n^{2h-1} + \frac{1}{4}h^2(h-1)^2n^{2h-2}}{h!} \end{aligned} \tag{3.20}$$

and rearranging (3.20) as

$$\begin{aligned} |hA| &\geq \frac{n^h}{h!} - \left(\frac{h(h-1)}{h!} + 21A(2,f,r)B(2h-3,f,r)\right)n^{h-1} \\ &\quad + \left(\frac{h^2(h-1)^2}{4\cdot h!} - \frac{A(2h-1,f,r)}{3}\right)n^{h-2} \\ &\geq \frac{n^h}{h!} - B(2h-1,f,r)n^{h-1} \end{aligned} \tag{3.21}$$

yields the lower bound for $A \subset \mathbb{C}^*$.
Steps 6,7 and 8 are dealt with in the following way. Let $0 \in A$ and consider the number of tuples $(a_1,\ldots,a_{2h}) \in A^{2h}$ with at least one term equal to 0. The number of such tuples is at most

$$\sum_{t=1}^{2h}\binom{2h}{t}D_0(2h-t) \leq D_0(2h-1)2^{2h} \leq 2^{2h}B(2h-1,f,r)n^{h-1}. \tag{3.22}$$

This follows from the observation that the number of tuples with exactly t terms equal to 0 is at most $\binom{2h}{t}D_0(2h-t)$. We have to add the right-hand side of (3.22) to the upper bound obtained in (3.16) for $E_A^+(h)$ and repeat the argument in step 5 to get a lower bound for $|hA|$ for any finite, non-empty subset A of $\mathbb{C}$. This leads to

$$|hA| \geq \frac{n^h}{h!} - \frac{2^{2h}+h!}{h!}B(2h-1,f,r)n^{h-1}, \tag{3.23}$$

which can be further lowered to

$$\begin{aligned} |hA| &\geq \frac{n^h}{h!} - \frac{2^{2h}+h!}{h!}e^{(2h-1)C(\epsilon)\log^{3+\epsilon}(K')}(8(2h-1))^{(2h-1)^6(2h-1+(2h-1)C(\epsilon)\log^{3+\epsilon}(K')+1)}n^{h-1} \\ &\geq \frac{n^h}{h!} - h^{(2h)^7C'(\epsilon)\log^{3+\epsilon}(K')}n^{h-1} \\ &\geq \frac{n^h}{h!} - \exp\left(C''(\epsilon)h^7(\log h)\cdot(\log K')^{3+\epsilon}\right)n^{h-1} \end{aligned}$$

for some positive numbers $C'(\epsilon), C''(\epsilon)$ depending only on ϵ. □

Proof of Corollary 1.21. Let $|A| = n$. By Theorem 1.20 for $K = \exp\left(c(h,\epsilon)(\log n)^{\frac{1-\epsilon}{3+\epsilon}}\right)$ with $c(h,\epsilon) := \frac{1}{\sqrt[3+\epsilon]{C(\epsilon)h^7\log(h)}}$ and with $n > n(h,\epsilon)$, where $n(h,\epsilon)$ has been chosen large enough to guarantee that $K > K_0(h,\epsilon)$, one has

$$\begin{aligned} |hA| &\geq \frac{n^h}{h!} - \exp\left(C(\epsilon)h^7(\log h)\cdot(\log K)^{3+\epsilon}\right) n^{h-1} \\ &\geq \frac{n^h}{h!} - \exp\left((\log n)^{1-\epsilon}\right) n^{h-1} \\ &\geq \frac{n^h}{h!} - n^{1-\epsilon}\cdot n^{h-1} \\ &= \frac{n^h}{h!} - n^{h-\epsilon}. \end{aligned}$$

□

References

[1] F. Amoroso, E. Viada, Small points on subvarieties of a torus. Duke Math. J., 150 (3) (2009), pp.407-442.
https://edoc.unibas.ch/8251/1/20100126133824_4b5ee240c8237.pdf

[2] J. Bourgain, M. C. Chang, On the size of k-fold sum and product sets of integers. J. Amer. Math. Soc., 17 (2004), Number 2, pp. 473–497.
http://math.ucr.edu/~mcc/paper/119%20On%20the%20size%20of%20k-fold%20Sum%20and%20Product%20Sets%20of%20Integer.pdf

[3] A. Bush, E. Croot, Few products, many h-fold sums. Int. J. Number Theory, 14 (2018), No. 08, pp. 2107-2128.
https://arxiv.org/pdf/1409.7349.pdf

[4] M. C. Chang, Sum and product of different sets. Contr. Discr. Math. 1, year 2006
https://pdfs.semanticscholar.org/38a0/b41488683513cb00148387448dbf8a7b4674.pdf

[5] M. C. Chang, Factorization in generalized arithmetic progressions and application to the Erdős- Szeméredi sum-product problem, Geom. Funct. Analysis, 13 (2003), pp. 720 - 736.
https://www.researchgate.net/publication/227328346_Factorization_in_generalized_arithmetic_progressions_and_application_to_the_Erdos-Szemeredi_sum-product_problems

