EXPLICIT MULTIPLICATIVE COMBINATORICS

E. KOWALSKI

We give explicit forms of some of the results in Tao's paper [3] on product set estimates in finite (non-necessarily abelian) groups, which are useful for implementing the Bourgain-Gamburd reduction of the expander properties for certain families of Cayley graphs to a suitable classification of approximate subgroups.

The presentation is highly condensed, and there might well be minor computational mistakes remaining – these points will hopefully be improved when incorporating this in the lecture notes [1].

Below all sets are subsets of a fixed finite group G, and are all non-empty. We use the notation $d(A,B)$ and $E(A,B)$ from [3] or [4] for the Ruzsa distance and the multiplicative energy.

1. Diagrams

We will use the following diagrammatic conventions to allow for bookkeeping of constants.

(1) If A and B are sets with $d(A,B) \leqslant \log\alpha$, we write

$$A \bullet\!\underset{\alpha}{\text{———}}\!\bullet B$$

(2) If A and B are sets with $|B| \leqslant \alpha|A|$, we write

$$B \bullet\!\xrightarrow{\alpha} A$$

and in particular if $|X| \leqslant \alpha$, we write

$$X \bullet\!\xrightarrow{\alpha} 1$$

(3) If A and B are sets with $e(A,B) = E(A,B)/(|A||B|)^{3/2} \geqslant 1/\alpha$, we write

$$A \bullet\!\overset{\alpha}{\leadsto}\!\bullet B$$

(4) If $A \subset B$, we write

$$A \rightarrowtail B\ .$$

The following rules are easy to check (in addition to some more obvious ones which we do not spell out):

(1) From

$$A \bullet\!\underset{\alpha}{\text{———}}\!\bullet B$$

we can get

$$A \bullet\!\xrightarrow{\alpha^2} B\ , \quad B \bullet\!\xrightarrow{\alpha^2} A\ .$$

(2) (Ruzsa's triangle inequality, [3, Lemma 3.2]) From

$$A \bullet\!\underset{\alpha_1}{\text{———}}\!\bullet B \bullet\!\underset{\alpha_2}{\text{———}}\!\bullet C$$

we get

$$A \bullet\!\underset{\alpha_1\alpha_2}{\text{———}}\!\bullet C\ .$$

(3) From

$$C \bullet\!\xrightarrow{\alpha_1} B \bullet\!\xrightarrow{\alpha_2} A$$

we get

$$C \bullet\!\xrightarrow{\alpha_1\alpha_2} A\ .$$

(4) ("Unfolding edges") From

$$B \bullet\!\xrightarrow{\ \alpha\ } A, \qquad B \bullet\!\underset{\beta}{\frown}\!\bullet A$$

we get

$$AB^{-1} \bullet\!\xrightarrow{\ \sqrt{\alpha}\beta\ } A$$

(note that by the second point in this list, we only need to have

$$B \bullet\!\underset{\beta}{\rule[0.5ex]{2em}{0.4pt}}\!\bullet A$$

to obtain the full statement with $\alpha = \beta^2$, which is usually qualitatively equivalent.)

(5) ("Folding") From

$$AB^{-1} \bullet\!\xrightarrow{\ \alpha\ } A \bullet\!\xrightarrow{\ \beta\ } B$$

we get

$$A \bullet\!\underset{\alpha\beta^{1/2}}{\rule[0.5ex]{5em}{0.4pt}}\!\bullet B\ .$$

Note that the relation $A \bullet\!\xrightarrow{\ \alpha\ } B$ is purely a matter of the size of A and B, while the other arrow types depend on structural relations involving the sets (for $A \rightarrowtail B$) and product sets (for $A \bullet\!\underset{\alpha}{\rule[0.5ex]{2em}{0.4pt}}\!\bullet B$ or $A \bullet\!\overset{\alpha}{\rightsquigarrow}\!\bullet B$).

