C. R. Acad. Sci. Paris, Ser. I 350 (2012) 793–796

Contents lists available at SciVerse ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Logic

A modular Szemerédi–Trotter theorem for hyperbolas ☆

Un théorème de type Szemerédi–Trotter modulaire pour hyperboles

Jean Bourgain

School of Mathematics, Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ 08540, USA

ARTICLE INFO

Article history:
Received 20 August 2012
Accepted 18 September 2012
Available online 15 October 2012

Presented by Jean Bourgain

ABSTRACT

We establish a Szemerédi–Trotter type result for hyperbolas in $\mathbb{F}_p \times \mathbb{F}_p$.

RÉSUMÉ

Nous démontrons une version du théorème de Szemerédi–Trotter pour des familles d'hyperboles dans $\mathbb{F}_p \times \mathbb{F}_p$.

Version française abrégée

Le théorème classique de Szemerédi–Trotter donne une estimée sur les incidences d'une famille finie P de points dans le plan et une famille finie L de droites (ou, plus généralement, de courbes algébriques de degré borné) ; dans sa généralité, cette estimée est optimale. Une version 'corps fini', pour L consistant de droites, est obtenue dans [3]. Nous nous proposons ici d'établir un résultat de ce type pour certaines familles d'hyperboles dans $\mathbb{F}_p \times \mathbb{F}_p$, définie par des équations

$$cxy - ax + dy - b = 0 \quad \text{où} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(p).$$

Essentiellement, la condition imposée sur L est que l'ensemble des matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ qui définit L ne soit pas contenu dans une translatée d'un sous-groupe propre de $SL_2(p)$; l'argument repose en effet sur les résultats de [2] sur l'expansion dans $SL_2(p)$.

1. Introduction and statement of the results

It is shown in [3] that if P and L are sets of points and lines in $\mathbb{P}^2(\mathbb{F}_p)$ with $|P| = |L| = n < p^{2-\varepsilon}$, then the number of incidences

$$I(P, L) = \left|\left\{(p, \ell) \in P \times L;\ p \in \ell\right\}\right| < cn^{\frac{3}{2}-\delta} \tag{1}$$

where $\delta = \delta(\varepsilon) > 0$. An explicit quantitative version of this result appears in [5]. Some of its various applications may be found in [1]. The following statement provides a result of a similar flavor for hyperbolas.

☆ The research was partially supported by NSF grants DMS-0808042 and DMS-0835373.
E-mail address: bourgain@math.ias.edu.

1631-073X/$ – see front matter
http://dx.doi.org/10.1016/j.crma.2012.09.011

Proposition 1. *For all $\varepsilon > 0$ and $r > 1$, there is a $\delta > 0$ such that the following holds. Let p be a large prime and $A \subset \mathbb{F}_p$, $S \subset SL_2(p)$ satisfy the conditions*

(2) $1 \ll |A| < p^{1-\varepsilon}$
(3) $\log |A| < r \log |S|$
(4) $|S \cap gH| < |S|^{1-\varepsilon}$ *for any proper subgroup $H \subset SL_2(p)$ and $g \in SL_2(p)$.*

For $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(p)$, denote $\Gamma_g \subset \mathbb{F}_p^2$ the curve

$$cxy - ax + dy - b = 0. \tag{5}$$

Then

$$\left|\left\{(x, y, g) \in A \times A \times S;\ (x, y) \in \Gamma_g\right\}\right| < |A|^{1-\delta}|S|. \tag{6}$$

Note that the conclusion would be obviously false if we removed assumption (4).

Proposition 2. *Assume given a polynomial function Φ on $\mathbb{F}_p$ taking values in $\mathrm{Mat}_2(\mathbb{F}_p)$, such that $\det \Phi$ does not vanish identically and is a quadratic residue (or a quadratic non-residue). Assume further that $\mathrm{Im}\, \Phi \cap GL_2(p)$ is not contained in a set $\mathbb{F}_p^* . gH$ for some $g \in SL_2(p)$ and $H \subset SL_2(p)$ a proper subgroup.*

Given $\varepsilon > 0$, $r > 1$, there is $\delta > 0$ such that if $A \subset \mathbb{F}_p$, $L \subset \mathbb{F}_p$ satisfy

(7) $1 \ll |A| < p^{1-\varepsilon}$
(8) $\log |A| < r \log L$.

