Sum-product estimates for rational functions

Boris Bukh

May 2010

A story of a romance between graphs and arithmetic

Joint work with Jacob Tsimerman

Addition and multiplication are separate

The sumset $A + B = \{a + b : a \in A,\ b \in B\}$

The productset $AB = \{ab : a \in A,\ b \in B\}$

Examples:

$A = \{1, 2, 3, 4, \dots, n\}$ $\quad |A + A| = 2n - 1$

$A = \{1, 2, 4, 8, \dots, 2^n\}$ $\quad |A + A| = n(n + 1)/2$

Theorem (Erdős–Szemerédi'83)

If $A \subset \mathbb{R}$ is a finite set, then

$$|A + A| + |AA| \gg |A|^{1+c}$$

for some absolute constant $c > 0$.

Addition and multiplication are separate

The sumset $A + B = \{a + b : a \in A,\ b \in B\}$
The productset $AB = \{ab : a \in A,\ b \in B\}$

Examples:
$A = \{1, 2, 3, 4, \ldots, n\}$ $|A + A| = 2n - 1$
$A = \{1, 2, 4, 8, \ldots, 2^n\}$ $|A + A| = n(n + 1)/2$

Theorem (Erdős–Szemerédi'83, . . . , Solymosi'08)

If $A \subset \mathbb{R}$ is a finite set, then

$$|A + A| + |AA| \gg |A|^{1+c}$$

for $c = 1/3 - o(1)$.

Addition and multiplication are separate

Theorem (Bourgain–Katz–Tao'04)

If $A \subset \mathbb{F}_p$ is of size $p^\epsilon \le |A| \le p^{1-\epsilon}$, then

$$|A + A| + |AA| \gg |A|^{1+c}$$

for some constant $c = c(\epsilon)$.

Addition and multiplication are separate

Theorem (Bourgain–Katz–Tao'04, Bourgain–Konyagin'03)

If $A \subset \mathbb{F}_p$ is of size $1 \leq |A| \leq p^{1-\epsilon}$, then

$$|A + A| + |AA| \gg |A|^{1+c}$$

for some constant $c = c(\epsilon)$.

Addition and multiplication are separate

Theorem (Bourgain–Katz–Tao'04, Bourgain–Konyagin'03)

If $A \subset \mathbb{F}_p$ is of size $1 \le |A| \le p^{1-\epsilon}$, then

$$|A+A| + |AA| \gg |A|^{1+c}$$

for some constant $c = c(\epsilon)$.

Six years and dozens of papers later:

$$|A+A|+|AA| \gg \begin{cases} |A|^{13/12}, & \text{if } |A| \le p^{1/2}, \\ |A|^{13/12}(|A|/\sqrt{p})^{1/12-o(1)}, & \text{if } p^{1/2} \le |A| \le p^{35/68}, \\ |A|(p/|A|)^{1/11-o(1)}, & \text{if } p^{35/68} \le |A| \le p^{13/24}, \\ |A| \cdot |A|/\sqrt{p}, & \text{if } p^{13/24} \le |A| \le p^{2/3}, \\ |A|(p/|A|)^{1/2}, & \text{if } |A| > p^{2/3}. \end{cases}$$

Rational functions

A rational function $f(x,y)$ is called *composite* if it is of the form $f(x,y) = F(g(x,y))$ for some F of degree $\deg F \geq 2$.

Theorem (Elekes–Rónyai'00)

Suppose $f(x,y) \in \mathbb{R}(x,y)$ *is non-composite of degree* d*, and is not of the form* $g(x)+h(y)$*,* $g(x)h(y)$ *or* $\frac{g(x)+h(y)}{1-g(x)h(y)}$*. If* $|A|=|B|=n$*, then*

$$|f(A,B)| \gg_d n^{1+c(d)}.$$

Rational functions

A rational function $f(x,y)$ is called *composite* if it is of the form $f(x,y) = F(g(x,y))$ for some F of degree $\deg F \geq 2$.

