On the size of the set $A(A + 1)$

Moubariz Z. Garaev
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
garaev@matmor.unam.mx

Chun-Yen Shen
Department of Mathematics
Indiana University
Rawles Hall, 831 East Third St.
Bloomington, IN 47405, USA
shenc@indiana.edu

December 16, 2008

Abstract
Let $F_p$ be the field of a prime order $p$. For a subset $A \subset F_p$ we consider the product set $A(A + 1)$. This set is an image of $A \times A$ under the polynomial mapping $f(x, y) = xy + x : F_p \times F_p \to F_p$. In the present note we show that if $|A| < p^{1/2}$, then
$$|A(A + 1)| \geq |A|^{106/105+o(1)}.$$ If $|A| > p^{2/3}$, then we prove that
$$|A(A + 1)| \gg \sqrt{p|A|}$$ and show that this is the optimal in general settings bound up to the implied constant. We also estimate the cardinality of $A(A + 1)$ when $A$ is a subset of real numbers. We show that in this case one has the Elekes type bound
$$|A(A + 1)| \gg |A|^{5/4}.$$
1 Introduction

Let $F_p$ be the field of residue classes modulo a prime number $p$ and let $A$ be a non-empty subset of $F_p$. It is known from [3, 4] that if $|A| < p^{1-\delta}$, where $\delta > 0$, then one has the sum-product estimate

$$|A + A| + |AA| \gg |A|^{1+\varepsilon}; \quad \varepsilon = \varepsilon(\delta) > 0.$$ 

This estimate and its proof consequently have been quantified and simplified in [2], [6]–[9], [11]–[15], [17]. From the sum-product estimate and Ruzsa’s triangle inequalities (see, [13] and [14]) it follows that the polynomial $f(x, y, z) = xy + z : F_p^3 \to F_p$ possesses an expanding property, in a sense that for any subsets $A, B, C$ with $|A| \sim |B| \sim |C| \sim p^\alpha$, where $0 < \alpha < 1$ is fixed, the set $f(A, B, C)$ has cardinality greater than $p^\beta$ for some $\beta = \beta(\alpha) > \alpha$. The problem raised by Widgerson asks to explicitly write a polynomial with two variables which would satisfy the expanding condition. This problem was solved by Bourgain [1], showing that one can take $f(x, y) = x^2 + xy$.

Now consider the polynomial $f(x, y) = xy + x$. This polynomial, of course, does not possess the expanding property in the way defined above. Nevertheless, from Bourgain’s work [1] it is known that if $|A| \sim p^\alpha$, where $0 < \alpha < 1$, then

$$|f(A, A)| = |A(A + 1)| \geq p^\beta; \quad \beta = \beta(\alpha) > \alpha.$$ 

In the present note we deal with explicit lower bounds for the size of the set $A(A + 1)$. Our first result addresses the most nontrivial case $|A| < p^{1/2}$.

**Theorem 1.** Let $A \subset F_p$ with $|A| < p^{1/2}$. Then

$$|A(A + 1)| \geq |A|^{106/105 + o(1)}.$$ 

Theorem 1 will be derived from the Balog-Szemerédi-Gowers type estimate and a version of the sum-product estimate given in [2]. We remark that the statement of Theorem 1 remains true in a slightly wider range than $|A| < p^{1/2}$. On the other hand, if $|A| > p^{2/3}$, then we have the optimal in general settings bound.

**Theorem 2.** For any subsets $A, B, C \subset F_p^*$ the following bound holds:

$$|AB| \cdot |(A + 1)C| \gg \min\left\{ p|A|, \frac{|A|^2 \cdot |B| \cdot |C|}{p} \right\}.$$
Theorem 2 can be compared with the following estimate from [7]:

\[ |A + B| \cdot |AC| \gg \min \left\{ p |A|, \frac{|A|^2 \cdot |B| \cdot |C|}{p} \right\}. \]

Taking \( B = A + 1 \), \( C = A \), Theorem 2 implies

\[ |A(A + 1)| \gg \min \left\{ \sqrt{p |A|}, \frac{|A|^2}{p^{1/2}} \right\}. \]

