PRODUCT SETS OF ARITHMETIC PROGRESSIONS

Mei-Chu Chang
Department of Mathematics
University of California, Riverside

Abstract. In this paper, we generalize a result of Nathanson and Tenenbaum on sum and product sets, partially answering the problem raised at the end of their paper [N-T]. More precisely, they proved that if A is a large finite set of integers such that $|2A| < 3|A| - 4$, then $|A^2| > (\frac{|A|}{\ell n\, |A|})^2 \gg |A|^{2-\varepsilon}$. It is shown here that if $|2A| < \alpha|A|$, for some fixed $\alpha < 4$, then $|A^2| \gg |A|^{2-\varepsilon}$. Furthermore, if $\alpha < 3$, then $|A^h| \gg |A|^{h-\varepsilon}$. Again, crucial use is made from Freiman's Theorem.

INTRODUCTION

Let A, B be finite sets of a commutative ring.

The *product* set of A, B is

$$AB \equiv \{ab \mid a \in A, b \in B\} \tag{0.1}$$

we denote by

$$A^h \equiv A \cdots A \ (h \text{ fold}) \tag{0.2}$$

the h-fold product of A.

Similarly, we define the *sum set* of A, B and h-fold sum of A.

$$A + B \equiv \{a + b \mid a \in A, b \in B\} \tag{0.3}$$

$$hA \equiv A + \cdots + A(h \text{ fold}). \tag{0.4}$$

In 1983, Erdös and Szemerédi [E-S] (see also [E]) made the following conjecture (see [T] and [K-T] for related aspects).

Conjecture (Erdös-Szemerédi). *For any* $\varepsilon > 0$ *and any* $h \in \mathbb{N}$ *there is* $k_0 = k_0(\varepsilon)$ *such that for any* $A \subset \mathbb{N}$ *with* $|A| \geq k_0$*, then*

$$|hA \cup A^h| \gg |A|^{h-\varepsilon}. \tag{0.5}$$

The first result toward the conjecture was obtained by Erdös and Szemerédi [E-S] (see also [Na3]).

Theorem (Erdös-Szemerédi). *Let* $f(k) \equiv \min_{|A|=k} |2A \cup A^2|$*. Then there are constants* c_1, c_2*, such that*

$$k^{1+c_1} < f(k) < k^2\, e^{-c_2 \frac{\ell n\, k}{\ell n\, \ell n\, k}}. \tag{0.6}$$

Nathanson showed that $f(k) < ck^{\frac{32}{31}}$, with $c = 0.00028\dots$

Elekes [El] used the Szemerédi-Trotter Theorem on line-incidences in the plane (see [S-T]), and proved that

$$|2A \cup A^2| > c|A|^{5/4}. \tag{0.7}$$

In [C2], we proved that if $|A^2| < \alpha|A|$, then

$$|2A| > 36^{-\alpha}|A|^2 \tag{0.8}$$

and

$$|hA| > c_h(\alpha)|A|^h, \tag{0.9}$$

where

$$c_h(\alpha) = (2h^2 - h)^{-h\alpha}. \tag{0.10}$$

On the other hand, Nathanson and Tenenbaum [N-T] concluded something stronger by assuming the sum set is small. They showed

Theorem (Nathanson-Tenenbaum). *If* $A \subset \mathbb{N}$ *with*

$$|2A| \leq 3|A| - 4, \tag{0.11}$$

then

$$|A^2| \gg \left(\frac{|A|}{\ell n\, |A|}\right)^2. \tag{0.12}$$

We generalize Nathanson and Tenenbaum's result in two directions.

Theorem 1. *Let $A \subset \mathbb{N}$ be finite. If*

$$|2A| < \alpha|A| \quad \text{with } \alpha < 4, \tag{0.13}$$

then $\forall\, \varepsilon > 0$, there exists $k_0 = k(\varepsilon)$ such that for all A with $|A| \geq k_0$,

$$|A^2| \gg |A|^{2-\varepsilon}. \tag{0.14}$$

Theorem 2. *Let $A \subset \mathbb{N}$ be finite. If*

$$|2A| < \alpha|A| \quad \text{with } \alpha < 3, \tag{0.15}$$

then $\forall\, \varepsilon > 0$, there exists $k_0 = k(\varepsilon)$ such that $\forall\ A$ with $|A| \geq k_0$,

