# The abelian case of a combinatorial conjecture of Dicks and Ivanov

Barcelona Group Theory Seminar, March 27, 2008

## 1 The result

**1.1 Notation.** Throughout, $G = (G, \cdot, 1, ^{-})$ will be a multiplicative group, and $A$ and $B$ will be finite subsets of $G$, thought of as row vectors.

We shall consider the matrix $A^{\mathrm{tr}} \cdot B$, where $(-)^{\mathrm{tr}}$ denotes the transpose; we usually imagine $A^{\mathrm{tr}} \cdot B$ as the content of a 'multiplication table'

$$\begin{array}{c||c} \cdot & B \\ \hline\hline A^{\mathrm{tr}} & A^{\mathrm{tr}} \cdot B \end{array}$$

For each $i \in \mathbb{N}$, we define $A{\cdot_i}B$ to be the set of those elements of $G$ which appear (at least) $i$ times in the matrix $A^{\mathrm{tr}} \cdot B$. We abbreviate $A{\cdot_1}B$ as $AB$.

We set $\Omega(A, B) := |A| + |B| - \frac{1}{2}|AB| - \frac{1}{2}|A{\cdot_2}B|$. $\square$

**1.2 Theorem.** [2, Theorem 1.2] *If $A$ and $B$ are finite subsets of an* abelian *group $G$ such that $|A| \geq 2$ and $|B| \geq 2$, then* $\Omega(A, B) \leq \max\{2, |gH| : H \leq G, g \in G, gH \subseteq A{\cdot_2}B\}$.

We present a proof taken from [3, Theorem 1.7]. In fact, [2, Theorem 1.2] provides the stronger inequality $\Omega(A, B) \leq \max\{2, |\operatorname{Stab}(A{\cdot_2}B)|\}$; of course, if $A{\cdot_2}B$ is empty, then $|AB| = |A||B| \geq |A||B| - (|A| - 2)(|B| - 2) = 2\Omega(A, B) + |AB| - 4$ and $\Omega(A, B) \leq 2$.

*Proof by induction on* $(|B|, |A|)$. Consider the case where $|B| = 2$. Say $B = \{b_1, b_2\}$. Then $|AB| + |A{\cdot_2}B| = |Ab_1 \cup Ab_2| + |Ab_1 \cap Ab_2| = |Ab_1| + |Ab_2| = 2|A|$. It then follows that $\Omega(A, B) = |B| = 2$, as desired. Thus, we may assume that $|B| \geq 3$.

Similarly, we may assume that $|A| \geq 3$.

We may assume that the implication holds for smaller pairs $(|B|, |A|)$.

By replacing $B$ with $B\overline{b}$, for any $b \in B$, we may assume that $1 \in B$.

Consider the case where $AB = A$. Let $H = \langle B \rangle$, the subgroup generated by $B$. Then $AB = A{\cdot_2}B = A = AH$ and $\Omega(A, B) = |B| \leq |H|$, as desired. Thus, we may assume that $AB \neq A$.

Hence, $AB \not\subseteq A$; hence, there exists $a \in A$ such that $aB \not\subseteq A$. By replacing $A$ with $\overline{a}A$ we may assume that $a = 1$.

Let $C = A \cap B$, $A' = A - B = A - C$, $B' = B - A = B - C$. Then $\{1\} \subseteq C \subset B$, $1 \leq |C| \leq |B| - 1$, and $A = C \vee A'$, $B = C \vee B'$, where $\vee$ denotes the disjoint union. Now

$A^{\mathrm{tr}} \cdot B$ is partitioned, $\begin{array}{c||c} \cdot & B \\ \hline\hline A^{\mathrm{tr}} & A^{\mathrm{tr}} \cdot B \end{array} \quad = \quad \begin{array}{c||c|c} \cdot & C & B' \\ \hline\hline C^{\mathrm{tr}} & C^{\mathrm{tr}} \cdot C & C^{\mathrm{tr}} \cdot B' \\ \hline A'^{\mathrm{tr}} & A'^{\mathrm{tr}} \cdot C & A'^{\mathrm{tr}} \cdot B' \end{array}$

**Case 1.** $|C| = 1$; thus, $\begin{array}{c||c} \cdot & B \\ \hline\hline A^{\mathrm{tr}} & A^{\mathrm{tr}} \cdot B \end{array} \quad = \quad \begin{array}{c||c|c} \cdot & 1 & B' \\ \hline\hline 1 & 1 & B' \\ \hline A'^{\mathrm{tr}} & A'^{\mathrm{tr}} & A'^{\mathrm{tr}} \cdot B' \end{array}$

