A noncommutative
Plünecke-type inequality

Imre Z. Ruzsa

Szemerédi conference
Budapest, 2010 august
Understanding sumsets

Aim: to understand the structure of sumsets; mainly: the structure of sets $A$ for which $2A = A + A$ is small.

Important tool: cardinality inequalities.

Well understood: sets in commutative groups.

Examples: if $|A| = n$, $|2A| = \alpha n$, then $|A - A| \leq \alpha^2 n$, $|3A| \leq \alpha^3 n$.

Noncommutative groups: things are

– often not true,

– even if true, difficult/impossible to prove.
Plünnecke’s inequality for sumsets

**Theorem.** Let \( j < h \) be integers, \( A, B \) sets in a commutative group and write \( |A| = m, |A + jB| = \alpha m \). There is an \( X \subset A, X \neq \emptyset \) such that

\[
|X + jB| \leq \alpha^{h/j} |X|.
\]

Generally \( X = A \) is not a good choice. \( |A + hB| \) can be much larger, it can be greater than \( m^{1+C(h)} \), even if \( \alpha < 2 \). \( X \) has to be selected carefully.
Since $|X+hB| \geq |hB|$ and $|X| \leq m$, we get the following immediate consequence.

**Corollary.** Let $j < h$ be integers, $A$, $B$ sets in a commutative group and write $|A| = m$, $|A + jB| = \alpha m$. We have

$$|hB| \leq \alpha^{h/j} m.$$
Sums and differences

A less trivial consequence (which suffices for 99% of applications):

**Theorem.** Let \( A, B \) be finite sets in a commutative group and write \( |A| = m, |A + B| = \alpha m \). For arbitrary nonnegative integers \( k, l \) we have

\[
|kB - lB| \leq \alpha^{k+l} m.
\]

To get differences we need the following:

**Theorem.** Let \( A, Y, Z \) be sets in a (not necessarily commutative) group. We have

\[
\]
The noncommutative case: examples

Some disheartening examples . . .

We take a free group, which is “very noncommutative”. Generators $a, b$.

Example 1: $2A$ small, $3A$ large.

$$A = \{a, 2a, \ldots, na, b\}.$$  

We have $|A| = n + 1$, $|2A| = 4n$ and $|3A| > n^2$ since all the elements $ia + b + ja, 1 \leq i, j \leq n$ are distinct.

(In a commutative group we would have $|3A| \leq 4^3 n$.)
Example 2: difference set small, sumset large.

\[ A = \{ ia + b : 1 \leq i \leq m \}. \]

Then both difference sets \( A - A \) and \(-A + A\) have \( 2m - 1 \) elements, while \( |2A| = m^2 \).

In the commutative case we have

\[ |A| = m, \; |A - A| \leq \alpha m \Rightarrow |2A| \leq \alpha^2 m. \]
Example 3: one difference set small, other large.

\[ A = \{ia + b : 1 \leq i \leq m\} \cup \{ia : 1 \leq i \leq m\}. \]

Then \(|A| = 2m\) and

\[ -A = \{-b - ja : 1 \leq j \leq m\} \cup \{-ja : 1 \leq j \leq m\}. \]

\(A - A\) contains the \(2m^2\) different elements \(ia \pm b - ja\),

\[-A + A = \{(i-j)a\} \cup \{(i-j)a+b\} \cup \{-b+(i-j)a\} \cup \{-b+(i-j)a+b\},\]

4\(m\) elements.

Comment: we have

\[ |A||Y - Z| \leq |A - Y||A - Z| \]

without commutativity, so if \(|A| = m\), \(|2A| \leq \alpha m\), then \(|-A + A| \leq \alpha^2 m\) and \(|A - A| \leq \alpha^2 m\).
First way out: two, three, many

If $3A$ is small, not just $2A$, then everything else is, just by an iterated use of the inequality


**Theorem.** Let $A, B$ be finite sets in a group and write

$$m = \min\{|A|, |B|\}.$$ 

If $|A + B - A| \leq \alpha m$ or $|A + 2B| \leq \alpha m$, then

$$|\underbrace{A \pm B \ldots \pm B -}_{k \text{ summands}} A| \leq \alpha^{2k} m.$$
Corollary. (case $B = \pm A$) Let $|A| = m$, and assume that the size of one of the triple sum-differences $\pm A \pm A \pm A$ is at most $\alpha m$. Then, for 6 of the possible 8 combinations of signs, any $k$-fold sum-difference combination has cardinality at most $\alpha^{2k} m$.