Theorem (Elekes–Rónyai'00)

Suppose $f(x,y) \in \mathbb{R}(x,y)$ is non-composite of degree d, and is not of the form $g(x) + h(y)$, $g(x)h(y)$ or $\frac{g(x)+h(y)}{1-g(x)h(y)}$. If $|A| = |B| = n$, then

$$|f(A,B)| \gg_d n^{1+c(d)}.$$

$\frac{x+y}{1-xy} = G(h(x)h(y))$ where $G(x) = \frac{x-1}{i(x+1)}$ and $h(x) = \frac{1+ix}{1-ix}$.

Rational functions

State of knowledge modulo p:

Theorem (Vu'08 after Hart–Iosevich–Solymosi'07)

If $f(x,y) \in \mathbb{F}_p[x,y]$ is a non-composite polynomial of degree d, which is not of the form $ax+by$, and $|A| > p^{1/2}$, then

$$|A+A| + |f(A,A)| \gg_d \begin{cases} |A|(|A|\sqrt{p})^{1/2}, & \text{if } |A| \le p^{7/10}, \\ |A|(p/|A|)^{1/3}, & \text{if } |A| \ge p^{7/10}. \end{cases}$$

New results

Class	Valid for	Why bother?	Main ideas
"Small sets"	Special functions Any $\lvert A\rvert$	Applications	Combinatorial
"Large sets"	All functions $\lvert A\rvert > p^{1/2}$	Look ahead	Algebraic

New results: small sets

Theorem

Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree $d \geq 2$. Then for every set $A \subset \mathbb{F}_p$ of size $|A| \leq \sqrt{p}$ we have

$$|A + A| + |f(A) + f(A)| \gg |A|^{1+\frac{1}{16\cdot 6^d}}.$$

New results: small sets

Theorem

Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree $d \geq 2$. Then for every set $A \subset \mathbb{F}_p$ of size $|A| \leq \sqrt{p}$ we have

$$|A+A| + |f(A)+f(A)| \gg |A|^{1+\frac{1}{16\cdot 6^d}}.$$

Theorem

Suppose $f = \sum_{i=1}^{k} a_i x^{d_i} \in \mathbb{F}_p[X]$ is a polynomial with k terms and degree d. Then for every $\varepsilon > 0$, and every set $A \subset \mathbb{F}_p$ of size $p^{\varepsilon} \leq |A| \leq \sqrt{p}$ we have

$$|AA| + |f(A)+f(A)| \gg |A|^{1+c},$$

where $c = c(\varepsilon, k, d)$.

New results: small sets

Theorem

Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree $d \geq 2$. Then for every set $A \subset \mathbb{F}_p$ of size $|A| \leq \sqrt{p}$ we have

$$|A + A| + |f(A) + f(A)| \gg |A|^{1+\frac{1}{16 \cdot 6^d}}.$$

Theorem

Suppose $f = \sum_{i=1}^{k} a_i x^{d_i} \in \mathbb{F}_p[X]$ is a polynomial with k terms and degree d. Then for every $\varepsilon > 0$, and every set $A \subset \mathbb{F}_p$ of size $p^{\varepsilon} \leq |A| \leq \sqrt{p}$ we have

$$|AA| + |f(A) + f(A)| \gg |A|^{1+c},$$

where $c = c(\varepsilon, k, d)$. Moreover, the dependence on d is logarithmic.

New results: large sets

Theorem

Let $f(x) \in \mathbb{F}_p(x)$, $g(x,y) \in \mathbb{F}_q(x,y)$ be non-constant rational functions, and $g(x,y)$ is not of the form $G(af(x)+bf(y)+c)$, $G(x)$, or $G(y)$. If $|A| \geq \sqrt{p}$, then

$$|f(A)+f(A)| + |g(A,A)| \gg \begin{cases} |A|(|A|/\sqrt{p})^{1/2}, & \text{if } |A| \leq p^{7/10}, \\ |A|(p/|A|)^{1/3}, & \text{if } |A| \geq p^{7/10}. \end{cases}$$