Then

$$\left|\left\{(x, y, t) \in A \times A \times L;\ (x, y) \in \Gamma_{\Phi(t)}\right\}\right| < |A|^{1-\delta}|L|. \tag{9}$$

Applications will be discussed elsewhere.

2. Preliminaries

The main ingredients in the proof are the expansion properties in $SL_2(p)$ obtained in [2] and based on [4].

More specifically, we make use of the so-called 'L^2-flattening lemma' that we recall next (in a version slightly more general than stated in [2] but similar proof).

Lemma 3. *Let η be a symmetric probability measure on $SL_2(p)$ and $1 \ll K < p^{\frac{1}{10}}$, such that*

(10) $\eta(gH) < K^{-1}$ *for any proper subgroup $H \subset SL_2(p)$, $g \in SL_2(p)$*
(11) $\|\eta\|_2 > Kp^{-3/2}$.

Then

$$\|\eta * \eta\|_2 < K^{-c}\|\eta\|_2 \tag{12}$$

with $c > 0$ an absolute constant.

Here $\|\eta\|_2 = [\sum_{g \in SL_2(p)} \eta(g)^2]^{\frac{1}{2}}$. Denoting $\eta^{(\ell)}$ the ℓ-fold convolution, iteration of Lemma 3 implies that for η satisfying (10)

$$\left\|\eta^{(2^\ell)}\right\|_2 \leqslant K^{-c\ell}\|\eta\|_2 + Kp^{-3/2} \tag{13}$$

and hence

$$\left\|\eta^{(2^{\ell+1})}\right\|_\infty \leqslant \left\|\eta^{(2^\ell)}\right\|_2^2 \leqslant 2K^{-2c\ell}\|\eta\|_2^2 + 2K^2p^{-3}. \tag{14}$$

Recall also that if $K > p^\gamma$, (14) combined with an argument due to [6] based on Frobenius multiplicity, implies that

$$\left\|\eta^{(\ell)}\right\|_\infty < 2p^{-3} \tag{15}$$

for some $\ell = \ell(\gamma)$. See [2] for details.

3. Sketch of the proof of Proposition 1

Using the action τ of $SL_2(p)$ on $\mathbb{P}^1(\mathbb{F}_p)$, rewrite Eq. (5) (since we may assume $cx+d\neq 0$) as

$$y=\frac{ax+b}{cx+d}=\tau_g(x).$$

The left-hand side of (6) equals

$$\sum_{g\in S}\big|A\cap\tau_{g^{-1}}(A)\big|=|S|.\Big\langle 1_A,\sum_g(1_A\circ\tau_g)\mu(g)\Big\rangle$$

with

$$\mu=\frac{1}{|S|}\sum_{g\in S}\delta_g$$

and $\langle\,,\rangle$ referring to the inner product on $L^2(\mathbb{F}_p)$.

Next, applying the Cauchy–Schwarz inequality, write

$$\Big\langle 1_A,\sum(1_A\circ\tau_g)\mu(g)\Big\rangle\leqslant|A|^{\frac12}\Big\|\sum_g(1_A\circ\tau_g)\mu(g)\Big\|_2=|A|^{\frac12}\Big[\sum\langle 1_A\circ\tau_g,1_A\rangle\big(\mu*\mu^{-1}\big)(g)\Big]^{\frac12}$$
$$\leqslant|A|^{\frac34}\Big\|\sum(1_A\circ\tau_g)\nu(g)\Big\|_2^{\frac12}$$

where $\nu=\mu*\mu^{-1}$ is symmetric. Iteration gives for any $\ell\in\mathbb{Z}_+$

$$\leqslant|A|^{1-2^{-\ell-1}}\Big\|\sum(1_A\circ\tau_g)\nu^{(2^{\ell-1})}(g)\Big\|_2^{2^{-\ell}}. \tag{16}$$

Note that, by our assumption (4), if $H\subset SL_2(p)$ is a proper subgroup and $g\in SL_2(p)$,

$$\nu(gH)<|S|^{-\varepsilon}. \tag{17}$$

It follows from (16) that if (6) fails, then

$$|A|^{\frac12-2^\ell\delta}<\Big\|\sum(1_A\circ\tau_g)\nu^{(2^{\ell-1})}(g)\Big\|_2 \tag{18}$$

and hence

$$|A|^{1-2^{\ell+1}\delta}<\sum_{x\in\mathbb{F}_p,\,g\in SL_2(p)}1_A(\tau_gx)1_A(x)\nu^{(2^\ell)}(g). \tag{19}$$

We distinguish two cases.

