A NOTE ON THE MULTIPLICATIVE STRUCTURE OF AN ADDITIVELY SHIFTED PRODUCT SET $AA+1$

Steven Senger
Department of Mathematics, University of Delaware, Newark, Deleware
senger@math.udel.edu

Received: 7/19/12, Revised: 3/1/13, Accepted: 4/28/13, Published: 6/14/13

Abstract

We consider the multiplicative structure of sets of the form $AA+1$, where A is a large, finite set of real numbers. In particular, we show that the additively shifted product set, $AA+1$, must have a large part outside of any proper non-degenerate generalized geometric progression of comparable length. We prove an analogous result in finite fields as well.

1. Introduction

There are many problems in additive combinatorics which seek to differentiate between additive and multiplicative structure. By additive (resp. multiplicative) structure in a set, we refer to some arrangement or information that is largely undisturbed by addition (resp. multiplication). A prime example is the sums and products problem. Let A be a large, finite set of n natural numbers. Define the sum set of A to be

$$A+A=\{a+b : a\in A, b\in A\}.$$

Define the product set of A to be

$$AA=\{ab : a\in A, b\in A\}.$$

Let $|\cdot|$ denote the size of a set. The sums and products problem conjectures that,

$$\max\{|A+A|,|AA|\}\geq cn^{2-\epsilon},$$

for any $\epsilon>0$, and some constant, $c=c(\epsilon)>0$, which is independent of n. In [1], Elekes made progress with an elegant proof based on the celebrated Szemerédi-Trotter point-line incidence theorem, from [9]. Many of the results in this area have seen largely geometric proofs, including the current record in [8]. Therein, Solymosi proved the remarkable result that either the set of sums or the set of products must

have more than about $n^{\frac{4}{3}}$ elements. See the book by Nathanson, [7], or the book by Tao and Vu, [10], for more.

One indication of multiplicative structure is how the size of a finite set A compares to the size of AA. If AA is not much bigger that A, then there must be some multiplicative structure in the set A. The construction of a product set will build in some multiplicative structure. This can often be estimated using tools such as multiplicative energy and the Plünnecke-Rusza inequalities. Again, see [7] and [10] for more details. Our main focus is to show that the multiplicative structure inherent in the product set of a large, finite set of numbers cannot be maximal after an additive shift. This will be made precise in the statement of the main theorem. First, however, we need to introduce some definitions and notation.

In what follows, we use the following asymptotic notation. If two positive quantities, X and Y, vary with respect to some parameter, n, we say $X \lesssim Y$ if $X \leq CY$, for some constant, $C > 0$, which does not depend on n. We write $X \approx Y$ when $X \lesssim Y$ and $Y \lesssim X$. In what follows, the implied constant may depend on some other parameters (such as δ or ϵ below), but it will be independent of the size of our set A.

If A is a set of numbers, then define its *additive shift* to be

$$A + 1 = \{a + 1 : a \in A\}.$$

Similarly, a *scaling* of A by some number s will be

$$sA = \{sa : a \in A\}.$$

We note that multiplicative behavior of additive shifts have been studied in relation to product sets by Garaev and Shen in [2], and Jones and Roche-Newton in [6]. However, they consider sets of the form $A(A + 1)$, which exhibit behavior which is quite different from that of sets of the form $AA + 1$, considered here.

Let $r_0, r_1, \ldots, r_d$ be real numbers called *generators*, and let $l_1, \ldots, l_d$ be positive integers greater than 2. We define the *d-dimensional generalized arithmetic progression*

$$\begin{aligned} R &= R(r_0, r_1, \ldots, r_d, l_1, \ldots, l_d) \\ &= \{r_0 + x_1 r_1 + \cdots + x_d r_d : x_j \in \mathbb{Z}, 0 \leq x_j < l_j, j = 1, \ldots, d\}. \end{aligned}$$

The related notion of a *d-dimensional generalized geometric progression* is defined as

$$G = G(g_0, R) = \{g_0^r : r \in R\},$$

where g_0 is some positive real number and R is some d-dimensional arithmetic progression. Either type of progression is said to be *proper* if every choice of $(x_1, x_2, \ldots, x_d)$ yields a distinct element of the set. Furthermore, we will call either type of generalized progression *degenerate* if d grows asymptotically with the size

of the progression. That is to say, if the number of generators is not like a constant compared to the length of the progression, it is degenerate.

Such progressions exhibit maximality in arithmetic, or, respectively, geometric structure. We clarify this with the following elementary proposition.

Proposition 1.1. *If R is a non-degenerate generalized arithmetic progression, we have that*

$$|R+R| \approx |R|.$$

Also, if G is a non-degenerate generalized geometric progression, we have that

$$|GG| \approx |G|.$$

We now state the main result.