[6] M. C. Chang, Erdős-Szemerédi Problem on sum set and product set, Ann. of Math., 157 (2003), pp. 939 - 957.
http://annals.math.princeton.edu/wp-content/uploads/annals-v157-n3-p07.pdf

[7] M. C. Chang, A sum-product estimate in algebraic division algebras over R, Israel J. Math., 150 (2005), pp. 369 - 380.
http://math.ucr.edu/~mcc/paper/116%20A%20sum-product%20estimate%20in%20algebraic%20division%20algebras%20over%20R.pdf

[8] Y. G. Chen, On sums and products of integers, Proc. Amer. Math. Soc., 127 (1999), pp. 1927–1933
https://www.ams.org/journals/proc/1999-127-07/S0002-9939-99-04833-9/S0002-9939-99-04833-9.pdf

[9] K. O. Chipeniuk, Sums and Products of Distinct Sets and Distinct Elements in Fields of Characteristic 0, J. of Integers, 5 (2009), pp. 639 - 667.
https://arxiv.org/pdf/0902.3506.pdf

[10] G. Elekes, On the number of sums and products, Acta Arith., 81 (1997), pp. 365 - 367.
http://matwbn.icm.edu.pl/ksiazki/aa/aa81/aa8145.pdf

[11] P. Erdős, E. Szemerédi, On sums and products of integers. Studies in Pure Mathematics (1983), Paul Erdős, László Alpár, Gábor Halász, András Sárközy, Springer, pp. 213 - 218,
https://users.renyi.hu/~p_erdos/1983-18.pdf

[12] J.-H. Evertse, H.P. Schlickewei, W.M. Schmidt, Linear equations in variables which lie in a multiplicative group, Ann. Math., 155 (2002), pp. 807 - 836.
https://arxiv.org/pdf/math/0409604.pdf

[13] K. Ford, Sums and products from a finite set of real numbers, The Ramanujan J., 2 (1998), pp. 59 - 66.
https://faculty.math.illinois.edu/~ford/wwwpapers/sumprod.pdf

[14] G.A. Freiman, Foundations of a Structural Theory of Set Addition. Transl. Math. Monographs (American Mathematical Society, Providence, 1973)

[15] A. Granville, An introduction to additive combinatorics, lecture notes, chapter I, section 9
http://people.math.gatech.edu/~ecroot/additive_combinatorics.pdf

[16] A. Granville, J. Solymosi, Sum-product formulae, Book Recent trends in Combinatorics, A. Beveridge, J. R. Griggs, L. Hogben, G. Musiker, P. Tetali, Springer, 2016, pp. 419 - 452.

[17] S. V. Konyagin, I. D. Shkredov, On sum sets of sets, having small product set, Proceed. Steklov Inst. Math., 290 (2015), pp. 288 - 299.
https://arxiv.org/pdf/1503.05771.pdf

[18] S. V. Konyagin, M. Rudnev, On new sum-product type estimates, SIAM J. Disc. Math., 27 (2014), pp. 973 - 990.
https://arxiv.org/pdf/1207.6785.pdf

[19] Y. Li, Plünnecke's theorem and rusza's covering lemma, lecture notes.
https://www.cs.mcgill.ca/~yli252/files/2Plunnecke.pdf

[20] M. B. Nathanson, On sums and products of integers, Proc. Amer. Math. Soc., 125 (1997), pp. 9 - 16.
https://www.jstor.org/stable/2161787?seq=1#page_scan_tab_contents

[21] M. B. Nathanson, G. Tenenbaum. Inverse theorems and the number of sums and products, Astérisque Soc. Math. France, 258 (1999)
https://pdfs.semanticscholar.org/a845/75add127307de03ea9dc67df1dbb05ad8a58.pdf

[22] M. Rudnev, I. D. Shkredov, S. Stevens, On the energy variant of the sum-product conjecture.
https://arxiv.org/pdf/1607.05053.pdf

[23] T. Sanders, The structure theory of set addition revisited, Bull. Amer. Math. Soc., 50 (2013), pp. 93–127
https://arxiv.org/pdf/1212.0458.pdf

[24] A. Sheffer, lecture notes, Chapter 2: The sum-product problem.
http://math.caltech.edu/~2015-16/3term/ma191c-sec6/02%20SumProd.pdf

[25] J. Solymosi, On sum-sets and product-sets of complex numbers, J. Th. Nombres Bordeaux, 17 (2005), pp. 921 - 924.
http://www.math.ubc.ca/~solymosi/sajatcikkek/complexjtnb.pdf

[26] J. Solymosi, On the number of sums and products, Bull. London Math. Soc., 37 (2005), pp. 491–494.
http://www.math.ubc.ca/~solymosi/sajatcikkek/sumprodbull.pdf

[27] J. Solymosi, Bounding multiplicative energy by the sumset, Adv. Math., 222 (2009), pp. 402 - 408.
https://www.sciencedirect.com/science/article/pii/S0001870809001182

[28] C. D. Toth, The Szemerédi-Trotter theorem in the complex plane, Combinatorica, 35 (2003), pp. 95 - 126
https://arxiv.org/pdf/math/0305283.pdf