SOME CONSEQUENCES OF THE
POLYNOMIAL FREIMAN-RUZSA CONJECTURE

Mei-Chu Chang

Summary. Assuming the weak polynomial Freiman-Ruzsa conjecture, we derive some consequences on sum-product and the growth of subset of $SL_3(\mathbb{C})$.

Résumé. En Supposant la conjecture polynomiale faible de Freiman-Ruzsa, on en déduit certaines conséquences sur les ensembles sommes-products ainsi que sur la croissance de sous-ensembles de $SL_3(\mathbb{C})$.

Version française abrégée

Soit $A$ un sous-ensemble fini d’un espace vectoriel $V$ et désignons $A + A = \{x + y : x, y \in A\}$ l’ensemble somme (de même, $nA = (n-1) + A$). Un lemme due à Freiman affirme que si $|A + A| < K|A|$ et $|A| > cK^2$, l’espace $\langle A \rangle$ engendré par $A$ est de dimension inférieure à $K$.

La conjecture polynomiale faible de Freiman-Ruzsa (WPFRC) est l’énoncé suivant: Si $A$ satisfait $|A + A| < K|A|$, il existe un sous-ensemble $A_1$ de $A$ telle que $|A_1| > K^{-c}|A|$ et $A_1 \subset \mathbb{Z}\xi_1 + \cdots + \mathbb{Z}\xi_d, \xi_i \in V$ et $d < c \log K$ où $c$ est une constante absolue.

Notons que WPFRC est une conséquence de la conjecture polynomiale de Freiman-Ruzsa (voir [TV] pour la formulation de celle-ci). Dans cette note, nous précisons quelques conséquence de la WPFRC et un théorème profond de Evertse-Schlickewei-Schmidt [ESS] sur des relations linéaires dans un sous-groupe de $\mathbb{C}^*$ de rang borné.
Théorème 1. Supposons WPFRC. Etant donné \( n \in \mathbb{Z}_+ \) et \( \varepsilon > 0 \), il existe \( \delta > 0 \) telle que si \( A \subset \mathbb{C}^* \) est un ensemble fini et
\[
|AA| < |A|^{1+\delta}
\]
(en supposant \( |A| \) suffisamment grand), on a
\[
|nA| > |A|^{n(1-\varepsilon)}.
\]

On a également la propriété suivante pour la croissance d’ensembles finis dans un groupe linéaire.

Théorème 2. Supposons WPFRC. Si \( A \subset SL_3(\mathbb{C}) \) satisfait
\[
|AA| < K|A|
\]
(\( |A| \) fini et suffisamment grand), il existe un sous-ensemble \( A' \) de \( A \) telle que
\[
|A'| > K^{-c}|A|
\]
et \( A' \) contenu dans un coset d’un sous-groupe nilpotent (\( c \) une constante absolue).

D’autre part nous mentionnons certains résultats plus faibles et ne dépendent pas de cette conjecture.

Notations.

The \( n \)-fold sum set and the \( n \)-fold product set of \( A \) are
\[
nA = A + \cdots + A = \{ a_1 + \cdots + a_n : a_1, \ldots, a_n \in A \}
\]
and
\[
A^n = A \cdots A = \{ a_1 \cdots a_n : a_i \in A \}
\]
respectively. The inverse set \( A^{-1} \) can be defined similarly. Let further
\[
A^{[n]} = (\{1\} \cup A \cup A^{-1})^n.
\]
The notation \( A^n \) is also used for the \( n \)-fold Cartesian product, when there is no ambiguity.

§1. Freiman’s theorem and related conjectures.
One way to formulate the Polynomial Freiman-Ruzsa Conjecture is as follows.