$$|A^h| \gg |A|^{h-\varepsilon}. \tag{0.16}$$

Our proof is similar to that in [N-T] and based on Freiman's theorem (see [Bi],[Na1],[El]). Thus, from the assumption, we get that A is contained in a generalized arithmetic progression P with $P < c|A|$ and $\dim P \leq 2$. (We recall that a s-dimensional progression is the translation of a homomorphic image of a s-dimensional coordinate box in $\mathbb{Z}$ from $\mathbb{Z}^s$. A more precise statement of Freiman's theorem will be given in Section 2.) The problem may then be reduced to bounding the number $\rho_{_P}(n)$ of representatives of integers n by a product of two elements in P (in the case of Theorem 1). Instead of establishing a (uniform) bound

$$\rho_{_P}(n) \ll |P|^{\varepsilon} \tag{0.17}$$

for each element n, we will bound

$$\sum_n \rho_{_P}^2(n) \ll |P|^{2+\varepsilon}. \tag{0.18}$$

Inequality (0.18) is weaker than (0.17), but also sufficient for our purpose. The advantage of considering the expression $\sum_n \rho_{_P}^2(n)$ is that the problem may be reduced to the case of a *homogeneous* progression (a homomorphic image without being translated) of the same dimension.

Obtaining (0.17) and hence (0.18) for a homogeneous progression (of dimension 2 in the context of the theorem) is rather easy, while directly proving (0.17) for a non-homogeneous 2-dimensional progression seems significantly harder. (See Remark 12.1.)

Notation: We use the convention

$$A \ll B \tag{0.19}$$

to mean that for every ε, there is a constant $c(\varepsilon)$ such that

$$A < c(\varepsilon)B. \tag{0.20}$$

The paper is organized as follows:

In Section 1, we prove some basic inequalities involving $\rho_P(n)$ and $\sum \rho_P^2 n$.

In Section 2, we prove the theorems.

Acknowledgement. The author would like to thank J. Bourgain for various advice and J. Stafney for helpful discussions.

Section 1. Preliminaries.

Let $\Lambda_1, \Lambda_2 \subset \mathbb{N}$ be finite. For $n \in \mathbb{N}$, we will use the following notations for the numbers of representatives as products and as differences between squares.

Notation:

$$\rho_{\Lambda_1,\Lambda_2}(n) \equiv |\{(n_1, n_2) \in \Lambda_1 \times \Lambda_2 \mid n_1 n_2 = n\}| \tag{1.1}$$

$$\sigma_{\Lambda_1,\Lambda_2}(n) \equiv |\{(n_1, n_2) \in \Lambda_1 \times \Lambda_2 \mid n_1^2 - n_2^2 = n\}| \tag{1.2}$$

$$\rho_\Lambda \equiv \rho_{\Lambda,\Lambda}. \tag{1.3}$$

The following lemma formulates the relation between the lower bound on the product set and the upper bound on the numbers of representatives as products.

Lemma 1. *Let* $\Lambda_1, \Lambda_2 \subset \mathbb{N}$. *Then*

$$|\Lambda_1 \Lambda_2| \geq \frac{|\Lambda_1|^2 |\Lambda_2|^2}{\sum\limits_{n \in \Lambda_1 \Lambda_2} \rho^2_{\Lambda_1,\Lambda_2}(n)} \tag{1.4}$$

Proof. Cauchy-Schwartz inequality gives

$$|\Lambda_1|\,|\Lambda_2| = \sum_{n \in \Lambda_1 \Lambda_2} \rho_{\Lambda_1,\Lambda_2}(n) \leq \Big(\sum \rho^2_{\Lambda_1,\Lambda_2}(n)\Big)^{1/2} (|\Lambda_1 \Lambda_2|)^{1/2}.$$

□

Sometimes it is more convenient to work with σ than with ρ.

Lemma 2. *The following inequalities between ρ and σ hold*
(i) $\rho_{\Lambda_1,\Lambda_2}(n) \leq \sigma_{\Lambda_1+\Lambda_2,\Lambda_1-\Lambda_2}(4n)$.
(ii) $\sigma_{\Lambda_1,\Lambda_2}(n) \leq \rho_{\Lambda_1+\Lambda_2,\Lambda_1-\Lambda_2}(n)$.

Proof. Inequality (i) follows from

$$4n_1n_2 = (n_1+n_2)^2 - (n_1-n_2)^2, \tag{1.5}$$

and inequality (ii) follows from

$$m_1^2 - m_2^2 = (m_1+m_2)(m_1-m_2). \tag{1.6}$$

□

The next elementary fact is used frequently.

Fact 3. *For $n \in \mathbb{Z}$,*

$$\int_0^1 e^{2\pi inx}\,dx = \begin{cases} 0 & \text{if } n \neq 0 \\ 1 & \text{if } n = 0 \end{cases}.$$

Our first goal is to give an upper bound on $\sum_n \rho_\Lambda^2(n)$ for an arbitrary finite set $\Lambda \subset \mathbb{N}$. (See Proposition 9).

