SUBSTRUCTURE FOR PRODUCT SET IN THE HEISENBERG GROUPS

NORBERT HEGYVÁRI AND FRANÇOIS HENNECART

Abstract. We show that for any sufficiently big *semi-brick* A of the 1-dimensional Heisenberg group H over the finite field $\mathbb{F}_p$, the 4-fold product set $A \cdot A \cdot A \cdot A$ contains at least $|A|/p$ many cosets modulo some non trivial subgroup of H_1.

1. **Introduction**

Let H be the Heisenberg group on the prime field $\mathbb{F}$ with p elements and denote by

$$[x, y, z] = \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}, \quad x, y, z \in \mathbb{F}$$

the elements of H. The product rule in H runs as follows:

$$[x, y, z] \cdot [x', y', z'] = [x + x', y + y', xy' + z + z'],$$
$$[x, y, z]^{-1} = [-x, -y, xy - z].$$

The Heisenberg group possesses an interesting structure in which we can prove that in general there is no *good model* for a subset A with a small *square set* $A \cdot A$ (see [2] and also [4]), unlike for subsets of Abelian group. Here by a good s-model for A we mean a subset A' of a finite group G' such that A is s-Freiman isomorphic to A' and $|G'| \ll_{s,K} |A'|$ where $K = |A \cdot A|/|A|$ is the squaring ratio (see [4] for more details).

The famous Freiman theorem for a given subset A of an abelian group G asserts that whenever $A \cdot A$ has its cardinality close to that of A, then A has a structure (cf. [3]). In the non-abelian Heisenberg group H this result is no longer true. Nevertheless under the stronger condition that $|A \cdot A \cdot A| \leq K|A|$ with $A \subset H$, Tao obtains in [7] a structure result for such subsets A. As a dual problem in the Heisenberg particular situation, we can ask the following question: is it true that for a not too small subset A of H, the product set $A \cdot A$ necessarily contains some non-trivial substructure of H ?

Date: March 15, 2013.

2000 *Mathematics Subject Classification.* primary 11B75, secondary 05D10.

Key words and phrases. Bases, Heisenberg groups.

A related question emerged in $\mathrm{SL}_2(\mathbb{F})$ in [6] (see also [1]) where it is proved that under some condition on $A \subset \mathrm{SL}_2(\mathbb{F})$, namely A is a not too big generating subset of $\mathrm{SL}_2(\mathbb{F})$, one has $|A \cdot A \cdot A| > |A|^{1+\varepsilon}$.

Nevertheless, the structure or even the size of the *square set* $A \cdot A$ cannot be handled in general. We will restrict our attention to subsets that will be called *semi-bricks*: for $U \subset \mathbb{F}^2$ and $Z \subset \mathbb{F}$ we define the so called *semi-brick* A in H by

$$A = \{[x, y, z] \text{ such that } (x, y) \in U,\ z \in Z\}.$$

For denoting this set we simply write $A = U \rtimes Z$. According to this notation we have $H = \mathbb{F}^2 \rtimes \mathbb{F}$ and $[x, y, \mathbb{F}] = \{(x, y)\} \rtimes \mathbb{F}$.

We may eventually expect that if A is a sufficiently big brick in H, that is a subset of the form $(X \times Y) \rtimes Z$, then $A \cdot A$ contains a substructure formed by a rich collection of cosets modulo the subgroup $[0, 0, \mathbb{F}]$. In fact we proved in [5] such a result in the n-dimensional Heisenberg group when n is large enough, namely $n \geq 5$. Moreover for any arbitrary big subset A of H, we also have a rich substructure for the 6-fold product set $A^6 = A{\cdot}A{\cdot}A{\cdot}A{\cdot}A{\cdot}A$ (see [4]). In what follows we focus on semi-bricks.

Our main result is the following.