Let $V$ be a $\mathbb{Z}$-module and $A \subset V$ a finite set satisfying

$$|A + A| < K|A|. \quad (1.1)$$

Then there exist a positive integer $d \in \mathbb{Z}_+$, a subset $A_1 \subset A$, a convex subset $B \subset \mathbb{R}^d$ and a group homomorphism $\phi : \mathbb{Z}^d \to V$ such that

$$d < c \log K, \quad (1.2)$$
$$|A_1| > K^{-c}|A|, \quad (1.3)$$
$$\phi(B \cap \mathbb{Z}^d) \supset A_1, \quad (1.4)$$
$$|B \cap \mathbb{Z}^d| < K^c|A|. \quad (1.5)$$

Here $c$ is an absolute constant.

Recall that if $A$ satisfies (1.1) and $cK^2 < |A|$, then $A \subset \phi(B \cap \mathbb{Z}^d)$ with $d \leq K$ and $B \subset \mathbb{R}^d$ a box satisfying

$$|B| < \exp(cK^2 \log^3 K)|A|. \quad (1.6)$$

(Quantitative version of Freiman’s theorem from [C1].)

More relevant in this note is the much simpler Freiman Lemma, stating that if (1.1) holds and $|A| > cK^2/\varepsilon$, then $A \subset \phi(\mathbb{Z}^d)$ with $d \leq [K - 1 + \varepsilon]$

The Polynomial Freiman-Ruzsa Conjecture implies in particular the following weaker conjecture, which is all we will use.

**Weak Polynomial Freiman-Ruzsa Conjecture (WPFRC).** If $A \subset V$ satisfies $|A + A| < K|A|$, then there exist a subset $A_1 \subset A$ with $|A_1| > K^{-c}|A|$, and elements $\xi_1, \ldots, \xi_d \in V$ with $d < c \log K$, so that

$$A_1 \subset \mathbb{Z}\xi_1 + \cdots + \mathbb{Z}\xi_d, \quad (1.7)$$

where $c$ is an absolute constant.

Note that if $A \subset \mathbb{R}_+$ is finite satisfying

$$|AA| < K|A| \quad (1.8)$$

and considering the set $\log A \subset \mathbb{R} =: V$, one would derive that there are elements $\eta_1, \ldots, \eta_d \in \mathbb{R}^*$ with $d < c \log K$ such that

$$|A \cap G| > K^{-c}|A|, \quad (1.9)$$

3
where $G < \mathbb{R}^*$ denotes the multiplicative group generated by $\eta_1, \ldots, \eta_d$.

The analogous statement would hold equally well for a finite subset $A \subset \mathbb{C}^*$ satisfying (1.8).

§2. Sets with small product sets.

We recall the deep theorem of Evertse-Schlickewei-Schmidt ([ESS], Theorem 1.1) on linear equations in multiplicative groups.

**Theorem ESS.** Let $\Gamma$ be a subgroup of the multiplicative group $(\mathbb{C}^*)^n$ of rank $r$ and let $a_1, \ldots, a_n \in \mathbb{C}^*$. Then the equation

$$a_1x_1 + \cdots + a_nx_n = 1 \quad \text{with } (x_1, \ldots, x_n) \in \Gamma$$

has at most

$$\exp((6n)^3(r + 1))$$

non-degenerate solutions, meaning that no proper subsum of $a_1x_1 + \cdots + a_nx_n$ vanishes.

The precise bound (2.2) is very important for our purpose.

Let $G < \mathbb{C}^*$ be a group generated by $d$ elements $\eta_1, \ldots, \eta_d$ with $d < c \log K$, and let $\Gamma = G^n$. Since $\Gamma$ is generated by the elements $(1, \ldots, \eta_i, \ldots, 1)$, we have $r := \text{rank } \Gamma \leq nd$. Therefore, given $a_1, \ldots, a_n \in \mathbb{C}^*$, the equation

$$a_1x_1 + \cdots + a_nx_n = 1 \quad \text{with } x_1, \ldots, x_n \in G$$

has at most

$$\exp((6n)^3(nd + 1)) < \exp(cn(6n)^3\log K) = K^{C(n)}$$

non-degenerate solutions, where $C(n)$ is a constant depending on $n$.