In particular, if \( |A| > p^{2/3} \), then

\[ |A(A + 1)| \gg \sqrt{p |A|}. \]

Let us show that this is optimal in general settings bound up to the implied constant. Let \( N < 0.1p \) be a positive integer, \( M = \lfloor 2\sqrt{Np} \rfloor \) and let \( g \) be a generator of \( F_p^\ast \). Consider the set

\[ X = \{ g^n - 1 : n = 1, 2, \ldots, M \}. \]

From the pigeon-hole principle, there is a number \( L \) such that

\[ |X \cap \{ g^{L+1}, \ldots, g^{L+M} \}| \geq \frac{M^2}{2p} \geq N. \]

Take

\[ A = X \cap \{ g^{L+1}, \ldots, g^{L+M} \}. \]

Then we have \( |A| \geq N \) and

\[ |A(A + 1)| \leq 2M \leq 2\sqrt{pN}. \]

Thus, it follows that for any positive integer \( N < p \) there exists a set \( A \subset F_p \) with \( |A| = N \) such that

\[ |A(A + 1)| \ll \sqrt{p |A|}. \]

This observation illustrates the precision of our result for large subsets of \( F_p \).

When \( |A| \cdot |B| \cdot |C| \approx p^2 \), Theorem 2 implies that

\[ |AB| \cdot |(A + 1)C| \gg |A|^3 \cdot |B| \cdot |C|. \]

This coincides with the bound that one can get when \( A, B, C \) are subsets of the set of real numbers \( \mathbb{R} \).
Theorem 3. Let $A, B, C$ be finite subsets of $\mathbb{R} \setminus \{0, -1\}$. Then

$$|AB| \cdot |(A + 1)C| \gg \sqrt{|A|^3 \cdot |B| \cdot |C|}.$$ 

In particular, taking $B = A + 1$, $C = A$, we obtain the bound

$$|A(A + 1)| \gg |A|^{5/4}.$$ 

We mention Elekes’ sum-product estimate [5] in the case of real numbers:

$$|A + A| + |AA| \gg |A|^{5/4}.$$ 

More generally Elekes’ work implies that if $A, B, C$ are finite subsets of the set $\mathbb{R} \setminus \{0\}$, then

$$|AB| \cdot |A + C| \gg \sqrt{|A|^3 \cdot |B| \cdot |C|}.$$ 

The best known bound up to date in the “pure” sum-product problem for real numbers is $|A + A| + |AA| \gg |A|^{4/3 + o(1)}$, due to Solymosi [16].

2 Proof of Theorem [1]

For $E \subset A \times B$ we write

$$A \sim_E B = \{a - b : (a, b) \in E\}.$$ 

A basic tool in the proof of Theorem [1] is the following explicit Balog-Szemerédi-Gowers type estimate given by Bourgain and Garaev [2].

**Lemma 1.** Let $A \subset F_p$, $B \subset F_p$, $E \subset A \times B$ be such that $|E| \geq |A||B|/K$. There exists a subset $A' \subset A$ such that $|A'| \geq 0.1|A|/K$ and

$$|A \sim_E B|^4 \geq \frac{|A' - A'| \cdot |A| \cdot |B|^2}{10^4 K^5}.$$ 

Theorem [1] will be derived from the combination of Lemma [1] with the following specific variation of the sum-product estimate from [2].

**Lemma 2.** Let $A \subset F_p$, $|A| < p^{1/2}$. Then,

$$|A - A|^8 \cdot |A(A + 1)|^4 \gg |A|^{13 + o(1)}$$
The proof of Lemma 2 follows from straightforward modification of the proof of Theorem 1.1 of [2], so we only sketch it. It suffices to show that

\[ |A - A|^5 \cdot |2A - 2A| \cdot |A(A + 1)|^4 \geq |A|^{11 + o(1)}. \]

Indeed, having this estimate established, one can apply it to large subsets of \( A \), iterate the argument of Katz and Shen [11] several times and finish the proof; for more details, see [2].