2 cases not covered: $A - A + A$ and $-A + A - A$. They may be small and $2A$ large (free-group example as above).
From 2 to 3 with an extra condition

Between double and triple sums we have the following inequality without commutativity:

\[ |X + Y + Z|^2 \leq |X + Y||Y + Z| \max_{y \in Y} |X + y + Z|. \]

**Problem.** Let \( A, B \) be finite sets in a noncommutative group, and define \( \alpha \) by

\[ \max_{b \in B} |A + b + B| = \alpha |A|. \]

Must there exist a nonempty \( X \subset A \) such that

\[ |X + 2B| \leq \alpha' |X| \]

with an \( \alpha' \) depending only on \( \alpha \)?
An important particular case:

**Theorem (Tao).**

If

$$\max_{a \in A} |A + a + A| \leq \alpha m,$$

then $|3A| \leq \alpha^c m$. 
Part 2: Plünnecke’s graphs

$A, B$ finite sets in a commutative group.

To understand the cardinality properties of the sets $A$, $A + B$, $A + 2B$, $\ldots$, we build a directed $(h + 1)$-partite graph with the sets $A$, $A + B$, $\ldots$, $A + hB$ as parts, and with edges going from each $x \in A + jB$ to all $x + b \in A + (j + 1)B$, $b \in B$.

This is the addition graph.

These graphs have certain properties which follow from the commutativity of addition, and hence Plünnecke called them commutative.
Commutative graphs

Directed graphs $G = (V, E)$, (vertices, edges).

Edge from $x$ to $y$: $x \rightarrow y$.

A graph is *semicommutative*, if for every collection $(x; y; z_1, z_2, \ldots, z_k)$ of distinct vertices such that $x \rightarrow y$ and $y \rightarrow z_i$ there are distinct vertices $y_1, \ldots, y_k$ such that $x \rightarrow y_i$ and $y_i \rightarrow z_i$ (we can replace a broom by a fork).
$\mathcal{G}$ is commutative, if both $\mathcal{G}$ and the graph $\hat{\mathcal{G}}$ with edges reversed are semicommutative.

The commutativity of the addition graph follows from the possibility of replacing a path $x \rightarrow x + b_1 \rightarrow x + b_1 + b_2$ by $x \rightarrow x + b_2 \rightarrow x + b_1 + b_2$. 
Layered graphs

An \(h\)-layered graph is a graph with a fixed partition of the set of vertices

\[ V = V_0 \cup V_1 \cup \ldots \cup V_h \]

into \(h+1\) disjoint sets (layers) such that every edge goes from some \(V_{i-1}\) into \(V_i\). (For the addition graph, \(A, A + B, \ldots\))

For \(X, Y \subseteq V\), the image of \(X\) in \(Y\) is
\[
\text{im}(X, Y) = \{ y \in Y : \exists \text{ a directed path from some } x \in X \text{ to } y \}. 
\]

The magnification ratio is
\[
\mu(X, Y) = \min \left\{ \frac{|\text{im}(Z, Y)|}{|Z|} : Z \subseteq X, Z \neq \emptyset \right\}. 
\]

In layered graph write
\[
\mu_j(G) = \mu(V_0, V_j). 
\]
Plünnecke’s graph theorem

sounds as follows.

Theorem. In a commutative layered graph $\mu_j^{1/j}$ is decreasing.

That is, $\mu_h \leq \mu_j^{h/j}$ for $j < h$.

Typically the only available upper estimate for $\mu_j$ is $|V_j|/|V_0|$. This
yields the following corollary (in fact, an equivalent assertion).

Corollary. Let $j < h$ be integers, $G$ a commutative layered graph
on the layers $V_0, \ldots, V_h$. Write $|V_0| = m$, $|V_j| = \alpha m$. There is an
$X \subset V_0$, $X \neq \emptyset$ such that

$$|\text{im}(X, V_h)| \leq \alpha^{h/j} |X|.$$
Different summands

The commutativity of the addition graph requires two assumptions: one is the commutativity of addition, the other is that the same set $B$ is added repeatedly.

The second assumption can be removed quite well.