Lemma 4. *Let $\Lambda \subset \mathbb{N}$. Then*

$$\sum \rho_\Lambda^2(n) \leq \Big(\sum \rho^2_{4\Lambda,2\Lambda-2\Lambda}(n)\Big)^{1/2} \Big(\sum \rho^2_{2\Lambda-2\Lambda}(n)\Big)^{1/2} \tag{1.7}$$

Proof. Lemma 2(i) gives

$$\rho_\Lambda(n) \leq \sigma_{2\Lambda,\Lambda-\Lambda}(4n). \tag{1.8}$$

Fact 3 says that the right hand side of (1.8) is

$$\sigma_{2\Lambda,\Lambda-\Lambda}(4n) = \int_0^1 e^{-2\pi i4nx} \sum_{m\in 2\Lambda} e^{2\pi i m^2 x} \sum_{m\in\Lambda-\Lambda} e^{-2\pi i m^2 x}\,dx \tag{1.9}$$

Let

$$f(x) = \sum_{m\in 2\Lambda} e^{2\pi i m^2 x} \sum_{m\in\Lambda-\Lambda} e^{-2\pi i m^2 x}. \tag{1.10}$$

Then (1.9) is the $4n$-th Fourier coefficient of $f(x)$, i.e.,

$$\sigma_{2\Lambda,\Lambda-\Lambda}(4n) = \hat{f}_{4n}(x). \tag{1.11}$$

Putting (1.8), and (1.11) together, and using Parseval equality, we have

$$\begin{aligned}\sum_n \rho^2_{\Lambda}(n) &\le \sum_n \sigma^2_{2\Lambda,\Lambda-\Lambda}(4n)\\ &= \sum_{n\in\Lambda^2} |\hat{f}_{4n}(x)|^2\\ &\le \sum_m |\hat{f}_m(x)|^2\\ &= \|f(x)\|_2^2.\end{aligned} \tag{1.12}$$

Now, we use (1.10) to bound (1.12),

$$\begin{aligned}\|f(x)\|_2^2 &= \int_0^1 |\sum_{m\in 2\Lambda} e^{2\pi i m^2 x}|^2\,|\sum_{m\in\Lambda-\Lambda} e^{-2\pi i m^2 x}|^2\,dx\\ &\le \Big(\int_0^1 |\sum_{m\in 2\Lambda} e^{2\pi i m^2 x}|^4\,dx\Big)^{\frac{1}{2}}\Big(\int_0^1 |\sum_{m\in\Lambda-\Lambda} e^{-2\pi i m^2 x} Product|^4\,dx\Big)^{\frac{1}{2}} && (1.13)\\ &= \Big(\sum \sigma^2_{2\Lambda,2\Lambda}(n)\Big)^{\frac{1}{2}}\Big(\sum \sigma^2_{\Lambda-\Lambda,\Lambda-\Lambda}(n)\Big)^{\frac{1}{2}} && (1.14)\\ &\le \Big(\sum \rho^2_{4\Lambda,2\Lambda-2\Lambda}(n)\Big)^{\frac{1}{2}}\Big(\sum \rho^2_{2\Lambda-2\Lambda}(n)\Big)^{\frac{1}{2}}. && (1.15)\end{aligned}$$

Here, (1.13) follows from Hölder inequality, (1.14) follows from sublemma 5 below; and (1.15) follows from Lemma 2(ii). □

Sublemma 5. *Let* $\Omega \subset \mathbb{N}$. *Then*

$$\int_0^1 |\sum_{m\in\Omega} e^{2\pi i m^2 x}|^4\,dx = \sum \sigma^2_{\Omega,\Omega}(n). \tag{1.16}$$

Proof.

$$\begin{aligned}|\sum_{m\in\Omega} e^{2\pi i m^2 x}|^4 &= |\Big(\sum_{m\in\Omega} e^{2\pi i m^2 x}\Big)\Big(\sum_{m\in\Omega} e^{-2\pi i m^2 x}\Big)|^2\\ &= |\sum \sigma_{\Omega,\Omega}(n) e^{2\pi i n x}|^2.\end{aligned} \tag{1.17}$$

Let

$$g(x) = \sum \sigma_{\Omega,\Omega}(n) e^{2\pi i n x} \tag{1.18}$$

Then

$$\hat{g}_n(x) = \sigma_{\Omega,\Omega}(n), \tag{1.19}$$

and the left-hand side of (1.16) is $\int_0^1 |g(x)|^2\,dx$, which is $\sum \|\hat{g}_n(x)\|_2^2$, by Parseval equality. Now (1.16) follows from (1.19). □

Lemma 6. *Let $\Lambda_1, \Lambda_2 \subset \mathbb{N}$. Then*

$$\sum \rho^2_{\Lambda_1,\Lambda_2}(n) \le \Big(\sum \rho^2_{\Lambda_1}(n)\Big)^{\frac{1}{2}} \Big(\sum \rho^2_{\Lambda_2}(n)\Big)^{\frac{1}{2}}. \tag{1.20}$$

We wil use the following "Fact 3 over $\mathbb{R}$", which comes from almost periodic function theory.

