ON GROWTH OF THE SET \( A(A+1) \) IN ARBITRARY FINITE FIELDS

ALI MOHAMMADI

Abstract. Let \( F_q \) be a finite field of order \( q \), where \( q \) is a power of a prime. For a set \( A \subset F_q \), under certain structural restrictions, we prove a new explicit lower bound on the size of the product set \( A(A+1) \). Our result improves on the previous best known bound due to Zhelezov and holds under more relaxed restrictions.

Key words. expanders, additive energy, sum-product, finite fields.

AMS subject classifications. 11B75

1. Introduction. Let \( p \) denote a prime, \( F_q \) the finite field consisting of \( q = p^m \) elements and \( F_q^* = F_q \setminus \{0\} \). For sets \( A, B \subset F_q \), we define the sum set \( A + B = \{a + b : a \in A, b \in B\} \) and the product set \( AB = \{ab : a \in A, b \in B\} \). Similarly, we define the difference set \( A - B \) and the ratio set \( A/B \).

The sum-product phenomenon in finite fields is the assertion that for \( A \subset F_q \), the sets \( A + A \) and \( AA \) cannot both simultaneously be small unless \( A \) closely correlates with a coset of a subfield. A result in this direction is due to Li and Roche-Newton \([6]\), who showed that if \( |A \cap cG| \leq |G|^{1/2} \) for all subfields \( G \) and elements \( c \in F_q \), then

\[
\max\{|A + A|, |AA|\} \gg (\log |A|)^{-5/11} |A|^{1+1/11}.
\]

In the same spirit and under a similar structural assumption on the set \( A \), one expects that, for all \( \alpha \in F_q^* \), either of the product sets \( AA \) or \( (A+\alpha)(A+\alpha) \) must be significantly larger than \( A \). Zhelezov \([11]\) proved the estimate

\[
\max\{|AB|, |(A+1)\cdot C|\} \gtrsim |A|^{1+1/559},
\]

for sets \( A, B, C \subset F_q \), under the condition that

\[
|AB \cap cG| \leq |G|^{1/2}
\]

for all subfields \( G \) of \( F_q \) and elements \( c \in F_q \). Then, taking \( B = A \) and \( C = A + 1 \), under restriction (1.2), we have

\[
\max\{|AA|, |(A+1)(A+1)|\} \gtrsim |A|^{1+1/559}.
\]

For sets \( B_1, B_2, X \subset F_q^* \), we recall Plünnecke’s inequality (see Lemma 2.7)

\[
|B_1B_2| \leq \frac{|B_1X||B_2X|}{|X|}.
\]

From this we can deduce that

\[
|A(A+1)|^2 \geq |A| \cdot \max\{|AA|, |(A+1)(A+1)|\}.
\]

Hence, by (1.3), we have the estimate

\[
|A(A+1)| \gtrsim |A|^{1+\delta}
\]

1. Introduction. Let \( p \) denote a prime, \( F_q \) the finite field consisting of \( q = p^m \) elements and \( F_q^* = F_q \setminus \{0\} \). For sets \( A, B \subset F_q \), we define the sum set \( A + B = \{a + b : a \in A, b \in B\} \) and the product set \( AB = \{ab : a \in A, b \in B\} \). Similarly, we define the difference set \( A - B \) and the ratio set \( A/B \).

The sum-product phenomenon in finite fields is the assertion that for \( A \subset F_q \), the sets \( A + A \) and \( AA \) cannot both simultaneously be small unless \( A \) closely correlates with a coset of a subfield. A result in this direction is due to Li and Roche-Newton \([6]\), who showed that if \( |A \cap cG| \leq |G|^{1/2} \) for all subfields \( G \) and elements \( c \in F_q \), then

\[
\max\{|A + A|, |AA|\} \gg (\log |A|)^{-5/11} |A|^{1+1/11}.
\]

In the same spirit and under a similar structural assumption on the set \( A \), one expects that, for all \( \alpha \in F_q^* \), either of the product sets \( AA \) or \( (A+\alpha)(A+\alpha) \) must be significantly larger than \( A \). Zhelezov \([11]\) proved the estimate

\[
\max\{|AB|, |(A+1)\cdot C|\} \gtrsim |A|^{1+1/559},
\]

for sets \( A, B, C \subset F_q \), under the condition that

\[
|AB \cap cG| \leq |G|^{1/2}
\]

for all subfields \( G \) of \( F_q \) and elements \( c \in F_q \). Then, taking \( B = A \) and \( C = A + 1 \), under restriction (1.2), we have

\[
\max\{|AA|, |(A+1)(A+1)|\} \gtrsim |A|^{1+1/559}.
\]

For sets \( B_1, B_2, X \subset F_q^* \), we recall Plünnecke’s inequality (see Lemma 2.7)

\[
|B_1B_2| \leq \frac{|B_1X||B_2X|}{|X|}.
\]

From this we can deduce that

\[
|A(A+1)|^2 \geq |A| \cdot \max\{|AA|, |(A+1)(A+1)|\}.
\]

Hence, by (1.3), we have the estimate

\[
|A(A+1)| \gtrsim |A|^{1+\delta}
\]
with $\delta = 1/1118$, which holds under restriction (1.2) with $B = A$. Alternatively, by (1.1), with $B = A + 1$ and $C = A$, the estimate (1.4) holds with $\delta = 1/559$.

For large sets, $A \subset \mathbb{F}_q$ with $|A| \geq q^{1/2}$, Garaev and Shen [2] proved the bound

$$|A(A + 1)| \gg \min\{q^{1/2}|A|^{1/2}, |A|^2/q^{1/2}\}. \quad (1.5)$$

Furthermore, it was demonstrated in [2] that in the range $|A| > q^{2/3}$, the bound (1.5) is optimal up to the implied constant.

