On a question of Sárközy and Sós on bilinear forms

Juanjo Rué
Joint work with Javier Cilleruelo

Departament de Matemàtica Aplicada 2 (MA2),
Universitat Politècnica de Catalunya (UPC)
A well known conjecture...

Conjecture (Erdös-Turan Conjecture)

If $A \subset \mathbb{N}$ is an infinite sequence then the representation function $r(n) = \#\{(a, a') \mid a + a' = n, \ a \leq a', \ a, a' \in A\}$ is not bounded.

Too much difficult for us...

We consider a “easier” problem.
¿What type of things do we want to study?

Change “bounded” by “constant for $n$ large enough”.

↓

¡In this situation many things are made, and many things are needed to be made!
Formulation of the problem: 
the question of Sárkozy and Sós

Let $k_1, k_2, \ldots, k_s$ be such that $\gcd(k_1, k_2, \ldots, k_s) = 1$.

Fix $A \subset \mathbb{N}$ and define

$$r_{k_1,k_2,\ldots,k_s}(n) = |\{k_1x_1 + \cdots + k_sx_s = n, x_1, x_2, \ldots, x_s \in A\}|$$

**Problem**

Does it exist an infinite set $A \subset \mathbb{N}$ such that the representation function $r_{k_1,k_2,\ldots,k_s}(n)$ is constant for $n$ large enough?
To start with...

It should be better to start with $s = 2$...

**Problem (Problem for bilinear forms)**

Let $k_1, k_2$ be such that $1 \leq k_1 < k_2$, $(k_1, k_2) = 1$.

Does it exist an infinite set $\mathcal{A} \subset \mathbb{N}$ such that the representation function $r_{k_1, k_2}(n)$ is constant for $n$ large enough?
The language of generating functions (GF)

For every set \( A \subseteq \mathbb{N} \) we write

\[
f_A(z) := f(z) = \sum_{a \in A} z^a
\]

**EXAMPLES**

- \( A = \{3, 5, 8, 234\} \rightarrow f(z) = z^3 + z^5 + z^8 + z^{234} \).
- \( A = \mathbb{N} \rightarrow f(z) = 1 + z + z^2 + \cdots = \frac{1}{1-z} \).
- \( A = 4\mathbb{N} + 3 \rightarrow f(z) = z^3(1 + z^4 + z^8 + \cdots) = \frac{z^3}{1-z^4} \).

In all cases, \( f(z) \) defines an analytic function around \( z = 0 \).

If \( |A| = \infty \), \( f \) has radius of convergence \( 1/\rho = 1 \) and at least one singularity at \( z = 1 \).
Translation into the realm of generating functions

If \( k_1 a + k_2 b = k_1 b + k_2 a \rightarrow a = b \Rightarrow \text{NO SYMMETRY!} \)

This problem is translated into the GF realm in this way:

Suppose that \( r_{k_1, k_2}(n) = c \) for all \( n \geq n_0 \). Then

\[
\begin{align*}
    f(z^{k_1})f(z^{k_2}) &= \sum_{a, b \in A} z^{k_1 a + k_2 b} = \sum_{n=0}^{\infty} r_{k_1, k_2}(n)z^n = \sum_{n=0}^{\infty} cz^n + Q(z)
\end{align*}
\]

where \( Q(z) \) is a polynomial in \( \mathbb{Z}[z] \).
An analytic problem

We can “forget” the combinatorial problem and try to solve the following analytic problem:

**Does it exist a GF** $f$ **which defines an analytic function on** $z = 0$ **with radius of convergence 1 such that**

$$f(z^{k_1})f(z^{k_2}) = \frac{P(z)}{1 - z}$$

**for some** $P(z) \in \mathbb{Z}[z]$ **with the property** $P(1) \neq 0$?

To ask this question we will use a little of analysis (infinite products, “zeros” of a function) and a little of algebra (roots of the unit, cyclotomic polynomials)
Easy cases: unordered case

The case $k_1 = k_2$ is well known for a long time ago:

**Theorem (Dirac, 1951)**

If $A \subset \mathbb{N}$ is an infinite sequence then the representation function $r(n) = \#\{(a, a'), a + a' = n, a \leq a', a, a' \in A\}$ is not eventually constant.

