A SUM-PRODUCT THEOREM IN FUNCTION FIELDS

THOMAS F. BLOOM AND TIMOTHY G. F. JONES

Abstract. Let $A$ be a finite subset of $\mathbb{F}_q((t^{-1}))$, the field of Laurent series in $1/t$ over a finite field $\mathbb{F}_q$. We show that for any $\epsilon > 0$ there exists a constant $C$ dependent only on $\epsilon$ and $q$ such that $\max\{|A + A|, |AA|\} \geq C|A|^{6/5-\epsilon}$.

In particular such a result is obtained for the rational function field $\mathbb{F}_q(t)$. Identical results are also obtained for finite subsets of the $p$-adic field $\mathbb{Q}_p$ for any prime $p$.

1. Introduction

Let $A$ be a non-empty finite subset of a ring. Consider the sumset

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

and the product set

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

It is conjectured that, provided $A$ does not contain ‘too many’ zero-divisors, at least one of $A + A$ or $AA$ must be large, in some sense to be discussed later, whenever $A$ is not close to being a subring. In this paper we make progress in this direction in the settings of global function fields and the $p$-adic numbers.

In what follows we say that $\delta$ is permissible for a collection of sets $\mathcal{A}$ if for all $A \in \mathcal{A}$ and $\epsilon > 0$

$$\max(|AA|, |A + A|) \gg \epsilon |A|^{1+\delta-\epsilon}.$$  

Erdős and Szemerédi [1983] conjectured that $1$ is permissible for all finite sets of integers. The best result towards this to date is due to Solymosi [2009], who showed that $1/3$ is permissible for all finite sets of real numbers. Konyagin and Rudnev [2012] have recently extended this result to the complex numbers. Previous results in the real and complex settings can be found in Elekes [1997], Ford [1998], Nathanson [1997], Solymosi [2005].

Much has also been achieved in the finite field setting. In a finite field of prime order, Bourgain et al. [2004] proved the existence of an absolute constant $\delta > 0$ which is permissible for all subsets of $\mathbb{F}_p$ that are not too close to being the entire field $\mathbb{F}_p$, for all primes $p$. More generally, Tao [2009] extended this result to general rings, covering all finite subsets that are not too close to being a subring.

Garaev made the Bourgain-Katz-Tao result explicit in two cases: when $|A| > p^{2/3}$ [Garaev, 2008] and when $|A| < p^{1/2}$ [Garaev, 2007]. The former estimate is sharp, but the latter has been subsequently improved [see Katz and Shen, 2008a, Shen, 2008, Bourgain and Garaev, 2009]. The most recent result is that $1/11$ is permissible for all sets $A \subset \mathbb{F}_p$ such that $|A| < p^{1/2}$, due to Rudnev [2012].

The authors are both supported by an EPSRC doctoral training grant.
Li and Roche-Newton [2011] built on a technique of Katz and Shen [2008b] to extend this estimate to any finite field, not necessarily of prime order, so long as $A$ is not too close to being a subfield.

In this paper we consider sum-product estimates for $\mathbb{F}_q((t^{-1}))$, the field of Laurent series over a finite field $\mathbb{F}_q$. We shall show that for subsets of such fields $1/5$ is permissible. Our methods also work for the $p$-adic setting so that $1/5$ is also permissible for any prime $p$ and finite subset of $\mathbb{Q}_p$. In particular, combined with the previous results over $\mathbb{R}$, this implies that $1/5$ is permissible for all finite subsets of any local field.

We indicate possible applications to constructions in theoretical computer science below, for which it is likely only an appeal to the theorem over $\mathbb{F}_q$ is necessary, which follows immediately since $\mathbb{F}_q[[t]] \subset \mathbb{F}_q((t^{-1}))$.

We will prove the following theorem.

**Theorem 1.1.** For any finite $A \subset \mathbb{F}_q((t^{-1}))$ and any $\epsilon > 0$ we have

$$|A + A|^3 |AA|^2 \gg q^{-1} |A|^{6-\epsilon}.$$ 

A sum-product result for $\mathbb{F}_q((t^{-1}))$ follows immediately.

