Thin groups and superstrong approximation
MSRI Publications
Volume **61**, 2013

Some Diophantine applications of the theory of group expansion

JEAN BOURGAIN

1. Introduction

The recent years have seen considerable progress in the theory of expansion and spectral gaps for so-called thin groups (as opposed to the classical theory of arithmetic groups.) These developments rely in part on methods and results from the rather novel research area of "arithmetic combinatorics" and underlying are general principles such as the "sum-product theorem" in finite fields and "product theorems" in linear groups. These advances turned out to be of interest well beyond group theory and have applications to geometry, number theory, theoretical computer science and even mathematical physics. At this point, many aspects of the extensive story were already accounted for in several survey papers, such as [Bourgain 2010], the Bourbaki exposé of E. Kowalski [2012] and those of B. Green [2009] and A. Lubotzky [2012] based on AMS lectures. A discussion of the "ubiquity" of thin groups from a broader perspective appears in [Sarnak 2014] in the present volume.

We will focus here on two specific number-theoretic applications. The first relates to integral Apollonian circle packings (ACP for short) and the problem of a local/global principle for the curvatures, as proposed in [Graham et al. 2003] and [Sarnak 2011]. The other concerns progress towards Zaremba's conjecture [1972] on continued fraction expansions of rationals and we will briefly review the paper [Bourgain and Kontorovich 2011]. Another exciting application of the theory of group expansion to finiteness in arithmetic geometry may be found in the work of J. Ellenberg, C. Hall and E. Kowalski [Ellenberg et al. 2012] but will not be discussed here. Neither will we get into the role of expansion to sieving theory (originating from [Bourgain et al. 2010a]) which triggered many of the later developments.

Our reference list is far from complete and strictly serves this exposé.

2. Background on expansion in Cayley graphs induced by thin groups

We start by recalling the notion of graph expansion and expander families. The reader is referred to the excellent survey paper [Hoory et al. 2006] for a detailed

discussion of this theory. Let $\mathcal{G}$ be a k-regular graph on a finite vertex set V, with $|V| = n$. Here one should see k as fixed whereas $n \to \infty$. The Busemann–Cheeger constant is then defined as

$$h(\mathcal{G}) = \min_{|S| \le n/2} \frac{|\partial S|}{|S|}, \tag{2-1}$$

where the minimum is taken over all subsets S of V and ∂S refers to the set of edges from S to $V \setminus S$. Having fixed k, a collection of k-regular graphs $\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3, \ldots$ on vertex sets $V_1, V_2, V_3, \ldots$ with $|V_i| \to \infty$ is called an expander family provided

$$h(\mathcal{G}_i) > c \quad \text{for all } i, \tag{2-2}$$

for some $c > 0$.

Expansion has a well-known spectral interpretation on the level of the adjacency matrix $A(\mathcal{G})$ of $\mathcal{G}$, defined by

$$A_{i,j} = \begin{cases} 1 \text{ if } (i,j) \in \mathcal{G}, \\ 0 \text{ otherwise.} \end{cases} \tag{2-3}$$

Since $\mathcal{G}$ is undirected, A is symmetric and $k = \lambda_0 \ge \lambda_1 \ge \cdots \ge \lambda_{n-1}$ since we assumed $\mathcal{G}$ k-regular. The following inequalities relate then the Cheeger constant to the "spectral gap" $\lambda_0 - \lambda_1$

$$\tfrac{1}{2}(k - \lambda_1) \le h(\mathcal{G}) \le \sqrt{2k(k - \lambda_1)}. \tag{2-4}$$

Do expander families exist? It was proven by Pinsker [1973] that given $k \ge 3$, a random (= typical) k-regular graph on n vertices ($n \to \infty$) is an expander graph. Around the same time, Margulis [1973] came up with explicit constructions based on Cayley graphs of groups. Recall that if $V = \langle S \rangle$ is a group generated by a finite set S of elements, the Cayley graphs $\mathcal{G}(V, S)$ consists of the edges $(x, y), x, y \in V$, for which $xy^{-1} \in S \cup S^{-1}$. Of particular importance to our discussion is Selberg's theorem on the congruence graphs induced by $\mathrm{SL}_2(\mathbb{Z})$.

Theorem 1. *Assume $\langle S \rangle$ a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and denote by $\pi_q : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(q)$ the $(\mathrm{mod}\, q)$ reduction. There is an integer q_0 such that the family of Cayley graphs*

$$\mathcal{G}\big(\mathrm{SL}_2(q), \pi_q(S)\big), \quad \textit{where } q \in \mathbb{Z}_+,\ (q, q_0) = 1, \tag{2-5}$$

is an expander family.

The assumption that $\langle S \rangle$ is of finite index is quite restrictive. What happens with "thin" subgroups? Recall that if G is an algebraic group, a subgroup $\Gamma \subset G(\mathbb{Z})$ is called "thin" provided $[G(\mathbb{Z}) : \Gamma] = \infty$. Assuming $\langle S \rangle \subset \mathrm{SL}_2(\mathbb{Z})$ contains the free group F_2 on 2 generators (equivalently, $\langle S \rangle$ is nonelementary

meaning that $\langle S\rangle$ does not contain a solvable subgroup of finite index), the Zariski closure of $\langle S\rangle$ equals SL_2. Citing the strong approximation property due to Matthews, Vaserstein, and Weisfeiler [1984], recall that if Γ is a subgroup of $\mathrm{SL}_d(\mathbb{Z})$ which is Zariski dense in SL_d, there is some $q_0 \in \mathbb{Z}_+$ such that $\pi_q(\Gamma) = \mathrm{SL}_d(\mathbb{Z}/q\mathbb{Z})$ for $(q, q_0) = 1$. Thus, if $\langle S\rangle \subset \mathrm{SL}_2(\mathbb{Z})$ is nonelementary, the Cayley graphs $\mathcal{G}\big(\mathrm{SL}_2(q), \pi_q(S)\big)$ for $q \in \mathbb{Z}_+$, $(q, q_0) = 1$ are connected. Moreover Theorem 1 generalizes.

Theorem 2. *Assume $\langle S\rangle$ a nonelementary subgroup of $\mathrm{SL}_2(\mathbb{Z})$. There is $q_0 \in \mathbb{Z}$ such that $\mathcal{G}\big(\mathrm{SL}_2(q), \pi_q(S)\big)$, $(q, q_0) = 1$, forms an expander family.*

Under the assumption that the limit set of $\Gamma = \langle S\rangle$ has dimension $\delta_\Gamma > \frac{5}{6}$, Theorem 2 is due to A. Gamburd [2002]. His result left unanswered Lubotzky's 1-2-3 problem [1994] (a folklore question in the subject), noting that Selberg's theorem applies to

$$S_1 = \left\{\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\right\} \quad \text{and} \quad S_2 = \left\{\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}\right\},$$

but not to

$$S_3 = \left\{\begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 3 & 1\end{pmatrix}\right\}.$$

The latter case was settled in [Bourgain and Gamburd 2008], which implies Theorem 2 for q prime. A crucial ingredient is Helfgott's product theorem in $\mathrm{SL}_2(p)$ [Helfgott 2008]. Theorem 2 for q square free was proven in [Bourgain et al. 2010a], motivated by applications to prime number sieving, and the case of unrestricted modulus follows from [Bourgain and Varjú 2012]. Meanwhile, based on deep work due to Helfgott [2011], Green, Breuillard, and Tao [2011] and Pyber and Szabó [2010] on the combinatorial side, Theorem 2 has been vastly generalized, at least for prime and square-free moduli (see [Varjú 2012; Salehi Golsefidy and Varjú 2012]). Although the work described later in this exposé is SL_2-based ($\mathrm{SL}_2(\mathbb{Z})$ and the Gauss-integer extension $\mathrm{SL}_2(\mathbb{Z}+i\mathbb{Z})\big)$, we record one of the most general results obtained in this context.