New results: large sets

Theorem

Let $f(x) \in \mathbb{F}_p(x)$, $g(x,y) \in \mathbb{F}_q(x,y)$ be non-constant rational functions, and $g(x,y)$ is not of the form $G(af(x)+bf(y)+c)$, $G(x)$, or $G(y)$. If $|A| \geq \sqrt{p}$, then

$$|f(A)+f(A)| + |g(A,A)| \gg \begin{cases} |A|(|A|/\sqrt{p})^{1/2}, & \text{if } |A| \leq p^{7/10}, \\ |A|(p/|A|)^{1/3}, & \text{if } |A| \geq p^{7/10}. \end{cases}$$

Theorem

Let $f(x,y) \in \mathbb{F}_p[x,y]$ be a polynomial of degree d which is non-composite, and is not of the form $g(x)+h(y)$ or $g(x)h(y)$. Suppose $f(x,y)$ is monic in each variable. Then if $|A| = |B| = n$,

$$|f(A,B)| \gg_d n^{1+c}, \qquad \text{for } p^{7/8+\varepsilon} \leq n \leq p^{1-\varepsilon}.$$

Combinatorial idea: cloning

Whenever there is a single copy of an object,
there are several overlapping copies.

Combinatorial idea: cloning

Whenever there is a single copy of an object,
there are several overlapping copies.

Example:

Turán's theorem	$\overset{\textit{regularity}}{\Longrightarrow}$	Erdős–Stone theorem
There is a K_t	$\Longrightarrow$	There is every t-chromatic graph

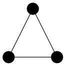
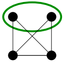
Combinatorial idea: cloning

Whenever there is a single copy of an object,
there are several overlapping copies.

Example:

Turán's theorem $\xRightarrow{\textit{regularity}}$ Erdős–Stone theorem

There is a K_t $\Longrightarrow$ There is every t-chromatic graph

 $\Longrightarrow$ 

Proof sketch (regularity-free):
Given graph G of density $\frac{1}{2} + \epsilon$. Turán gives *many* copies of K_3 in G. Some of these copies must share a pair of vertices by the pigeonhole principle.

Combinatorial idea: cloning

Given a set A and a function f. If $B = f(A, A)$ is small, $|B| \sim |A|$,

$$|f(A, A)| \sim |A| \implies |A|^2 \text{ solutions to } f(a_1, a_2) = b$$

Combinatorial idea: cloning

Given a set A and a function f. If $B = f(A, A)$ is small, $|B| \sim |A|$,

$$\begin{aligned} |f(A,A)| \sim |A| &\implies |A|^2 \text{ solutions to } f(a_1, a_2) = b \\ &\implies |A|^3 \text{ solutions to } f(a_1, a_2) = f(a_3, a_4) \end{aligned}$$

Combinatorial idea: cloning

Given a set A and a function f. If $B = f(A, A)$ is small, $|B| \sim |A|$,

$$
\begin{aligned}
|f(A,A)| \sim |A| &\implies |A|^2 \text{ solutions to } f(a_1, a_2) = b \\
&\implies |A|^3 \text{ solutions to } f(a_1, a_2) = f(a_3, a_4) \\
&\implies |A|^3 \text{ solutions to } \begin{cases} f(a_1, a_2) = f(a_3, a_4), \\ f(a_2, a_3) = b \end{cases}
\end{aligned}
$$

Combinatorial idea: cloning

Given a set A and a function f. If $B = f(A, A)$ is small, $|B| \sim |A|$,

$$
\begin{aligned}
|f(A,A)| \sim |A| &\implies |A|^2 \text{ solutions to } f(a_1,a_2) = b \\
&\implies |A|^3 \text{ solutions to } f(a_1,a_2) = f(a_3,a_4) \\
&\implies |A|^3 \text{ solutions to } \begin{cases} f(a_1,a_2) = f(a_3,a_4), \\ f(a_2,a_3) = b \end{cases} \\
&\implies |A|^4 \text{ solutions to } \begin{cases} f(a_1,a_2) = f(a_3,a_4), \\ f(a_2,a_3) = f(a_5,a_6) \end{cases} \\
&\implies \text{and so forth}
\end{aligned}
$$

Combinatorial idea: cloning

Example:
If $f(x,y) = x + y$, then $f(A,A) = A + A$.