**Corollary 1.2.** For any finite $A \subset \mathbb{F}_q((t^{-1}))$ and any $\epsilon > 0$ we have

$$\max \{|A + A|, |AA|\} \gg_{\epsilon,q} |A|^{1 + \frac{1}{5} - \epsilon}.$$ 

The sum-product exponent of $1/5$ for $\mathbb{F}_q((t^{-1}))$ lies between the $1/11$ known for finite fields and the $1/3$ known for $\mathbb{R}$. It is natural to conjecture that the correct answer for $\mathbb{F}_q((t^{-1}))$ is 1.

We remark that the dependence on $q$ cannot be removed, since $\mathbb{F}_q((t^{-1}))$ contains $\mathbb{F}_q$ as a subfield, which is closed under both addition and multiplication. This contrasts with the finite field setting for sum-products, where we think of $q$ as being large, as it is an upper bound for the cardinality of our sets. Clearly any finite field sum-product result for which the constants depended on $q$ would be meaningless, since we could write everything as $O_q(1)$.

Aside from their intrinsic interest these theorems may have applications to constructions in theoretical computer science. Sum-product results over finite fields have seen recent applications to extractors; see for example Bourgain [2005]. A key idea in these previous applications is the observation that a string of $n$ bits, that is, an element of $\mathbb{F}_2^n$, can be interpreted as an element of the field $\mathbb{F}_{2^n}$ so that the full power of the sum-product machinery can be brought to bear. An alternative is to interpret it as an element of $\mathbb{F}_2[t]$. Given that the sum-product results now available in $\mathbb{F}_2[t]$ are better than those in $\mathbb{F}_{2^n}$ (with an exponent of $1/5$ rather than $1/11$) we expect that constructions along a similar line to those in Bourgain [2005] will be quantitatively stronger over $\mathbb{F}_2[t]$ rather than $\mathbb{F}_{2^n}$.

For number theory and geometric applications it is worth pointing out that any global function field, that is, a field of transcendence degree 1 over a finite field, can be embedded into $\mathbb{F}_q((t^{-1}))$ for some $q$, where $q$ depends only on the field of constants and genus of the function field. In particular Theorem 1.1 will also hold for any finite subset of a global function field.

Finally, we remark that it is crucial to the result that the field of constants for $\mathbb{F}_q((t^{-1}))$ is finite. Obtaining a sum-product result in, say, $\mathbb{Q}(t)$ requires a different approach, and has been done with a non-explicit exponent by Croot and Hart [2010].
A SUM-PRODUCT THEOREM IN FUNCTION FIELDS

(whose methods would also likely lead to a sum-product result over \( \mathbb{F}_q(t) \) but almost certainly with a weaker exponent).

The proof is written in the language of \( \mathbb{F}_q((t^{-1})) \) for concreteness, but all that is required of the field we are working in is that it has a non-archimedean norm and furthermore has a finite residue field. In particular, the methods in this paper also prove the following sum-product theorem for the \( p \)-adic numbers \( \mathbb{Q}_p \), where nothing was previously known.

**Theorem 1.3.** For any prime \( p \), finite \( A \subset \mathbb{Q}_p \), and any \( \epsilon > 0 \) we have

\[
|A + A|^3 |AA|^2 \gg_{\epsilon, p} |A|^{6-\epsilon}.
\]

Finally, we remark that, if desired, the arguments that follow could be adapted to cover the case of partial sum and product sets, giving sum-product estimates in terms of the additive or multiplicative energy directly. For applications to exponential sums or theoretical computer science this approach via energy would be quantitatively stronger.

The approach used in this paper is based on a geometric argument used by Solymosi [2005a] in the complex numbers, coupled with some striking structural properties of non-archimedean geometry.

The next section provides more of the necessary background on function fields, and explains the structure of the proof and the rest of the paper.