Theorem 1. *Let $A = U \rtimes Z$ be a semi-brick in H. If $|A| \geq 2^{-1/3}p^{8/3}$ then the four-fold product set $A \cdot A \cdot A \cdot A$ contains at least $|U|\left(1 - \frac{p^4}{\sqrt{2}|A|^{3/2}}\right)$ cosets of the type $[x, y, \mathbb{F}]$.*

This theorem will be proved in the last section, based on some partial results shown in the second section.

2. Preliminary results

2.1. For $a = [a_1, a_2, a_3]$, $b = [b_1, b_2, b_3]$ and $c = [c_1, c_2, c_3]$ we have the product rule

$$abca^{-1} = [b_1 + c_1, b_2 + c_2, b_3 + c_3 + a_1(b_2 + c_2) - a_2(b_1 + c_1) + b_1c_2].$$

We fix a semi-brick $A = U \rtimes Z$ in H and a subset $\tilde{A} = \tilde{U} \rtimes Z$ of A being also a semi-brick in H ; it means that $\tilde{U} \subset U$. In order to show that $\tilde{A} \cdot A \cdot A \cdot \tilde{A}^{-1}$ contains many cosets of $[0, 0, \mathbb{F}]$ we will restrict our consideration to elements of this product set of the particular form $abca^{-1}$ with $a \in \tilde{A},\ b, c \in A$. For fixed x, y, t we denote by $R(x, y, t)$ the number of solutions to the system

$$[x, y, t] = abca^{-1},\ a \in \tilde{A},\ b, c \in A.$$

In the sequel $\tilde{A} = A$ will be a natural choice but we shall see in the concluding section that a more appropriate choice for $\tilde{A}$ will help us to obtain our main result Theorem 1.

It is then obvious that $R(x,y,t)$ is the number of solutions to the equation

$$\begin{cases} t = b_3 + c_3 + a_1 y - a_2 x + (b_1 y - b_1 b_2), \\ (a_1,a_2) \in \tilde{U},\ (b_1,b_2) \in V_{x,y},\ b_3, c_3 \in Z, \end{cases}$$

where $x = b_1 + c_1$, $y = b_2 + c_2$ and $V_{x,y} = U \cap ((x,y) - U)$.

Letting $\mathrm{e}_p(\theta) = \exp(2i\pi\theta/p)$, one has

$$R(x,y,t) = \frac{1}{p}\sum_r \sum_{\substack{(a_1,a_2)\in\tilde{U} \\ (b_1,b_2)\in V_{x,y} \\ (b_3,c_3)\in Z^2}} \mathrm{e}_p\Big(r(b_3 + c_3 + a_1 y - a_2 x + b_1 y - b_1 b_2 - t)\Big). \tag{1}$$

We let

$$\Delta(x,y) = \max_t \left| R(x,y,t) - \frac{|\tilde{U}||V_{x,y}||Z|^2}{p} \right|,$$

after observing that $\frac{|\tilde{U}||V_{x,y}||Z|^2}{p}$ is the contribution of $r=0$ in the right-hand side of (1).

Then

$$\begin{aligned} \Delta(x,y) &\le \frac{1}{p}\sum_{r\neq 0} |\widehat{Z}(r)|^2 \Big| \sum_{\substack{(a_1,a_2)\in\tilde{U} \\ (b_1,b_2)\in V_{x,y}}} \mathrm{e}_p\Big(r(a_1 y - a_2 x + b_1 y - b_1 b_2)\Big)\Big| \\ &\le \frac{1}{p}\sum_{r\neq 0} |\widehat{Z}(r)|^2 |V_{x,y}| \Big| \sum_{(a_1,a_2)\in\tilde{U}} \mathrm{e}_p\Big(r(a_1 y - a_2 x)\Big)\Big| \\ &< |Z||V_{x,y}| \max_{r\neq 0} \Big| \sum_{(a_1,a_2)\in\tilde{U}} \mathrm{e}_p\Big(r(a_1 y - a_2 x)\Big)\Big|, \end{aligned}$$

by Parseval inequality.