For $S_1, \ldots, S_n \subset \mathbb{C}$, we denote the additive energy of $S_1, \ldots, S_n$ by

$$E(S_1, \ldots, S_n) = |\{(x_1, y_1, \ldots, x_n, y_n) \in S_1^2 \times \cdots \times S_n^2 : x_1 + \cdots + x_n = y_1 + \cdots + y_n\}|$$

Recall the following lower bound on the size of the sum-set $S_1 + \cdots + S_n$.

$$|S_1 + \cdots + S_n| \geq \frac{|S_1|^2 \cdots |S_n|^2}{E(S_1, \ldots, S_n)}.$$  (2.5)
Corollary 1. Let $G < \mathbb{C}^*$ be a group generated by $d$ elements with $d < c \log K$ and let $A_1 \subset G$ be finite. Then

$$E(A_1, \ldots, A_1) \leq K^{C(n)} |A_1|^{n-1} + \frac{(2n)!}{n!} |A_1|^n,$$

where $C(n)$ is a constant depending on $n$.

Proof. Consider the equation

$$x_1 + \cdots + x_n - x_{n+1} - \cdots - x_{2n} = 0, \quad x_i \in A_1. \quad (2.7)$$

We decompose (2.7) in minimal vanishing subsums. Each decomposition corresponds to a partition

$$\{1, \ldots, 2n\} = \bigcup_{\alpha=1}^{\beta} E_\alpha. \quad (2.8)$$

Since $|E_\alpha| \geq 2$, we have $\beta \leq n$. The case $\beta = n$ clearly contributes to the last term in (2.6). If $|E_\alpha| \geq 3$, we rewrite the equation

$$\sum_{i \in E_\alpha} \pm x_i = 0 \quad (2.9)$$

as

$$\sum_{i \in E_\alpha \setminus \{r_1\}} \pm \frac{x_i}{x_{r_1}} = 1. \quad (2.10)$$

(Specify some element $r_1 \in E_\alpha$.) Since no subsum of (2.9), (2.10) is assumed to vanish, the estimate (2.4) in Theorem ESS applies for the number of non-degenerate solutions of

$$\sum_{i \in E_\alpha \setminus \{r_1\}} \pm \frac{z_i}{z_{r_1}} = 1 \quad \text{with } z_i \in G. \quad (2.11)$$

Therefore (2.9) has at most

$$K^{C(|E_\alpha|)} |A_1| \quad (2.12)$$

non-degenerate solutions. It follows that the number of solutions of (2.7) corresponding to the partition (2.8) is bounded by

$$|A_1|^{\beta} \prod_{\alpha=1}^{\beta} K^{C(|E_\alpha|)}, \quad (2.13)$$

where $\beta \leq n - 1$. Summing over all possible partitions, we prove (2.6). \[\square\]

The next corollary is conditional to the Weak Polynomial Freiman-Ruzsa Conjecture.
Corollary 2. Assume WPFRC. Given \(n \in \mathbb{Z}_+\) and \(\varepsilon > 0\), there is \(\delta > 0\) such that if \(A \subset \mathbb{C}^*\) is finite with \(|A|\) large and

\[ |AA| < |A|^{1+\delta}, \tag{2.14} \]

then the \(n\)-fold sumset \(nA\) satisfies

\[ |nA| > |A|^{n(1-\varepsilon)}. \tag{2.15} \]

Proof. Take \(K = |A|^\delta\) in (1.8). WPFRC, Corollary 1 (letting \(A_1 = A \cap G\) in (1.9)), and (2.5) imply

\[
|nA| \geq |nA_1| \geq \frac{|A_1|^{2n}}{K^{c(n)} |A_1|^{n-1} + \frac{(2n)!}{n!} |A_1|^n} \\
> \min \left( \frac{n!}{(2n)!} |A_1|^n, K^{-C(n)} |A_1|^{n+1} \right) \\
> \min \left( \frac{n!}{(2n)!} K^{-c_1 n} |A|^n, K^{-C(n)} |A|^{n+1} \right). \tag{2.16} \]

Note that one has the following stronger conclusion.