## 2. Function fields

Let \( \mathbb{F}_q((t^{-1})) \) be the field of Laurent series over a finite field \( \mathbb{F}_q \) with \( q \) elements. Recall that elements of \( \mathbb{F}_q((t^{-1})) \) have the shape

\[
\sum_{i \leq N} a_i t^i,
\]

where \( a_i \in \mathbb{F}_q \), for some \( N \in \mathbb{Z} \). Throughout this paper \( q \) will be reserved for the size of \( \mathbb{F}_q \) and \( p \) for the characteristic of \( \mathbb{F}_q \), so that \( q \) is a power of \( p \).

There is a non-archimedean norm on \( \mathbb{F}_q((t^{-1})) \) given by \( \|x\| = q^{\deg x} \) where \( \deg \) is the familiar degree map; that is, if

\[
x = \sum_{i \leq N} a_i t^i
\]

and \( a_N \neq 0 \) then we say that \( \deg x = N \). We define \( \|0\| = 0 \). This has the crucial non-archimedean property

\[
\|x + y\| \leq \max(\|x\|, \|y\|)
\]

and furthermore \( \|x\| = \|-x\| \). Both of these properties will be used frequently without further mention in what follows. As a consequence of the non-archimedean property \( \mathbb{F}_q((t^{-1})) \) has an unusually rigid geometry, which will be exploited when proving sum-product estimates. A particular concern will be the behaviour of balls, which are sets of the form

\[
B(x, r) = \{ y \in \mathbb{F}_q((t^{-1})) : \|x - y\| \leq r \}.
\]

We will call \( r \in \mathbb{R} \) the radius of the ball \( B(x, r) \). The non-archimedean property implies the following result which is considered standard.
Lemma 2.1. If $B_1$ and $B_2$ are balls in $F_q((t^{-1}))$ then either they are disjoint, or $B_1 \subset B_2$, or $B_2 \subset B_1$. If in addition $B_1$ and $B_2$ have the same radius then either they are disjoint or $B_1 = B_2$.

Proof. Let $B_1 = B(x, r)$ and $B_2 = B(y, s)$. If there exists $a \in B(x, r) \cap B(y, s)$ then
\[ \|x - y\| \leq \max \{\|a - x\|, \|a - y\|\} \leq \max \{r, s\}. \]
If $r \leq s$ then this implies $B(x, r) \subset B(y, s)$ since if $b \in B(x, r)$ then
\[ \|y - b\| \leq \max \{\|y - x\|, \|b - x\|\} \leq \max \{r, s\} = s. \]
Conversely if $s \leq r$ then $B(y, s) \subset B(x, r)$. Hence if $r = s$ then $B(x, r) = B(y, s)$.  

The proof of Theorem 1.1 builds upon an approach of Solymosi [2005a] for sum-products in $\mathbb{C}$. When adapting this method, the non-archimedean geometry of function fields turns out to be a mixed blessing.

First, the bad news. Solymosi’s argument fails at a critical point in the function field setting, for the following reason. For each $a \in A$, let $a' \in A \setminus \{a\}$ be such that $\|a - a'\|$ is minimal, and let $B_a$ be the ball of radius $\|a - a'\|$ centred on $a$. Solymosi’s method uses the crucial fact that a single complex number can be contained in at most $O(1)$ of the $B_a$. This fails spectacularly in $F_q((t^{-1}))$, where an element could be contained in as many as $|A|$ of the $B_a$, as demonstrated by the following example: let $A = \{t^j : 0 \leq j \leq n\}$ so that $B_{t^j} = \{x \in F_q((t^{-1})) : |x| \leq q^j\}$ for $j \geq 1$ and $B_1 = B_{t^1}$, meaning that every one of the $|A|$ balls contains 0 as an element.

But all is not lost. In the example above, the astute reader will notice that $|A + A| \approx |A|^2$, and so a strong-sum product estimate holds despite the failure of Solymosi’s argument. In fact we will be able to show that something like this is possible whenever Solymosi’s argument fails, by considering a special type of structure to be defined in the following section: separable sets.