In this section we assume that $r\tilde{U} = \tilde{U}$ for any $r \neq 0$. Then the sum in the right-hand side does not depend on r. Hence in this case

$$\sum_{x,y} \Delta(x,y) < |Z| \sum_{x,y} |V_{x,y}| \Big| \sum_{(a_1,a_2)\in\tilde{U}} \mathrm{e}_p\Big(a_1 y - a_2 x\Big)\Big| \tag{2}$$

and by Cauchy-Schwarz

$$\sum_{x,y} \Delta(x,y) < |Z| \Big(\sum_{x,y} |V_{x,y}|^2 \Big)^{1/2} \times \Big(\sum_{x,y} \sum_{\substack{(a_1,a_2)\in\tilde{U} \\ (a_1',a_2')\in\tilde{U}}} \mathrm{e}_p\Big((a_1 - a_1')y - (a_2 - a_2')x\Big)\Big)^{1/2} \tag{3}$$

By the definition of $V_{x,y}$, one has $|V_{x,y}| \le |U|$ hence

$$\sum_{x,y} |V_{x,y}|^2 \le |U| \sum_{x,y} |V_{x,y}| = |U|^3, \tag{4}$$

and that the last sum in the right-hand side of equation (3) is equal to $p^2|\tilde{U}|$. Hence

$$\sum_{x,y} \Delta(x,y) < p|Z||U|^{3/2}|\tilde{U}|^{1/2}.$$

If for any x, y, there exists $t = t(x,y)$ such that $R(x,y,t) = 0$ then

$$\Delta(x,y) \geq \frac{|\tilde{U}||V_{x,y}||Z|^2}{p}$$

and we would have

$$\sum_{x,y} \frac{|\tilde{U}||V_{x,y}||Z|^2}{p} < p|Z||U|^{3/2}|\tilde{U}|^{1/2}$$

which implies

$$|\tilde{U}||U|^2|Z|^2 < p^2|Z||U|^{3/2}|\tilde{U}|^{1/2}.$$

One gets a contradiction if $|\tilde{U}||U||Z|^2 \geq p^4$ or equivalently $|\tilde{A}||A| \geq p^4$.

We thus have proved the following partial result.

Proposition 2. *Let $A = U \rtimes Z$ a semi-brick in H and assume that $\tilde{A}$ is at the same time a subset of A and a semi-brick $\tilde{A} = \tilde{U} \rtimes Z$ such that $r\tilde{U} = \tilde{U}$ for any $r \in \mathbb{F}\setminus\{0\}$. If $|A||\tilde{A}| \geq p^4$ then $\tilde{A} \cdot A \cdot A \cdot \tilde{A}^{-1}$ contains a coset $[x, y, \mathbb{F}]$.*

2.2. We will now modify our argument in order to avoid the strong assumption $r\tilde{U} = \tilde{U}$, $r \neq 0$. From equation (3) and (4), one gets

$$\sum_{x,y} \Delta(x,y) \leq |Z||U|^{3/2} \times \Bigg(\sum_{x,y} \max_{r\neq 0} \sum_{\substack{(a_1,a_2)\in\tilde{U} \\ (a_1',a_2')\in\tilde{U}}} \mathrm{e}_p\Big(r((a_1-a_1')y-(a_2-a_2')x)\Big)\Bigg)^{1/2}$$

Then by replacing the maximum on $r \neq 0$ by the summation on any $r \neq 0$ we get

$$\sum_{x,y} \Delta(x,y) < |Z||U|^{3/2} \times \Bigg(\frac{1}{2}\sum_{x,y}\sum_{r\neq 0} \sum_{\substack{(a_1,a_2)\in\tilde{U} \\ (a_1',a_2')\in\tilde{U}}} \mathrm{e}_p\Big(r((a_1-a_1')y-(a_2-a_2')x)\Big)\Bigg)^{1/2}$$

where the factor 1/2 comes from the fact the modulus of a single term in the summation over $r \neq 0$ is the same as the modulus of its conjugate. By interchanging the sum on x, y and the sum on r we easily deduce in the same way as in the previous section

$$\sum_{x,y} \Delta(x,y) < \frac{|Z||U|^{3/2}((p-1)p^2|\tilde{U}|)^{1/2}}{\sqrt{2}} < \frac{p^{3/2}|Z||U|^{3/2}|\tilde{U}|^{1/2}}{\sqrt{2}}. \tag{5}$$