Fact 7. *Let $\lambda \in \mathbb{R}$. For an integrable function $f(x)$, we define*

$$\|f(x)\|_{\text{a.p.}} \equiv \frac{1}{T} \lim_{T\to\infty} \int_0^T f(x)\,dx. \tag{1.21}$$

Then

$$\|e^{2\pi i\lambda x}\|_{\text{a.p.}} = \begin{cases} 0 & \text{if } \lambda \ne 0 \\ 1 & \text{if } \lambda = 0 \end{cases}. \tag{1.22}$$

Sublemma 8. *Let $\{\lambda_s\}_s \subset \mathbb{R}$ be a set of distinct real numbers. Then*

$$\Big\| \,|\sum_s a_s e^{2\pi i\lambda_s x}|^2 \Big\|_{\text{a.p.}} = \sum |a_s|^2. \tag{1.23}$$

Proof. The left-hand side of (1.23) is

$$\Big\| \sum_{s,t} a_s \overline{a}_t e^{2\pi i(\lambda_s - \lambda_t)x} \Big\|_{\text{a.p.}}.$$

Now, use (1.22). $\square$

Proof of Lemma 6. To use Sublemma 8, we take the set $\{\ell n\, n\}_{n\in\mathbb{N}}$ of distinct real numbers.

Inequality (1.20) is equivalent to

$$\begin{aligned} &\Big\| \,|\sum_n \rho_{\Lambda_1,\Lambda_2}(n) e^{2\pi i x \ell n\, n}|^2 \Big\|_{\text{a.p.}} \\ \le &\Big\| \,|\sum_{n_1} \rho_{\Lambda_1}(n_1) e^{2\pi i x\ell n\, n_1}|^2 \Big\|^{1/2}_{\text{a.p.}} \Big\| \,|\sum_{n_2} \rho_{\Lambda_2}(n_2) e^{2\pi i x\ell n\, n_2}|^2 \Big\|^{1/2}_{\text{a.p.}}. \end{aligned} \tag{1.24}$$

It suffices to show that

$$\begin{aligned} &\int_0^T |\sum_n \rho_{\Lambda_1,\Lambda_2}(n) e^{2\pi i x\ell n\, n}|^2\, dx \\ \le &\Big(\int_0^T |\sum_{n_1} \rho_{\Lambda_1}(n_1) e^{2\pi i x\ell n\, n_1}|^2\, dx\Big)^{\frac{1}{2}} \Big(\int_0^T |\sum_{n_2} \rho_{\Lambda_2}(n_2) e^{2\pi i x\ell n\, n_2}|^2\, dx\Big)^{\frac{1}{2}}. \end{aligned} \tag{1.25}$$

The left-hand side of (1.25) is

$$\begin{aligned}&\int_0^T \Big|\sum_{n_1\in\Lambda_1} e^{2\pi i x \ell n\, n_1}\Big|^2 \Big|\sum_{n_2\in\Lambda_2} e^{2\pi i x \ell n\, n_2}\Big|^2 dx\\ \le &\Big(\int_0^T \Big|\sum_{n_1\in\Lambda_1} e^{2\pi i x \ell n\, n_1}\Big|^4 dx\Big)^{1/2} \Big(\int_0^T \Big|\sum_{n_2\in\Lambda_2} e^{2\pi i x \ell n\, n_2}\Big|^4 dx\Big)^{1/2}.\end{aligned} \tag{1.26}$$

The last inequality is Cauchy Schwartz. It is clear that the right-hand sides of (1.25) and (1.26) are the same. □

Proposition 9. *Let $\Lambda \subset \mathbb{N}$. Then*

$$\sum \rho^2_{\Lambda}(n) \le \Big(\sum \rho^2_{2\Lambda-2\Lambda}(n)\Big)^{3/4} \Big(\sum \rho^2_{4\Lambda}(n)\Big)^{1/4}. \tag{1.27}$$

Proof. Combining Lemma 4 and Lemma 6, we have

$$\begin{aligned}\sum \rho^2_{\Lambda}(n) &\le \Big(\sum \rho^2_{4\Lambda, 2\Lambda-2\Lambda}(n)\Big)^{1/2} \Big(\sum \rho^2_{2\Lambda-2\Lambda}(n)\Big)^{1/2}\\ &\le \Big(\big(\sum \rho^2_{4\Lambda}(n)\big)^{1/2} \big(\sum \rho^2_{2\Lambda-2\Lambda}(n)\big)^{1/2}\Big)^{1/2} \Big(\sum \rho^2_{2\Lambda-2\Lambda}(n)\Big)^{1/2},\end{aligned}$$

which is (1.27). □

Next, we want to bound $\rho_P(n)$ by the length of the progression, for some special 2-dimensional progression P.