Separability is fairly unexciting in the complex setting, as it holds trivially for any non-empty finite set, but in the non-archimedean regime of function fields it is a stronger notion. The rigid geometry makes it harder to find separable sets, but where they do exist it will in fact imply the existence of large sumsets. The idea, therefore, is to show that a large separable set must exist whenever Solymosi’s argument fails. Combining this with an analysis of separable sets as having large sumsets will lead to a proof of Theorem 1.1.

In what follows, Section 3 analyses separable sets and shows that their sumsets have maximal growth. Section 4 then adapts Solymosi’s proof from [Solymosi 2005a] to establish that if $|A + A|$ and $|AA|$ are both small then there must exist a large separable set, and uses this to prove Theorem 1.1.

3. Separable sets

A finite set $A \subset F_q((t^{-1}))$ is separable if its elements can be indexed as
\[ A = \{a_1, \ldots, a_{|A|}\} \]
in such a way that for each \(1 \leq j \leq |A|\) there is a ball \(B_j\) with
\[ A \cap B_j = \{a_1, \ldots, a_j\}. \]

**Lemma 3.1.** If \(A \subset \mathbb{F}_q(\!(t^{-1})\!)\) is a finite separable set then
\[ |kA| \gg_k |A|^k \]
for any natural number \(k\).

**Proof.** Let \(E_k(A)\) denote the \(k\)-fold additive energy of \(A\), i.e. the number of solutions to
\[ a_1 + \ldots + a_k = b_1 + \ldots + b_k \]
with \(a_i, b_i \in A\). For \(x \in kA\) write \(\mu(x)\) for the number of solutions to
\[ x = a_1 + \ldots + a_k. \]
By the Cauchy-Schwarz inequality
\[ |A|^{2k} = \left( \sum_{x \in kA} \mu(x) \right)^2 \leq |kA|E_k(A) \]
and so it suffices to show that \(E_k(A) \ll_k |A|^k\).

Say that a solution \((a_1, \ldots, b_k)\) to \((\ref{1})\) is trivial if there are at most \(k\) distinct elements of \(A\) in \(\{a_1, \ldots, b_k\}\). By elementary counting there are at most \(O_k(|A|^k)\) trivial solutions, so it suffices to show that there are no non-trivial solutions.

Suppose for a contradiction that a non-trivial solution to \((\ref{1})\) exists. Gathering terms gives an expression of the form
\[ n_1c_1 + \ldots + ntc_t = 0 \]
where the \(c_i\) are distinct elements of \(A\) and \(n_i \in \mathbb{Z}\{0\}\). The assumption of non-triviality implies that \(t \geq 2\). Additionally, note that
\[ n_1 + \ldots + n_t = 0. \]
Indeed, after gathering terms on the left the different multiplicities \(n_i\) must sum to zero, since there are the same number of terms on the left of \((\ref{1})\) as on the right.

An easy calculation shows that since the solution is non-trivial there exists \(n_j\) such that \(|n_j| = 1\). Without loss of generality, let this be \(n_1\). Since \(A\) is separable and the \(c_i\) are in \(A\) we may relabel them if necessary to assume the existence of a ball \(B(x, r)\) such that \(c_1 \notin B\) but \(c_2, \ldots, c_t \in B\). By \((\ref{2})\),
\[ ||c_1 - x|| = ||n_1c_1 - n_1x|| = ||n_2c_2 + \ldots + n_tc_t + n_1x||. \]

By \((\ref{3})\) and the non-archimedean property it follows that
\[ ||c_1 - x|| = ||n_2(c_2 - x) + \ldots + n_t(c_t - x)|| \leq \max \{||c_2 - x||, \ldots, ||c_t - x||\} \leq r \]
and hence \(c_1 \in B(x, r)\) which is a contradiction, and the proof is complete. \(\square\)
4. Finding separable sets

The goal in this section is to show that if the sumset and product set of a set $A$ are both small then $A$ must contain a large separable set. For this we adapt the argument of Solymosi [2005a] for complex sum-products discussed in Section 2.