We can assume that \( A \cap \{0, -1\} = \emptyset \) and \( |A| \geq 10 \). There exists a fixed element \( b_0 \in A \) such that

\[
\sum_{a \in A} |(a + 1)A \cap (b_0 + 1)A| \geq \frac{|A|^3}{|A(A + 1)|}.
\]

Decomposing into level sets, we get a positive integer \( N \) and a subset \( A_1 \subset A \) such that

\[
N \leq |(a + 1)A \cap (b_0 + 1)A| < 2N \quad \text{for any} \quad a \in A_1, \tag{1}
\]

\[
N|A_1| \geq \frac{|A|^3}{2|A(A + 1)| \cdot \log |A|}. \tag{2}
\]

In particular,

\[
N \geq \frac{|A|^2}{2|A| \cdot |A(A + 1)| \cdot \log |A|}. \tag{3}
\]

We can assume that \( |A_1| > 1 \). Due to the observation of Glibichuk and Konyagin [8], either

\[
\frac{A_1 - A_1}{A_1 - A_1} = F_p
\]

or we can choose elements \( b_1', b_2', b_3', b_4' \in A_1 \) such that

\[
\frac{b_1' - b_2'}{b_3' - b_4'} - 1 \notin \frac{A_1 - A_1}{A_1 - A_1}.
\]

Using the step of Katz and Shen [11], we deduce that in either case there exist elements \( b_1, b_2, b_3, b_4 \in A_1 \) such that

\[
|(b_1 - b_2)A + (b_3 - b_4)A| \gg \frac{|A_1|^3}{|A - A|}. \tag{4}
\]

To each element \( x \in (b_1 - b_2)A + (b_3 - b_4)A \) we attach one fixed representation

\[
x = (b_1 - b_2)a(x) + (b_3 - b_4)a'(x), \quad a(x), a'(x) \in A. \tag{5}
\]
Denote
\[ S = (b_1 - b_2)A + (b_3 - b_4)A, \quad S_i = (b_i + 1)A \cap (b_0 + 1)A; \quad i = 1, 2, 3, 4. \]
As in [2], we consider the mapping
\[ f : S \times S_1 \times S_2 \times S_3 \times S_4 \to (2A - 2A) \times (A - A) \times (A - A) \times (A - A) \times (A - A) \]
defined as follows. Given
\[ x \in S, \quad x_i \in S_i; \quad i = 1, 2, 3, 4, \]
we represent \( x \) in the form (5), represent \( x_i \) in the form
\[ x_i = (b_i + 1)a_i(x_i), \quad a_i(x_i) \in A, \quad a_i'(x_i) \in A, \quad (i = 1, 2, 3, 4), \]
and define
\[ f(x, x_1, x_2, x_3, x_4) = (u, u_1, u_2, u_3, u_4), \]
where
\[ u = a'_1(x_1) - a'_2(x_2) + a'_3(x_3) - a'_4(x_4), \]
\[ u_1 = a(x) - a_1(x_1), \quad u_2 = a(x) - a_2(x_2), \]
\[ u_3 = a'(x) - a_3(x_3), \quad u_4 = a'(x) - a_4(x_4). \]
From the construction we have
\[ x = (b_1 + 1)u_1 - (b_2 + 1)u_2 + (b_3 + 1)u_3 - (b_4 + 1)u_4 + (b_0 + 1)u. \]
Therefore, the vector \((u, u_1, u_2, u_3, u_4)\) determines \( x \) and thus determines \( a(x), a'(x) \) and consequently determines \( a_1(x_1), a_2(x_2), a_3(x_3), a_4(x_4) \) which determines \( x_1, x_2, x_3, x_4 \). Hence, since \(|(b_1 + 1)A \cap (b_0 + 1)A| \geq N\), we get that
\[ |(b_1 - b_2)A + (b_3 - b_4)A|N^4 \leq |A - A|^4 \cdot |2A - 2A|. \]
Taking into account (4), we get
\[ |A - A|^4 \cdot |2A - 2A| \gg \frac{|A|^3N^4}{|A - A|}. \]
Using (1)–(3), we conclude the proof of Lemma 2.
We proceed to prove Theorem 1. Denote
\[ E = \{(x, x + xy) : x \in A, y \in A\} \subset A \times A(A + 1), \]
Then,
\[ |E| = |A|^2 = \frac{|A| \cdot |A(A + 1)|}{K}, \quad K = \frac{|A(A + 1)|}{|A|}. \]