We will use

Fact 10. *Let $d(n)$ be the number of divisors of n, i.e.,*

$$d(n) \equiv |\{m \in \mathbb{N} \mid m|n\}|.$$

Then $\forall \varepsilon > 0, d(n) \ll n^{\varepsilon}$. In particular,

$$\rho_{\Lambda_1, \Lambda_2}(n) \ll n^{\varepsilon}. \tag{1.28}$$

The following was in [N-T]. We include it here for completeness.

Lemma 11. *Let P_1, P_2 be 1-dimensional progressions of length ℓ, i.e.,*

$$P_i \equiv \{b_i + ja_i \mid 1 \leq j \leq \ell\}. \tag{1.29}$$

Then for $n \in \mathbb{N}$

$$\rho_{P_1,P_2}(n) \ll \ell^\varepsilon, \quad \forall \varepsilon > 0. \tag{1.30}$$

Proof. It is clear that we may assume

$$(a_i, b_i) = 1, \quad \text{for } i = 1, 2. \tag{1.31}$$

Claim 1. For $\omega \neq \omega' \in P_1$, let (ω, ω') be the greatest common divisor. Then $(\omega, \omega') < \ell$.

Proof of Claim 1. . Let $\omega = b_1 + ja_1$ and $\omega' = b_1 + j'a_1$. Then

$$\omega - \omega' = (j - j')a_1. \tag{1.32}$$

In particular,

$$(\omega, \omega') \mid (j - j')a_1. \tag{1.33}$$

(1.31) implies that

$$(\omega, a_1) = 1. \tag{1.34}$$

Hence

$$(\omega, \omega') \mid (j - j'). \tag{1.35}$$

In particular,

$$(\omega, \omega') \leq |j - j'| < \ell. \tag{1.36}$$

□

Claim 2. $n \geq \ell^{-3}\omega\omega'\omega''$, where $\omega, \omega', \omega'' \in P_1$ are any three distinct divisors of n.

Proof of Claim 2. Let $[\omega, \omega', \omega'']$ be the least common multiple of $\omega, \omega', \omega''$.
Then

$$[\omega, \omega', \omega''] \mid n. \tag{1.37}$$

Therefore

$$n \geq [\omega, \omega', \omega''] = \frac{\omega\omega'\omega''}{(\omega, \omega')(\omega', \omega'')(\omega'', \omega)} > \frac{\omega\omega'\omega''}{\ell^3}. \qquad \square$$

To finish the proof of Lemma 10, take three factorizations of n,

$$n = \omega_1\omega_2 = \omega_1'\omega_2' = \omega_1''\omega_2'', \tag{1.38}$$

with ω_i, ω_i'', $\omega_i'' \in P_i$.

Then, claim 2 implies

$$\begin{aligned} n &\geq \ell^{-3}\omega_1\omega_1'\omega_1'', \quad \text{and} \\ n &\geq \ell^{-3}\omega_2\omega_2'\omega_2''. \end{aligned} \tag{1.39}$$

Combining the inequalities in (1.39), we have

$$n^2 \geq \ell^{-6} n^3,$$

or

$$\ell^6 \geq n \tag{1.40}$$

The proof is concluded by (1.28) and (1.40). $\square$

Now we bound $\rho_{P_0}(n)$, when the progression P_0 is the homomorphic image of a coordinate rectangle.

Proposition 12. *Let P_0 be a 2-dimensional proper "homogeneous" progression, i.e.,*

$$P_0 \equiv \{j_1a_1 + j_2a_2 \mid 1 \leq j_i \leq J_i\}. \tag{1.41}$$

Then for any $n \in \mathbb{N}$,

$$\rho_{P_0}(n) \ll J^\varepsilon, \quad \forall \varepsilon > 0. \tag{1.42}$$

Here $J = J_1J_2 = |P|$.