Theorem 3 [Salehi Golsefidy and Varjú 2012]. *Let k be a number field and $\Gamma \subset \mathrm{SL}_d(k)$, $\Gamma = \langle S\rangle$ with S a finite symmetric set. Assume the Zariski-closure of Γ is semisimple. Then the Cayley graphs $\mathcal{G}(\pi_q(\Gamma), \pi_q(S))$ form a family of expanders when q ranges over square-free ideals of the integers $\mathbb{O}$ of k with large prime factors.*

Returning to Lubotzky's problem, let us also mention the Lubotzky–Weiss conjecture, stating that expansion in $\mathrm{SL}_2(p)$ or, more generally, $\mathrm{SL}_n(p)$-Cayley graphs, is in fact a group property:

Conjecture 4. *There is an absolute constant $c = c_k > 0$ such that*

$$h\big(\mathcal{G}(\mathrm{SL}_2(p), S)\big) > c, \tag{2-6}$$

whenever $S \subset \mathrm{SL}_2(p), |S| = k$, is generating and p prime.

A positive answer would be conceptually very pleasing.

Evidence of its truth is the result of Breuillard and Gamburd [2010] establishing the conjecture for p outside a small exceptional set of the primes. Lubotzky–Weiss' problem will not be essential in our subsequent discussion as the Cayley graphs will be induced by a fixed set of elements in $\mathrm{SL}_2(\mathbb{Z})$ or $\mathrm{SL}_2(\mathbb{Z}+i\mathbb{Z})$. On the other hand, what is essential for us is to have unrestricted modulus q.

3. Hyperbolic lattice point counting

The spectral gap in congruence Cayley graphs described above in conjunction with Brun's combinatorial sieve, have been used to carry out prime and pseudo-prime sieving in the orbits of thin groups (see [Bourgain et al. 2010a; Sarnak 2008; Salehi Golsefidy and Sarnak 2011] for the ultimate generalization of this theory.) The "balls" involved in the sieving process are defined in terms of the word metric on the generators.

Other number-theoretic applications as presented in the next sections are based on different analytical tools (more specifically, the Hardy–Littlewood circle method) and require precise counting in Archimedean balls in the congruence subgroups. Such information may be obtained by hyperbolic lattice point counting and we briefly review the results for thin groups obtained in [Bourgain et al. 2011]. See the same paper also for related references.

Denote by $\mathbb{H} = \mathbb{H}^2 = \{x + iy \in \mathbb{C} : y > 0\}$ the hyperbolic plane on which $\mathrm{SL}_2(\mathbb{R})$ acts by Moebius transformation

$$gz = \frac{az+b}{cz+d}, \quad \text{where } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}). \tag{3-1}$$

Note that the theory discussed below has a counterpart for $\mathbb{H}^3$ and the action of $\mathrm{SL}_2(\mathbb{C})$, which is relevant for the application to the Apollonian group discussed in the next section. With g as in (3-1), we have

$$\|g\|^2 = a^2 + b^2 + c^2 + d^2 = 4u(gi, i) + 2, \tag{3-2}$$

where

$$u(z, w) = \frac{|z-w|^2}{4 \operatorname{Im} z \operatorname{Im} w} \quad \text{and} \quad \cosh d_{\mathbb{H}}(z, w) = 1 + 2u(z, w).$$

This clarifies the significance of hyperbolic space to the Archimedean counting problem.

Next, let Γ be a finitely generated subgroup of $\mathrm{SL}_2(\mathbb{Z})$, $L = L(\Gamma) \subset \mathbb{R}$ its limit set and $\delta = \delta_\Gamma$ the Hausdorff dimension of L. The assumption that Γ is nonelementary is equivalent to $0 < \delta \leq 1$. Thus our goal is Archimedean counting in the orbits of Γ and its congruence subgroups. We distinguish two cases.

• $\delta > \frac{1}{2}$: In this case, the hyperbolic surface $\mathbb{H}/\Gamma$ (which has infinite volume if $\delta < 1$) has an L^2-spectral theory and we rely on Lax–Phillips' theory based on automorphic methods and the wave equation.

• $\delta > 0$: If $0 < \delta \leq \frac{1}{2}$, there is no L^2-spectral theory and instead we use the thermodynamical approach based on symbolic dynamics and Ruelle's transfer operator, as developed by Lalley, Dolgopyat, Naud and others. This method is quite flexible and applies also in the semigroup setting (relevant in the application to Zaremba's problem in Section 5.)

We first discuss the spectral approach, assuming $\delta(L) > \frac{1}{2}$. The spectrum

$$0 \leq \lambda_0 < \lambda_1 \leq \cdots \leq \lambda_{\max} < \tfrac{1}{4} \quad \xrightarrow{\text{continuous spectrum}} \tag{3-3}$$

of the Laplace operator on $\mathbb{H}/\Gamma$ has lowest eigenvalue $\lambda_0 = \delta(1-\delta)$ and $\lambda_1 > \lambda_0$. Defining δ_j by $\lambda_j = \delta_j(1-\delta_j)$ and denoting by $\{\varphi_j\}$ the corresponding eigenfunctions, we state the theorem of Lax and Phillips [1982].

Theorem 5. *With the above notation, one has for $w_0, w \in \mathbb{H}$*

$$\big|\{\gamma \in \Gamma : d_{\mathbb{H}}(w, \gamma w_0) \leq s\}\big| = \sum_{j \geq 0} C_j \varphi_j(w)\varphi_j(w_0) e^{\delta_j s} + O\big(e^{\frac{1}{3}(1+\delta_0)s}\big). \tag{3-4}$$

What happens in congruence subgroups $\Gamma(q) = \big\{\gamma \in \Gamma : \gamma = \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right) (\mathrm{mod}\, q)\big\}$?

Considering the spectrum of $\mathbb{H}/\Gamma(q)$, it is an elementary fact that $\lambda_0(\Gamma(q)) = \lambda_0(\Gamma)$ and the issue is a uniform gap $\lambda_1(\Gamma(q)) - \lambda_0$ when q varies. When $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Selberg proved that $\lambda_1(\Gamma(q)) \geq \frac{3}{16}$ and conjectured $\lambda_1(\Gamma(q)) \geq \frac{1}{4}$ (no exceptional eigenvalues). The current record seems to be

$$\lambda_1(\Gamma(q)) > \tfrac{1}{4} - \big(\tfrac{7}{64}\big)^2,$$

due to Kim and Sarnak [1995].

Returning to thin groups $\Gamma = \langle S \rangle$ with $\delta_\Gamma > \frac{1}{2}$, one has the following extension of Selberg's result.

Theorem 6. *There is $\varepsilon = \varepsilon(\Gamma) > 0$ such that $\lambda_1(\Gamma(q)) > \lambda_0 + \varepsilon$ for all $q \in \mathbb{Z}_+$.*

The proof relies essentially on the expander family $\mathcal{G}\big(\mathrm{SL}_2(q), \pi_q(S)\big)$ and the conversion of the combinatorial spectral gap to a geometric one follows arguments due to Burger and Brooks in the finite volume case.

Combining Theorem 5 and Theorem 6 leads to the following Archimedean-modular distributional property.

Corollary 7. *Let* $\Gamma = \langle S \rangle \subset \mathrm{SL}_2(\mathbb{Z})$, *and* $\delta_\Gamma > \frac{1}{2}$. *There is some* $q_0 = q_0(\Gamma) \in \mathbb{Z}$ *such that, if* $(q, q_0) = 1$ *and* $g \in \mathrm{SL}_2(q)$,

$$\left|\{\gamma \in \Gamma : \|\gamma\| \leq N \text{ and } \pi_q(\gamma) = g\}\right| = \frac{cN^{2\delta}}{|\mathrm{SL}_2(q)|} + O(q^C N^{2\delta-\varepsilon}), \quad (3\text{-}5)$$

where ε, c *and* C *only depend on* Γ.