As above we conclude that we cannot have $\Delta(x,y) \geq \frac{|\tilde{U}||V_{x,y}||Z|^2}{p}$ for any x, y if

$$\sqrt{2}|\tilde{U}||U|^2|Z|^2 \geq p^{5/2}|Z||U|^{3/2}|\tilde{U}|^{1/2}.$$

Hence the following result

Proposition 3. *Let $A = U \rtimes Z$ a semi-brick in H and assume that $\tilde{A} = \tilde{U} \rtimes Z$ is a semi-brick which is a subset of A. If $2|A||\tilde{A}| \geq p^5$ then $\tilde{A} \cdot A \cdot A \cdot \tilde{A}^{-1}$ contains a coset $[x, y, \mathbb{F}]$.*

By letting $E := \sum_{x,y} |V_{x,y}|^2$ the *energy* of the set U which already appeared in (4), we showed in fact that if $\tilde{A} \cdot A \cdot A \cdot \tilde{A}^{-1}$ does not contain any coset $[x, y, \mathbb{F}]$ then $\sqrt{2}|\tilde{U}||U|^2|Z|^2 < p^{5/2}|Z|E^{1/2}|\tilde{U}|^{1/2}$. Hence

$$E > \frac{2|\tilde{U}||U|^4|Z|^2}{p^5}. \tag{6}$$

Instead of the simple deviation $\max_t \left| R(x, y, t) - \frac{|\tilde{U}||V_{x,y}||Z|^2}{p} \right|$ it could provide an advantage to consider the following quadratic mean value

$$\sigma(x, y) := \sum_t \left(R(x, y, t) - \frac{|\tilde{U}||V_{x,y}||Z|^2}{p} \right)^2$$

and $\sigma = \sum_{x,y} \sigma(x, y)$. We now assume that for any x, y there is at least one t such that $R(x, y, t) = 0$. Then by (6)

$$\sigma \geq \frac{|\tilde{U}|^2|Z|^4}{p^2} \cdot E > \frac{2|\tilde{U}|^3|U|^4|Z|^6}{p^7}. \tag{7}$$

On the other hand

$$\sigma(x, y) = \sum_t \Big(\frac{1}{p} \sum_{r \neq 0} \sum_{\substack{(a_1,a_2) \in \tilde{U} \\ (b_1,b_2) \in V_{x,y} \\ b_3, c_3 \in Z}} e_p(r(a_1 y - a_2 x + b_1 y - b_1 b_2 + b_3 + c_3 - t)) \Big)^2$$

$$= \frac{1}{p} \sum_{r \neq 0} \Big(\sum_{(a_1,a_2) \in \tilde{U}} e_p(r(a_1 y - a_2 x)) \Big)^2 \Big(\sum_{(b_1,b_2) \in V_{x,y}} e_p(r(b_1 y - b_1 b_2)) \Big)^2 \Big(\sum_{b_3, c_3 \in Z} e_p(r(b_3 + c_3)) \Big)^2$$

after developing and summing on t. Hence

$$\sigma(x, y) \leq \frac{|V_{x,y}|^2}{p} \sum_{r \neq 0} |\hat{Z}(r)|^4 \Big(\sum_{(a_1,a_2) \in \tilde{U}} e_p(r(a_1 y - a_2 x)) \Big)^2.$$