Note that all of the analysis remains in the $\mathbb{F}_q[t^{-1}]$ setting; indeed some of the facts of non-archimedean geometry deployed here are manifestly false in $\mathbb{C}$.

A couple of new definitions are required. For a finite set $A \subset \mathbb{F}_q[t^{-1}]$ and an element $a \in A$, define

$$r_A(a) = \min_{a' \in A \setminus \{a\}} |a - a'|$$

$$B_A(a) = B(a, r_A(a)).$$

Additionally, for any $n \geq 1$ we say that $C = (c_1, \ldots, c_n) \in A^n$ is an $A$-chain of length $n$ if $c_i \neq c_j$ for $1 \leq i < j \leq n$ and

$$B_A(c_1) \subset \cdots \subset B_A(c_n).$$

We will be rather cavalier about using $C$ for both a chain, an ordered tuple of elements from $A$, and the unordered set of such elements; which is intended will be clear from the context. The following argument, a strengthened form of that found in Solymosi [2005a], finds a large chain in $A$ as long as the sumset and partial product set are both small. If this condition were to fail then a suitable sum-product result would follow immediately.

**Lemma 4.1.** Let $A \subset \mathbb{F}_q[t^{-1}]$ be any finite set. Then $A$ contains an $A$-chain of cardinality at least

\[ |A|^5 \quad 2^7|A + A| |AA|^2 |(\log_2 |A|)|^3 \]

**Proof.** For each $a \in A$ write $N(a)$ for the maximal length $N$ of an $A$-chain $C = (c_1, \ldots, c_N)$ for which $c_N = a$. Note for future reference that

$$N(a) \leq |B_A(a) \cap A|$$

since if $C$ is such an $A$-chain then $C \subseteq A$ by definition and for each $c \in C$ we have $c \in B_A(c) \subseteq B_A(a)$.

It suffices to find $a \in A$ such that

$$N(a) \geq \frac{|A|^5}{2^7|A + A|^2 |AA|^2 |(\log_2 |A|)|^3}. $$

Begin with a dyadic pigeonholing. For each $0 \leq j \leq \log_2 |A|$ define $A_j$ to be the set of $a \in A$ for which $2^j \leq N(a) < 2^{j+1}$. The $A_j$ partition $A$ and so

$$\sum_{j=0}^{\log_2 |A|} |A_j| = |A|.$$

Hence there exists some $j_0$ for which $|A_{j_0}| \geq |A|/\log_2 |A|$. We shall show that

$$2^{j_0} \geq \frac{|A|^5}{2^7|A + A|^2 |AA|^2 |(\log_2 |A|)|^3}.$$
To this end, say that a pair \((a, c) \in A \times A\) is additively good if
\[
|(A + A) \cap (B_A(a) + c)| \leq \frac{2^{2h+3}|A + A|}{|A_j|}
\]
and that \((a, d) \in A \times A\) is multiplicatively good if
\[
|(AA) \cap (d \cdot B_A(a))| \leq \frac{2^{2h+3}|AA|}{|A_j|}.
\]

Say that a quadruple \((a, b, c, d) \in A^4\) is good if

(4) \(a \in A_j\).

(5) \(b \in B_A(a) \cap A\).

(6) \((a, c)\) is additively good.

(7) \((a, d)\) is multiplicatively good.