This type of result plays a key role in the diophantine applications discussed in the next sections of this exposé. A similar (though slightly weaker) statement may be obtained in the general case $\delta_\Gamma > 0$ following the thermodynamical approach which we review next.

Assuming $\Gamma = \langle T_1, \ldots, T_k \rangle \subset \mathrm{SL}_2(\mathbb{Z})$ has no parabolic elements, one identifies Γ with the set Σ_* of finite sequences on the alphabet $\{\pm 1, \ldots, \pm k\}$ compatible with a transition matrix and the limit set $L(\Gamma)$ with the corresponding set Σ of infinite sequences. The Nielsen map $F : L \to L$ corresponds to a finite type shift $\sigma : \Sigma \to \Sigma$ under the symbolic conversion and the distortion function $f = \log |F'|$ is expressed by $\tau(x) = d_{\mathbb{H}}(i, xi) - d_{\mathbb{H}}(i, x_2 x_3 \ldots i)$ for $x = (x_1, x_2, \ldots) \in \Sigma$. Taking $0 < \rho < 1$, we define a metric on Σ by

$$d(x, y) = \rho^m, \quad \text{with } m = \max\{j : x_j = y_j\}, \quad (3\text{-}6)$$

and denote by $\mathscr{F}$ the corresponding space of Hölder functions f, i.e., those satisfying

$$|f(x) - f(y)| \leq K d(x, y) \quad \text{for some } K > 0. \quad (3\text{-}7)$$

Given a function $f \in \mathscr{F}$, define the transfer operator $\mathscr{L}_f : \mathscr{F} \to \mathscr{F}$ by

$$(\mathscr{L}_f g)(x) = \sum_{\sigma(y) = x} e^{f(y)} g(y). \quad (3\text{-}8)$$

Recall Ruelle's theorem to the effect that for $f \in \mathscr{F}$ real, there is a simple largest eigenvalue $\lambda_f > 0$ of $\mathscr{L}_f$ with strictly positive eigenfunction h_f and a Borel probability measure ν_f on Σ satisfying

$$\mathscr{L}^* \nu = \lambda \nu \quad \text{and} \quad \int h \, d\nu = 1.$$

Denote by $P(f) = \log \lambda_f$ the pressure function. Taking $f = -s\tau$ with τ as above, $P(-s\tau)$ is strictly increasing in $s \in \mathbb{R}$ and, according to a result due to Patterson and Sullivan, vanishes at $s = \delta = \dim L(\Gamma)$.

The renewal approach to the counting problem consists in introducing a counting function

$$N_\phi(T, x) = \sum_{n=0}^{\infty} \sum_{\sigma^n y = x} \phi(y) 1_{\{S_n \tau(y) \leq T\}}, \quad (3\text{-}9)$$

where

$$S_n f = f + (f \circ \sigma) + \cdots + (f \circ \sigma^{n-1}). \tag{3-10}$$

Thus in particular, for x the identity and $\phi = 1$, we obtain the number of elements of Γ for which $d_{\mathbb{H}}(\gamma i, i) \le T$.

The counting function satisfies the renewal equation

$$N_\phi(T, x) = \phi(x) 1_{\{T \ge 0\}} + \sum_{\sigma(y)=x} N_\phi(T - \tau(y), y). \tag{3-11}$$

Introducing its Laplace transform

$$F(s, x) = \int_{-\infty}^{\infty} e^{-sT} N(T, x)\, dT \quad (\operatorname{Re} s \gg 1), \tag{3-12}$$

(3-11) is converted to

$$F(s, x) = -\mathcal{R}_s \frac{\phi(x)}{s}, \tag{3-13}$$

where $\mathcal{R}_s = (I - \mathcal{L}_{-s\tau})^{-1}$ is the resolvent and is analytic for $\operatorname{Re} s > \delta$. The following statement results from the work of Lalley and Naud (based on work of Dolgopyat).

Theorem 8. (i) *$\mathcal{R}_s$ has a meromorphic extension to a strip* $\operatorname{Res} > \delta - \varepsilon$ *with a simple pole at $s = \delta$.*

(ii) $\|\mathcal{R}_s\| < C(1 + |\operatorname{Im} s|^2)$ *for* $|s| \to \infty$.

(iii) $|\{\gamma \in \Gamma : d_{\mathbb{H}}(i, \gamma i) \le s\}| = Ce^{\delta s} + O(e^{(\delta-\varepsilon)s})$.

Statement (iii) follows from (i) and (ii) by standard Tauberian arguments (see [Bourgain et al. 2011] for details) and a widening of the analyticity region leads to improved error terms in the counting.

The next step consists in extending this theory in order to capture congruence subgroups $\Gamma(q)$ of Γ with uniformity in q.

Replace Σ by $\Sigma \times \mathrm{SL}_2(q)$ and $\mathcal{F}$ by the space $\mathcal{F}_q = \mathcal{F}\big(\Sigma \times \mathrm{SL}_2(q)\big)$ of vector-valued Hölder functions f on Σ with norm

$$\|f\|_\rho = \|f\|_\infty + |f|_\rho,$$

where

$$\|f\|_\infty = \max_x \bigg(\sum_{g \in \mathrm{SL}_2(q)} |f(x, g)|^2 \bigg)^{\frac{1}{2}} \tag{3-14}$$

and

$$|f|_\rho = \max_m \frac{\operatorname{Var}_m f}{\rho^m}, \tag{3-15}$$

with

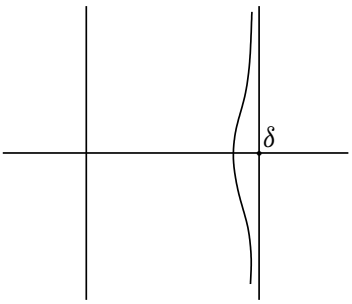
$$\mathrm{Var}_m\, f = \sup\left\{\Big(\sum_{g\in \mathrm{SL}_2(q)} |f(x,g)-f(y,g)|^2\Big)^{\frac{1}{2}} : x_j = y_j \text{ for } j\le m\right\} \quad (3\text{-}16)$$

On the extended space $\mathscr{F}_q$, introduce the transfer operator as

$$(\mathscr{L}_{-s\tau} f)(x,g) = \sum_{\sigma(y)=x} e^{s\tau(y)} f(y, yx^{-1}g). \quad (3\text{-}17)$$

The resonance-free region obtained in [Bourgain et al. 2011] is of the form

$$\mathrm{Re}\, s > \delta - \frac{c}{\log(2+|\mathrm{Im}\, s|)}, \quad (3\text{-}18)$$



where (3-18) is uniform in q. The proof makes again essential use of the expansion in $\Gamma/\Gamma(q)$. Using (3-18), following analogue of Corollary 7 is deduced.

Theorem 9. *There is* $q_0 = q_0(\Gamma) \in \mathbb{Z}$ *such that for* $(q, q_0) = 1$ *and* $g \in \mathrm{SL}_2(q)$

$$\big|\{\gamma \in \Gamma : \|\gamma\| \le N \text{ and } \pi_q(\gamma) = g\}\big| = \frac{cN^{2\delta}}{|\mathrm{SL}_2(q)|}\big(1 + O(N^{-1/\log\log N})\big) + O(q^C N^{2\delta-\varepsilon}). \quad (3\text{-}19)$$

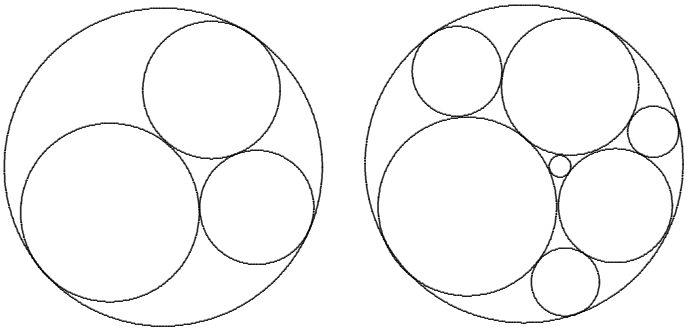
Compared with Corollary 7, the error term is a bit worse, but the term in $O\big(N^{-1/\log\log N}\big)$ may be further reduced (and even removed) if $1_{[\|\gamma\|\le N]}$ is replaced by a suitable weighted average.