If $|AB - AB'| \geq 2$, we perform the *$B$-truncation*, $(A, B) \mapsto (A, B')$.

$$\begin{array}{c||c} \cdot & B \\ \hline\hline A^{\mathrm{tr}} & A^{\mathrm{tr}} \cdot B \end{array} \quad = \quad \begin{array}{c||c|c} \cdot & 1 & B' \\ \hline\hline A^{\mathrm{tr}} & A^{\mathrm{tr}} & A^{\mathrm{tr}} \cdot B' \end{array} \quad \mapsto \quad \begin{array}{c||c} \cdot & B' \\ \hline\hline A^{\mathrm{tr}} & A^{\mathrm{tr}} \cdot B' \end{array}$$

Clearly, $A{\cdot_2}B' \subseteq A{\cdot_2}B$. Moreover, $\Omega(A, B') \geq \Omega(A, B)$ because $|B'| = |B| - 1$ and $|AB'| \leq |AB| - 2$. Here, the desired conclusion follows by the induction hypothesis. Thus, we may assume that

$$1 \geq |AB - AB'| = |((A \vee B') \cup A'B') - (B' \cup A'B')| = |A - A'B'| = |A| - |A \cap A'B'|.$$

Similarly, we may assume that $1 \geq |B - A'B'| \geq |B' - A'B'| = |B'| - |B' \cap A'B'|$.
Now $A{\cdot_2}B \supseteq (\{1\} \vee A' \vee B') \cap A'B'$. Hence

$$|A{\cdot_2}B| \geq |(A \vee B') \cap A'B'| = |A \cap A'B'| + |B' \cap A'B'| \geq |A| - 1 + |B'| - 1 = |A| + |B| - 3.$$

Since $AB \supseteq \{1\} \vee A' \vee B'$, we see that $|AB| \geq |A| + |B| - 1$.
Hence $2\ \Omega(A, B) \leq 4$, as desired.

**Case 2.** $|C| \neq 1$; thus, $2 \leq |C| \leq |B| - 1$.
Here, we perform *the Dyson transform*, $(A, B) \mapsto (A \cup B, A \cap B) = (C \vee A' \vee B', C)$.

$$\begin{array}{c||c} \cdot & B \\ \hline\hline A^{\mathrm{tr}} & A^{\mathrm{tr}} \cdot B \end{array} \quad = \quad \begin{array}{c||c|c} \cdot & C & B' \\ \hline\hline C^{\mathrm{tr}} & C^{\mathrm{tr}} \cdot C & C^{\mathrm{tr}} \cdot B' \\ \hline A'^{\mathrm{tr}} & A'^{\mathrm{tr}} \cdot C & A'^{\mathrm{tr}} \cdot B' \end{array} \quad \mapsto \quad \begin{array}{c||c} \cdot & C \\ \hline\hline C^{\mathrm{tr}} & C^{\mathrm{tr}} \cdot C \\ \hline A'^{\mathrm{tr}} & A'^{\mathrm{tr}} \cdot C \\ \hline B'^{\mathrm{tr}} & B'^{\mathrm{tr}} \cdot C \end{array}$$

Clearly, $|C \vee A' \vee B'| + |C| = |A| + |B|$. *Since $G$ is abelian,* $B'^{\mathrm{tr}} \cdot C = (C^{\mathrm{tr}} \cdot B')^{\mathrm{tr}}$. Hence, $(C \vee A' \vee B'){\cdot_i}C \subseteq A{\cdot_i}B$, for all $i \in \mathbb{N}$. In particular, $(C \vee A' \vee B'){\cdot_2}C \subseteq A{\cdot_2}B$ and $\Omega(C \vee A' \vee B', C) \geq \Omega(A, B)$. Here, the desired conclusion follows by the induction hypothesis.

This completes the proof. $\square$

## 2 Kemperman's Theorem

John Olson [6] extracted the following statement from [4] by combining Theorem 5, the proof of Theorem 5, and Theorem 3, thereof.