The fundamental equation is

$$\frac{f(z)^2 + f(z^2)}{2} = \frac{P(z)}{1 - z}$$

Make $z \to -1$ in the region of analicity of $f$...and that’s all!
**Easy cases (I): \( A + kA \)**

We try with \( P(z) = 1 \):

\[
f(z)f(z^k) = \frac{1}{1 - z}
\]

We apply Moser’s argument (An application of generating series, 1962):

\[
\begin{align*}
f(z)f(z^k) &= \frac{1}{1 - z} \\
f(z^k)f(z^{k^2}) &= \frac{1}{1 - z^k}
\end{align*}
\]

\[
\left\{ \begin{array}{c}
f(z)f(z^k) = \frac{1}{1 - z} \\
f(z^k)f(z^{k^2}) = \frac{1}{1 - z^k}
\end{array} \right\} \rightarrow f(z) = f(z^{k^2}) \frac{1 - z^k}{1 - z} = \ldots
\]

So, we obtain that:

\[
f(z) = (1 + z + \cdots + z^{k-1})(1 + z^{k^2} + \cdots + z^{k^3-k^2}) \ldots
\]
**Easy cases (and II):** \( A + kA \)

Is \( f \) a good solution for our problem?

- \( f \) defines an analytic function around 0.
- All its Taylor’s coefficients are either 0 or 1 by the unique representation of integers in basis \( k \).

For example, for \( k = 2 \),

\[
f(z) = (1 + z)(1 + z^4)(1 + z^{16})\ldots
\]

and \( A \) is the set of integers whose representation in basis 2 has 0 in the powers \( 2 \cdot 4^n \).

\[
f(z)f(z^2) = (1 + z)(1 + z^2)(1 + z^4)\cdots = 1 + z + z^2 + z^3 + \ldots
\]

(unique representation in basis 2)
Main problem: $2A + 3A$

Which are the main problems here?

- We cannot apply Moser’s argument, or we don’t know to adapt it...
- Formal manipulation doesn’t give us many things...
- Analytic problems over the circle of radius 1: $f$ cannot be treated as an analytic function...

Instead of trying to find $f$, we concentrate on proving that such an $f$ cannot exist...

¡AND WE SUCCEED!
Main problem: notation used

We write

\[ \xi_n = e^{2\pi i / 2^n} ; \omega_m = e^{2\pi i / 3^m} ; \mu_{n,m} = e^{2\pi i / (2^n 3^m)}. \]

The **conjugates** of \( \xi_n \) are the complex numbers of the form:

\[ \xi_r^n : \gcd(r, 2^n) = 1 \]

(*mutatis mutandis* for \( \omega_m, \mu_{n,m} \))

For a point \( \alpha \in \mathbb{C}, |\alpha| = 1 \), we denote by \( f(\alpha) \) the value of the radial limit of \( z \) towards \( \alpha \). (Possibly \( \infty \), possibly it do not exist)
Main problem: a little about cyclotomic polynomials

The cyclotomic polynomial of degree \( n \) \((\text{Irr}(e^{2\pi i/n}, \mathbb{Q}))\) is denoted by \( \Phi_n(z) \).

Recall two points:

- The roots of \( \Phi_{2^n}(z) \) are \( \xi_n \) and its conjugates.
- If \( P(z) \in \mathbb{Z}[z] \) and \((z - e^{2\pi i/n})|P(z)\) then \( \Phi_n(z)|P(z) \).

We write

\[
P(z) = \overline{P}(z) \prod_{n=0}^{\infty} \Phi_{2^n}(z)^{s_n}
\]

where \( s_n = 0 \) for \( n > n_0 \) for some \( n \) (\( P \) is a POLYNOMIAL!)
**Sketch of the proof: a reformulation and a crucial definition**

We work with \( F(z) = f^2(z) \):

\[
F(z^2)F(z^3) = \frac{P^2(z)}{(1 - z)^2}
\]

With this notation, and \( \alpha \in \mathbb{C}, |\alpha| = 1 \) we say that:

- \( F(z) \) has a **zero of order** \( r \) at \( \alpha \) if
  
  \[
  \lim_{z \to \alpha} \frac{F(z)}{(z - \alpha)^r}
  \]
  
  is neither \( \infty \) nor 0. (\( r \) possibly negative, possibly rational)

- \( F \) is **good** at \( \alpha \) if it do not have a zero at \( \alpha \). (zero of order 0)
Sketch of the proof: behavior of $F$ over $\xi_n$

Try to compute $F(1)$:

$$F(1)^2 = \frac{P(1)^2}{1-1} \rightarrow F(1) \rightarrow \infty$$

Writing $F(z) = (1 - z)^{r_0} G(z)$ we obtain that $r_0 = -1$ and $G$ is good at $z = 1$.

Denote by $r_n$ the order of the zero of $F$ in $z = \xi_n$.

Lemma

$F$ has a zero of odd (in particular, $\neq 0!!$) order $r_n$ in $\xi_n$ and in all its conjugates, and the values $r_n$ satisfies the recurrence relation:

$$r_0 = 1, r_n + r_{n-1} = 2s_n$$

The same lemma holds for $\omega_m$ and its conjugates...
Sketch of the proof: a graphic representation

The previous lemma says to us that \( F(\xi_n) \) is either 0 or \( \infty \). This information can be represented in the following way:

\[
\begin{array}{ccccccc}
0 & 1 & 2 & 3 & 4 & \ldots & s-1 & s & s+1 & \ldots \\
\hline
\infty & 0 & 0 & \infty & 0 & \ldots & \infty & 0 & \infty & \ldots
\end{array}
\]

There are two regions:

1. **The transitory region**: depending on \( s_n \), we have either a 0 or an \( \infty \). This region is bounded.

2. **The stationary region**: alternating sequence 0, \( \infty \), 0, \( \infty \), \ldots

In any case we obtain the sequence \( \infty, \infty \).

We do the same in the vertical axe, and we want to complete all the interior positions with either and 0 or a \( \infty \ldots \)
**Sketch of the proof: a crucial rule for the stationary region**

Observe that $\mu_{n,m}^2 = \mu_{n-1,m}$ and $\mu_{n,m}^3 = \mu_{n,m-1}$.

Denote by $r_{n,m}$ the degree of the zero of $F$ on $\mu_{n,m}$

Then, in the stationary region, $r_{n-1,m} + r_{n,m-1} = 0$, because,

$$F(\mu_{n,m}^2)F(\mu_{n,m}^3) = F(\mu_{n-1,m})F(\mu_{n,m-1}) = \frac{P^2(\mu_{n,m})}{(1 - \mu_{n,m})^2} \neq 0$$

Because $r_{n,0} = r_n$ we can make this calculus recursively!
Sketch of the proof: the pieces of the puzzle do not fit!
¿And the general case?

¡Change 2 by $k_1$ and 3 by $k_2$ and the same argument works!
**Conclusions**

\[ A + kA \text{ work and } 2A + 3A \text{ do not work because:} \]

1. The case \( A + kA \) works because \((1, k) = 1\) but \(1|k\) for all \(k\).
2. In the problem \( k_1A + k_2A \) we have the first condition but the second do not hold.

The previous ideas can be used to prove something similar but writing “periodic” instead of “constant”.
Some results on multilinear forms

1. The same problem for $A + A + \ldots + A$ is easy if $p$ is a prime number.

2. If not, we must use a little of Cauchy’s integrals...

3. The next step is try to generalize the previous arguments to $k_1A + \cdots + k_rA$, where $\text{gcd}(k_i, k_j) = 1$ for $i \neq j$.

“...Estamos trabajando en ello...”
To conclude...

¿And all of this... can be used to solve Erdos-Turan conjecture?

The assumption of polynomial is crucial to establish a stationary region (Where all works)

Theorem (Sz"ego’s Theorem)

Let $f(z)$ be an analytic function at the origin whose Taylor coefficients belongs to a finite set. Then, either $f(z)$ can be extended to a rational function or its natural boundary is the circle or radius 1.
...The key point must be...

Distribution of Taylor’s coefficients

Distribution of singularities in the unit circle
¡Muchas gracias por vuestra atención!\footnote{Thank you for your attention!}