In the realm of small sets $A \subset \mathbb{F}_q$, with $|A| \ll p^{5/8}$, Stevens and de Zeeuw [9] obtained

$$|A(A + 1)| \gg |A|^{1+1/5}. \quad (1.6)$$

This result is based on a bound on incidences between points and lines in Cartesian products, proved in the same paper, which itself relies on a bound on incidences between points and planes due to Rudnev [8]. We point out that the main result of [8] has led to many quantitatively strong sum-product type estimates, however these estimates are restricted to sets of size smaller than $p$.

Our main result, stated below, relies on a somewhat more primitive approach towards the sum-product problem in finite fields, often referred to as the additive pivot technique. Specifically, we adopt our main tools and ideas from [4] and [6].

**Theorem 1.1.** Let $A \subseteq \mathbb{F}_q$. Suppose that

$$|A \cap cG| \ll \max\{|G|^{1/2}, |A|^{25/26}\} \quad (1.6)$$

for all proper subfields $G$ of $\mathbb{F}_q$ and elements $c \in \mathbb{F}_q$. Then for all $\alpha \in \mathbb{F}_q^*$, we have

$$|A(A + \alpha)| \gtrsim \min \left\{ |A|^{1+1/52}, q^{1/48}|A|^{1-1/48} \right\}. \quad (1.7)$$

Theorem 1.1 provides a quantitative improvement over the relevant estimates implied by (1.1) and holds under a more relaxed condition than those given by (1.2). It also improves on (1.5) in the range $q^{1/2} \leq |A| \lesssim q^{1/2+1/102}$.

Given a set $A \subset \mathbb{F}_q$, we define the additive energy of $A$ as the quantity

$$E_+(A) = |\{(a_1, a_2, a_3, a_4) \in A^4 : a_1 + a_2 = a_3 + a_4\}|. \quad (1.8)$$

As an application of Theorem 1.1, we record a bound on the additive energy of subsets of $\mathbb{F}_q$.

**Corollary 1.2.** Let $A \subseteq \mathbb{F}_q$. Suppose that

$$|A \cap cG| \ll \max\{|G|^{1/2}, |AA|^{50/53}\} \quad (1.7)$$

for all proper subfields $G$ of $\mathbb{F}_q$ and elements $c \in \mathbb{F}_q$. Then for any $\alpha \in \mathbb{F}_q^*$, we have

$$|A \cap (A - \alpha)| \lesssim |AA|^{1-1/53} + q^{-1/47}|AA|^{1+1/47}. \quad (1.8)$$

Consequently, under restriction (1.7), we have

$$E_+(A) \lesssim |A|^2(|AA|^{1-1/53} + q^{-1/47}|AA|^{1+1/47}). \quad (1.9)$$

**Asymptotic notation.** We use standard asymptotic notation. In particular, for positive real numbers $X$ and $Y$, we use $X = O(Y)$ or $X \ll Y$ to denote the existence of an absolute constant $c > 0$ such that $X \leq cY$. If $X \ll Y$ and $Y \ll X$, we write $X = \Theta(Y)$ or $X \asymp Y$. We also use $X \leq Y$ to denote the existence of an absolute constant $c > 0$, such that $X \ll (\log Y)^c Y$. 


2. Preparations. For $X \subset \mathbb{F}_q$, let $R(X)$ denote the quotient set of $X$, defined by

$$R(X) = \left\{ \frac{x_1 - x_2}{x_3 - x_4} : x_1, x_2, x_3, x_4 \in X, x_3 \neq x_4 \right\}.$$ 

We present a basic extension of [10, Lemma 2.50].

**Lemma 2.1.** Let $X \subset \mathbb{F}_q$ and $r \in \mathbb{F}_q^*$. If $r \not\in R(X)$, for any nonempty subsets $X_1, X_2 \subseteq X$, we have

$$|X_1| - |X_2| = |X_1 - rX_2|.$$ 

**Proof.** Consider the mapping $\phi : X_1 \times X_2 \rightarrow X_1 - rX_2$ defined by $\phi(x_1, x_2) = x_1 - rx_2$. Suppose that $(x_1, x_2), (y_1, y_2) \in X_1 \times X_2$ are distinct pairs satisfying $x_1 - rx_2 = y_1 - ry_2$. Then we get

$$r = \frac{x_1 - y_1}{x_2 - y_2},$$

which contradicts the assumption that $r \not\in R(X)$. We deduce that $\phi$ is injective, which in turn implies the required result. 

The next lemma, which appeared in [10, Corollary 2.51], is a simple corollary of Lemma 2.1.

**Lemma 2.2.** Let $X \subset \mathbb{F}_q$ with $|X| > q^{1/2}$, then $R(X) = \mathbb{F}_q$.

We have extracted Lemma 2.3, stated below, from the proof of the main result in [6].

**Lemma 2.3.** Let $X \subset \mathbb{F}_q$ be such that

$$1 + R(X) \subseteq R(X) \quad \text{and} \quad X \cdot R(X) \subseteq R(X).$$

Then $R(X)$ is the subfield of $\mathbb{F}_q$ generated by $X$.

The next result has been stated and proved in the proof of [7, Theorem 1].

**Lemma 2.4.** Let $X \subset \mathbb{F}_q$ with $|R(X)| \gg |X|^2$. Then there exists $r \in R(X)$ such that for any subset $X' \subset X$ with $|X'| \approx |X|$, we have

$$|X' + rX'| \gg |X|^2.$$ 

The following lemma enables us to extend our main result to sets which are larger than $q^{1/2}$. See [1, Lemma 3] for a proof.