Since $|V_{x,y}| \leq |U|$ we obtain by developing the square of the sum over (a_1, a_2) and summing over x and y

$$\sigma \leq p|U|^2|\tilde{U}| \sum_{r \neq 0} |\hat{Z}(r)|^4 \leq p^2|U|^2|\tilde{U}||Z|^3. \tag{8}$$

Together with (7), we get

$$\frac{2|\tilde{U}|^3|U|^4|Z|^6}{p^7} < p^2|U|^2|\tilde{U}||Z|^3.$$

We thus have slightly improved Proposition 3:

Proposition 4. *Let $A = U \rtimes Z$ a semi-brick in H and assume that $\tilde{A} = \tilde{U} \rtimes Z$ is a semi-brick which is a subset of A. If $2|A|^2|\tilde{A}|^2 \geq p^9|Z|$ then $\tilde{A} \cdot A \cdot A \cdot \tilde{A}^{-1}$ contains a coset $[x, y, \mathbb{F}]$.*

We could take $\tilde{A} = A$ in Proposition 3. This does not imply that A^4 contains a coset and does not give any lower bound for the number of such cosets. We will treat these questions in the next section.

3. Proof of the main result

Here we assume that A is a semi-brick satisfying the hypothesis of Theorem 1.

3.1. By the averaging argument there exists an $[x_0, y_0, z_0]$ such that

$$\big|A \cap (A^{-1} \cdot [x_0, y_0, z_0])\big| \geq \frac{|A|^2}{p^3}. \tag{9}$$

Let $\tilde{U}$ the image of the intersection $A \cap (A^{-1} \cdot [x_0, y_0, z_0])$ by the projection on the first two coordinates and write $\tilde{A} = \tilde{U} \rtimes Z$. Clearly $\tilde{U} \subset U$ and

$$A \cap (A^{-1} \cdot [x_0, y_0, z_0]) \subset \tilde{A} \text{ and } |\tilde{A}| \geq \frac{|A|^2}{p^3}.$$

We apply Proposition 3 to A and $\tilde{A} \subset A$. It follows that if $2|A|^3 \geq p^8$ then $\tilde{A} \cdot A \cdot A \cdot \tilde{A}^{-1}$ contains a coset $[x, y, \mathbb{F}]$ hence $\tilde{A} \cdot A \cdot A \cdot \tilde{A}^{-1}[x_0, y_0, z_0]$ contains a coset $[x + x_0, y + y_0, \mathbb{F}]$. But

$$\tilde{A} \cdot A \cdot A \cdot \tilde{A}^{-1}[x_0, y_0, z_0] \subset \tilde{A} \cdot A \cdot A \cdot A^{-1}[x_0, y_0, z_0] \subset \tilde{A} \cdot A \cdot A \cdot \tilde{A} \subset A^4,$$

hence the following proposition.

Proposition 5. *Let $A = U \rtimes Z$ a semi-brick in H. If $2^{1/3}|A| \geq p^{8/3}$ then $A \cdot A \cdot A \cdot A$ contains a coset $[x_1, y_1, \mathbb{F}]$.*

3.2. We keep the notation of the preceding paragraph. Let S be the set of pairs (x, y) such that there exists t with $R(x, y, t) = 0$. Then for those x, y

$$\Delta(x, y) \geq \frac{|\tilde{U}||V_{x,y}||Z|^2}{p}.$$

Denote by $\overline{S}$ the complementary set of S in $\mathbb{F}^2$. Then by (5)

$$\sum_{(x,y)\in S} \frac{|\tilde{U}||V_{x,y}||Z|^2}{p} \leq \sum_{(x,y)\in S} \Delta(x, y) \leq \sum_{x,y} \Delta(x, y) < \frac{p^{3/2}|Z||\tilde{U}|^{1/2}|U|^{3/2}}{\sqrt{2}}.$$