Corollary 3. Assume WPFRC. Given \(n \in \mathbb{Z}_+\) and \(\varepsilon > 0\), there is \(\delta > 0\) such that if \(A \subset \mathbb{C}^*\) is a sufficiently large finite set satisfying (2.14) and \(B \subset A\) is any subset such that

\[ |B| > |A|^\varepsilon, \tag{2.17} \]

then

\[ |nB| > |B|^{n(1-\varepsilon)}. \tag{2.18} \]

Proof. As in the proof of Corollary 2, we start from \(A_1 = A \cap G\) satisfying (1.9). Let \(z_1, \ldots, z_s\) be a maximal subset of \(A\) such that \(z_i A_1 \cap z_j A_1 = \emptyset\) for any \(i \neq j\). Hence

\[ s \leq \frac{|AA_1|}{|A_1|} \leq K^c \frac{|AA|}{|A|} < K^{c+1} \tag{2.19} \]

and by construction, if \(z \in A\), then \(z A_1 \cap z_i A_1 \neq \emptyset\) for some \(1 \leq i \leq s\). Therefore,

\[ A \subset \bigcup_{i=1}^{s} z_i A_1 A_i^{-1} \tag{2.20} \]
and
\[ B \subset \bigcup_{i=1}^{s} (B \cap z_i A_1 A_1^{-1}). \]

Hence there is \(1 \leq i \leq s\) such that
\[ \left| B_1 := B \cap z_i A_1 A_1^{-1} \right| \geq \frac{|B|}{s}. \quad (2.21) \]

Note that since \(A_1 A_1^{-1} \subset G\), Corollary 1 remains valid for \(z_i^{-1} B_1 \subset A_1 A_1^{-1}\). In (2.16) \(A, A_1\) are replaced by \(B, B_1\). (Note also that \(|z_i^{-1} B_1| = |B_1|\), etc.) \(\square\)

There are various weaker forms of Corollary 2 and Corollary 3 that hold unconditionally. The following is a version of Corollary 2.

**Proposition 4.** Given \(m > 1\), there is \(\delta > 0\) and \(n \in \mathbb{Z}_+\) such that if \(A \subset \mathbb{C}^*\) is a sufficiently large finite set satisfying
\[ |AA| < |A|^{1+\delta}, \quad (2.22) \]
then
\[ |nA| > |A|^m. \quad (2.23) \]

Using the terminology in [TV], a set \(A\) satisfying (2.22) is called an *approximate multiplicative group*. It was shown in [B] (See also [TV], Theorem 2.60.) that given \(H \neq \emptyset\) in \(\mathbb{F}_p\) with \(|HH| \leq K|H|\), and \(m > 1, \varepsilon > 0\), there is an integer \(n = n(m, \varepsilon) \in \mathbb{Z}_+\) such that
\[ |nH| > c(m, \varepsilon)K^{-C(m, \varepsilon)} \min(|H|^m, p^{1-\varepsilon}). \quad (2.24) \]

For \(A \subset \mathbb{C}^*\), the same argument allows to show that
\[ |nA| > c(m, \varepsilon)K^{-C(m, \varepsilon)} |A|^m \quad (2.25) \]
and hence the proposition holds.

Regarding Corollary 3, there is the result from [BC1] for finite subsets \(A \subset \mathbb{Z}\) and generalized in [BC2] for sets \(A\) of algebraic numbers of bounded degree.
Proposition 5. Given \( d, n \in \mathbb{Z}_+ \) and \( \varepsilon > 0 \), there is \( \delta > 0 \) such that the following holds. Let \( A \subset \mathbb{C}^* \) be a sufficiently large finite set of algebraic numbers of degree at most \( d \). Assume
\[
|AA| < |A|^{1+\delta}.
\]
(2.26)
Then, for any nonempty subset \( B \subset A \),
\[
|nB| > |A|^{-\varepsilon}|B|^n.
\]
(2.27)

Note that in Proposition we do not require all elements of \( A \) to be contained in the same extension of \( \mathbb{Q} \) of bounded degree. This bounded degree hypothesis is removed because of WPFRC.