**Lemma 2.5.** Let $X_1, X_2 \subset \mathbb{F}_q$. There exists an element $\xi \in \mathbb{F}_q^*$ such that

$$|X_1 + \xi X_2| \geq \frac{|X_1||X_2|\left(q - 1\right)}{|X_1||X_2| + \left(q - 1\right)}.$$ 

Next, we recall Ruzsa’s triangle inequality. See [10, Lemma 2.6] for a proof.

**Lemma 2.6.** Let $X, B_1, B_2$ be nonempty subsets of an abelian group. We have

$$|B_1 - B_2| \leq \frac{|X + B_1||X + B_2|}{|X|}.$$
In particular, for \( A \subseteq F_q^* \), by a multiplicative application of Lemma 2.6, we have the useful inequality

\[
|A/A| \leq \frac{|A(A + 1)|^2}{|A|}.
\]

In the next two lemmas we state variants of the Plünnecke-Ruzsa inequality, which can also be found in [5].

**Lemma 2.7.** Let \( X, B_1, \ldots, B_k \) be nonempty subsets of an abelian group. Then

\[
|B_1 + \cdots + B_k| \leq \frac{|X + B_1| \cdots |X + B_k|}{|X|^{k-1}}.
\]

**Lemma 2.8.** Let \( X, B_1, \ldots, B_k \) be nonempty subsets of an abelian group. For any \( 0 < \epsilon < 1 \), there exists a subset \( X' \subseteq X \) with \( |X'| \geq (1 - \epsilon)|X| \) such that

\[
|X' + B_1 + \cdots + B_k| \ll \epsilon \frac{|X + B_1| \cdots |X + B_k|}{|X|^{k-1}}.
\]

The following two lemmas are due to Jones and Roche-Newton [4].

**Lemma 2.9.** Let \( Z \subseteq F_q^* \). Suppose that \( X, Y \subseteq xZ + y \) for some \( x \in F_q^* \) and \( y \in F_q \). Fix \( 0 < \epsilon < 1/16 \). Then, \( (1-\epsilon)|X| \) elements of \( X \) can be covered by \( O_\epsilon \left( \frac{|Z(Z + 1)|^2 |Z/Z|}{|X||Y|^2} \right) \) translates of \( Y \). Similarly, \( (1-\epsilon)|X| \) elements of \( X \) can be covered by this many translates of \( -Y \).

**Lemma 2.10.** Let \( A \subseteq F_q^* \). There exists a subset \( A' \subseteq A \) with \( |A'| \approx |A| \) such that

\[
|A' - A'| \ll \frac{|A(A + 1)|^4 |A/A|^2}{|A|^5}.
\]

Next, we record a popularity pigeonholing argument. A proof is provided in [3, Lemma 9].

**Lemma 2.11.** Let \( X \) be a finite set and let \( f \) be a function such that \( f(x) > 0 \) for all \( x \in X \). Suppose that

\[
\sum_{x \in X} f(x) \geq K.
\]

Let \( Y = \{ x \in X : f(x) \geq K/2|X| \} \). Then

\[
\sum_{y \in Y} f(y) \geq \frac{K}{2}.
\]

Additionally, if \( f(x) \leq M \) for all \( x \in X \), then \( |Y| \geq K/(2M) \).

For sets \( X, Y \subseteq F_q \), we define the multiplicative energy between \( X \) and \( Y \) as the quantity

\[
E_X(X, Y) = |\{(x_1, x_2, y_1, y_2) \in X^2 \times Y^2 : x_1 y_1 = x_2 y_2\}|
\]

and write simply \( E_X(X) \) instead of \( E_X(X, X) \). For \( \xi \in Y/X \), let

\[
r_{Y/X}(\xi) = |\{(x, y) \in X \times Y : y/x = \xi\}|.
\]
Then, we have the identities
\begin{equation}
\sum_{\xi \in Y/X} r_{Y:X}(\xi) = |X||Y|,
\end{equation}
\begin{equation}
\sum_{\xi \in Y/X} r^2_{Y:X}(\xi) = E_\times(X, Y).
\end{equation}

By a simple application of the Cauchy-Schwarz inequality we have
\begin{equation}
E_\times(X, Y)|XY| \geq |X|^2|Y|^2.
\end{equation}

The remaining two lemmas together form the basis for the proof of Theorem 1.1. Lemma 2.13 is a slight generalisation of [7, Lemma 3].

**Lemma 2.12.** Let \(X, Y \subset F_q\) with \(|Y| \leq |X|\). There exists a set \(D \subseteq Y/X\) and an integer \(N \leq |Y|\) such that \(E_\times(X, Y) \ll (\log |X|)|D|N^2\) and \(|D|N < |X||Y|\). Also, for \(\xi \in D\) we have \(r_{Y:X}(\xi) \approx N\). Namely, the set of points
\[P = \{(x, y) \in X \times Y : y/x \in D\}\]
is supported on \(|D|\) lines through the origin, with each line containing \(\Theta(N)\) points of \(P\).