Since

$$\sum_{(x,y)\in S} |V_{x,y}| = \sum_{x,y} |V_{x,y}| - \sum_{(x,y)\in \overline{S}} |V_{x,y}| = |U|^2 - \sum_{(x,y)\in \overline{S}} |V_{x,y}|$$

and $|V_{x,y}| \leq |U|$, it follows that

$$|U||\overline{S}| > |U|^2 - \frac{p^{5/2}|U|^{3/2}}{\sqrt{2}|Z||\tilde{U}|^{1/2}} = |U|^2 \left(1 - \frac{p^{5/2}}{\sqrt{2}|Z||\tilde{U}|^{1/2}|U|^{1/2}}\right).$$

Hence

$$|\overline{S}| > \frac{|A|}{|Z|}\left(1-\sqrt{\frac{p^5}{2|A||\tilde{A}|}}\right) \geq \frac{|A|}{|Z|}\left(1-\frac{p^4}{\sqrt{2}|A|^{3/2}}\right)$$

since $|\tilde{A}| \geq |A|^2/p^3$.

This completes the proof of Theorem 1.

3.3. We assume here that A is such $A \cdot A \cdot A \cdot A$ does not contain any coset $[x, y, \mathbb{F}]$. By Proposition 4 and the arguments of subsection 3.1, we infer

$$2|A|^2|\tilde{A}|^2 < p^9|Z| \tag{10}$$

where $\tilde{A}$ is any set of the kind $\tilde{A} = \tilde{U'} \rtimes Z$, $\tilde{U'}$ is the projection on the first two coordinates of some $A' \cap (A'^{-1} \cdot [x_0, y_0, z_0])$ with $A' \subset A$. With the choice of $\tilde{A}$ that we made in subsection 3.1, we get

$$2|A|^6 < p^{15}|Z|. \tag{11}$$

Hence the more $|Z|$ is small, the more the above condition is sharp. Now from (6) we obtain

$$2|A||\tilde{A}| < \frac{p^5}{K}, \tag{12}$$

where K is defined by $K = |U|^3/E$ and E denotes the energy of the set U. With the same selection of $\tilde{A}$ we obtain

$$2|A|^3 < \frac{p^8}{K}, \tag{13}$$

When K is big this condition becomes stronger and on the other hand for small K we could apply the Balog-Szemerédi-Gowers Theorem (see [8, pages 78-79]). We infer that there is an absolute constant $C > 1$ ($C = 5$ is an admissible value) and two subsets U', U'' of U such that

$$|U'|, |U''| \gg K^{-1}|U| \quad \text{and} \quad |U' + U''| \ll K^C|U|.$$

We write $A' := U' \rtimes Z \subset A$ and $A'' := U'' \rtimes Z \subset A$. Arguing as in subsection 3.1, we deduce that there exists $[x_0', y_0', z_0'] \in A' \cdot A''$ such that

$$\left|A \cap (A^{-1} \cdot [x_0', y_0', z_0'])\right| \geq \left|A'' \cap (A'^{-1} \cdot [x_0', y_0', z_0'])\right| \geq \frac{|A'||A''|}{|A' \cdot A''|}.$$

Letting $\tilde{A} = A \cap (A^{-1} \cdot [x_0', y_0', z_0'])$ and noticing that $A' \cdot A'' \subset (U' + U'') \rtimes \mathbb{F}$ one deduces $|\tilde{A}| \gg K^{-C-2}|A||Z|/p$. Hence by (10), $|A|^4|Z| \ll K^{2C+4}p^{11}$. Multiplying this inequality together with (11) we get the condition $|A|^{10} \ll K^{2C+4}p^{26}$, namely

$$|A|^5 \ll K^{C+2}p^{13}.$$

Together with (13) we may eliminate the parameter K: this gives

$$|A|^{11+3C} \ll p^{29+8C},$$

hence

$$|A| \ll p^{(29+8C)/(11+3C)}.$$

We may notice that the exponent grows in the interval $(\frac{29}{11}, \frac{8}{3})$ when C ranges from 0 to infinity. This provides an improved version of Proposition 5 which plainly yields a corresponding slight improvement on Theorem 1. Letting $C = 5$ we get the following result.