**2.1 Kemperman's Theorem.** *Let $A$ and $B$ be finite (nonempty) subsets of a group $G$, and let $(a, b) \in A \times B$. Then $|A| + |B| - |AB| \leq \max\{|H| : H \leq G,\ aHb \subseteq AB\}$. Moreover, if $AB \neq A{\cdot_2}B$ then $|A| + |B| - |AB| \leq 1$.*

*Proof by induction on* $(2|AB| - |A| - |B|,\ |AB| - |A|)$. We prove both parts in parallel putting in boxes the additional steps corresponding to the proof of the second part.

$\boxed{\text{Suppose that } ab \in A{\cdot_{[=1]}}B.}$

By replacing $(A, B)$ with $(\overline{a}A, B\overline{b})$, we may assume that $(a, b) = (1, 1)$. Thus, $1 \in A \cap B$ and $AB \supseteq A \cup B$.

$\boxed{\text{We have } 1 \in A \cdot_{[=1]} B.}$

**Case 1.** $A(A \cap B) = A$.

Let $H = \langle A \cap B \rangle$.

$\boxed{\text{For each } x \in B - \{1\},\ 1 \in A1 \text{ but } 1 \notin Ax, \text{ and, hence, } Ax \neq A. \text{ Thus, } H \text{ is trivial.}}$

Now

$$AB \quad \supseteq \quad A \cup B \quad \supseteq \quad A \quad = \quad AH \quad \supseteq \quad H \quad = \quad \langle A \cap B \rangle \quad \supseteq \quad A \cap B.$$

Hence $AB \supseteq H$, and $|H| \geq |A \cap B| = |A| + |B| - |A \cup B| \geq |A| + |B| - |AB|$, as desired.

**Case 2.** There exists some $x \in A \cap B$ such that $Ax \neq A$.

Let

$$A^+ = A \cup Ax, \quad B^- = B \cap \overline{x}B, \quad A^- = A \cap A\overline{x}, \quad B^+ = B \cup xB.$$

Notice that 1 lies in all four of these sets, since $x \in A \cap B$. Also, $A^+B^- \subseteq AB$ and $A^-B^+ \subseteq AB$.

We claim that $1 \in A^+ \cdot_{[=1]} B^-$.
Suppose that $(c, d) \in A^+ \times B^-$ such that $cd = 1$. Notice $c = \overline{d}$ and

$$(\overline{d}, d) \in A^+ \times B^- \quad = \quad (A \times B^-) \cup (Ax \times B^-) \quad \subseteq \quad (A \times B) \cup (Ax \times \overline{x}B).$$

Now, $1 \notin xB \supseteq \{xd\}$, $xd \neq 1$, $(\overline{d}\,\overline{x}, xd) \neq (1, 1)$, $(\overline{d}\,\overline{x}, xd) \notin A \times B$, and $(\overline{d}, d) \notin Ax \times \overline{x}B$.
Thus $(\overline{d}, d) \in A \times B$, and, hence $d = 1$.
Thus, $1 \in A^+ \cdot_{[=1]} B^-$, as claimed.
Similarly, $1 \in A^- \cdot_{[=1]} B^+$.

Notice that $|A^+| + |A^-| = |A^+| + |A^-x| = |A| + |Ax| = 2|A|$, and similarly, $|B^+| + |B^-| = 2|B|$. Thus,

$$\text{either} \quad |A^+| + |B^-| \ \leq \ |A| + |B| \quad \text{or} \quad |A^-| + |B^+| \ < \ |A| + |B|.$$

We can apply the induction hypothesis to $(A^+, B^-)$ in the former case, and to $(A^-, B^+)$ in the latter case. The result then follows by induction. □

# References


[1] Warren Dicks and S. V. Ivanov, *On the intersection of free subgroups in free products of groups*, Math. Proc. Cambridge Phil. Soc., to appear. http://arxiv.org/abs/math/0702363

[2] David J. Grynkiewicz, *Extending Pollard's Theorem for t-representable sums*, preprint, 22 pages. http://arxiv.org/abs/0803.2601

[3] Y. O. Hamidoune and O. Serra, *A note on Pollard's Theorem*, preprint, 10 pages, 2008.

[4] J. H. B. Kemperman, *On complexes in a semigroup*, Indag. Math. **18**(1956), 247–254.

[5] Henry B. Mann, *A proof of the fundamental theorem on the density of sums of sets of positive integers*, Ann. Math. (2) **43**(1942), 523–527.

[6] John E. Olson, *On the sum of two sets in a group*, J. Number Theory **18**(1984), 110–120.