In both Corollary 7 and Theorem 9, one may moreover specify the expanding direction v_+ of g to be in a sector I, with the effect of introducing a factor $\mu(I)$ in the main term, where μ is the Sullivan–Patterson measure.

4. Integral Apollonian circle packings

For background, see [Graham et al. 2003; Sarnak 2011]. Recall Apollonius' theorem: Given three mutually tangent circles in the plane, there are exactly two circles tangent to all three. Starting from four mutually tangent circles as

depicted below and filling in repeatedly the lacunae with tangent circles leads to so-called Apollonian circle packings (ACPs):



It was observed by F. Soddy that if the curvatures of the initial four circles — known as the *root quadruple* — are integers, all circles in the packing will have integral curvature, leading to integral ACPs. An example is shown in Figure 1.

This phenomenon may be explained by considering the Descartes quadratic form

$$F(x_1, x_2, x_3, x_4) = 2(x_1^2 + x_2^2 + x_3^2 + x_4^2) - (x_1 + x_2 + x_3 + x_4)^2, \quad (4\text{-}1)$$

since $F(x_1, x_2, x_3, x_4) = 0$ is tantamount to x_1, x_2, x_3, x_4 being curvatures of four mutually tangent circles.

Which integers are produced in a given integral ACP? That is the general question proposed in [Graham et al. 2003] and [Sarnak 2011], where the following conjectures were formulated.

(A) *The positive density conjecture*: the set of curvatures in any integral ACP is of positive density in $\mathbb{Z}$.

(B) *Local to global principle*: all integers are produced, up to a finite congruence condition.

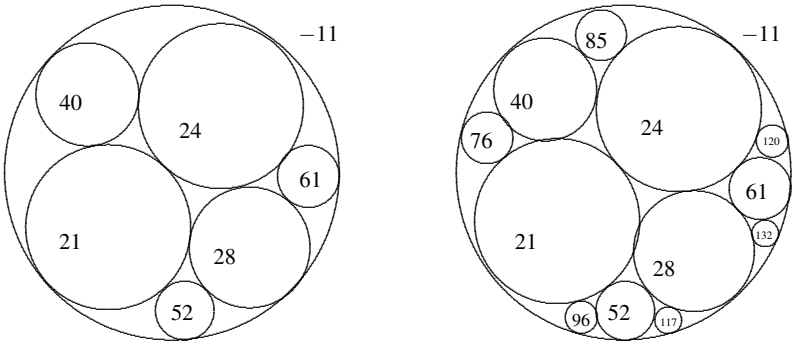


Figure 1. Packing $\mathcal{P}_0$ with root quadruple $(-11, 21, 24, 28)$.

Obviously (B) implies (A).

It turns out that the curvatures in a given integral ACP with root quadruple (a, b, c, d) are obtained as the orbit of a group, the so called Apollonian packing group A, which is the subgroup of the orthogonal group $\mathbb{O}_F$ associated to (4-1), generated by the matrices

$$S_1 = \begin{bmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad S_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$S_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 2 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad S_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & -1 \end{bmatrix}.$$

A first important feature of A is that, under the spin double cover, it identifies with a finitely generated subgroup Γ of $\mathrm{SL}_2(\mathbb{Z}+i\mathbb{Z})$ to which the spectral method discussed in the previous section apply. More specifically considering the action on $\mathbb{H}^3$, the limit set L has dimension

$$\delta = \delta_\Gamma = 1.30568\ldots, \tag{4-2}$$

and Lax–Phillips theory is applicable. Denoting $a(C)$ the curvature of the circle C, for any packing $\mathcal{P}$ the Poincaré series

$$\sum_{C \in \mathcal{P}} a(C)^{-s} \tag{4-3}$$

has exponent of convergence equal to δ, which is the dimension of the residual set of the packing $\mathcal{P}$ (and is independent of $\mathcal{P}$).

The other feature of A are its arithmetic subgroups $\langle S_1, S_2, S_3\rangle$, $\langle S_2, S_3, S_4\rangle$, $\langle S_3, S_4, S_1\rangle$, $\langle S_4, S_1, S_2\rangle$, isomorphic to a finite index subgroup of $SO(2,1)(\mathbb{Z})$, and which orbits may be described by binary quadratic forms. Both spectral and arithmetical aspects are important in understanding the properties of the sets of curvatures.

Let

$$N_{\mathcal{P}}(T) = \#\{C \in \mathcal{P} : a(C) \le T\}, \tag{4-4}$$

be the number of curvatures at most T in the packing $\mathcal{P}$, counted with multiplicity. The exact asymptotic is provided by the following result, which is and based on spectral methods.

Theorem 10 [Kontorovich and Oh 2011]. *$N_{\mathcal{P}}(T) \sim bT^\delta$ as $T \to \infty$, where $b = b(\mathcal{P})$.*

For instance, Fuchs and Sanden showed that $b(\mathcal{P}_0) = 0.0458\ldots$.

Assuming $\mathcal{P}$ primitive, that is, $(a, b, c, d) = 1$, denote further by $\pi^{\mathcal{P}}(T)$ the number of prime circles in $\mathcal{P}$ of curvature at most T and by $\pi_2^{\mathcal{P}}(T)$ the number of twin (= tangent) prime circles.

Theorem 11 [Kontorovich and Oh 2011].

$$\pi^{\mathcal{P}}(T) \ll \frac{T^\delta}{\log T} \quad \textit{and} \quad \pi_2^{\mathcal{P}}(T) \ll \frac{T^\delta}{(\log T)^2} \textit{ as } T \to \infty. \tag{4-5}$$

Lower bounds of the same order but for "pseudoprime circles" hold. This is a result in similar vein as [Bourgain et al. 2010a; Bourgain et al. 2011], based on sieving methods combined with a spectral input.

Let us now return to the diophantine aspects and conjectures (A) and (B).

Theorem 12 [Fuchs 2010; Fuchs and Sanders 2010]. *Determination of* $\pi_q(A) \subset \mathrm{GL}_4(\mathbb{Z}/q\mathbb{Z})$ *for every* q: *The ramified set consists only of the primes* 2 *and* 3.

Theorem 13 [Bourgain and Fuchs 2011]. *The positive density conjecture holds.*

Theorem 14 [Bourgain and Kontorovich 2012]. *The local/global principle holds up to an exceptional set of size at most* $T^{1-\varepsilon}$, *for some* $\varepsilon > 0$.

As an example, consider the packing $\mathcal{P}_0$ introduced above. The only congruence restrictions are

$$a(C) \in \{0, 4, 12, 13, 16, 21\} \pmod{24}, \tag{4-6}$$

and by Theorem 14

$$\#\big\{a < T : \pi_{24}(a) \in \{0, 4, 12, 13, 16, 21\} \text{ and } a \text{ is not a } \mathcal{P}_0\text{-curvature}\big\} < T^{1-\varepsilon}.$$

Initial results towards Theorem 13 were obtained by Sarnak [2011] and Fuchs [2010] and their work also introduced several of the methods needed to attack these questions.

Several ingredients are involved in the proof of Theorems 12, 13 and 14:

(i) representation of integers by binary quadratic forms;[1]

(ii) Lax–Phillips theory and spectral gap;

(iii) the Hardy–Littlewood circle method.