Proof. We may assume

$$(a_1, a_2) = 1 \tag{1.43}$$

If n has two factorizations

$$\begin{aligned} n &= (j_1a_1 + j_2a_2)(k_1a_1 + k_2a_2) \\ &= (j_1'a_1 + j_2'a_2)(k_1'a_1 + k_2'a_2) \end{aligned} \tag{1.44}$$

with

$$j_2k_2 - j_2'k_2' \neq 0, \tag{1.45}$$

then (1.43) and (1.44) imply

$$a_1 \mid (j_2k_2 - j_2'k_2').$$

Hence

$$|a_1| < |j_2k_2 - j_2'k_2'| < J_2^2. \tag{1.46}$$

If all factorizations (see (1.44)) of n have the same j_2k_2, then the choices of $\{j_2, k_2\}$ is

$$d(j_2k_2) \leq d(J_2^2) \ll (J_2^2)^{\varepsilon_1} \ll J^{\varepsilon_2}, \tag{1.47}$$

by Fact 10.

On the other hand, for each $\{j_2, k_2\}$ fixed, to bound the number of factorizations (1.44), we can apply Lemma 11 with $b_1 = j_2a_2, b_2 = k_2a_2$, and derive

$$\rho_{P_0}(n) \ll J^{\varepsilon_2} J_1^{\varepsilon_3} < J^{\varepsilon}. \tag{1.48}$$

Similarly, we have either

$$|a_2| < J_1^2, \tag{1.49}$$

or (1.48) again.

Putting (1.46) and (1.49) together, we have

$$|j_1a_1 + j_2a_2| \leq J_1J_2^2 + J_2J_1^2 < 2J^2 \tag{1.50}$$

Fact 10 gives

$$\rho_{P_0}(n) \ll n^{\varepsilon_4} \ll (2J^2)^{\varepsilon_4} < J^{\varepsilon}. \qquad \square$$

Remark 12.1. Proposition 12 can be proved for the nonhomogeneous case, which would provide another proof of Theorem 1. This argument, however, is technically much more complicated.

Section 2. The Proofs.

The following structure theorem (see [Bi],[Fr1],[Fr2],[Fr3],[C1]), is essential to our proof

Freiman Theorem. *Let $A \subset \mathbb{Z}$ be finite. If there is a constant $\alpha, \alpha < \sqrt{|A|}$, such that $|2A| < \alpha|A|$, then A is contained in a s-dimensional proper progression P, i.e., there exist $\beta, \alpha_1, \ldots, \alpha_s \in \mathbb{Z}$ and $J_1, \ldots, J_s \in \mathbb{N}$ such that*

$$P = \{\beta + j_1\alpha_1 + \cdots + j_s\alpha_s \mid 1 \leq j_i \leq J_i\} \tag{2.1}$$

and $|P| = J_1 \cdots J_s$.

Moreover, $s \leq \alpha$, and if $|A| > \frac{\lfloor\alpha\rfloor\lfloor\alpha+1\rfloor}{2(\lfloor\alpha+1\rfloor-\alpha)}$, then

$$s \leq \lfloor \alpha - 1 \rfloor. \tag{2.2}$$

Furthermore, for any integer $h \geq 1$, the progression

$$P_0^{(h)} \equiv \{j_1\alpha_1 + \cdots + j_s\alpha_s \mid 1 \leq j_i \leq hJ_i\} \tag{2.3}$$

is proper (i.e., $|P_0^{(h)}| = h^s J_1 \cdots J_s$) and

$$J = J_1 \cdots J_s < c(h)|A|. \tag{2.4}$$

Proof of Theorem 1. Let P be the progression allowed by Freiman's Theorem,

$$A \subset P = \{b + j_1a_1 + j_2a_2 \mid 1 \leq j_i \leq J_i\} \tag{2.5}$$

To use Lemma 1, we want to bound $\sum \rho_{_P}^2(n)$.

Proposition 9 gives

$$\sum \rho_{_P}^2(n) \leq \left(\sum \rho_{_{2P-2P}}^2(n)\right)^{3/4} \left(\sum \rho_{_{4P}}^2(n)\right)^{1/4}. \tag{2.6}$$

Here

$$2P - 2P \equiv P_0 \equiv \{j_1a_1 + j_2a_2 \mid -2J_i \leq j_i \leq 2J_i\} \tag{2.7}$$

and

$$4P \equiv P_1 \equiv \{4b + j_1a_1 + j_2a_2 \mid 1 \leq j_i \leq 4J_i\}$$

are both proper, and P_0 is of the form (1.41) in Proposition 12.

Therefore

$$\rho_{_{P_0}}(n) \ll J^\varepsilon, \quad \forall \varepsilon > 0.$$

Hence

$$\begin{aligned} \sum \rho_{_{P_0}}^2(n) \ll J^\varepsilon \sum_{n \in P_0^2} \rho_{_{P_0}}(n) &= J^\varepsilon |P_0|^2 \\ &\ll J^{2+\varepsilon} \\ &\ll |A|^{2+\varepsilon}. \end{aligned} \tag{2.8}$$

The last inequality follows from (2.4).