Let \( B = A(A + 1) \). Observe that
\[ -AA = A \bar{A} B. \]

According to Lemma 1 there exists \( A' \subset A \) with
\[ |A'| \gg |A| = \frac{|A|^2}{K(A(A + 1))}. \]

such that
\[ |AA|^4 |A(A + 1)|^3 \gg |A' - A'| |A|^6. \]

Raising to eights power and multiplying by \( |A(A + 1)|^4 \geq |A'(A' + 1)|^4 \), we get
\[ |AA|^32 \cdot |A(A + 1)|^{28} \gg |A'|^8 |A'(A' + 1)|^4 |A|^{48}. \]

Combining this with Lemma 2 (applied to \( A' \)), we obtain
\[ |AA|^32 \cdot |A(A + 1)|^{28} \gg |A'|^{13} |A|^{48+o(1)}. \]

Taking into account the inequality (6), we get
\[ |AA|^32 \cdot |A(A + 1)|^{41} \gg |A|^{74+o(1)}. \]

From Ruzsa’s triangle inequalities in multiplicative form, we have
\[ |AA| \leq \frac{|A(A + 1)| \cdot |(A + 1)A|}{|A + 1|} = \frac{|A(A + 1)|^2}{|A|}. \]

Putting last two inequalities together, we conclude that
\[ |A(A + 1)|^{105} \geq |A|^{106+o(1)}. \]

3 Proof of Theorem 2

Let \( J \) be the number of solutions of the equation
\[ x^{-1}y(z^{-1}t - 1) = 1, \quad (x, y, z, t) \in AB \times B \times C \times (A + 1)C. \]

Observe that for any given triple \( (a, b, c) \in A \times B \times C \) the quadruple \( (x, y, z, t) = (ab, b, c, (a + 1)c) \) is a solution of this equation. Thus,
\[ J \geq |A| \cdot |B| \cdot |C|. \]
On the other hand for any nonprincipal character $\chi$ modulo $p$ we have

$$\left| \sum_{z \in C} \sum_{t \in (A+1)C} \chi(z^{-1}t - 1) \right| \leq \sqrt{p |C| \cdot |(A+1)C|},$$

see, for example, the solution to exercise 8 of [18, Chapter V]. Therefore, the method of solving multiplicative ternary congruences implies that

$$J = \frac{1}{p-1} \sum_{\chi} \sum_{x,y,z,t} \chi(x^{-1}y(z^{-1}t - 1)) =$$

$$= \frac{1}{p-1} \sum_{x,y,z,t} \chi_0(x^{-1}y(z^{-1}t - 1)) + \frac{1}{p-1} \sum_{\chi \neq \chi_0} \sum_{x,y,z,t} \chi(x^{-1}) \chi(y) \chi(z^{-1}t - 1)$$

$$\leq \frac{|AB| \cdot |B| \cdot |C| \cdot |(A+1)C|}{p-1} + \sqrt{p |C| \cdot |(A+1)C| \cdot |AB| \cdot |B|}.$$

Comparing this with (7), we conclude the proof.

Remark. In Karatsuba’s survey paper [10] the interested reader will find many applications of character sums to multiplicative congruences.

4 Proof of Theorem 3

Since $A \cap \{0, -1\} = \emptyset$, we can assume that $|A|$ is large. We will use the Szemerédi-Trotter incidence theorem, which claims that if $P$ is a finite set of points $(x, y) \in \mathbb{R}^2$ and $L$ is a finite set of lines $\ell \subset \mathbb{R}^2$, then

$$\#\left\{ (x, y), \ell \in P \times L : (x, y) \in \ell \right\} \ll |P| + |L| + (|P||L|)^{2/3}.$$ 