Write \(Q\) for the number of good quadruples. We shall bound \(Q\) from below to obtain
\[
Q \geq 2^{h-1}|A_j||A|^2
\]
and bound it from above to obtain
\[
Q \leq \frac{2^{2h+6}|A + A|^2|AA|^2}{|A_j|^2}.
\]

Comparing (8) and (9) will then give the required bound on \(2^h\) since \(|A_j| \geq |A|/\log_2 |A|\). Let’s first establish (8). For fixed \(c \in A\) we have
\[
\sum_{a \in A_j} |(A + A) \cap (B_A(a) + c)| = \sum_{a \in A_j} \sum_{u \in A + A} 1_{u \in B_A(a) + c}
\]
\[
= \sum_{v \in A + A - c} \sum_{a \in A_j} 1_{v \in B_A(a)}
\]
\[
= \sum_{v \in A + A - c} |C_j(v)|
\]
where \(C_j(v)\) is the set of \(a \in A_j\) with \(v \in B_A(a)\).

Observe that the elements of \(C_j(v)\) may be ordered to form an \(A\)-chain. This follows from Lemma 2.1 since for any two \(a, b \in C_j(v)\) we have \(v \in B_A(a) \cap B_A(b)\) and so either \(B_A(a) \subseteq B_A(b)\) or \(B_A(b) \subseteq B_A(a)\).

Now since \(C_j(v) \subseteq A_j\) and \(C_j(v)\) is an \(A\)-chain, there is an \(a \in A_j\) for which
\[
|C_j(v)| \leq N(a) \leq 2^{h+1}.
\]
We therefore have
\[
\sum_{a \in A_j} |(A + A) \cap (B_A(a) + c)| \leq 2^{h+1}|A + A|
\]
and hence
\[
|(A + A) \cap (B_A(a) + c)| \leq \frac{2^{2h+3}|A + A|}{|A_j|}
\]
holds for at least \(3|A_j|/4\) elements \(a \in A_j\). So for fixed \(c \in A\) there are at least \(3|A_j|/4\) elements \(a \in A_j\) for which \((a, c)\) is additively good.

By the same argument we may show that for fixed \(d \in A\) there are at least \(3|A_j|/4\) elements \(a \in A_j\) for which \((a, d)\) is multiplicatively good.
Thus for any $c \in A$ and $d \in A$ there are at least $|A_{j_{0}}|/2$ elements $a \in A_{j_{0}}$ for which $(a, c)$ is additively good and $(a, d)$ is multiplicatively good, i.e. for which conditions (6) and (7) hold. Furthermore for each such $a \in A_{j_{0}}$ there are at least $2^{j_{0}}$ elements $b \in A$ for which condition (5) holds, since

$$2^{j_{0}} \leq N(a) \leq |B_{A}(a) \cap A|.$$ 

In total therefore,

$$Q \geq |A|^2 |A_{j_{0}}| 2^{j_{0} - 1}$$

which concludes the proof of (8).

We now prove (9). Note that the map

$$(a, b, c, d) \mapsto (a + c, b + c, ad, bd)$$

is injective and so it suffices to bound the number of possibilities for this latter expression, subject to the constraint that $(a, b, c, d)$ is good. There are certainly at most $|A + A|$ possibilities for $a + c$ and at most $|AA|$ for $ad$, so it suffices to show that if these are fixed then there are at most $2^{j_{0} + 3}|A + A|/|A_{j_{0}}|$ possibilities for $b + c$ and at most $2^{j_{0} + 3}|AA|/|A_{j_{0}}|$ for $bd$.

First establish the bound on the number of $b + c$. Note that if $a + c = a' + c'$ then either

$$B_{A}(a) + c \subseteq B_{A}(a') + c'$$

or

$$B_{A}(a') + c' \subseteq B_{A}(a) + c$$

since both sets are balls with the same centre $a + c$.