2. Statements and "Proofs"

Theorem 2.1 (Ruzsa covering lemma; Tao, Lemma 3.6)**.** *If*

$$AB \bullet\!\xrightarrow{\ \alpha\ } A\ ,$$

there exists a set X which satisfies

$$X \rightarrowtail B\ , \qquad X \bullet\!\xrightarrow{\ \alpha\ } 1\ , \qquad B \rightarrowtail A^{-1}AX\ ,$$

and symmetrically, if

$$BA \bullet\!\xrightarrow{\ \alpha\ } A\ ,$$

there exists Y with

$$Y \rightarrowtail B\ , \qquad Y \bullet\!\xrightarrow{\ \alpha\ } 1\ , \qquad B \rightarrowtail YAA^{-1}\ .$$

Definition 2.2 (Approximate group; Tao, Def. 3.8)**.** A set H is an α-approximate group if $1 \in H$, $H = H^{-1}$, and there exists a set X with

$$X \bullet\!\xrightarrow{\ \alpha\ } 1\ ,\ H^{(2)} \rightarrowtail XH\ .$$

Next is another result which is essentially due to Ruzsa: the tripling constant of a symmetric set controls all other n-fold product sets.

Theorem 2.3 (Ruzsa)**.** *If A is symmetric and*

$$A^{(3)} \bullet\!\xrightarrow{\ \alpha\ } A\ ,$$

then we have

$$A^{(n)} \bullet\!\xrightarrow{\ \alpha^{n-2}\ } A$$

for all $n \geqslant 3$. In particular, we get

$$A^{(7)} \bullet\!\xrightarrow{\ \alpha^{5}\ } A\ .$$

In [2, Th. 1.6] or [3, Lemma 3.4], one finds versions of this result with A^n replaced by any n-fold product of factors equal to A or A^{-1}. But we will only use symmetric subsets, in which case the above has much better constants.

Theorem 2.4 (Tao, Th. 3.9 and Cor. 3.10)**.** *Let $A = A^{-1}$ with $1 \in A$ and*

$$A^{(3)} \bullet\!\xrightarrow{\alpha} A \ .$$

Then $H = A^{(3)}$ is a $(2\alpha^5)$-approximate subgroup containing A.

Proof. We have first

$$H \bullet\!\xrightarrow{\alpha} A \ , \qquad A \rightarrowtail H \ .$$

Then by Ruzsa's resut, we get

$$AH^{(2)} = A^{(7)} \bullet\!\xrightarrow{\alpha^5} A \ ,$$

and by the Ruzsa covering lemma there exists X with

$$X \rightarrowtail H^{(2)} \ , \qquad X \bullet\!\xrightarrow{\alpha^5} 1 \ ,$$

such that

$$H^{(2)} \rightarrowtail A^{(2)}X \rightarrowtail A^{(3)}X = HX \ .$$

Taking $X_1 = X \cup X^{-1}$, we get

$$X_1 \rightarrowtail H^{(2)} \ , \qquad X_1 \bullet\!\xrightarrow{2\alpha^5} 1 \ ,$$

and

$$H^{(2)} \rightarrowtail HX \ , \qquad H^{(2)} \rightarrowtail XH \ ,$$

which are the properties defining a $(2\alpha^5)$-approximate subgroup. ☐

Theorem 2.5 (Tao, Th. 4.6, (i) implies (ii))**.** *Let A and B with*

$$A \bullet\!\underset{\alpha}{\text{———}}\!\bullet B^{-1}$$

Then there exists a γ-approximate subgroup H and a set X with

$$X \bullet\!\xrightarrow{\gamma_1} 1 \ , \qquad A \rightarrowtail XH \ , \qquad B \rightarrowtail HX \ , \qquad H \bullet\!\xrightarrow{\gamma_2} A \ ,$$

where

$$\gamma \leqslant 2^{21}\alpha^{80}, \qquad \gamma_1 \leqslant 2^{28}\alpha^{104}, \qquad \gamma_2 \leqslant 8\alpha^{14}.$$

Furthermore, one can ensure that

$$H^{(3)} \bullet\!\xrightarrow{2^{10}\alpha^{40}} H \ . \tag{1}$$

Proof. From

$$A \bullet\!\xrightarrow{1} A \ , \quad A \bullet\!\underset{\alpha^2}{\frown}\!\bullet A$$

we get first

$$AA^{-1} \bullet\!\xrightarrow{\alpha^2} A \ .$$

By [3, Prop. 4.5], we find a set S with[1] $1 \in S$ and $S = S^{-1}$ such that

$$A \bullet\!\xrightarrow{2\alpha^2} S \ , \qquad AS^{(n)}A^{-1} \bullet\!\xrightarrow{2^n\alpha^{4n+2}} A$$

for all $n \geqslant 1$. In particular, we get

$$AS^{-1} = AS \bullet\!\xrightarrow{2\alpha^6} A \ , \qquad S \bullet\!\xrightarrow{2\alpha^6} A \ .$$