**Proof.** For \(j \geq 0\), let \(L_j = \{\xi \in Y/X : 2^j \leq r_{Y:X}(\xi) < 2^{j+1}\}\). Then, by (2.3), we have
\[\sum_{j=0}^{\log_2|X|} \sum_{\xi \in L_j} r^2_{Y:X}(\xi) = E_\times(X, Y)\]
By the pigeonhole principle there exists some \(N \geq 1\) such that, letting \(D = \{\xi \in Y/X : N \leq r_{Y:X}(\xi) < 2N\}\), we have
\[E_\times(X, Y) \ll \sum_{\xi \in D} r^2_{Y:X}(\xi) \ll |D|N^2\]
Furthermore, by (2.2), we have
\[|D|N \leq \sum_{\xi \in D} r_{Y:X}(\xi) \leq |X||Y|\]

**Lemma 2.13.** Let \(X, Y \subset F_q\). Suppose \(P \subset X \times Y\) is a set of points supported on \(L\) lines through the origin, with each line containing \(\Theta(N)\) points of \(P\), so that \(|P| \approx LN\). For \(x_s \in X\) and \(y_s \in Y\), we write \(Y_{x_s} = \{y \in Y : (x_s, y) \in P\}\) and \(X_{y_s} = \{x \in X : (x, y_s) \in P\}\). There exists a popular abscissa \(x_0\) and a popular ordinate \(y_0\), so that
\[|Y_{x_0}| \gg \frac{LN}{|X|} \quad |X_{y_0}| \gg \frac{LN}{|Y|}\]
For \(\xi \in F_q\), we write \(P_\xi = \{x : (x, \xi x) \in P\}\). There exists a subset \(\widetilde{Y}_{x_0} \subseteq Y_{x_0}\) with
\begin{equation}
|\widetilde{Y}_{x_0}| \gg \frac{L^2N^2}{|X|^2|Y|},
\end{equation}
such that for every \(z \in \widetilde{Y}_{x_0}\), we have
\begin{equation}
|P_{z/x_0} \cap X_{y_0}| \gg \frac{L^2N^3}{|X|^2|Y|^2}.
\end{equation}
Proof. Observing that
\[ \sum_{y \in Y} |X_y| = |P| \approx LN, \]
by Lemma 2.11, there exists a subset \( Y' \subseteq Y \) such that, for all \( y \in Y' \), we have \( |X_y| \gg LN/|Y| \). Let \( P' = \{(x, y) \in P : y \in Y'\} \) so that \( |P'| \gg LN \). Then
\[ \sum_{x \in X} |Y_x \cap Y'| = \sum_{y \in Y'} |X_y| = |P'| \gg LN. \]

By Lemma 2.11, there exists a subset \( X' \subseteq X \) such that for all \( x \in X' \) we have
\[ |Y_x \cap Y'| \gg LN/|X|. \] (2.7)

Letting \( P'' = \{(x, y) : x \in X'\} \), we have \( |P''| \gg LN \).

Let \( D = \{y/x : (x, y) \in P''\} \) and let \( D' \subseteq D \) denote the set of elements \( \xi \) such that the lines \( L_\xi \), determined by \( \xi \), each contain \( \Omega(N) \) points of \( P'' \). It follows by Lemma 2.11 that \( |D'| \gg L \). Now, we proceed to establish a lower bound on the sum
\[ \Sigma = \sum_{(x, y) \in X' \times Y'} \sum_{z \in Y_x} |P_{z/x} \cap X_y|. \] (2.8)

We write \( z \sim x \), if \((x, z)\) is a point of \( P \). Then
\[ \Sigma \gg \sum_{(x, y) \in X' \times Y'} \sum_{z \sim x} |P_{z/x} \cap X_y| \]
\[ \gg N \sum_{\xi \in D'} \sum_{y \in Y'} |P'_\xi \cap X_y|. \]

For a fixed \( \xi \in D' \), the inner sum may be bounded by the observation that
\[ \sum_{y \in Y'} |P'_\xi \cap X_y| = \sum_{x \in P'_\xi} |Y_x \cap Y'|. \]

Recall that \( |D'| \gg L \) and that for \( \xi \in D' \), we have \( |P'_\xi| \gg N \). Then, by (2.7), we have
\[ \Sigma \gg N \cdot L \cdot N \cdot \frac{LN}{|X|}. \]

By the pigeonhole principle, applied to (2.8), there exist \((x_0, y_0) \in X' \times Y'\) such that
\[ \sum_{z \in Y_{x_0}} |P_{z/x_0} \cap X_{y_0}| \gg \frac{L^2 N^3}{|X|^2 |Y|}. \]

By our assumption, that every line through the origin contains \( O(N) \) points of \( P \), it follows that for all \( z \in Y \), we have \( |P_{z/x_0}| \ll N \). Then, letting \( Y_{x_0} \subseteq Y_{x_0} \) to denote the set of \( z \in Y_{x_0} \) with the property that
\[ |P_{z/x_0} \cap X_{y_0}| \gg \frac{L^2 N^3}{|X|^2 |Y|^2}, \]
by Lemma 2.11, we have
\[ |Y_{x_0}| \gg \frac{L^2 N^2}{|X|^2 |Y|}. \] \( \blacksquare \)
3. Proof of Theorem 1.1. It suffices to prove the required result for $\alpha = 1$. Then the general statement immediately follows since under condition (1.6) the set $A$ can be replaced by any of its dilates $cA$, for $c \in \mathbb{F}_q^*$. Without loss of generality assume $0 \notin A$. By Lemma 2.10, combined with (2.1), there exists a subset $A' \subseteq A$, with $|A'| \approx |A|$, such that

$$|A' - A'| \ll \frac{|A(A + 1)|^8}{|A|^7}.$$  

By Lemma 2.8 there exists a further subset $A'' \subseteq A'$, with $|A''| \approx |A'|$, such that

$$|A'' - A' - A'' - A''| \ll \frac{|A' - A'|^3}{|A|^2}.$$  

Since $|A''| \approx |A|$, we reset the notation $A''$ back to $A$ and henceforth assume the inequalities

$$|A - A| \ll \frac{|A(A + 1)|^8}{|A|^7},$$

$$|A - A - A - A| \ll \frac{|A(A + 1)|^{24}}{|A|^{23}}.$$  

We apply Lemma 2.12 to identify a set $D \subseteq A/(A + 1)$ and an integer $N \geq 1$ such that for $\xi \in D$ we have $r_{A,(A+1)}(\xi) \approx N$. Additionally, letting $L = |D|$, in view of (2.4), we have

$$M := LN^2 \gg \frac{E_x(A+1,A)}{\log |A|} \geq \frac{|A|^4}{|A(A+1)||\log |A||}.$$  