As a consequence, if $G \subseteq A \times A$ is the set of additively good pairs $(a, c)$, then for any $x \in A + A$ there is a fixed additively good pair $(a_{x}, c_{x})$ such that

$$B_{A}(a) + c \subseteq B_{A}(a_{x}) + c_{x}$$

whenever $a + c = x$ and $(a, c)$ is additively good. Thus if $a + c = x$ is the fixed first co-ordinate and $b + c$ is a possible second co-ordinate then since $b \in B_{A}(a) \cap A$ and $c \in A$ we have

$$b + c \in (A + A) \cap (B_{A}(a) + c)$$

$$\subseteq (A + A) \cap (B_{A}(a_{x}) + c_{x}).$$

Since $(a_{x}, c_{x})$ is additively good, there are, as required, at most $2^{j_{0} + 3}|A + A|/|A_{j_{0}}|$ possibilities for $b + c$. The argument that there are at most at most $2^{j_{0} + 3}|AA|/|A_{j_{0}}|$ for $bd$ is similar.

In total therefore

$$Q \leq \frac{2^{2j_{0} + 6}|A + A|^2 |AA|^2}{|A_{j_{0}}|^2}$$

which concludes the proof of (9) and thus of the lemma. \[\square\]

The following result shows that any chain contains a large separable subset, allowing Lemma 3.1 to be applied to the large chain found in Lemma 4.1.

**Lemma 4.2.** If $C$ is the set of elements of an $A$-chain for some $A \subseteq \mathbb{F}_{q}((t^{-1}))$ then $C$ contains a separable set of cardinality at least $|C|/q$. 
Proof. It is clear that any subset \( \{c_1, \ldots, c_n\} \subset C \) with
\[
B_A(c_1) \subsetneq \ldots \subsetneq B_A(c_n).
\]
is separable. Define an equivalence relation on elements of \( A \) by \( a \sim b \) if and only if \( B_A(a) = B_A(b) \). To prove the lemma it suffices to show that each equivalence class contains at most \( q \) elements of \( A \).

Note first that if \( a \sim b \) and \( a \neq b \) then 
\[
\|a - b\| = r_A(a) = r_A(b).
\]
Indeed, since \( B_A(a) = B_A(b) \) it follows that \( b \in B_A(a) \) and so \( \|a - b\| \leq r_A(a) \). Similarly \( \|a - b\| = r_A(b) \).

Suppose for a contradiction that there is an equivalence class containing elements \( a_1, \ldots, a_{q+1} \). Consider the differences \( a_1 - a_i \) for \( 2 \leq i \leq q+1 \). By the last paragraph we have
\[
\|a_i - a_j\| = r_A(a_i) = r_A(a_j)
\]
for all \( 1 \leq i < j \leq q + 1 \). To complete the proof it suffices to show that there are distinct \( i, j \) and \( k \) in \( \{1, \ldots, q^d + 1\} \) such that
\[
\deg(a_i - a_j) < \deg(a_i - a_k),
\]
as this yields a contradiction to (10) by the definition of the norm \( \|\cdot\| \).

Consider the \( q \) distinct elements \( a_1 - a_i \) for \( 2 \leq i \leq q+1 \). Since none of these are 0 they have leading coefficient belonging to \( \mathbb{F}_q \setminus \{0\} \), and hence by the pigeonhole principle there are \( i \neq j \) such that \( a_1 - a_i \) and \( a_1 - a_j \) have the same leading coefficient.

It follows that if \( \deg(a_1 - a_i) = \deg(a_1 - a_j) \) then \( \deg(a_i - a_j) < \deg(a_1 - a_j) \). Hence either way there is a choice of distinct \( i, j \) and \( k \) such that (11) holds, completing the proof.

\( \square \)

Theorem 1.1 follows by combining Lemma 3.1 with Lemmata 4.1 and 4.2 as follows.

Proof of Theorem 1.1. Let
\[
K = \frac{|A|^5}{q|A + A|^2|A \cdot A|^2 \log^3 |A|}.
\]
By Lemmata 4.1 and 4.2 the set \( A \) contains a separable subset \( U \) of cardinality \( \Omega(K) \). For any natural number \( k \), Lemma 3.1 implies that
\[
|kA| \geq |kU| \gg_k K^k
\]
By Plünnecke’s inequality (see Petridis 2011 for a recent simple proof) we know that \( |kA| \ll_k \frac{|A + A|^k}{|A|^k} \) and so, after taking \( k \)-th roots,
\[
|A + A| \gg_k |A|^{1-1/k}K
\]
\[
= \frac{|A|^{6-1/k}}{q|A + A|^2|A \cdot A|^2 \log^3 |A|}
\]
Theorem 1.1 follows by taking \( k \) sufficiently large. \( \square \)
Acknowledgements

The authors would like to thank Oliver Roche-Newton, Misha Rudnev, and Trevor Wooley for reading earlier drafts of this paper and many helpful comments and corrections.