$$\begin{aligned} |A+A| \sim |A| &\implies |A|^2 \text{ solutions to } a_1 + a_2 = b \\ &\implies |A|^3 \text{ solutions to } a_1 + a_2 = a_3 + a_4 \\ &\implies |A|^3 \text{ solutions to } a_1 + a_2 - a_3 = a_4 \end{aligned}$$

Combinatorial idea: cloning

Example:

If $f(x, y) = x + y$, then $f(A, A) = A + A$.

$$\begin{aligned} |A + A| \sim |A| &\implies |A|^2 \text{ solutions to } a_1 + a_2 = b \\ &\implies |A|^3 \text{ solutions to } a_1 + a_2 = a_3 + a_4 \\ &\implies |A|^3 \text{ solutions to } a_1 + a_2 - a_3 = a_4 \end{aligned}$$

Theorem (Balog–Szemerédi–Gowers, Sudakov–Szemerédi–Vu)

Suppose $|A| \sim |B|$ and $a_1 + a_2 + a_3 = b$ has many solutions in $a_1, a_2, a_3 \in A, b \in B$. Then there is large $A' \subset A$ such that $|A' + A' + A'| \sim |A|$.

Combinatorial idea: cloning

Example:

If $f(x, y) = x + y$, then $f(A, A) = A + A$.

$$
\begin{aligned}
|A+A| \sim |A| &\implies |A|^2 \text{ solutions to } a_1 + a_2 = b \\
&\implies |A|^3 \text{ solutions to } a_1 + a_2 = a_3 + a_4 \\
&\implies |A|^3 \text{ solutions to } a_1 + a_2 - a_3 = a_4 \\
&\overset{approx.}{\implies} |A + A - A| \sim |A|
\end{aligned}
$$

Theorem (Balog–Szemerédi–Gowers, Sudakov–Szemerédi–Vu)

Suppose $|A| \sim |B|$ and $a_1 + a_2 + a_3 = b$ has many solutions in $a_1, a_2, a_3 \in A, b \in B$. Then there is large $A' \subset A$ such that $|A' + A' + A'| \sim |A|$.

Proof of $|A+A| + |f(A)+f(A)| \geq |A|^{1+c(d)}$.

Let $\deg f = d$. Induction on d. Proof by contradiction.

Proof of $|A+A| + |f(A)+f(A)| \geq |A|^{1+c(d)}$.

Let $\deg f = d$. Induction on d. Proof by contradiction.

Induction step, $d \geq 3$:

- $|A+A| \sim |A| \implies$ many solutions to $a_1 + a_2 = a_3 + a_4$
- There is a t with many solutions to $a_1 - a_3 = t$
- $A' = \{a \in A : a + t \in A\}$ has about $|A|$ elements
- Let $g(x) = f(x+t) - f(x)$.
  $g(A') + g(A') \subset f(A) - f(A) + f(A) - f(A)$
- $|f(A) + f(A)| \sim |A| \implies |f(A) - f(A) + f(A) - f(A)| \sim |A|$
- $|A' + A'| \leq |A + A| \sim |A|$. Done by induction applied to A' and g.

Proof of $|A+A| + |f(A)+f(A)| \geq |A|^{1+c(d)}$.

Let $\deg f = d$. Induction on d. Proof by contradiction.

Induction step, $d \geq 3$:

- $|A+A| \sim |A| \implies$ many solutions to $a_1 + a_2 = a_3 + a_4$
- There is a t with many solutions to $a_1 - a_3 = t$
- $A' = \{a \in A : a + t \in A\}$ has about $|A|$ elements
- Let $g(x) = f(x+t) - f(x)$.
  $g(A') + g(A') \subset f(A) - f(A) + f(A) - f(A)$
- $|f(A) + f(A)| \sim |A| \implies |f(A) - f(A) + f(A) - f(A)| \sim |A|$
- $|A' + A'| \leq |A + A| \sim |A|$. Done by induction applied to A' and g.

Proof of $|A+A| + |f(A)+f(A)| \geq |A|^{1+c(d)}$.

Let $\deg f = d$. Induction on d. Proof by contradiction.