§3. Finite subsets of linear groups.

We recall the following theorem from [C2], [C3].

For all \( \varepsilon > 0 \), there is \( \delta > 0 \) such that if \( A \subset SL_3(\mathbb{Z}) \) is a finite set, then one of the following alternatives holds.

(i) \( A \) intersects a coset of a nilpotent subgroup in a set of size at least \( |A|^{1-\varepsilon} \).

(ii) \( |A^2| > |A|^{1+\delta} \).

The proof makes essential use of Theorem ESS, applied with \( \Gamma \) the unit group of the extension of a cubic polynomial over \( \mathbb{Q} \). This is the only significant place where a generalization to subset \( A \subset SL_3(\mathbb{C}) \) is problematic. Here we will discuss in some greater detail how the WPFRC allows us to recover the theorem in its full strength for subsets \( A \subset SL_3(\mathbb{C}) \).

Theorem 6. Assume WPFRC. Given a finite subset \( A \subset SL_3(\mathbb{C}) \) satisfying
\[
|AA| < K|A|,
\]
(4.1)
then there is a subset \( A' \subset A \) such that
\[
|A'| > K^{-c}|A|
\]
(4.2)
and \( A' \) is contained in a coset of a nilpotent group.

Proof. An initial key step in [C2] (borrowed from Helfgott’s work [H]) is to construct a set \( D \subset A^{-1}A \) of commuting elements, where
\[
|D| > K^{-C}|A|^\theta
\]
(4.3)
with $C, \theta$ absolute constants. This step is completely general and applies equally well to subsets $A \subset \text{SL}_d(\mathbb{C})$ with $\theta = \theta(d)$. Change of bases permits simultaneous diagonalization of the elements of $D$. They form the key ingredient in the amplification.

Going back to (4.1), one applies first Tao’s non-commutative version of the Balog-Szemerédi-Gowers Lemma (see [TV]) and replaces $A$ by a subset $A_1 \subset A$ satisfying that

$$|A_1| > K^{-c}|A|$$

(4.4)

and $A_1$ is an approximate group, i.e. there is a subset $X \subset \text{SL}_d(\mathbb{C})$ such that

$$|X| < K^c \quad \text{and} \quad A_1 A_1 \subset X A_1 \cap A_1 X,$$

(4.5)

where $c$ is an absolute constant.

Identifying $A$ and $A_1$ and using (4.5), one can control the size of all product sets

$$|A^{[s]}| < K^{cs}|A|$$

(4.6)

for given $s \in \mathbb{Z}^*$. Let $D \subset A^{-1} A \subset A^{[2]}$ be the diagonal set obtained above, satisfying (4.3). The next aim is to ensure that $D$ has small multiplicative doubling.

Denote the set of diagonal matrices over $\mathbb{C}$ by $D$ and let $D_s = D \cap A^{[s]}$ for $s \geq 2$. Hence $D_s \supset D_2 \supset D$ satisfies (4.3). Consider a minimal subset $B \subset A^{[2]}$ satisfying

$$A^{[2]} \subset B D.$$  

(4.7)

It follows that

$$g D \cap g' D = \emptyset, \quad \forall g \neq g' \in B$$

(4.8)

and also

$$A^{[2]} \subset B D_4.$$  

(4.9)

Therefore, $|A| \leq |A^{[2]}| \leq |B||D_4|$. Also, $D_4 D_4 \subset D_8$ and by (4.8) and (4.6)

$$|D_8||B| = |D_8 B| \leq |A^{[10]}| < K^{10c}|A|. $$

(4.9)

Consequently

$$|D_4 D_4| \leq |D_8| \leq K^{10c} \frac{|A|}{|B|} \leq K^{10c} |D_4|. $$

(4.10)