If $|A|>p^{\frac{1}{10}}$, then, by (3), $|S|>p^{\frac{1}{10r}}$ and, applying (15) with $K=p^{\frac{\varepsilon}{10r}}$ gives $|\nu^{(2^\ell)}\|_\infty<2p^{-3}$ for some $\ell=\ell(\varepsilon,r)$. Hence, from (19), $|A|^{1-2^{\ell+1}\delta}<2p^{-1}|A|^2$, contradicting (2) for δ small enough.

If $|A|\leqslant p^{\frac{1}{10}}$, denote $\nu_1=\nu^{(2^\ell)}$ and write using (19) and Hölder

$$\sum_g\Big[\sum_{x_1,x_2,x_3\in A}1_A(\tau_gx_1)1_A(\tau_gx_2)1_A(\tau_gx_3)\Big]\nu_1(g)>|A|^{3-32^{\ell+1}\delta}. \tag{20}$$

Assuming $2^\ell\delta<\frac{1}{10}$, it follows from (20) that there are distinct elements $x_1,x_2,x_3\in A$ such that

$$\nu_1\big[g\in SL_2(p);\ \tau_gx_i\in A\text{ for }i=1,2,3\big]>\frac12|A|^{-32^{\ell+1}\delta}. \tag{21}$$

Since the equations $\tau_gx_i=y_i$ $(i=1,2,3)$ determine g up to bounded multiplicity, (21) implies $\|\nu_1\|_\infty|A|^3>c|A|^{-32^{\ell+1}\delta}$. Since by (14), applied with $K=|A|^{\frac{\varepsilon}{r}}$, $\|\nu_1\|_\infty\leqslant 2|A|^{-2c(\ell-1)\frac{\varepsilon}{r}}+p^{-2}$, it follows

$$|A|^{3-2c(\ell-1)\frac{\varepsilon}{r}}+|A|^3p^{-2}>c|A|^{-32^{\ell+1}\delta}. \tag{22}$$

Taking $\ell=\ell(\varepsilon,r)$ appropriately and δ small enough gives again a contradiction.

4. Proof of Proposition 2

We may assume that $\det \Phi(t) \in \mathbb{F}_p$ is a quadratic residue (otherwise replace Φ by $\Phi(t_0)\Phi$ with $\det \Phi(t_0) \neq 0$). We can also assume that $\det \Phi(t) \neq 0$ for $t \in L$. Apply Proposition 1 to

$$S = \{\sigma(t)\Phi(t);\ t \in L\} \subset SL_2(p) \tag{23}$$

where $\sigma(t) \in \mathbb{F}_p^*$ is chosen such that $\sigma(t)^2 \det \Phi(t) = 1$. It remains to verify condition (4). From our assumption on Φ,

$$\mathbb{F}_p^* . \langle \Phi(t_1)^{-1}\Phi(t_2);\ \det \Phi(t_1) \neq 0,\ \det \Phi(t_2) \neq 0 \rangle = GL_2(p). \tag{24}$$

Using the bicommutator characterization of large proper subgroups of $SL_2(p)$, (24) implies that also

$$\mathbb{F}_p^* \langle \Phi(t_1)^{-1}\Phi(t_2);\ t_1, t_2 \in L_1 \rangle = GL_2(p) \tag{25}$$

for any sufficiently large subsets L_1 of L. Hence

$$\{\sigma(t)\Phi(t);\ t \in L_1\}$$

is not contained in a coset of a proper $SL_2(p)$-subgroup.

References

[1] J. Bourgain, More on the sum-product phenomenon in prime fields and its applications, Int. J. Number Theory 1 (1) (2005) 1–32.
[2] J. Bourgain, A. Gamburd, Uniform expansion bounds for Cayley graphs of $SL_2(\mathbb{F}_p)$, Annals of Math. 167 (2008) 625–642.
[3] J. Bourgain, N. Katz, T. Tao, A sum-product estimate in finite fields and applications, GAFA 14 (2004) 27–57.
[4] H. Helfgott, Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$, Annals of Math. 167 (2) (2008) 601–623.
[5] H. Helfgott, M. Rudnev, An explicit incidence theorem in $\mathbb{F}_p$, arXiv:1001.1980v2.
[6] P. Sarnak, X. Xue, Bounds for multiplicities of automorphic representations, Duke Math. J. 64 (1991) 207–227.