We define $P \subseteq (A + 1) \times A$ by

$$P = \{(x, y) \in (A + 1) \times A : y/x \in D\}.$$  

Then $|P| \approx LN$. Now, since $LN < |A|^2$ and $N < |A|$, we get

$$N, L > \frac{M}{|A|^2}.$$  

For $\xi \in D$, we define the projection onto the $x$-axis of the line with slope $\xi$ as

$$P_\xi = \{x : (x, \xi x) \in P\} \subset A + 1.$$  

Similarly for $\lambda \in D^{-1}$ let

$$Q_\lambda = \{y : (\lambda y, y) \in P\} \subset A.$$  

Then for $\xi \in D$ and $\lambda \in D^{-1}$, we have

$$|P_\xi|, |Q_\lambda| \approx N, \quad \xi P_\xi \subset A \quad \text{and} \quad \lambda Q_\lambda \subset A + 1.$$  

By Lemma 2.13, with $X = A + 1$ and $Y = A$, there exists a pair of elements $(x_0, y_0) \in (A + 1) \times A$ such that the sets $A_{x_0} \subseteq A$ and $B_{y_0} \subseteq A + 1$ satisfy

$$|A_{x_0}|, |B_{y_0}| \gg \frac{LN}{|A|}, \quad x_0^{-1}A_{x_0} \subset D \quad \text{and} \quad y_0^{-1}B_{y_0} \subset D^{-1}.$$
Moreover, there exists a further subset $\tilde{A}_{x_0} \subseteq A_{x_0}$, with

\begin{equation}
|\tilde{A}_{x_0}| \gg \frac{LM}{|A|^3},
\end{equation}

such that for all $z \in \tilde{A}_{x_0}$, letting $S_z = P_{z/x_0} \cap B_{y_0}$, we have

\begin{equation}
|S_z| \gg \frac{LMN}{|A|^4}.
\end{equation}

We require the following corollary of Lemma 2.9 throughout the remainder of the proof.

**Claim 3.1.** For $n \leq 4$ let $a_1, \ldots, a_n$ denote arbitrary elements of $\tilde{A}_{x_0}$. Given any set $C \subseteq A + 1$, there exists a subset $C' \subseteq C$, with $|C'| \approx |C|$, such that the sets $a_iC'$ can each be covered by

\begin{equation}
O\left(\frac{|A(A + 1)|^4}{|C||A|^N}ight)
\end{equation}

translates of $\pm x_0 A$.

Suppose $b_1, \ldots, b_4 \in B_{y_0}$. Let

\begin{equation}
\Gamma := \frac{|A|^2|A(A + 1)|^4}{M^2}.
\end{equation}

There exists a subset $A' \subseteq \tilde{A}_{x_0}$, with $|A'| \approx |\tilde{A}_{x_0}|$, such that for $1 \leq i \leq 4$ the sets $b_i A'$ can each be covered by $O(\Gamma)$ translates of $\pm y_0 A$.

**Proof.** We apply Lemma 2.9, with $X = a_iC$, $Y = a_i P_{a_i/x_0}$, $Z = A$, $x = a_i$, $y = a_i$ and $0 < \epsilon < 1/16$. Then there exist sets $C_{a_i} \subseteq C$ with $|C_{a_i}| \geq (1 - \epsilon)|C|$ such that each of $a_i C_{a_i}$ can be covered by

\begin{equation}
O\left(\frac{|A(A + 1)|^2|A/A|}{|C||a_i P_{a_i/x_0}|^2}ight)
\end{equation}

translates of $a_i P_{a_i/x_0} \subseteq x_0 A$ and by at most as many translates of $-x_0 A$. Let $C' = C_{a_1} \cap \cdots \cap C_{a_n}$, so that $|C'| \geq (1 - n\epsilon)|C| \geq (3/4)|C|$. Then, by (2.1) and (3.5), it follows that (3.9) denotes the number of translates of $\pm x_0 A$ required to cover the sets $a_i C'$ for $1 \leq i \leq n$.

Next, we apply Lemma 2.9, with $X = b_i \tilde{A}_{x_0}$, $Y = b_i Q_{b_i/y_0}$, $Z = A$, $x = b_i$ and $y = 0$. Recalling (3.5), (3.6), (3.7) and proceeding similarly as above, we can identify a subset $A' \subseteq \tilde{A}_{x_0}$, with $|A'| \approx |\tilde{A}_{x_0}|$, such that the sets $b_i A'$ are each fully contained in $O(\Gamma)$ translates of $\pm y_0 A$.

We proceed to split the proof into four cases based on the nature of the quotient set $R(\tilde{A}_{x_0})$.