References

J. Bourgain. “On the construction of affine extractors” Geom. Funct. Anal. 17, no. 1 (2005): 33–57.
Bourgain, J. and M. Garaev. “On a variant of sum-product estimates and explicit exponential sum bounds in prime fields” Math. Proc. Cambridge Philos. Soc. 146, no. 1 (2009): 1–21.
Bourgain, J., N. Katz and T. Tao. “A sum-product estimate in finite fields and applications” Geom. Funct. Anal. 14, no. 1 (2004): 27–57.
Croot, E. and D. Hart. “On sums and products in $\mathbb{C}[x]$” Ramanujan J. 22, no. 1 (2010): 33–54.
G. Elekes. “On the number of sums and products” Acta. Arith. 81, no. 4 (1997): 365–367.
Erdős, P., and E. Szemerédi. “On sums and products of integers” Stud. Pure Math. (1983): 213–218.
Ford, K. “Sums and products from a finite set of real numbers” Ramanujan J. 2, no. 1-2 (1998): 59–66.
M. Garaev. “An explicit sum-product estimate in $\mathbb{F}_p$.” Int. Math. Res. Not. no. 11 (2007): 1–11.
M. Garaev. “The sum-product estimate for large subsets of prime fields” Proc. Amer. Math. Soc. 136, no. 8 (2008): 2735–2739.
Katz, N., and C. Shen. “A slight improvement to Garaev’s sum product estimate” Proc. Amer. Math. Soc. 136, no. 7 (2008a): 2499–2504.
Katz, N., and C. Shen. “Garaev’s inequality in finite fields not of prime order” Online J. Anal. Comb. no. 3 (2008b).
Konyagin, S., and M. Rudnev. “On new sum-product type estimates” preprint available at arXiv:1207.6785
Li, L. “Slightly improved sum-product estimates in fields of prime order” Acta Arith. 147, no. 2 (2011): 153–160.
Li, L., and O. Roche-Newton. “An improved sum-product estimate for general finite fields” SIAM J. Discrete Math. 25, no. 3 (2011): 1285–1296.
Petridis, G. “Plünnecke’s inequality” Combin. Probab. Comput. 20, no. 6 (2011): 921–938.
M. Nathanson. “On sums and products of integers” Proc. Amer. Math. Soc. 125, no. 1 (1997): 9–16.
M. Rudnev. “An improved sum-product inequality in fields of prime order” Int. Math. Res. Notices 16 (2012): 3693–3704.
C. Shen. “Quantitative sum product estimates on different sets” Electron. J. Combin. 15, no. 1 (2008).
Solymosi, J. “On sum-sets and product-sets of complex numbers” J. Théor. Nombres Bordeaux 17, no. 3 (2005a): 921–924.
Solymosi, J. “On the number of sums and products” Bull. London Math. Soc. 37, no. 4 (2005b): 491–494.
Solymosi, J. “Bounding multiplicative energy by the sumset” *Adv. Math.* 222, no. 2 (2009): 402–408.
Tao, T. “The sum-product phenomenon in arbitrary rings” *Contrib. Discrete Math.* 4, no. 2 (2009): 59–82.
Tao, T., and V. Vu. *Additive Combinatorics*, 1st ed. Cambridge University Press, 2006.

Department of Mathematics, University of Bristol, University Walk, Clifton, Bristol BS8 1TW, United Kingdom
E-mail address: matfb@bristol.ac.uk and tgf.jones@bristol.ac.uk