Induction step, $d \geq 3$:

- $|A+A| \sim |A| \implies$ many solutions to $a_1 + a_2 = a_3 + a_4$
- There is a t with many solutions to $a_1 - a_3 = t$
- $A' = \{a \in A : a + t \in A\}$ has about $|A|$ elements
- Let $g(x) = f(x+t) - f(x)$.
  $g(A') + g(A') \subset f(A) - f(A) + f(A) - f(A)$
- $|f(A) + f(A)| \sim |A| \implies |f(A) - f(A) + f(A) - f(A)| \sim |A|$
- $|A' + A'| \leq |A+A| \sim |A|$. Done by induction applied to A' and g.

Proof of $|A+A| + |f(A)+f(A)| \geq |A|^{1+c(d)}$.

Let $\deg f = d$. Induction on d. Proof by contradiction.

Induction step, $d \geq 3$:

- $|A+A| \sim |A| \implies$ many solutions to $a_1 + a_2 = a_3 + a_4$
- There is a t with many solutions to $a_1 - a_3 = t$
- $A' = \{a \in A : a + t \in A\}$ has about $|A|$ elements
- Let $g(x) = f(x+t) - f(x)$.
  $g(A') + g(A') \subset f(A) - f(A) + f(A) - f(A)$
- $|f(A) + f(A)| \sim |A| \implies |f(A) - f(A) + f(A) - f(A)| \sim |A|$
- $|A' + A'| \leq |A + A| \sim |A|$. Done by induction applied to A' and g.

Proof of $|A+A| + |f(A)+f(A)| \geq |A|^{1+c(d)}$.

Let $\deg f = d$. Induction on d. Proof by contradiction.

Induction step, $d \geq 3$:

- $|A+A| \sim |A| \implies$ many solutions to $a_1 + a_2 = a_3 + a_4$
- There is a t with many solutions to $a_1 - a_3 = t$
- $A' = \{a \in A : a + t \in A\}$ has about $|A|$ elements
- Let $g(x) = f(x+t) - f(x)$.
  $g(A') + g(A') \subset f(A) - f(A) + f(A) - f(A)$
- $|f(A)+f(A)| \sim |A| \implies |f(A) - f(A) + f(A) - f(A)| \sim |A|$
- $|A' + A'| \leq |A+A| \sim |A|$. Done by induction applied to A' and g.

Proof of $|A+A| + |f(A)+f(A)| \geq |A|^{1+c(d)}$.

Let $\deg f = d$. Induction on d. Proof by contradiction.

Induction step, $d \geq 3$:

- $|A+A| \sim |A| \implies$ many solutions to $a_1 + a_2 = a_3 + a_4$
- There is a t with many solutions to $a_1 - a_3 = t$
- $A' = \{a \in A : a + t \in A\}$ has about $|A|$ elements
- Let $g(x) = f(x+t) - f(x)$.
  $g(A') + g(A') \subset f(A) - f(A) + f(A) - f(A)$
- $|f(A) + f(A)| \sim |A| \implies |f(A) - f(A) + f(A) - f(A)| \sim |A|$
- $|A' + A'| \leq |A + A| \sim |A|$. Done by induction applied to A' and g.

Proof of $|A+A| + |f(A)+f(A)| \geq |A|^{1+c(d)}$.

Let $\deg f = d$. Induction on d. Proof by contradiction.

Induction step, $d \geq 3$:

- $|A+A| \sim |A| \implies$ many solutions to $a_1 + a_2 = a_3 + a_4$
- There is a t with many solutions to $a_1 - a_3 = t$
- $A' = \{a \in A : a + t \in A\}$ has about $|A|$ elements
- Let $g(x) = f(x+t) - f(x)$.
  $g(A') + g(A') \subset f(A) - f(A) + f(A) - f(A)$
- $|f(A) + f(A)| \sim |A| \implies |f(A) - f(A) + f(A) - f(A)| \sim |A|$
- $|A' + A'| \leq |A + A| \sim |A|$. Done by induction applied to A' and g.

Proof of $|A+A| + |f(A)+f(A)| \geq |A|^{1+c(d)}$.