**Case 1:** $R(\tilde{A}_{x_0}) \neq R(B_{y_0})$.

**Case 1.1:** There exist elements $a, b, c, d \in \tilde{A}_{x_0}$ such that

$$r = \frac{a - b}{c - d} \in R(\tilde{A}_{x_0}) \nsubseteq R(B_{y_0}).$$
By Lemma 2.1, for any subset \( Y \subseteq B_{y_0} \) with \(|Y| \approx |B_{y_0}|\), we have
\[
(3.11) \quad |B_{y_0}|^2 \approx |Y|^2 = |Y - rY| = |aY - bY - cY + dY|.
\]
By Claim 3.1 and (3.6), there exists a subset \( B' \subseteq B_{y_0} \), with \(|B'| \approx |B_{y_0}|\), such that \( dB' \) is contained in
\[
O\left(\frac{|A(A+1)|^4}{LN^3}\right)
\]
translates of \(-x_0A\) and \(aB', bB', cB'\) are contained in at most the same number of translates of \(x_0A\). Thus, setting \( Y = B' \), by (3.11), we have
\[
\left(\frac{LN}{|A|}\right)^2 \ll |A - A - A|\left(\frac{|A(A+1)|^4}{LN^3}\right)^4.
\]
Then, by (3.2), we get
\[
M^6N^2|A|^{21} \ll |A(A+1)|^{40}.
\]
By (3.3) and (3.4), we conclude the inequality
\[
|A(A+1)|^{48} \gg (\log |A|)^{-8}|A|^{49}.
\]

**Case 1.2:** There exist elements \( a, b, c, d \in B_{y_0} \), such that
\[
r = \frac{a - b}{c - d} \in R(B_{y_0}) \not\subseteq R(\hat{A}_{x_0}).
\]
Then for any subset \( Y \subseteq \hat{A}_{x_0} \) with \(|Y| \approx |\hat{A}_{x_0}|\), by Lemma 2.1, we have
\[
(3.12) \quad |\hat{A}_{x_0}|^2 \approx |Y|^2 = |Y - rY| = |aY - bY - cY + dY|.
\]
By Claim 3.1, there exists a subset \( A' \subseteq \hat{A}_{x_0} \), with \(|A'| \approx |\hat{A}_{x_0}|\), such that the sets \(aA', bA'\) and \(cA'\) are each fully contained in \(O(\Gamma)\) translates of \(y_0A\) and \(dA'\) can be covered by \(O(\Gamma)\) translates of \(y_0A\). Thus, setting \( Y = A' \), by (3.12), we have
\[
\left(\frac{LM}{|A|^3}\right)^2 \ll |A - A - A|\left(\frac{|A|^2|A(A+1)|^4}{M^2}\right)^4.
\]
Applying (3.2) yields
\[
M^{10}L^2|A|^{9} \ll |A(A+1)|^{40}.
\]
Hence, by (3.3) and (3.4), we get
\[
|A(A+1)|^{52} \gg (\log |A|)^{-12}|A|^{53}.
\]

**Case 2:** \( 1 + R(\hat{A}_{x_0}) \not\subseteq R(\hat{A}_{x_0}) \). There exist elements \( a, b, c, d \in \hat{A}_{x_0} \) such that
\[
r = 1 + \frac{a - b}{c - d} \not\in R(\hat{A}_{x_0}) = R(B_{y_0}).
\]
Let \( Y_1 \subseteq B_{y_0} \) and \( Y_2 \subseteq S_a \) be any sets with \(|Y_1| \approx |B_{y_0}|\) and \(|Y_2| \approx |S_a|\). By Lemma 2.8, with \( X = (c - d)Y_1 \), there exists a subset \( Y'_1 \subseteq Y_1 \), with \(|Y'_1| \approx |Y_1|\), such that
\[
(3.13) \quad |Y'_1 - rY_2| = |(c - d)Y'_1 - (c - d)Y_2 - (a - b)Y_2| \ll \frac{|Y_1 - Y_2|}{|Y_1|}|(c - d)Y_1 - (a - b)Y_2|.
\]
Recall that $Y_1' \subseteq B_{y_0}$ and $Y_2 \subseteq S_a \subseteq B_{y_0}$. Then Lemma 2.1 gives
\[ |Y_1'||Y_2| = |Y_1' - rY_2|. \]
Thus, by (3.13) we have
\[ (3.14) \quad |Y_1'||Y_2| \ll |Y_1 - Y_2||cY_1 - dY_1 - aY_2 + bY_2|. \]
Since $Y_1, Y_2 \subseteq B_{y_0} \subseteq A + 1$, we have
\[ |Y_1 - Y_2| \leq |A - A|. \]
Recall that $|Y_1'| \approx |Y_1| \approx |B_{y_0}|$ and $|Y_2| \approx |S_a|$. Then by (3.6), (3.8) and noting that $aY_2 \subseteq x_0A$, we have
\[ (3.15) \quad \left( \frac{LN}{|A|} \right)^2 \left( \frac{LMN}{|A|^4} \right) \ll |A - A||cY_1 - dY_1 - x_0A + bY_2|. \]
Now, by Claim 3.1, there exist positively proportioned subsets $B_{y_0}' \subseteq B_{y_0}$ and $S_a' \subseteq S_a$ such that $cB_{y_0}'$ and $dB_{y_0}'$ can be covered by
\[ O\left( \frac{|A(A+1)|^4}{LN^3} \right) \]
translates of $x_0A$ and $bS_a'$ can be covered by
\[ O\left( \frac{|A|^3|A(A+1)|^4}{LMN^3} \right) \]
translates of $-x_0A$. Thus, setting $Y_1 = B_{y_0}'$ and $Y_2 = S_a'$, by (3.15) it follows that
\[ \left( \frac{LN}{|A|} \right)^2 \left( \frac{LMN}{|A|^4} \right) \ll |A - A||A - A - A - A| \left( \frac{|A|^3|A(A+1)|^4}{LMN^3} \right) \left( \frac{|A(A+1)|^4}{LN^3} \right)^2. \]
Using (3.1) and (3.2), this is further reduced to
\[ M^8|A|^{21} \ll |A(A+1)|^{44}. \]
Thus, by (3.3), we get
\[ |A(A+1)|^{52} \gg (\log |A|)^{-8}|A|^{53}. \]