We have

$$S^{(3)} \bullet\!\xrightarrow{8\alpha^{14}} A \bullet\!\xrightarrow{2\alpha^2} S \ ,$$

[1] The property $1 \in S$ is not explicitly stated in [3], but follows from the explicit definition used by Tao, namely $S = \{x \in G \mid |A \cap Ax| > (2\alpha^2)^{-1}|A|\}$.

and Theorem 2.4 says that $H = S^{(3)}$ is a γ-approximate subgroup containing S, with $\gamma = 2(16\alpha^{16})^5 = 2^{21}\alpha^{80}$, and (as we see)

$$H \bullet\!\xrightarrow{8\alpha^{14}} A\ .$$

Moreover, we have

$$H^{(3)} = S^{(9)} \rightarrowtail AS^{(9)}A^{-1} \bullet\!\xrightarrow{2^9\alpha^{38}} A \bullet\!\xrightarrow{2\alpha^2} S\ ,$$

which gives (1).

Now from

$$AH = AS^{(3)} \bullet\!\xrightarrow{8\alpha^{14}} A \bullet\!\xrightarrow{2\alpha^2} S \bullet\!\xrightarrow{1} H\ ,$$

we see by the Ruzsa covering lemma that there exists Y with

$$Y \rightarrowtail A\ , \quad Y \bullet\!\xrightarrow{16\alpha^{16}} 1\ , \quad A \rightarrowtail YHH\ .$$

By definition of an approximate subgroup, there exists Z with

$$Z \bullet\!\xrightarrow{\gamma} 1\ , \quad HH \rightarrowtail ZH\ ,$$

and hence

$$A \rightarrowtail (YZ)H\ .$$

Now we go towards B. First we have

$$AH^{-1} = AS^{(3)} \bullet\!\xrightarrow{8\alpha^{14}} A \bullet\!\xrightarrow{2\alpha^2} H$$

which, again by folding, gives

$$A \bullet\!\underset{\alpha_1}{\text{———}}\!\bullet H$$

with $\alpha_1 = 8\sqrt{2}\alpha^{15}$. Hence we can write

$$H \bullet\!\underset{\alpha_1}{\text{———}}\!\bullet A \bullet\!\underset{\alpha}{\text{———}}\!\bullet B^{-1}\ ,$$

and so

$$H \bullet\!\underset{\alpha\alpha_1}{\text{————}}\!\bullet B^{-1}\ .$$

In addition, we have

$$H \bullet\!\xrightarrow{8\alpha^{14}} A \bullet\!\xrightarrow{\alpha^2} B^{-1}\ ,$$

and therefore we get

$$H \bullet\!\xrightarrow{8\alpha^{16}} B^{-1}, \qquad H \bullet\!\underset{\alpha\alpha_1}{\text{————}}\!\bullet B^{-1}$$

from which it follows by unfolding that

$$B^{-1}H^{-1} = B^{-1}H \bullet\!\xrightarrow{32\alpha^{20}} B^{-1} \bullet\!\xrightarrow{\alpha^2} A \bullet\!\xrightarrow{2\alpha^2} H\ .$$

Once more by the Ruzsa covering lemma, we find Y_1 with

$$Y_1 \rightarrowtail B^{-1}\ , \quad Y_1 \bullet\!\xrightarrow{2^6\alpha^{24}} 1\ , \quad B^{-1} \rightarrowtail Y_1HH \rightarrowtail (Y_1Z)H\ .$$

Now we need only take $X = (Y_1Z \cup YZ)$, so that

$$X \bullet\!\xrightarrow{\gamma_1} 1$$

with $\gamma_1 = \gamma(64\alpha^{24} + 16\alpha^{16})$, in order to conclude. Since

$$\gamma_1 \leqslant 2^{28}\alpha^{104},$$

we are done. □

The next result is a version of the Balog-Gowers-Szemerédi Lemma.

Theorem 2.6 (Balog-Gowers-Szemerédi; Tao, Th. 5.2)**.** *Let A and B with*

$$A \overset{\alpha}{\bullet\!\!\leftrightsquigarrow\!\!\bullet} B\ .$$

Then there exist A_1, B_1 with

$$A_1 \rightarrowtail A\ , \qquad B_1 \rightarrowtail B\ ,$$

as well as

$$A \bullet\!\!\xrightarrow{\ 8\sqrt{2}\alpha\ } A_1\ , \qquad B \bullet\!\!\xrightarrow{\ 8\alpha\ } B_1\ ,$$

and

$$A_1 \underset{\alpha_1}{\bullet\!\!-\!\!\!-\!\!\bullet} B_1^{-1}$$

where $\alpha_1 = 2^{23}\alpha^9$.