Let $\deg f = d$. Induction on d. Proof by contradiction.
Base case $d = 2$: similar to $d-1 \implies d$, but slightly harder.
Induction step, $d \geq 3$:

- $|A+A| \sim |A| \implies$ many solutions to $a_1 + a_2 = a_3 + a_4$
- There is a t with many solutions to $a_1 - a_3 = t$
- $A' = \{a \in A : a + t \in A\}$ has about $|A|$ elements
- Let $g(x) = f(x+t) - f(x)$.
  $g(A') + g(A') \subset f(A) - f(A) + f(A) - f(A)$
- $|f(A) + f(A)| \sim |A| \implies |f(A) - f(A) + f(A) - f(A)| \sim |A|$
- $|A' + A'| \leq |A + A| \sim |A|$. Done by induction applied to A' and g.

Combinatorial idea: pigeonhole

Suppose $|AA|$ and $f(A)+f(A)$ are small. Then what?

- If $f(x)=x$, then AA or $A+A$ is large by the sum-product.
- If $f(x)=x^2$, then $B=f(A)$ satisfies $|BB|=|AA|$. But BB and $B+B$ are small.
- If $f(x)=x+x^2$, then

- If $t_1-t_2+t_3\cdots=0$, then done by the above.
- There are *many* t. By the pigeonhole there is a solution to $t_1+t_3\cdots=t_2+t_4\cdots$

Combinatorial idea: pigeonhole

Suppose $|AA|$ and $f(A)+f(A)$ are small. Then what?

- If $f(x)=x$, then AA or $A+A$ is large by the sum-product.
- If $f(x)=x^2$, then $B=f(A)$ satisfies $|BB|=|AA|$. But BB and $B+B$ are small.
- If $f(x)=x+x^2$, then $f(A)-f(A)+f(A)-f(A)+\cdots$ is small
- There is a t and a large $A_t \subset A$ such that $tA_t \subset A$.
- Hence $f(t_1 A_{t_1}) - f(t_2 A_{t_2}) + \cdots + f(t_k A_{t_k})$ is small.
- Imaging $A_{t_1} = \cdots = A_{t_k} = A'$. For $g(x) = (t_1^2 - t_2^2 + t_3^2 \cdots)x^2 + (t_1 - t_2 + t_3 \cdots)x$, we have $g(A) + \cdots + g(A)$ is small.
- If $t_1 - t_2 + t_3 \cdots = 0$, then done by the above.
- There are *many* t. By the pigeonhole there is a solution to $t_1 + t_3 \cdots = t_2 + t_4 \cdots$

Combinatorial idea: pigeonhole

Suppose $|AA|$ and $f(A)+f(A)$ are small. Then what?

- If $f(x)=x$, then AA or $A+A$ is large by the sum-product.
- If $f(x)=x^2$, then $B=f(A)$ satisfies $|BB|=|AA|$. But BB and $B+B$ are small.
- If $f(x)=x+x^2$, then $f(A)-f(A)+f(A)-f(A)+\cdots$ is small
- There is a t and a large $A_t\subset A$ such that $tA_t\subset A$.
- Hence $f(t_1A_{t_1})-f(t_2A_{t_2})+\cdots+f(t_kA_{t_k})$ is small.
- Imaging $A_{t_1}=\cdots=A_{t_k}=A'$. For $g(x)=(t_1^2-t_2^2+t_3^2\cdots)x^2+(t_1-t_2+t_3\cdots)x$, we have $g(A)+\cdots+g(A)$ is small.
- If $t_1-t_2+t_3\cdots=0$, then done by the above.
- There are *many* t. By the pigeonhole there is a solution to $t_1+t_3\cdots=t_2+t_4\cdots$

Combinatorial idea: pigeonhole

Suppose $|AA|$ and $f(A)+f(A)$ are small. Then what?