The use of binary quadratic forms may be briefly summarized as follows.

Fix $(a, b, c, d) \in \mathcal{P}$ and set

$$A = a + b \quad B = \tfrac{1}{2}(a + b - c + d) \quad C = a + d. \tag{4-7}$$

[1] As originally pointed out by Sarnak in a letter to Lagarias.

Consider the quadratic form

$$f(x, y) = Ax^2 + 2Bxy + Cy^2 \text{ with discriminant } D_f = 4(B^2 - AC) = -4a^2.$$

Then all integers represented by $f - a$ appear as curvatures of circles C in $\mathcal{P}$ that are tangent to the circle C_a with curvature a.

This observation, going back to Sarnak and Fuchs, leads to the question of understanding how many integers can be represented by a given quadratic form of large discriminant.

Theorem 15 [Blomer and Granville 2006; Bourgain and Fuchs 2012]. *Let*

$$f(x, y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[X, Y],$$

suppose $D = b^2 - 4ac < 0$ *and denote by* $U_f(M)$ *the number of integers not exceeding* M *that are representable by* f. *Assume further that*

$$\log |D| < O(\log \log M). \tag{4-8}$$

(i) *Assume*

$$|D| \ll (\log M)^{(\log 2)-\varepsilon}. \tag{4-9}$$

Then

$$U_f(M) \gg \frac{M}{(\log M)^{\frac{1}{2}+}}. \tag{4-10}$$

(ii) *Assuming* (4-9), f *represents all integers that are representable by the genus of* f, *up to an exceptional set of size at most* $M(\log M)^{-(1/2)-\varepsilon'}$.

(iii) *Assume*

$$|D| \gg (\log M)^{2(\log 2)+\varepsilon}. \tag{4-11}$$

Then

$$U_f(M) \asymp \frac{M}{\sqrt{|D|}}. \tag{4-12}$$

Statements (i) and (iii) appear in [Blomer and Granville 2006]. As explained there, the different behavior for small and large discriminant has to do with the interplay between the class group and the prime factorization of a typical integer $< M$ representable by the genus of f; the intermediate range being difficult to analyze. Statement (ii) is proven in [Bourgain and Fuchs 2012] and relies on a more general principle in combinatorial group theory.

It is worthwhile to point out that while the initial progress towards conjecture (A) exploits the range (4-9), the proof of Theorem 13 in [Bourgain and Fuchs 2012] uses the range (4-11). Combining part (ii) of Theorem 15 with Iwaniec's half-dimensional sieve [1972], [Friedlander and Iwaniec 2010] gives the following refinement of a result in [Sarnak 2011].

Theorem 16 [Bourgain and Fuchs 2012]. *Let C_a be a circle with curvature a in the packing $\mathcal{P}$ and assume*

$$a < (\log T)^{\frac{1}{2}\log 2-\varepsilon}. \tag{4-13}$$

There are at least $T(\log T)^{-(3/2)-\varepsilon}$ prime circles C in $\mathcal{P}$ with $a(C) < T$ that are tangent to C_a.

In order to discuss Theorem 14, which combines all three ingredients, we need to recall the basics around the circle method. This discussion is also relevant to the next section.

Let λ be a (probability) distribution on $\{1, 2, \dots, N\}$, that we expect to be roughly equidistributed and set

$$R = \operatorname{supp}\lambda = \{n : \lambda(n) > 0\}. \tag{4-14}$$

In order to estimate $N - |R|$, introduce the exponential sum

$$S(\theta) = \sum_1^N \lambda(n)e(n\theta), \quad \theta \in \mathbb{T} = \mathbb{R}/\mathbb{Z}, \tag{4-15}$$

so that

$$\lambda(n) = \hat{S}(n) = \int_0^1 S(\theta)e(-n\theta)\,d\theta.$$

Let $B = B(N)$ be a parameter and make a subdivision of $\mathbb{T}$ in major arcs

$$\mathcal{M} = \bigcup_{q<B} \bigcup_{(a,q)=1} \left[\frac{a}{q} - \frac{B}{N}, \frac{a}{q} + \frac{B}{N}\right] \tag{4-16}$$

and the minor arcs $\mathbb{T}\backslash\mathcal{M}$.

Define

$$\lambda_1(n) = \int_{\mathcal{M}} S(\theta)e(-n\theta)\,d\theta. \tag{4-17}$$

Assume that S is "small" on the minor arcs, in the sense that

$$\int_{\mathbb{T}\backslash\mathcal{M}} |S(\theta)|^2\,d\theta < \frac{\varepsilon(N)}{N}. \tag{4-18}$$

It follows then from Parseval that

$$\sum |\lambda(n) - \lambda_1(n)|^2 < \frac{\varepsilon(N)}{N}.$$

Assuming $\lambda_1(n) \sim 1/N$ for $n \in R_1 \subset \{1, \dots, N\}$, it follows that

$$N - |R| \le N - |R_1| + O(\varepsilon(N)N).$$

The goal is to have a precise description of $S(\theta)$ for $\theta \in \mathcal{M}$, leading to an arithmetical description of λ_1 of the form

$$\lambda_1(n) = \mathfrak{S}(n)\pi(n), \tag{4-19}$$

with

$$\mathfrak{S}(n) = \prod_p \mathfrak{S}_p(n) = \text{ the singular series}, \tag{4-20}$$

$$\pi(n) = \text{ singular integral} \sim \frac{1}{N}. \tag{4-21}$$

In order to achieve this, $B(N)$ will have to be taken sufficiently small. On the other hand, the larger $B(N)$, the smaller $\varepsilon(N)$ will be.

Since λ_1 satisfies the local to global principle, so will R, up to an exceptional set.

Returning to ACPs, let $\mathcal{P}$ be the primitive packing obtained from the root quadruple $v = (a, b, c, d)$. The goal is to introduce an appropriate generating set of curvatures in $\mathcal{P}$. We proceed as follows.

Let $T = T_0 X^2$ with T_0 a small power of T. Define

$$B_{T_0} = \{\gamma \in A : \|\gamma\| \sim T_0\} \tag{4-22}$$

and

$$\xi_{x,y} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ * & * & * & * \\ * & * & * & * \\ 4x^2 + 2xy + y^2 - 1 & 4x^2 + 2xy & -2xy & 2xy + y^2 \end{pmatrix} \in \langle S_2, S_3, S_4 \rangle, \tag{4-23}$$

where $x, y \asymp X$, $(2x, y) = 1$. Hence

$$\langle \xi_{x,y} \gamma v, e_4 \rangle \in \mathcal{P}, \tag{4-24}$$

and produces the generating distribution. The corresponding exponential sum is given by

$$S_T(\theta) = \sum_{\gamma \in B_{T_0}} \sum_{\substack{x,y \asymp X \\ (2x,y)=1}} e\big(\langle \xi_{xy} \gamma v, e_4 \rangle \theta\big). \tag{4-25}$$

The estimates on the minor arcs exploits the arithmetical element ξ_{xy} and families of quadratic forms in x, y.

The major arcs analysis is based on precise Archimedean/modular distributional properties of B_{T_0} obtained from Lax–Phillips theory and congruence spectral gaps, as discussed in Section 3.

5. Partial quotients of rationals and Zaremba's conjecture

Use the standard notation $[a_1, \dots, a_k]$ for the continued fraction expansion

$$\cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \; + \cfrac{1}{a_k}}}$$

For given $A \in \mathbb{Z}_+$, define

$$\mathcal{R}_A = \left\{ \frac{b}{d} = [a_1, \dots, a_k] : 1 \le a_j \le A \text{ for all } j = 1, \dots, k \right\} \tag{5-1}$$

and let

$$\mathcal{D}_A = \left\{ d \in \mathbb{Z}_+ : \text{ there is } (b,d) = 1 \text{ with } \frac{b}{d} \in \mathcal{R}_A \right\} \tag{5-2}$$

the corresponding set of denominators.