Combining with (2.6), we have

$$\sum \rho_{_P}^2(n) \ll |A|^{\frac{3}{4}(2+\varepsilon)} \left(\sum \rho_{_{P_1}}^2(n)\right)^{\frac{1}{4}}. \tag{2.9}$$

To bound $\sum \rho^2_{P_1}(n)$, we write

$$P_1 = \bigcup_{\alpha=1}^{16} P_\alpha, \tag{2.10}$$

where each P_α is a translation of P in (2.5).

Then

$$\rho_{P_1}(n) = \sum_{\alpha,\alpha'=1}^{16} \rho_{P_\alpha, P_{\alpha'}}(n). \tag{2.11}$$

Hence

$$\begin{aligned}
\left(\sum_n \rho^2_{P_1}(n)\right)^{\frac{1}{2}} &\le \sum_{\alpha,\alpha'=1}^{16} \left(\sum_n \rho^2_{P_\alpha, P_{\alpha'}}(n)\right)^{\frac{1}{2}} \\
&\le \sum_{\alpha,\alpha'=1}^{16} \left(\sum_n \rho^2_{P_\alpha}(n)\right)^{\frac{1}{4}} \left(\sum_n \rho^2_{P_{\alpha'}}(n)\right)^{\frac{1}{4}} \\
&\le 16^2 \max_\alpha \left(\sum \rho^2_{P_\alpha}(n)\right)^{\frac{1}{2}}. \qquad (2.12)
\end{aligned}$$

The first is the triangle inequality, the second is Lemma 6.

Putting (2.9) and (2.12) together, we have

$$\sum_n \rho^2_P(n) \ll |A|^{\frac{3}{4}(2+\varepsilon)} \left(\sum_n \rho^2_{\bar{P}}(n)\right)^{\frac{1}{4}}, \tag{2.13}$$

where $\bar{P}$ is the translation of P such that $\sum_n \rho^2_{\bar{P}}(n)$ is the maximum among all translations of P.

This whole argument could start with any translation of P. In particular, in (2.13) P could be replaced by $\overline{P}$. Therefore,

$$\sum \rho^2_{\bar{P}}(n) \ll |A|^{\frac{3}{4}(2+\varepsilon)} \left(\sum \rho^2_{\bar{P}}(n)\right)^{\frac{1}{4}},$$

i.e.,

$$\sum \rho^2_{\bar{P}}(n) \ll |A|^{2+\varepsilon}.$$

Hence

$$\sum \rho^2_P(n) \le \max_\alpha \sum \rho^2_{P_\alpha}(n) \le \sum \rho^2_{\bar{P}}(n) \ll |A|^{2+\varepsilon}.$$

Lemma 1 implies

$$|A^2| \geq \frac{|A|^4}{\sum \rho^2_{_A}(n)} \geq \frac{|A|^4}{\sum \rho^2_{_P}(n)} \gg |A|^{2-\varepsilon}.$$

$\square$

Next, we prove Theorem 2.

From Freiman's Theorem, A is contained in a 1-dimensional progression

$$A \subset P \equiv \{b + ja \mid 1 \leq j \leq J\}, \quad \text{with } J < c(A) \tag{2.17}$$

Defining

$$\rho_{_h}(n) \equiv \big|\{(n_1, \dots, n_h) \in P \times \dots \times P \mid n_1 \cdots n_h = n\}\big| \tag{2.18}$$

we get, (since $A \subset P$)

$$|A^h| \geq \frac{|A|^h}{\max_n \rho_h(n)}. \tag{2.19}$$

Therefore, we want to show that $\forall \varepsilon > 0$, there is a constant $c(\varepsilon)$, such that

$$\rho_{_h}(n) \ll |A|^{\varepsilon}, \ \ \forall n. \tag{2.20}$$

We may assume

$$(a, b) = 1 \quad \text{and } b \neq 0 \tag{2.21}$$

Let

$$n = (b + j_1 a) \cdots (b + j_h a) \tag{2.22}$$

be a factorization of n into h factors in P.

We want to bound the number of choices of $\bar{j} = (j_1, \dots, j_h)$.