This is not entirely spelled out in [3], but only the last two or three inequalities in the proof need to be made explicit to obtain this value of α_1.

Theorem 2.7 (Tao, Th. 5.4; (i) implies (iv))**.** *Let A and B with*

$$A \overset{\alpha}{\bullet\!\!\leftrightsquigarrow\!\!\bullet} B\ .$$

Then there exist a β-approximate subgroup H and x, $y \in G$, such that

$$H \bullet\!\!\xrightarrow{\beta_2} A\ , \qquad A \bullet\!\!\xrightarrow{\beta_1} A \cap xH\ , \qquad B \bullet\!\!\xrightarrow{\beta_1} B \cap Hy\ ,$$

where

$$\beta \leqslant 2^{1861}\alpha^{720}, \qquad \beta_1 \leqslant 2^{2424}\alpha^{937}, \qquad \beta_2 \leqslant 2^{325}\alpha^{126}.$$

Moreover, one can ensure that

$$H^{(3)} \bullet\!\!\xrightarrow{\beta_3} H$$

where $\beta_3 = 2^{930}\alpha^{360}$.

Proof. By the Balog-Gowers-Szemerédi Theorem, we get A_1, B_1 with

$$A_1 \rightarrowtail A\ , \qquad B_1 \rightarrowtail B\ ,$$

as well as

$$A \bullet\!\!\xrightarrow{\ 8\sqrt{2}\alpha\ } A_1\ , \qquad B \bullet\!\!\xrightarrow{\ 8\alpha\ } B_1\ ,$$

and

$$A_1 \underset{\alpha_1}{\bullet\!\!-\!\!\!-\!\!\bullet} B_1^{-1}$$

where $\alpha_1 = 2^{23}\alpha^9$. Applying Theorem 2.5 to A_1 and B_1, we get a β-approximate subgroup H and a set X with

$$H \bullet\!\!\xrightarrow{\ 8\alpha_1^{14}\ } A_1 \bullet\!\!\xrightarrow{1} A$$

and

$$X \bullet\!\!\xrightarrow{\gamma} 1\ , \qquad A_1 \rightarrowtail XH\ , \qquad B_1 \rightarrowtail HX\ ,$$

where

$$\beta = 2^{21}\alpha_1^{80} = 2^{1861}\alpha^{720}, \qquad \gamma = 2^{28}\alpha_1^{104} = 2^{2420}\alpha^{936},$$

and moreover

$$H^{(3)} \bullet\!\!\xrightarrow{\beta_3} H$$

where $\beta_3 = 2^{10}\alpha_1^{40} = 2^{930}\alpha^{360}$.

Applying the pigeonhole principle, we find x such that

$$A \bullet\!\!\xrightarrow{\ 8\sqrt{2}\alpha\ } A_1 \bullet\!\!\xrightarrow{\gamma} A_1 \cap xH \rightarrowtail A \cap xH$$

and y with

$$B \bullet\!\xrightarrow{8\alpha} B_1 \bullet\!\xrightarrow{\gamma} B_1 \cap Hy \rightarrowtail B \cap Hy\ .$$

This gives what we want with

$$\beta_1 \leqslant 8\sqrt{2}\alpha\gamma \leqslant 2^{2424}\alpha^{937}, \qquad \beta_2 = 8\alpha_1^{14} = 2^{325}\alpha^{126}.$$

□

References

[1] E. Kowalski: *Expander graphs*, lecture notes (in progress), available at `www.math.ethz.ch/~kowalski/expander-graphs.pdf`

[2] G. Petridis: *New proofs of Plünnecke-type estimates for product sets in groups*, preprint (2011), `arXiv:1101.3507v3`.

[3] T. Tao: *Product set estimates for non-commutative groups*, Combinatorica 28 (2008), 547–594.

[4] T. Tao and V. Vu: *Additive combinatorics*, Cambridge Studies Adv. Math. 105, Cambridge Univ. Press (2006).

E-mail address: `kowalski@math.ethz.ch`