Theorem 1.2. *Let $A \subset \mathbb{R}$, be a large, finite set of numbers. Let G be any proper non-degenerate generalized geometric progression with $|G| \approx |AA|$. We have that for any $\delta > 0$*

$$|(AA+1) \setminus G| \gtrsim |A|^{1-\delta}.$$

The proof of Theorem 1.2 works for some slightly more general progressions. Remark 2.3 provides some insight into how to modify the proof to slightly relax the assumptions of properness and non-degeneracy. Two direct corollaries follow.

Corollary 1.3. *Let $A \subset \mathbb{R}$, be a large, finite set of numbers. Let G be any proper non-degenerate generalized geometric progression with $|G| \approx |AA|$. We have that*

$$(AA+1) \not\subset G.$$

Notice that for any non-degenerate geometric progression, $H \subset \mathbb{R}$, there exists a set $H' \subset \mathbb{R}$ such that $|H'H'| \approx |H|$ and $H \subset H'H'$. If we apply Theorem 1.2 with $A = H'$, we get the following corollary.

Corollary 1.4. *Let G and H be any two large, finite, proper non-degenerate generalized geometric progressions with $|G| \approx |H|$. We have that*

$$(H+1) \not\subset G.$$

We suspect that the additive shift disrupts multiplicative structure even more than Theorem 1.2 indicates, as suggested by the following conjecture.

Conjecture 1.5. *Let $A \subset \mathbb{R}$, be a large, finite set of numbers. If*

$$|(AA+1) \cap BC| \approx |AA|, \text{ and } |BC| \approx |AA|,$$

where B and C are also finite sets of numbers, then $\min\{|B|, |C|\} \lesssim 1$.

The next result is of a similar type, but in the setting of finite fields.

Theorem 1.6. *Let $A \subset \mathbb{F}_q$ such that the following two conditions hold:*

1. *There exists a real number $\epsilon > 0$ such that $|A||AA| \gtrsim q^{\frac{3}{2}+\epsilon}$.*
2. *There exists a real number $\delta > 0$ such that $|AA| \lesssim q^{1-\delta}$.*

Let G be any proper non-degenerate generalized geometric progression with $|G| \approx |AA|$. We have $|(AA+1) \setminus G| \gtrsim q^{\delta}$.

One should note that some condition like (2), the bound on $|AA|$, is necessary to avoid triviality. However, it is reasonable to expect that one can improve this result in either of two ways. First, condition (1), the bound on $|A||AA|$, could probably be lowered, and second, the bound on $|(AA+1) \setminus G|$ could probably be raised. As before, the proof will still work for some more general types of progressions. Again, see the Remark 2.3.

2. Proof of Theorem 1.2

The basic outline of the proof is to start with a given large, finite subset of $\mathbb{R}$. Then, with this set and any appropriate generalized geometric progression, we construct two large, finite sets of points in $\mathbb{R}^2$. We will then apply a recent result by Iosevich, Roche-Newton, and Rudnev regarding the set of dot products determined by our point sets, from [5]. The underlying arithmetic of the dot product set will allow us to compare the elements of the shifted product set to the elements of the progression.

The key ingredient to their proof is inspired by recent developments in the study of the Erdős distance problem. The classical Erdős distance problem asks for the minimum number of distinct distances which can be determined by any large, finite set of n points. The conjecture in the plane was that any such set must determine at least $n^{1-\epsilon}$ distinct distances, for any $\epsilon > 0$. Guth and Katz proved this in [3] with a blend of cell-decomposition and algebraic geometry, applied to an incidence problem in three dimensions. Shortly thereafter, Iosevich, Roche-Newton, and Rudnev, used similar techniques to prove a related result on the number of distinct dot products determined by such point sets in the plane. Specifically, they proved the following theorem.

Theorem 2.1. *Consider any large finite point sets $E, F \subset \mathbb{R}^2$ of n points each, neither of which is contained in a single line. Let $\Pi(E,F)$ denote the set of dot products $\Pi(E,F) = \{x \cdot y : x \in E, y \in F\}$. Then, for any $\epsilon > 0$, the number of distinct dot products is bounded below by $|\Pi(E,F)| \gtrsim n^{1-\epsilon}$.*

We now prove Theorem 1.2.

Proof. Fix any large finite set $A \subset \mathbb{R}$, and a real number $\delta > 0$. Let $G = G(g_0, R)$ be any non-degenerate generalized geometric progression with $|G| \approx |AA|$. Consider $R = R(r_0, r_1, \ldots, r_d, l_1, \ldots, l_d)$, the d-dimensional arithmetic progression defining the exponents of g_0 which make up G. Since G is non-degenerate, R must also be non-degenerate. We will define g_1 to be the "first element" of G, namely, $g_1 := g_0^{r_0}$. In what follows, we need to work with the normalized progression, G' which will be defined as

$$G' := \frac{G}{g_1} = \left\{ \frac{g}{g_1} : g \in G \right\}.$$

Notice that $|G| = |G'|$. Now, define the set B to be

$$B := \{g \in G' : gg \in G'\} = \{g \in G' : g = g_0^{x_1 r_1 + \cdots + x_d r_d}, x_j < l_j, x_j \in 2\mathbb{N}, j = 1, \ldots, d\}.$$

Claim 2.2. $|B| \approx |G|$.