Claim. *If for all $(j_1, \dots, j_h)$ in (2.22), the product $\prod\limits_{c=1}^{h} j_i$ is a constant, then (2.20) holds.*

Proof of Claim. Recall our notation of $d(m)$ in Fact 10. The number of choices of $\bar{j} = (j_1, \dots, j_h)$ is

$$\rho_h(n) \leq \Big(d(\prod_{c=1}^{h} j_i)\Big)^h \ll \Big((J^h)^{\varepsilon_1}\Big)^h = J^{\varepsilon_2} \ll |A|^{\varepsilon}.$$

The second inequality is Fact 10, and the last is (2.17). $\square$

Now we return to the proof of Theorem 2.

Let $\bar{j}' = (j'_1, \dots, j_h)$ be *any* other choice in (2.22). Then we have

$$b^{h-1}[s_1(\bar{j}) - s_1(\bar{j}')]a + \cdots + [s_h(\bar{j}) - s_h(\bar{j}')]a^h = 0, \tag{2.23}$$

where $s_k(\bar{j})$ is the kth elementary symmetric function in $\{j_i\}_i$.

We have the following cases.

Case 1. $|a| > (hJ)^h$. Dividing (2.23) by a, and using (2.21), we have

$$a \bigm| |s_1(\bar{j}) - s_1(\bar{j}')\bigm| . \tag{2.24}$$

Our assumption on a gives

$$s_1(\bar{j}) - s_1(\bar{j}') = 0 \tag{2.25}$$

keeping this process on (2.23) until we reach

$$s_h(\bar{j}) - s_h(\bar{j}') = 0, \tag{2.26}$$

which is our hypothesis in the claim. Hence the theorem is proved.

Case 2. $|b| > J^h$. Again, (2.23) gives (2.26), and the same reasoning as above concludes this case.

Case 3. $|a| \le (hJ)^h$ and $|b| \le J^h$. Using (2.22), we have

$$|n| \le (|b| + J|a|)^h < (hJ)^{h(h+1)}. \tag{2.27}$$

Fact 10 implies

$$\rho_{_h}(n) \ge \big(d(n)\big)^h \ll n^{\varepsilon_1} \ll J^{\varepsilon}. \qquad \square$$

References

[Bi]. Y. Bilu, *Structure of sets with small sumset*, in Structure Theory of Set Addition, Astérisque 258, 1999, pp. 77-1-8..

[C1]. M.-C. Chang paper A polynomial bound in Freiman's theorem, Duke Math. J. (to appear).

[C2]. ______, *Erdös-Szemerédi problem on sum set and product set*, (preprint).

[El]. G. Elekes, *On the number of sums and products*, Acta Arithmetic **81** (Fase 4 (1997)), 365-367.

[E]. P. Erdös, *Problems and results on combinatorial number theory*, III, in Number Theory Day (M. Nathanson, ed.), New York 1976; volume 626 of Lecture Notes in Mathemaqtics, Springer-Verlag, Berlin, 1977, pp. 43–72.

[E-S]. P. Erdös and E. Szemerédi, *On sums and products of integers*, in Studies in Pure Mathematics, Birkhaüser, Basel, 1983, pp. 213-218.

[Fr1]. G Freiman, *Foundations of a structural theory of set addition*, in Translations of Math. Monographs, vol. 37, AMS, 1973.

[Fr2]. ———, *On the addition of finite sets*, I, Izv Vysh. Zaved. matematika **13(6)** (1959), 202-213.

[Fr3]. ———, *Inverse problems of additive number theory* VI*, on the addition of finite sets* III, Izv. Vysh. Ucheb, Zaved. Matematika **28(3)** (1962), 151-157.

[H-T]. R. R. Hall and G. Tenenbaum, *Divisors*, Number 90 in Cambridge Tracts in Mathematics, Cambridge University Press, Cambridge (1988)..

[K-T]. N. Katz and T. Tao, *Some connections between the Falconer and Furstenburg conjectures*, New York J. Math.

[Na1]. M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, springer, 1996.

[Na2]. ———, *The simplest inverse problems in additive number theory*, in Number Theory with an Emphasis on the markoff Spectrum (A. Pollington and W. Moran, eds.), Marcel Dekker, 1993, pp. 191-206.

[Na3]. ———, *On sums and products of integers*, submitted, 1994.

[N-T]. M. Nathanson and G. Tenenbaum, *Inverse theorems and the number of sums and products*, in Structure theory of Set addition, Astérisque 258, 1999.

[Ru]. I. Ruzsa, *Generalized arithmetic progressions and sumsets*, Acta Math. Hungar. **65** (1995), 379-388, no 4.

[S-T]. E. Szemerédi and W. Trotter, *Extremal problems in discrete geometry*, Combinatorica **3** (1983), 381-392.

[T]. T. Tao, *From rotating needles to stability of waves: emerging connections between combinatorics, analysis and PDE*, Notices, Amer. Math. Soc.