**Case 3: $x_0^{-1}\hat{A}_{x_0}. R(\hat{A}_{x_0}) \not\subseteq R(\hat{A}_{x_0})$.** There exist elements $a, b, c, d, e \in \hat{A}_{x_0}$ such that
\[ r = \frac{a - b - c}{x_0 d - e} \not\in R(\hat{A}_{x_0}) = R(B_{y_0}). \]
Given any set $Y_1 \subseteq B_{y_0}$, recalling that $S_a \subseteq B_{y_0}$, it follows from Lemma 2.1 that
\[ |Y_1||S_a| = |Y_1 - rS_a|. \]
For an arbitrary set $Y_2$, we apply Lemma 2.7, with $X = \frac{b - c}{d - e}Y_2$, to get
\[ |Y_2||Y_1||S_a| = |Y_2||Y_1 - rS_a| \]
\[ \leq Y_1 + \frac{b - c}{d - e}Y_2 \left| Y_2 - \frac{a}{x_0}S_a \right| \]
\[ \leq |dY_1 - cY_1 + bY_2 - cY_2||Y_2 - A|. \]
By Claim 3.1, we can identify sets $C_1 \subseteq S_d$ and $C_2 \subseteq P_{c/x_0}$ with $|C_1| \approx |S_d|$ and $|C_2| \approx |P_{c/x_0}| \approx N$, such that $eC_1$ is covered by

$$O\left(\frac{|A|^3|A(A+1)|^4}{LMN^3}\right)$$

translates of $x_0A$ and $bC_2$ is covered by

$$O\left(\frac{|A(A+1)|^4}{|A|^3}\right)$$

translates of $-x_0A$. We set $Y_1 = C_1$ and $Y_2 = C_2$. Then, by (3.5), (3.8) and particularly noting that $dY_1, cY_2 \subset x_0A$ and $Y_2 \subset A + 1$, we have

$$N\left(\frac{LMN}{|A|^4}\right)^2 \ll |A - A||A - A - A|\left(\frac{|A|^3|A(A+1)|^4}{LMN^3}\right)\left(\frac{|A(A+1)|^4}{|A|^3}\right).$$

Using (3.1) and (3.2) we get

$$M^6N^3|A|^{20} \ll |A(A+1)|^{40}.$$ 

By (3.3) and (3.4), we conclude

$$|A(A+1)|^{49} \gg (\log |A|)^{-9}|A|^{50}.$$

**Case 4:** Suppose that Cases 1-3 do not happen. Observing that $R(x_0^{-1} \tilde{A}_{x_0}) = R(\tilde{A}_{x_0})$, by Lemma 2.3 we deduce that $R(\tilde{A}_{x_0})$ is the field generated by $x_0^{-1} \tilde{A}_{x_0}$. Then according to the assumptions of Theorem 1.1, we consider the following three cases.

**Case 4.1:** $R(\tilde{A}_{x_0}) = \mathbb{F}_q$ and $|\tilde{A}_{x_0}| > q^{1/2}$. Let $Y$ denote an arbitrary subset of $\tilde{A}_{x_0}$ with $|Y| \approx |\tilde{A}_{x_0}|$. By Lemma 2.5, there exists an element $\xi \in \mathbb{F}_q^*$ such that $q \ll |Y + \xi Y|$. Since $R(B_{y_0}) = R(\tilde{A}_{x_0}) = \mathbb{F}_q$, there exist elements $a, b, c, d \in B_{y_0}$, such that

$$q \ll |aY - bY + cY - dY|.$$

By Claim 3.1, we can identify a positively proportioned subset $A' \subset \tilde{A}_{x_0}$, such that $aA'$, $bA'$ and $dA'$ can be covered by $O(\Gamma)$ translates of $y_0A$ and $cA'$ can be covered by $O(\Gamma)$ translates of $-y_0A$. Thus, setting $Y = A'$, we have

$$q \ll |A - A - A - A|\left(\frac{|A|^2|A(A+1)|^4}{M^2}\right)^4.$$

By (3.2), we get

$$M^8|A|^{15}q \ll |A(A+1)|^{40}.$$ 

By (3.3), this gives the bound

$$|A(A+1)|^{48} \gg q(\log |A|)^{-8}|A|^{47}.$$

We point out that if $|\tilde{A}_{x_0}| > q^{1/2}$ then one only needs to consider Cases 1.1 and 4.1, since by Lemma 2.2 we have $R(\tilde{A}_{x_0}) = \mathbb{F}_q$. 