Since $B \subset G'$, it is clear that $|B| \lesssim |G|$. Now we need only to show that $|B| \gtrsim |G|$. Notice that for an element to be in B, its square must be in G', hence the evenness condition on the x_j in the definition of B. So, we can count the number of elements in B by counting the number of elements of G' whose corresponding x_j are all even. By definition of the l_j, we get

$$|B| \geq \prod_{j=1}^{d} \left\lfloor \frac{l_j}{2} \right\rfloor \geq \prod_{j=1}^{d} \frac{l_j}{3} \geq \frac{|G|}{3^d}, \tag{2.1}$$

as $|G|$ is equal to the product of the l_j, and the claim is proved.

By Claim 2.2, $|B| \approx |G|$, so we have that $|BB| \approx |AA|$. Now, we construct E and F, finite subsets of $\mathbb{R}^2$,

$$E := \left\{(g_1 b, g_1 ba) \in \mathbb{R}^2 : b \in B, a \in A\right\}, \text{and } F := \left\{(b, ba) \in \mathbb{R}^2 : b \in B, a \in A\right\}.$$

These sets will have size $|E| = |F| = |A||B| \approx |A||G|$.

Remark 2.3. Note that the size estimate in Claim 2.2 could be satisfied by some slightly more general types of progressions. Specifically, as long as Claim 2.2 holds for progression G, we can get the desired result.

We will consider $\Pi(E, F)$, the set of distinct dot products determined by pairs in $E \times F$. Notice that

$$\begin{aligned} \Pi(E, F) &= \{(g_1 b, g_1 ba) \cdot (b', b'a') : a, a' \in A, b, b' \in B\} \\ &= \{g_1 bb'(aa' + 1) : a, a' \in A, b, b' \in B\} \\ &= g_1 BB(AA + 1) \subset G(AA + 1). \end{aligned}$$

By construction, $|\Pi(E, F)| = |g_1 BB(AA + 1)| \leq |G(AA + 1)|$.

Set $\epsilon = \delta/3$. Since $\epsilon > 0$, Theorem 2.1 gives us that

$$|\Pi(E,F)| \gtrsim |E|^{1-\epsilon} \gtrsim (|A||B|)^{1-\epsilon}.$$

Comparing upper and lower bounds on $|\Pi(E,F)|$ gives us

$$|G(AA+1)| \gtrsim (|A||B|)^{1-\epsilon}. \tag{2.2}$$

Our aim is to get a lower bound on the exceptional set $C := (AA+1) \setminus G$. From (2.2), we get

$$(|A||B|)^{1-\epsilon} \lesssim |G(AA+1)| = |G((G \cap (AA+1)) \cup C)| = |G(G \cap (AA+1)) \cup GC|.$$

Notice that the first term in the above union is a subset of GG, and therefore has size $\lesssim |G|$, by Proposition 1.1. So we can conclude that

$$|GC| \gtrsim (|A||B|)^{1-\epsilon} \approx (|A||G|)^{1-\epsilon},$$

which, by simple counting, gives us that

$$|C| \gtrsim \frac{(|A||G|)^{1-\epsilon}}{|G|} = |A|^{1-\epsilon}|G|^{-\epsilon}. \tag{2.3}$$

Again, by a simple counting argument, we see that $|A|^2 \gtrsim |AA|$. Since $|G| \approx |AA|$, we can rewrite (2.3) as

$$|C| \gtrsim |A|^{1-\epsilon}|G|^{-\epsilon} \gtrsim |A|^{1-\epsilon}|A|^{-2\epsilon} \gtrsim |A|^{1-\delta},$$

where the last line follows by definition of ϵ. □

3. Proof of Theorem 1.6

We follow a similar program to the proof of Theorem 1.2. Therefore, some details are omitted. The dot product set estimate in the finite field setting is in a slightly different form. It is due to Hart, Iosevich, Koh, and Rudnev. The statement of the theorem in [4] is for one set, but the proof works, with obvious modifications, for two sets. We consider the special case that both sets have the same size. For this section, define $\Pi(E,F)$ as before, except for subsets of $\mathbb{F}_q^2$ instead of $\mathbb{R}^2$. Also, let $\mathbb{F}_q^*$ denote the multiplicative group of $\mathbb{F}_q$.