Proposition 6. *Let $A = U \rtimes Z$ a semi-brick in H. If $|A| \gg p^{69/26}$ then $A \cdot A \cdot A \cdot A$ contains at least one coset $[x, y, \mathbb{F}]$.*

3.4. From Theorem 1 we obtain that for $A = U \rtimes Z$ with $|A| \geq 2^{-1/3}p^{8/3}$, the product set A^4 contains at least $|A|/p$ many different cosets $[x, y, \mathbb{F}]$ if $|Z| \leq p/2$. If $|Z| > p/2$ then $Z+Z = \mathbb{F}$ and it is not hard to conclude to the same result since in this case $A \cdot A = 2U \rtimes \mathbb{F}$ plainly contains at least $|2U| \geq |U| \geq |A|/p$ many cosets $[x, y, \mathbb{F}]$. Indeed for any $[u, v, t] \in 2U \rtimes \mathbb{F}$, it is possible to find (x, y) and (x', y') both in U such that $u = x + x'$ and $v = y + y'$. We then select $z, z' \in Z$ such that $z + z' = t - xy'$, which is possible by our extra assumption $Z + Z = \mathbb{F}$. Finally $[x, y, z] \cdot [x', y', z'] = [u, v, t]$ with $[x, y, z], [x', y', z'] \in A$ as requested.

3.5. By considering the semi-brick $A = U \rtimes \mathbb{F}$, with $|U| \gg p^{5/3}$ we observe that $A^4 = 4U \rtimes \mathbb{F}$ hence A^4 is the union of $|4U|$ cosets $[x, y, \mathbb{F}]$. With $U = I \times \mathbb{F}$ where I is an interval in $\mathbb{F}$, one has $|4U| = 4|U| - 3$. Hence A^4 is the union of $4|U| - 3$ many cosets modulo the subgroup $[0, 0, \mathbb{F}]$. Thus according to Theorem 1 we can ask the question of finding the optimal number of cosets of $[0, 0, \mathbb{F}]$ contained in A^4 where $A = U \rtimes Z$ is a semi-brick which is big enough. By the above discussion, this number is less than $4|U| - 3$ and bigger than $(1 - \epsilon)|U|$ at least for $p^{8/3}/2^{1/3} \leq |A| \leq p^{3-\eta}$.

Acknowledgement. The authors warmly thank the anonymous referee who pointed out that our Propositions 3 and 5 could be refined by Propositions 4 and 6.

References

[1] N. Gill, H.A. Helfgott: Growth of small generating sets in $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$, *Int. Math. Res. Not.* 2011, no. 18, 4226–4251.

[2] B. Green: A note on Freiman models, unpublished note (2008).

[3] B. Green & I.Z. Ruzsa: Freiman's theorem in an arbitrary abelian group. *J. Lond. Math. Soc.* (2) **75** (2007), no. 1, 163–175.

[4] N. Hegyvári & F. Hennecart: A note on Freiman models in Heisenberg groups, *Israel J. of Math.* **189** (2012), 397–411.

[5] N. Hegyvári & F. Hennecart: A structure result for bricks in Heisenberg groups, preprint, 2012.

[6] H.A. Helfgott: Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$, *Ann. of Math.* **167** (2008), 601–623.

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

[8] T. Tao & V.H. Vu; *Additive combinatorics.* Cambridge Studies in Advanced Mathematics, 105. Cambridge University Press, Cambridge, 2006. xviii+512 pp.

Norbert Hegyvári, ELTE TTK, Eötvös University, Institute of Mathematics, H-1117 Pázmány st. 1/c, Budapest, Hungary

E-mail address: hegyvari@elte.hu

François Hennecart, Université Jean-Monnet, Institut Camille Jordan, 23, rue du Docteur Paul Michelon, 42023 Saint-Etienne Cedex 02, France

E-mail address: francois.hennecart@univ-st-etienne.fr