Conjecture 1 [Zaremba 1966; 1972]. *For some sufficiently large A, we have*

$$\mathcal{D}_A = \mathbb{Z}_+.$$

In fact, $A = 5$ should suffice ($54 \notin \mathcal{D}_4$).

Conjecture 2 [Niederreiter 1978]. $\mathcal{D}_3$ *contains every sufficiently large integer.*

Conjecture 3 [Hensley 1996]. *Same statement for* $\mathcal{D}_2$.

Note that $\mathcal{R}_1 = \{f_n/f_{n+1}\}, \mathcal{D}_1 = \{f_n\}$ is the Fibonacci sequence.

Using an explicit construction, Niederreiter [1986] showed that $\{2^j\} \subset \mathcal{D}_3$ and similar results were established for other lacunary sequences.

Zaremba's interest in the problem comes from numerical integration, Monte Carlo methods and pseudo-random numbers.

Let us recall the notion of discrepancy. Let

$$X = \{x_j\}_{j \le N} \subset Q = [0,1]^s,$$

and define

$$D(X) = \max_{\substack{I \subset Q \\ \text{box}}} \left| |I| - \frac{1}{N} \#\{j \le N : x_j \in I\} \right|. \tag{5-3}$$

The significance of this notion is illustrated by results such as the Hlawka–Koksma inequality. Let f be a function of bounded variation on Q; thus

$$V = \max_{\alpha \subset \{1,\dots,s\}} \| \partial^{(\alpha)} f \|_{L^1(Q)} < \infty. \tag{5-4}$$

Then

$$\left|\int_Q f(x)\,dx - \frac{1}{N}\sum_{j=1}^{N} f(x_j)\right| \le C\,VD(X). \tag{5-5}$$

The problem is how to construct explicitly sequences with small discrepancy when $s \ge 2$. The following result addresses this question when $s = 2$.

Theorem 17 [Zaremba 1966; 1972]. *Take* $(b, d) = 1$ *with* $b/d \in \mathcal{R}_A$. *Let*

$$X = \left\{x_j = \left(\frac{j}{d}, \frac{bj}{d}\right) : 1 \le j \le d\right\}, \tag{5-6}$$

where bj/d *is reduced* (mod 1). *Then*

$$D(X) < \left(\frac{4A}{\log(A+1)} + \frac{4A+1}{\log d}\right)\frac{\log d}{d}. \tag{5-7}$$

Inequality (5-7) clarifies the role of the diophantine properties of b/d. One of the simplest pseudo-random number generators (PRNG) is the linear congruential

$$x \mapsto bx + c \ (\mathrm{mod}\, d), \tag{5-8}$$

where $(b, d) = 1$ and b primitive (mod d). Set $c = 0$ in (5-8). The quality of the corresponding PRNG depends in particular on the statistical properties of

$$X_1 = \left\{\frac{b^j}{d} (\mathrm{mod}\, 1) : 1 \le j \le d\right\} \tag{5-9}$$

and especially

$$X_2 = \left\{\left(\frac{b^j}{d}, \frac{b^{j+1}}{d}\right) (\mathrm{mod}\, 1) : 1 \le j \le d\right\} \tag{5-10}$$

(serial correlation of pairs). Note that $D(X_2)$ is essentially $D(X)$ with X defined in (5-6). Figure 2 on the next page shows two examples.

Returning to (5-7), apart from the prefactor depending on A, the discrepancy is essentially the optimal one, as implied by the following result due to W. Schmidt.

Theorem 18 [Schmidt 1972]. *Any sequence* $X = \{x_j\}_{1 \le j \le N}$ *in* $[0, 1]^2$ *satisfies*

$$D(X) > c\frac{\log N}{N}, \tag{5-11}$$

where c *is an absolute constant.*

Returning to Zaremba's conjecture, partial progress was achieved:

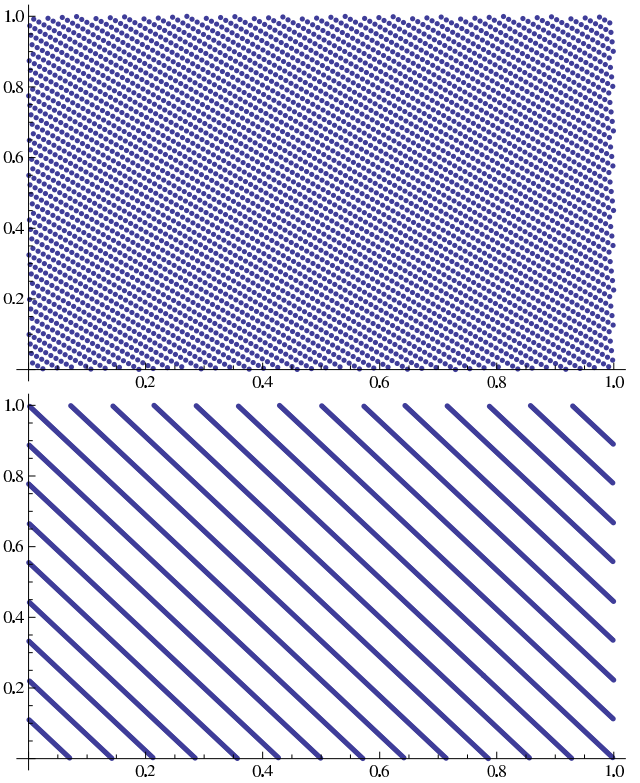


Figure 2. The set

$$\left\{\left(\frac{b^n}{d}, \frac{b^{n+1}}{d}\right) \bmod 1\right\}_{n=1}^{d},$$

where b/d equals $\frac{3523}{4547} = [1, 3, 2, 3, 1, 2, 3, 2, 1, 3]$ (top) and $\frac{3535}{4547} = [1, 3, 2, 35, 1, 1, 1, 4]$ (bottom).

Theorem 19 [Bourgain and Kontorovich 2011]. *For $A = 50$, $\mathscr{D}_A$ is of density* 1. *Quantitatively, setting*

$$\mathscr{D}_A(N) = \mathscr{D}_A \cap [1, N],$$

we have

$$|\mathscr{D}_A(N)| = N + 0\big(N^{1-\frac{c}{\log\log N}}\big). \tag{5-12}$$

Corollary 20 (linear congruential PRNG). *$\mathscr{R}_{51}$ contains infinitely many fractions b/d with d prime, so that the multiplier b is a primitive root* (mod d).

How to produce elements from $\mathscr{R}_A$? We note that

$$\frac{b}{d} = [a_1, \ldots, a_k]$$

is equivalent with

$$\begin{pmatrix} * & b \\ * & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & a_k \end{pmatrix}. \tag{5-13}$$

Hence we are considering the orbit of $e_2 \equiv (0,1)$ under the semigroup $\mathcal{G}_A \subset \mathrm{GL}_2(\mathbb{Z})$ generated by the matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}, \quad \text{with } 1 \le a \le A. \tag{5-14}$$

Clearly $\mathcal{O}_A = \mathcal{G}_A.e_2$ is in one-to-one correspondence with $\mathcal{G}_A$ and

$$\mathcal{D}_A = \langle \mathcal{G}_A.e_2, e_2 \rangle. \tag{5-15}$$

The proof of Theorem 19 is an adaptation of [Bourgain and Kontorovich 2010] with this difference that instead of a finitely generated subgroup $\Gamma \subset \mathrm{SL}_2\,\mathbb{Z})$ with δ_Γ close to 1, we are dealing with a semigroup. The role of large A should be explained. Set

$$\mathcal{C}_A = \left\{ [a_1, \ldots, a_j, \ldots] : a_j \le A \text{ for all } j \ge 1 \right\} \subset [0,1] \tag{5-16}$$

and let δ_A denote the Hausdorff dimension of $\mathcal{C}_A$.