Replacing $D$ by $D_4$, we obtain a subset of diagonal matrices in $A^{[4]}$ satisfying (4.3) and

$$|D D| < K^c |D|.$$  

(4.11)
To use Theorem ESS, we need a large subset of $D$ whose entries lie in a subgroup of $C$ of small rank. Let $D'$ be the projection of $D$ on the $(1,1)$ entry

$$\pi : D \to D', \quad (g_{i,j}) \mapsto g_{1,1}. $$

By the lemma below, there are subsets $E' \subset D'$ and $E := \pi^{-1}(E') \subset D$ such that for some $h$

$$\left|\pi^{-1}(x)\right| \sim h, \quad \forall x \in E'$$

and

$$|E| > \frac{1}{\log K} |D|. \quad (4.12)$$

We note that

$$|E| \sim h|E'| \quad \text{and} \quad |EE| > h|E'E'|.$$

Thus, $|EE| < |DD| < K(\log |K|)|E|$ implies

$$|E'E'| < K(\log |K|)|E'|.$$

Next, we apply WPFRC to get a subset $F' \subset E'$ such that $|F'| > K^{-c}|E'|$ and $F'$ is contained in a subgroup $\Gamma_1 < C$ with $\text{rank}(\Gamma_1) < c \log K$. Let

$$F = \pi^{-1}F' \subset E.$$

Hence

$$|F| > \frac{1}{K^c} |E|.$$

Replace $D$ by $F$ and start over with the projection on the $(2,2)$ entry etc. Eventually one gets a subset $F$ of $D$ that is large and each $(i,i)$-projection sits in a group $\Gamma_i$ of small rank. Therefore the multiplicative group $\Gamma$ spanned $\{\Gamma_i\}_{i=1}^{3}$ has rank bounded by $c \log K$ and one can apply Theorem ESS on $\Gamma$. □

**Lemma 7.** Let $A \subset A' \times R$ be finite and let $\pi : A \to A'$ be the projection to the first coordinate. Assume

$$|2A| = |A + A| < K|A|. \quad (4.13)$$

Then there exist $C \subset A$ such that $|C| > \frac{1}{2 \log K} |A|$ and for every $x \in C$, $|\pi^{-1}(\pi(x))| \sim h$ for some $h$.

**Proof.** Let $m = \max\{|\pi^{-1}(x)| : x \in A'\}$. Then

$$|2A| \geq |A'| m \quad (4.14)$$
and
\[ |3A| \geq |2A'| m. \quad (4.15) \]

Obviously
\[ |A| \leq |A'| m. \quad (4.16) \]

Plünnecke's inequality and (4.13) imply
\[ |3A| < K^3 |A|. \quad (4.17) \]

Hence (4.15), (4.17) and (4.16) imply
\[ |2A'| < K^3 |A'|. \quad (4.18) \]

Also, since by (4.13) and (4.14),
\[ |A| > |A'| \frac{m}{K}, \]

there is clearly a subset \( B \subset A \) such that \(|B| > \frac{1}{2}|A|\) and \( \forall x \in B, |\pi^{-1}(\pi(x))| > \frac{m}{2K} \).

On the other hand, \(|\pi^{-1}(\pi(x))| \leq m\) is obvious. Hence, proceeding with \( B \) instead of \( A \), there is a further subset \( C \subset B \) with fibers of comparable size and so that \(|C| > \frac{1}{\log K}|B|\). \( \square \)

**Remarks.**

1. We expect that generalization of the theorem to subsets \( A \subset SL_d(\mathbb{Z}) \), with \( d \) arbitrary, is only a technical matter.

2. It may be possible to reach the conclusion of Theorem 6 unconditionally by following the approach in [H].

3. Statements of this type have been suggested by B. Green.

**References**


[BC2]. ____, *Sum-product theorems in algebraic number fields*, Journal d'Analyse Mathematique.


Department of Mathematics, University of California, Riverside CA 92521 USA

E-mail address: mcc@math.ucr.edu