

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 $d(A, B) \leq \log \alpha$, we write

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

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

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

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

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

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

$$A \bullet \overset{\alpha}{\rightsquigarrow} \bullet B$$

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

$$A \triangleright \longrightarrow B .$$

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

- (1) From

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

we can get

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

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

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

we get

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

- (3) From

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

we get

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

(4) (“Unfolding edges”) From

$$\begin{array}{c} B \bullet \xrightarrow{\alpha} A \\ \quad \quad \quad \curvearrowright \\ \quad \quad \quad \beta \end{array}$$

we get

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

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

$$B \bullet \xrightarrow{\beta} A$$

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

$$A \bullet \xrightarrow{\alpha\beta^{1/2}} B .$$

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 $A \succ \rightarrow B$) and product sets (for $A \bullet \xrightarrow{\alpha} B$ or $A \bullet \overset{\alpha}{\curvearrowright} B$).

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

$$X \succ \rightarrow B , \quad X \bullet \xrightarrow{\alpha} 1 , \quad B \succ \rightarrow A^{-1}AX ,$$

and symmetrically, if

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

there exists Y with

$$Y \succ \rightarrow B , \quad Y \bullet \xrightarrow{\alpha} 1 , \quad B \succ \rightarrow XAA^{-1} .$$

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

$$X \bullet \xrightarrow{\alpha} 1 , \quad H^{(2)} \succ \rightarrow XH .$$

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 $n \geq 3$. 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 $(2\alpha^{44})$ -approximate subgroup containing A .

Proof. We have first

$$H \bullet \xrightarrow{\alpha} A , \quad A \succ \longrightarrow H .$$

Then by Ruzsa's result, we get

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

and by the Ruzsa covering lemma there exists X with

$$X \succ \longrightarrow H^{(2)} , \quad X \bullet \xrightarrow{\alpha^5} 1 ,$$

such that

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

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

$$X_1 \succ \longrightarrow H^{(2)} , \quad X_1 \bullet \xrightarrow{2\alpha^5} 1 ,$$

and

$$H^{(2)} \succ \longrightarrow HX , \quad H^{(2)} \succ \longrightarrow XH ,$$

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*

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

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

$$X \bullet \xrightarrow{\gamma_1} 1 , \quad A \succ \longrightarrow XH , \quad B \succ \longrightarrow HX , \quad H \bullet \xrightarrow{\gamma_2} A ,$$

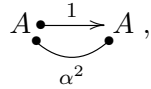
where

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

Furthermore, one can ensure that

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

Proof. From

$$A \bullet \xrightarrow{1} A ,$$


we get first

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

By [3, Prop. 4.5], we find a set S with¹ $1 \in S$ and $S = S^{-1}$ such that

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

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

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

Thus

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

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

which gives

$$A \bullet \xrightarrow{\beta} S$$

by folding, with $\beta = 2\sqrt{2}\alpha^7$.

In addition, we have

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

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

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

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

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

By definition of an approximate subgroup, there exists Z with

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

and hence

$$A \succ \xrightarrow{} (YZ)H .$$

Now we go towards B . First we have

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

which, again by folding, gives

$$A \bullet \xrightarrow{\alpha_1} H$$

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

$$H \bullet \xrightarrow{\alpha_1} A \bullet \xrightarrow{\alpha} B^{-1} ,$$

and so

$$H \bullet \xrightarrow{\alpha\alpha_1} B^{-1} .$$

In addition, we have

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

and therefore we get

$$H \bullet \xrightarrow{8\alpha^{16}} B^{-1} ,$$

$\alpha\alpha_1$

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

$$Y_1 \succ \xrightarrow{} B^{-1} , \quad Y_1 \bullet \xrightarrow{32\alpha^{20}} 1 , \quad B^{-1} \succ \xrightarrow{} Y_1HH \succ \xrightarrow{} (Y_1Z)H .$$

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

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

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*

$$A \overset{\alpha}{\rightsquigarrow} B.$$

Then there exist A_1, B_1 with

$$A_1 \succrightarrow A, \quad B_1 \succrightarrow B,$$

as well as

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

and

$$A_1 \bullet \xrightarrow{\alpha_1} B_1^{-1}$$

where $\alpha_1 = 2^{20}\alpha^9$.

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*

$$A \overset{\alpha}{\rightsquigarrow} B.$$

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

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

where

$$\beta \leq 2^{1621}\alpha^{720}, \quad \beta_1 \leq 2^{2112}\alpha^{937}, \quad \beta_2 \leq 2^{283}\alpha^{126}.$$

Moreover, one can ensure that

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

where $\beta_3 = 2^{810}\alpha^{360}$.

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

$$A_1 \succrightarrow A, \quad B_1 \succrightarrow B,$$

as well as

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

and

$$A_1 \bullet \xrightarrow{\alpha_1} B_1^{-1}$$

where $\alpha_1 = 2^{20}\alpha^9$. Applying Theorem 2.5 to A_1 and B_1 , we get a β -approximate subgroup H and a set X with

$$H \bullet \xrightarrow{2\alpha_1^{14}} A_1 \bullet \xrightarrow{1} A$$

and

$$X \bullet \xrightarrow{\gamma} 1, \quad A_1 \succrightarrow XH, \quad B_1 \succrightarrow HX,$$

where

$$\beta = 2^{21}\alpha_1^{80} = 2^{1621}\alpha^{720}, \quad \gamma = 2^{28}\alpha_1^{104} = 2^{2108}\alpha^{936},$$

and moreover

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

where $\beta_3 = 2^{10} \alpha_1^{40} = 2^{810} \alpha^{360}$.

Applying the pigeonhole principle, we find x such that

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

and y with

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

This gives what we want with

$$\beta_1 \leq 8\sqrt{2}\alpha\gamma \leq 2^{2112} \alpha^{937}, \quad \beta_2 = 8\alpha_1^{14} = 2^{283} \alpha^{126}.$$

□

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](https://arxiv.org/abs/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