Then

$$\mathcal{C}_1 = \left\{ \frac{1}{\varphi} \right\}, \quad \text{where } \varphi = \frac{1+\sqrt{5}}{2},$$

and $\mathcal{C}_2$ is a Cantor set, which dimension $\delta_2 = 0,5312805\ldots$ was calculated by Jenkinson and Pollicott [2001] up to high accuracy using the thermodynamical approach.

Theorem 21 [Hensley 1989; 1992]. *For large A,*

$$\delta_A = 1 - \frac{6}{\pi^2}\frac{1}{A} - \frac{72}{\pi^4}\frac{\log A}{A^2} + O\left(\frac{1}{A^2}\right). \tag{5-17}$$

Theorem 22 [Hensley 1989]. *Set*

$$\mathcal{R}_A(N) = \left\{ \frac{b}{d} \in \mathcal{R}_A : (b,d) = 1 \text{ and } 1 \le b < d < N \right\}. \tag{5-18}$$

Then

$$\#\mathcal{R}_A(N) \asymp N^{2\delta_A} \quad \text{for } N \to \infty. \tag{5-19}$$

This gives the complete analogy with the group setting with $\mathcal{C}_A$ and δ_A replacing $L(\Gamma)$ and δ_Γ.

Again, the diophantine analysis of the set $\mathcal{D}_A$, based on (5-15), is carried out using the circle method. Rather than considering balls $B_N = \{\gamma \in \mathcal{G}_A : \|\gamma\| \le N\}$, we introduce sets of the form

$$\Omega_N = B_{N_1} B_{N_2} \dots B_{N_\ell}, \tag{5-20}$$

where $N \sim N_1 N_2 \dots N_\ell$ and N_j suitably chosen. Considering the exponential sums

$$S_N(\theta) = \sum_{\gamma \in \Omega_N} e\big(\langle \gamma e_2, e_2\rangle \theta\big), \tag{5-21}$$

the interest of the multilinear structure (5-20) is to enable to carry out minor arcs estimates by means of general Vinogradov-type bilinear technology. This part of the analysis is completely similar to [Bourgain and Kontorovich 2010] and depends on having δ_A close enough to 1.

Again, the evaluation of $S_N(\theta)$ on major arcs depends on precise Archimedean/modular distributional properties of the balls $B_N \subset \mathcal{G}_A$. However, since $\mathcal{G}_A$ is only a semigroup, the Lax–Phillips automorphic approach (as used in [Bourgain and Kontorovich 2010] in the setting of [Bourgain et al. 2010b] and in [Bourgain and Kontorovich 2012] using [Vinogradov 2012]; see also [Mohammadi and Oh 2012]), is not applicable. Instead, we rely on the thermodynamical method and in particular Theorem 9.

It turns out that the error in (5-12) may be further reduced to N^{1-c} for some $c > 0$. This stronger statement has some additional interest in the context of some questions proposed to the author by R. Kenyon (private communication) and related to extensions of Hall's theorem on sums of continued fractions. M. Hall [1947] showed that every number in the interval $[\sqrt{2}-1, 4\sqrt{2}-4[$ is sum of two continued fractions whose partial quotients do not exceed four.

A natural problem would be to obtain a result of the flavor of Hall's theorem for the rational numbers. There are several possible formulations.

One could ask for instance if there is an absolute constant C such that given $b/q \in \mathbb{Q} \cap I$, I a suitable interval, there is a representation of b as a sum of at most C positive integers b_i such that each of the fractions b_i/q has its partial quotients bounded by C. Of course, if we require moreover that $(b, q) = 1$, Zaremba's conjecture ought to be proven first. While we are not able to contribute directly to this question, the methods from [Bourgain and Kontorovich 2011] permit to show the following.

Theorem 23 [Bourgain 2012]. *There is an absolute constant C such that any rational $b/q \in]0, 1[$, $(b, q) = 1$, admits a representation as a finite sum,*

$$\frac{b}{q} = \sum_\alpha \pm \frac{b_\alpha}{q_\alpha}, \quad (b_\alpha, q_\alpha) = 1, \tag{5-22}$$

such that

$$\sum_{\alpha} \sum_{i} a_i \left(\frac{b_\alpha}{q_\alpha} \right) \leq C \log q, \tag{5-23}$$

where $\{a_i(x)\}$ *stands for the sequence of partial quotients of* x.

Note that since $\sum_i a_i(b_\alpha/q_\alpha) \geq \log q_\alpha$, (5-23) is essentially optimal. As pointed out by Kenyon, a statement of this kind may be viewed as a measure of complexity of rationals of given height.

References

[Blomer and Granville 2006] V. Blomer and A. Granville, "Estimates for representation numbers of quadratic forms", *Duke Math. J.* **135**:2 (2006), 261–302.

[Bourgain 2010] J. Bourgain, "New developments in combinatorial number theory and applications", pp. 233–251 in *European Congress of Mathematics*, edited by A. Ran et al., Eur. Math. Soc., Zürich, 2010.

[Bourgain 2012] J. Bourgain, "Partial quotients and representation of rational numbers", *C. R. Math. Acad. Sci. Paris* **350**:15–16 (2012), 727–792.

[Bourgain and Fuchs 2011] J. Bourgain and E. Fuchs, "A proof of the positive density conjecture for integer Apollonian circle packings", *J. Amer. Math. Soc.* **24**:4 (2011), 945–967.

[Bourgain and Fuchs 2012] J. Bourgain and E. Fuchs, "On representation of integers by binary quadratic forms", *Int. Math. Res. Not.* **2012**:24 (2012), 5505–5553.

[Bourgain and Gamburd 2008] J. Bourgain and A. Gamburd, "Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$", *Ann. of Math.* (2) **167**:2 (2008), 625–642.

[Bourgain and Kontorovich 2010] J. Bourgain and A. Kontorovich, "On representations of integers in thin subgroups of $\mathrm{SL}_2(\mathbb{Z})$", *Geom. Funct. Anal.* **20**:5 (2010), 1144–1174.

[Bourgain and Kontorovich 2011] J. Bourgain and A. Kontorovich, "On a conjecture of Zaremba", preprint, 2011. arXiv 1107.3776

[Bourgain and Kontorovich 2012] J. Bourgain and A. Kontorovich, "On the strong density conjecture for integral Apollonian circle packings", preprint, 2012. arXiv 1205.4416

[Bourgain and Varjú 2012] J. Bourgain and P. P. Varjú, "Expansion in $\mathrm{SL}_d(\mathbf{Z}/q\mathbf{Z})$, q arbitrary", *Invent. Math.* **188**:1 (2012), 151–173.

[Bourgain et al. 2010a] J. Bourgain, A. Gamburd, and P. Sarnak, "Affine linear sieve, expanders, and sum-product", *Invent. Math.* **179**:3 (2010), 559–644.

[Bourgain et al. 2010b] J. Bourgain, A. Kontorovich, and P. Sarnak, "Sector estimates for hyperbolic isometries", *Geom. Funct. Anal.* **20**:5 (2010), 1175–1200.

[Bourgain et al. 2011] J. Bourgain, A. Gamburd, and P. Sarnak, "Generalization of Selberg's $3/16$ theorem and affine sieve", *Acta Math.* **207**:2 (2011), 255–290.

[Breuillard and Gamburd 2010] E. Breuillard and A. Gamburd, "Strong uniform expansion in $\mathrm{SL}(2, p)$", *Geom. Funct. Anal.* **20**:5 (2010), 1201–1209.

[Breuillard et al. 2011] E. Breuillard, B. Green, and T. Tao, "Approximate subgroups of linear groups", *Geom. Funct. Anal.* **21**:4 (2011), 774–819.

[Ellenberg et al. 2012] J. S. Ellenberg, C. Hall, and E. Kowalski, "Expander graphs, gonality, and variation of Galois representations", *Duke Math. J.* **161**:7 (2012), 1233–1275.