Case 4.2: Either $R(\tilde{A}_{x_0}) = \mathbb{F}_q$ and $|\tilde{A}_{x_0}| \leq q^{1/2}$ or $R(\tilde{A}_{x_0})$ is a proper subfield and $|A \cap cR(\tilde{A}_{x_0})| \ll |R(\tilde{A}_{x_0})|^{1/2}$ for all $c \in \mathbb{F}_q$. Since $R(\tilde{A}_{x_0})$ is the field generated by $x_0^{-1}\tilde{A}_{x_0}$, we have $\tilde{A}_{x_0} \subseteq x_0 R(\tilde{A}_{x_0})$. Hence

$$|\tilde{A}_{x_0}|^2 = |\tilde{A}_{x_0} \cap x_0 R(\tilde{A}_{x_0})|^2 \leq |A \cap x_0 R(\tilde{A}_{x_0})|^2 \ll |R(\tilde{A}_{x_0})|.$$ 

Now, recalling that $R(\tilde{A}_{x_0}) = R(B_{y_0})$, by Lemma 2.4, there exist elements $a, b, c, d \in B_{y_0}$ such that for any subset $Y \subseteq \tilde{A}_{x_0}$ with $|Y| \approx |\tilde{A}_{x_0}|$, we have

$$(3.16) \quad |Y|^2 \ll |aY - bY + cY - dY|.$$ 

By Claim 3.1, there exists a subset $A' \subseteq \tilde{A}_{x_0}$, with $|A'| \approx |\tilde{A}_{x_0}|$, such that $cA'$ can be covered by $O(\Gamma)$ translates of $-y_0 A$ and $aA', bA', dA'$ can be covered by $O(\Gamma)$ translates of $y_0 A$. We set $Y = A'$ so that, by (3.16), we obtain

$$\left(\frac{LM}{|A|^3}\right)^2 \ll |A - A - A - \left(\frac{|A|^2 A(A + 1)|^4}{M^2}\right)^4.$$ 

Applying (3.2) gives

$$M^{10} L^2 |A|^9 \ll |A(A + 1)|^{40}.$$ 

Then, by (3.3) and (3.4), we have

$$|A(A + 1)|^{52} \gg (\log |A|)^{-12} |A|^{53}.$$ 

Case 4.3: $R(\tilde{A}_{x_0})$ is a proper subfield and $|A \cap x_0 R(\tilde{A}_{x_0})| \ll |A|^{25/26}$. Recall that $\tilde{A}_{x_0} \subseteq x_0 R(\tilde{A}_{x_0})$. Then, by (3.7) and (3.4), we get

$$\frac{M^2}{|A|^5} \ll |\tilde{A}_{x_0}| \ll |A|^{25/26}.$$ 

Using (3.3), we recover the bound

$$|A(A + 1)|^{52} \gg (\log |A|)^{-52} |A|^{53}.$$ 

4. Proof of Corollary 1.2. Let $\alpha \in \mathbb{F}_q^*$ and denote $S = A \cap (A - \alpha)$. Observing that $S, S + \alpha \subseteq A$, we deduce $|S(S + \alpha)| \leq |AA|$. Then, estimate (1.8) follows by applying Theorem 1.1 to the set $S$. Now, since $S \subseteq A$, if $A$ satisfies restriction (1.7), then $S$ can fail to satisfy restriction (1.6) only if $|S| \ll |AA|^{52/53}$, which in fact gives the required estimate. This concludes the proof of estimate (1.8).

Next, noting that

$$|A \cap (A - \alpha)| = |\{(a_1, a_2) \in A^2 : a_1 - a_2 = \alpha\}|,$$

similarly to (2.2) and (2.3), we have the identities

$$|A|^2 = \sum_{\alpha \in A - A} |A \cap (A - \alpha)| \quad \text{and} \quad E_+(A) = \sum_{\alpha \in A - A} |A \cap (A - \alpha)|^2.$$ 

In particular, it follows that

$$E_+(A) \ll |A|^2 \cdot \max_{\alpha \in \mathbb{F}_q^*} |A \cap (A - \alpha)|.$$ 

Thus the required bound on $E_+(A)$ follows from (1.8).
Acknowledgments. The author would like to thank Igor Shparlinski for helpful conversations.

REFERENCES

[1] J. Bourgain and A. Glibichuk, ‘Exponential sum estimates over a subgroup in an arbitrary finite field’, J. Anal. Math., 115(1) (2011), 51–70.
[2] M. Z. Garaev and C.-Y. Shen, ‘On the size of the set $A(A + 1)$’, Mathematische Zeitschrift, 265(1) (2010), 125–132.
[3] T. G. F. Jones, ‘Explicit incidence bounds over general finite fields’, Acta Arith., 150(3) (2011), 241–262.
[4] T. G. F. Jones and O. Roche-Newton, ‘Improved bounds on the set $A(A + 1)$’, J. Combin. Theory, Series A., 120(3) (2013), 515–526.
[5] N. H. Katz and C.-Y. Shen, ‘A slight improvement to Garaev’s sum product estimate’, Proc. Amer. Math. Soc., 136(7) (2008), 2499–2504.
[6] O. Roche-Newton and L. Li, ‘An improved sum-product estimate for general finite fields’, SIAM J. Discrete Math., 25(3) (2011), 1285–1296.
[7] M. Rudnev, ‘An improved sum-product inequality in fields of prime order’ Int. Math. Res. Not. IMRN, 16 (2012), 3693–3705.
[8] M. Rudnev, ‘On the number of incidences between planes and points in three dimensions’ Combinatorica, 38(1) (2018), 219–254.
[9] S. Stevens and F. de Zeeuw, ‘An improved point-line incidence bound over arbitrary fields’, Bull. London Math. Soc., 49(5) (2017), 842–858.
[10] T. Tao and V. Vu, ‘Additive combinatorics’, Cambridge Univ. Press, 2006.
[11] D. Zhelezov, ‘On additive shifts of multiplicative almost-subgroups in finite fields’, Preprint arXiv:1507.05548v1 [math.NT] 20 Jul 2015.