Case $j = 1$:

**Theorem.** Let $A, B_1, \ldots, B_h$ be sets in a commutative group $G$ and write $|A| = m$, $|A + B_i| = \alpha_i m$. There is an $X \subset A$, $X \neq \emptyset$ such that

$$|X + B_1 + \ldots + B_h| \leq \alpha_1 \alpha_2 \ldots \alpha_h |X|.$$ 

The case of general $j$ is in a paper by Gyarmati, Matolcsi, Ruzsa, Building Bridges vol.
Left, right, left, right

Plünnecke’s method can be modified to handle some noncommutative situations.

**Theorem.** Let $A, L, R$ be sets in a (typically noncommutative group) $G$ and write $|A| = m$, $|L + A| = \alpha m$, $|A + R| = \beta m$. There is an $X \subset A$, $X \neq \emptyset$ such that

$$|L + X + R| \leq \alpha \beta |X|.$$
Commutative graph
from noncommutative operation

\[
\begin{align*}
L + A \\
A & \quad \rightarrow \quad L + A + R \\
A + R
\end{align*}
\]

\[
\begin{align*}
y + x + z_1 \\
y + x \in L + A \\
x
\end{align*}
\]

changes into

\[
\begin{align*}
x & \rightarrow x + z_1 \in A + R \\
x + z_k \in A + R & \quad \rightarrow \quad y + x + z_1 \\
\end{align*}
\]
More than two

Reason for above: multiplication from left and multiplication from right do commute (assocativity): \((bx)c = b(xc)\).

No more directions: you cannot multiply from above and below. For \(> 2\) summands we need an extra condition.

**Definition.** A collection of sets \(B_1, \ldots, B_k\) in a (noncommutative) group is *exocommutative*, if for all \(x \in B_i, y \in B_j\) with \(i \neq j\) we have \(x + y = y + x\).
Theorem. Let $A, L_1, L_2, \ldots, L_k, R_1, R_2, \ldots, R_l$ be sets in a (typically noncommutative) group $G$ and write $|A| = m$, $|L_i + A| = \alpha_i m$, $i = 1, \ldots, k$, $|A + R_j| = \beta_j m$, $j = 1, \ldots, l$. Assume that both collections $L_1, \ldots, L_k$ and $R_1, \ldots, R_l$ are exocommutative. There is a set $X \subseteq A$, $X \neq \emptyset$ such that

$$|L_1 + \ldots + L_k + X + R_i + \ldots + R_l| \leq \alpha_1 \ldots \alpha_k \beta_1 \ldots \beta_l |X|.$$
From set addition to maps

The role of $A$ and of $L, R$ are very different.

Each $b \in L$ induces a map of $G$: $x \mapsto bx$.

Each $c \in R$ induces a map of $G$: $x \mapsto xc$.

**Theorem.** Let $H$ be a set, $G$ the group of permutations of $H$. Let $B_1, \ldots, B_k \subset G$, and write $|A| = m$, $|B_i(A)| = \alpha_i m$, $i = 1, \ldots, k$. Assume that both $B_1, \ldots, B_k$ are exocommutative. Then there is an $X \subset A$, $X \neq \emptyset$ such that

$$|B_1 B_2 \ldots B_k(A)| \leq \alpha_1 \ldots \alpha_k |X|.$$
Finding a large subset

Typically the set $X$ whose existence is asserted in our theorems is a proper subset of the starting set $A$. However, once we can find some subset, by repeating the selection we can find a subset that contains 99% of the elements of $A$.

**Theorem.** Let $A, L, R$ be sets in a group $G$ and write $|A| = m$, $|L + A| = \alpha m$, $|A + R| = \beta m$. Let a real number $\varepsilon$ be given, $0 \leq \varepsilon < m$. There exists an $X \subset A$, $|X| > (1 - \varepsilon)m$ such that

$$|L + X + R| \leq \alpha \beta |X| \left( \frac{2}{\varepsilon} - 1 \right).$$
Corollary. Let $A$ be a finite set in a group $G$ and write $|A| = m$, $|A + A| = \alpha m$. Let a real number $\varepsilon$ be given, $0 \leq \varepsilon < m$. There exists an $X \subset A$, $|X| > (1 - \varepsilon)m$ such that

$$|3X| \leq |A + X + A| \leq \alpha \beta |X| \left(\frac{2}{\varepsilon} - 1\right).$$