[Friedlander and Iwaniec 2010] J. Friedlander and H. Iwaniec, *Opera de cribro*, American Mathematical Society Colloquium Publications **57**, American Mathematical Society, Providence, RI, 2010.

[Fuchs 2010] E. Fuchs, *Arithmetic properties of Apollonian circle packings*, Ph.D. thesis, Princeton University, 2010, http://math.berkeley.edu/∼efuchs/efuchsthesis.pdf.

[Fuchs and Sanders 2010] E. Fuchs and K. Sanders, "Some experiments with integral Apollonian circle packings", preprint, 2010. arXiv 1001.1406

[Gamburd 2002] A. Gamburd, "On the spectral gap for infinite index "congruence" subgroups of $\mathrm{SL}_2(\mathbb{Z})$", *Israel J. Math.* **127** (2002), 157–200.

[Graham et al. 2003] R. L. Graham, J. C. Lagarias, C. L. Mallows, A. R. Wilks, and C. H. Yan, "Apollonian circle packings: Number theory", *J. Number Theory* **100**:1 (2003), 1–45.

[Green 2009] B. Green, "Approximate groups and their applications: Work of Bourgain, Gamburd, Helfgott and Sarnak", preprint, 2009. arXiv 0911.3354

[Hall 1947] M. Hall, Jr., "On the sum and product of continued fractions", *Ann. of Math.* (2) **48** (1947), 966–993.

[Helfgott 2008] H. A. Helfgott, "Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$", *Ann. of Math.* (2) **167**:2 (2008), 601–623.

[Helfgott 2011] H. A. Helfgott, "Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$", *J. Eur. Math. Soc.* (*JEMS*) **13**:3 (2011), 761–851.

[Hensley 1989] D. Hensley, "The distribution of badly approximable numbers and continuants with bounded digits", pp. 371–385 in *Théorie des nombres* (Quebec, 1987), edited by J.-M. D. Koninck and C. Levesque, de Gruyter, Berlin, 1989.

[Hensley 1992] D. Hensley, "Continued fraction Cantor sets, Hausdorff dimension, and functional analysis", *J. Number Theory* **40**:3 (1992), 336–358.

[Hensley 1996] D. Hensley, "A polynomial time algorithm for the Hausdorff dimension of continued fraction Cantor sets", *J. Number Theory* **58**:1 (1996), 9–45.

[Hoory et al. 2006] S. Hoory, N. Linial, and A. Wigderson, "Expander graphs and their applications", *Bull. Amer. Math. Soc.* (*N.S.*) **43**:4 (2006), 439–561.

[Iwaniec 1972] H. Iwaniec, "Primes of the type $\phi(x, y) + A$ where ϕ is a quadratic form", *Acta Arith.* **21** (1972), 203–234.

[Jenkinson and Pollicott 2001] O. Jenkinson and M. Pollicott, "Computing the dimension of dynamically defined sets: E_2 and bounded continued fractions", *Ergodic Theory Dynam. Systems* **21**:5 (2001), 1429–1445.

[Kontorovich and Oh 2011] A. Kontorovich and H. Oh, "Apollonian circle packings and closed horospheres on hyperbolic 3-manifolds", *J. Amer. Math. Soc.* **24**:3 (2011), 603–648.

[Kowalski 2012] E. Kowalski, "Crible en expansion", exposé 1028 (pp. 17–64) in *Séminaire Bourbaki* 2010/2011, Astérisque **348**, Soc. Math. de France, Paris, 2012.

[Lax and Phillips 1982] P. D. Lax and R. S. Phillips, "The asymptotic distribution of lattice points in Euclidean and non-Euclidean spaces", *J. Funct. Anal.* **46**:3 (1982), 280–350.

[Lubotzky 1994] A. Lubotzky, *Discrete groups, expanding graphs and invariant measures*, Birkhäuser, Basel, 1994.

[Lubotzky 2012] A. Lubotzky, "Expander graphs in pure and applied mathematics", *Bull. Amer. Math. Soc.* (*N.S.*) **49**:1 (2012), 113–162.

[Margulis 1973] G. A. Margulis, "Explicit constructions of expanders", *Problemy Peredači Informacii* **9**:4 (1973), 71–80. In Russian; Translated in English in *Problems of Information Transmission* **9**:4 (1973), 325–332, 1975.

[Matthews et al. 1984] C. R. Matthews, L. N. Vaserstein, and B. Weisfeiler, "Congruence properties of Zariski-dense subgroups. I", *Proc. London Math. Soc.* (3) **48**:3 (1984), 514–532.

[Mohammadi and Oh 2012] A. Mohammadi and H. Oh, "Matrix coefficients, counting and primes for orbits of geometrically finite groups", preprint, 2012. To appear in *J. Eur. Math. Soc.* arXiv 1208.4139

[Niederreiter 1978] H. Niederreiter, "Quasi-Monte Carlo methods and pseudo-random numbers", *Bull. Amer. Math. Soc.* **84**:6 (1978), 957–1041.

[Niederreiter 1986] H. Niederreiter, "Dyadic fractions with small partial quotients", *Monatsh. Math.* **101**:4 (1986), 309–315.

[Pinsker 1973] M. S. Pinsker, "On the complexity of a concentrator", pp. 318/1–318/4 in *7th International Teletrafic Conference* (Stockholm, 1973), 1973.

[Pyber and Szabó 2010] L. Pyber and E. Szabó, "Growth in finite simple groups of Lie type of bounded rank", preprint, 2010. arXiv 1005.1858

[Salehi Golsefidy and Sarnak 2011] A. Salehi Golsefidy and P. Sarnak, "Affine sieve", preprint, 2011. arXiv 1109.6432

[Salehi Golsefidy and Varjú 2012] A. Salehi Golsefidy and P. P. Varjú, "Expansion in perfect groups", *Geom. Funct. Anal.* **22**:6 (2012), 1832–1891.

[Sarnak 1995] P. Sarnak, "Selberg's eigenvalue conjecture", *Notices Amer. Math. Soc.* **42**:11 (1995), 1272–1277.

[Sarnak 2008] P. Sarnak, "Equidistribution and primes", pp. 225–240 in *Géométrie différentielle, physique mathématique, mathématiques et société, II*, Astérisque **322**, 2008.

[Sarnak 2011] P. Sarnak, "Integral Apollonian packings", *Amer. Math. Monthly* **118**:4 (2011), 291–306.

[Sarnak 2014] P. Sarnak, "Notes on thin matrix groups", pp. 343–362 in *Thin groups and superstrong approximation*, edited by H. Oh and E. Breuillard, Math. Sci. Res. Inst. Publ. **61**, Cambridge Univ. Press, Cambridge, 2014.

[Schmidt 1972] W. M. Schmidt, "Irregularities of distribution, VII", *Acta Arith.* **21** (1972), 45–50.

[Varjú 2012] P. P. Varjú, "Expansion in $\mathrm{SL}_d(O_K/I)$, I square-free", *J. Eur. Math. Soc.* (*JEMS*) **14**:1 (2012), 273–305.

[Vinogradov 2012] I. Vinogradov, "Effective bisector estimate with application to Apollonian circle packings", preprint, 2012. arXiv 1204.5498

[Zaremba 1966] S. C. Zaremba, "Good lattice points, discrepancy, and numerical integration", *Ann. Mat. Pura Appl.* (4) **73** (1966), 293–317.

[Zaremba 1972] S. K. Zaremba, "La méthode des "bons treillis" pour le calcul des intégrales multiples", pp. 39–119 in *Applications of number theory to numerical analysis (Proc. Sympos., Univ. Montreal)* (Montreal, Que., 1971), edited by S. K. Zaremba, Academic Press, New York, 1972.

bourgain@ias.edu

Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ 08540, United States