Theorem 3.1. *Let $E, F \subset \mathbb{F}_q^d$ such that $|E| = |F| > q^{\frac{d+1}{2}}$. Then*

$$\mathbb{F}_q^* \subset \Pi(E,F) = \{x \cdot y : x \in E, y \in F\}.$$

Notice that the size condition in Theorem 3.1 is given with constant 1. This is why we include the ϵ in the size condition of Theorem 1.6, although a slightly more general statement is also true. Also, notice that we only use the case that $d = 2$.

Proof. Let $A \subset \mathbb{F}_q$ be given, and suppose that it satisfies the two size conditions:

1. There exists a real number $\epsilon > 0$ such that $|A||AA| \gtrsim q^{\frac{3}{2}+\epsilon}$.
2. There exists a real number $\delta > 0$ such that $|AA| \lesssim q^{1-\delta}$.

Now, let $G = G(g_0, R)$ be any non-degenerate generalized geometric progression with $|G| \approx |AA|$. Again, let

$$g_1 := g_0^{r_0}, G' := \frac{G}{g_1} = \left\{ \frac{g}{g_1} : g \in G \right\}, \text{ and } B := \{g \in G' : gg \in G'\}.$$

Claim 2.2 still holds in this context, so, as before, we have $|B| \approx |BB| \approx |AA|$. Now, we construct E and F, finite subsets of $\mathbb{F}_q^2$,

$$E := \left\{(g_1 b, g_1 ba) \in \mathbb{F}_q^2 : b \in B, a \in A\right\}, \text{and } F := \left\{(b, ba) \in \mathbb{F}_q^2 : b \in B, a \in A\right\}.$$

As in the proof of Theorem 1.2, the set of dot products determined by pairs in $E \times F$ will be

$$\Pi(E, F) = g_1 BB(AA + 1).$$

We also know that $|E| = |F| = |A||B| \approx |A||G|$. So, by the first size condition satisfied by A, and the fact that $|G| \approx |AA|$, we see that $|E| \gtrsim q^{\frac{3}{2}+\epsilon}$. Since E is large enough to satisfy the hypotheses of Theorem 3.1, we are guaranteed that $|\Pi(E, F)| \geq q - 1$. Specifically, using the proof of Theorem 1.2 as a guide, we get

$$q - 1 \leq |\Pi(E, F)| = |g_1 BB(AA + 1)| \leq |G(AA + 1)|. \tag{3.1}$$

We again seek a lower bound on the exceptional set. Define $C \subset \mathbb{F}_q$ to be $(AA + 1) \setminus G$. By (3.1), we get

$$q - 1 \leq |G(AA + 1)| = |G((G \cap (AA + 1)) \cup C)| \leq |G(G \cap (AA + 1)) \cup GC|$$

Again, the first term in the union will have size $\lesssim |G| \approx |AA|$. The second size condition satisfied by A tells us that $|AA| \lesssim q^{1-\delta}$, so the second term dominates. This gives us that $|GC| \approx q$, which, by simple counting and the fact that $|G| \approx |AA|$, yields

$$|C| \gtrsim \frac{q}{|AA|} = q^{\delta},$$

as claimed. □

noindent**Acknowledgment** I would like to thank the anonymous referee for the careful analysis and useful comments, which improved the final presentation.

References

[1] Gy. Elekes, *On the number of sums and products,* Acta Arith. **81** (1997), 365–367.

[2] M. Z. Garaev and C.-Y. Shen, *On the size of the set $A(A+1)$*, Mathematische Z. **265** (2010), 125–132.

[3] L. Guth and N. H. Katz, *On the Erdős distinct distance problem in the plane,* preprint, arXiv:1011:4015, (2010).

[4] D. Hart, A. Iosevich, D. Koh, and M. Rudnev, *Averages over hyperplanes, sum-product theory in finite fields, and the Erdős-Falconer distance conjecture,* Trans. Amer. Math. Soc. **363** (2011), 3255–3275.

[5] A. Iosevich, O. Roche-Newton, and M. Rudnev, *On an application of the Guth-Katz theorem*, Math. Res. Lett. **18** (2011), no. 4, 691-697.

[6] T. Jones and O. Roche-Newton, *Improved bounds on the set $A(A+1)$*, J. Combin. Theory Ser. A **120** (2013), 515–526

[7] M. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Grad. Texts in Math., Vol. 165, Springer-Verlag, 1996.

[8] J. Solymosi, *Bounding the multiplicative energy by the sumset*, Adv. Math., Volume 222, Issue 2, 1 October 2009, 402–408.

[9] E. Szemerédi and W. T. Trotter, Jr., *Extremal problems in discrete geometry,* Combinatorica **3** (1983), no. 3-4, 381–392.

[10] T. Tao and V. Vu, *Additive Combinatorics*. Cambridge Stud. Adv. Math., 2006.