- If $f(x)=x$, then AA or $A+A$ is large by the sum-product.
- If $f(x)=x^2$, then $B=f(A)$ satisfies $|BB|=|AA|$. But BB and $B+B$ are small.
- If $f(x)=x+x^2$, then $f(A)-f(A)+f(A)-f(A)+\cdots$ is small
- There is a t and a large $A_t \subset A$ such that $tA_t \subset A$.
- Hence $f(t_1A_{t_1})-f(t_2A_{t_2})+\cdots+f(t_kA_{t_k})$ is small.
- Imaging $A_{t_1}=\cdots=A_{t_k}=A'$. For $g(x)=(t_1^2-t_2^2+t_3^2\cdots)x^2+(t_1-t_2+t_3\cdots)x$, we have $g(A)+\cdots+g(A)$ is small.
- If $t_1-t_2+t_3\cdots=0$, then done by the above.
- There are *many* t. By the pigeonhole there is a solution to $t_1+t_3\cdots=t_2+t_4\cdots$

Combinatorial idea: pigeonhole

Suppose $|AA|$ and $f(A)+f(A)$ are small. Then what?

- If $f(x)=x$, then AA or $A+A$ is large by the sum-product.
- If $f(x)=x^2$, then $B=f(A)$ satisfies $|BB|=|AA|$. But BB and $B+B$ are small.
- If $f(x)=x+x^2$, then $f(A)-f(A)+f(A)-f(A)+\cdots$ is small
- There is a t and a large $A_t \subset A$ such that $tA_t \subset A$.
- Hence $f(t_1 A_{t_1}) - f(t_2 A_{t_2}) + \cdots + f(t_k A_{t_k})$ is small.
- Imaging $A_{t_1} = \cdots = A_{t_k} = A'$. For $g(x) = (t_1^2 - t_2^2 + t_3^2 \cdots)x^2 + (t_1 - t_2 + t_3 \cdots)x$, we have $g(A) + \cdots + g(A)$ is small.
- If $t_1 - t_2 + t_3 \cdots = 0$, then done by the above.
- There are *many* t. By the pigeonhole there is a solution to $t_1 + t_3 \cdots = t_2 + t_4 \cdots$

Combinatorial idea: pigeonhole

Suppose $|AA|$ and $f(A)+f(A)$ are small. Then what?

- If $f(x)=x$, then AA or $A+A$ is large by the sum-product.
- If $f(x)=x^2$, then $B=f(A)$ satisfies $|BB|=|AA|$. But BB and $B+B$ are small.
- If $f(x)=x+x^2$, then $f(A)-f(A)+f(A)-f(A)+\cdots$ is small
- There is a t and a large $A_t\subset A$ such that $tA_t\subset A$.
- Hence $f(t_1A_{t_1})-f(t_2A_{t_2})+\cdots+f(t_kA_{t_k})$ is small.
- Imaging $A_{t_1}=\cdots=A_{t_k}=A'$. For $g(x)=(t_1^2-t_2^2+t_3^2\cdots)x^2+(t_1-t_2+t_3\cdots)x$, we have $g(A)+\cdots+g(A)$ is small.
- If $t_1-t_2+t_3\cdots=0$, then done by the above.
- There are *many* t. By the pigeonhole there is a solution to $t_1+t_3\cdots=t_2+t_4\cdots$

Combinatorial idea: pigeonhole

Suppose $|AA|$ and $f(A)+f(A)$ are small. Then what?

- If $f(x)=x$, then AA or $A+A$ is large by the sum-product.
- If $f(x)=x^2$, then $B=f(A)$ satisfies $|BB|=|AA|$. But BB and $B+B$ are small.
- If $f(x)=x+x^2$, then $f(A)-f(A)+f(A)-f(A)+\cdots$ is small
- There is a t and a large $A_t\subset A$ such that $tA_t\subset A$.
- Hence $f(t_1A_{t_1})-f(t_2A_{t_2})+\cdots+f(t_kA_{t_k})$ is small.
- Imaging $A_{t_1}=\cdots=A_{t_k}=A'$. For $g(x)=(t_1^2-t_2^2+t_3^2\cdots)x^2+(t_1-t_2+t_3\cdots)x$, we have $g(A)+\cdots+g(A)$ is small.
- If $t_1-t_2+t_3\cdots=0$, then done by the above.
- There are *many* t. By the pigeonhole there is a solution to $t_1+t_3\cdots=t_2+t_4\cdots$

The End