We mention that this theorem was applied by Elekes in the above mentioned work [5] to the sum-product problem for subsets of $\mathbb{R}$. In application to our problem, we let

$$P = \{(x, y) : x \in AB, y \in (A+1)C\}$$

and let $L$ to be the family of lines $\{\ell = \ell(z, t) : z \in C, t \in B\}$ given by the equation

$$y - \frac{z}{t} x - z = 0.$$ 

In particular,

$$|P| = |AB| \cdot |(A+1)C|, \quad |L| = |B||C|.$$
Each line $\ell(z, t) \in \mathcal{L}$ contains $|A|$ distinct points $(x, y) \in \mathcal{P}$ of the form

$$(x, y) = (at, (a+1)z); \quad a \in A.$$  

Thus,

$$\# \left\{ \left( (x, y), \ell \right) \in \mathcal{P} \times \mathcal{L} : (x, y) \in \ell \right\} \geq |A||\mathcal{L}| = |A| \cdot |B| \cdot |C|.$$  

Therefore, the Szemerédi-Trotter incidence theorem implies that

$$|A| \cdot |B| \cdot |C| \ll |AB| \cdot |(A+1)C| + |B||C| + \left( |AB| \cdot |(A+1)C| \cdot |B| \cdot |C| \right)^{2/3}.$$  

Since $|A|$ is large and $|AB| \cdot |(A+1)C| \geq |A|^2$, the result follows.

References

[1] J. Bourgain, More on sum-product phenomenon in prime fields and its applications, Int. J. Number Theory 1 (2005), 1–32.

[2] J. Bourgain and M. Z. Garaev, On a variant of sum-product estimates and explicit exponential sum bounds in prime fields, Math. Proc. Cambridge Philos. Soc., Published online by Cambridge University Press 17 Nov 2008 doi:10.1017/S0305004108001230.

[3] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, Estimates for the number of sums and products and for exponential sums in fields of prime order, J. London Math. Soc. (2) 73 (2006), 380–398.

[4] J. Bourgain, N. Katz and T. Tao, A sum-product estimate in finite fields and their applications, Geom. Func. Anal. 14 (2004), 27–57.

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

[6] M. Z. Garaev, An explicit sum-product estimate in $F_p$, Int. Math. Res. Notices (2007) Vol. 2007, doi:10.1093/imrn/rnm035.

[7] M. Z. Garaev, The sum-product estimate for large subsets of prime fields, Proc. Amer. Math. Soc. 136 (2008), 2735-2739.

[8] A. A. Glibichuk and S. V. Konyagin, Additive properties of product sets in fields of prime order, Centre de Recherches Mathématiques, CRM Proceedings and Lecture Notes, 43, 279–286 (2007).
[9] D. Hart, A. Iosevich and J. Solymosi, *Sum product estimates in finite fields via Kloosterman sums*, Int. Math. Res. Notices (2007) Vol. 2007, doi:10.1093/imrn/rnm007.

[10] A. A. Karatsuba, *Arithmetic problems in the theory of Dirichlet characters*, Russian Math. Surveys 63 (2008), 641-690.

[11] N. H. Katz and Ch.-Y. Shen, *A slight improvement to Garaev’s sum product estimate*, Proc. Amer. Math. Soc. 136 (2008), 2499–2504.

[12] N. H. Katz and Ch.-Y. Shen, *Garaev’s inequality in finite fields not of prime order*, Online Journal of Analytic Combinatorics, Issue 3 (2008), #3.

[13] I. Z. Ruzsa, *An application of graph theory to additive number theory*, Scientia, Ser. A 3 (1989), 97–109.

[14] I. Z. Ruzsa, *Sums of finite sets*, Number theory (New York, 1991–1995), 281–293 (Springer, New York, 1996).

[15] Ch.-Y. Shen, *An extension of Bourgain and Garaev’s sum-product estimates*, Acta Arith. (to appear).

[16] J. Solymosi, *An upper bound on multiplicative energy*, arXiv:0806.1040.

[17] T. Tao and V. Vu, “Additive combinatorics” (Cambridge University Press, Cambridge, 2006).

[18] I. M. Vinogradov, “An introduction to the theory of numbers”, Pergamon Press, London & New York, 1955.