*Ergod. Th. & Dynam. Sys.* (2009), **29**, 1705–1722 © *2009 Cambridge University Press*
doi:10.1017/S0143385708000898 *Printed in the United Kingdom*

# Some effective results for $\times a \times b$

JEAN BOURGAIN†, ELON LINDENSTRAUSS‡§, PHILIPPE MICHEL¶‖ and AKSHAY VENKATESH**††

† *Institute for Advanced Study, Princeton, NJ 08540, USA*
‡ *Princeton University, Princeton, NJ 08544, USA*
§ *The Hebrew University, 91904 Jerusalem, Israel*
¶ *EPFL, 1015 Lausanne, Switzerland*
‖ *Universit Montpellier, 34095 Montpellier, France*
** *Stanford University, Stanford, CA 94305, USA*
†† *Courant Institute of Mathematical Sciences, New York, NY 10012, USA*

(*Received* 17 *April* 2008 *and accepted in revised form* 25 *September* 2008)

*In memory of Bill Parry*

*Abstract*. We provide effective versions of theorems of Furstenberg and Rudolph–Johnson regarding closed subsets and probability measures of $\mathbb{R}/\mathbb{Z}$ invariant under the action of a non-lacunary multiplicative semigroup of integers. In particular, we give an explicit rate at which the sequence $\{a^n b^k x\}_{n,k}$ becomes dense for $a$, $b$ fixed multiplicatively independent integers and $x \in \mathbb{R}/\mathbb{Z}$ Diophantine generic.

## 1. *Introduction*

1.1. Let $a, b > 1$ be multiplicatively independent integers, i.e. not powers of the same integer, or equivalently so that $\log a/\log b \notin \mathbb{Q}$ (for example, $a$, $b$ relatively prime). In [**5**], Furstenberg showed that the only closed, infinite subset of $\mathbb{R}/\mathbb{Z}$ invariant under the maps $t_a : x \mapsto a.x$ and $t_b : x \mapsto b.x$ is $\mathbb{R}/\mathbb{Z}$ (with $a.x = ax \bmod 1$). This implies that, for any irrational $x$,

$$\overline{\{a^k b^\ell.x \mid k, \ell \geq 0\}} = \mathbb{R}/\mathbb{Z}. \tag{1.1a}$$

Furstenberg raised the question of what are the $t_a$,$t_b$-invariant measures on $\mathbb{R}/\mathbb{Z}$, conjecturing that the only non-atomic such measure† is the Lebesgue measure $\lambda$. A theorem of Rudolph for $a$, $b$ relatively prime [**9**], generalized by Johnson to the case of $a$, $b$ multiplicatively independent [**7**], asserts that a probability measure on the circle $\mathbb{R}/\mathbb{Z}$ that is invariant and ergodic with respect to the semigroup generated by the maps $t_a : x \mapsto ax$ and $t_b : x \mapsto bx$, and has positive entropy with respect to $t_a$, is equal to $\lambda$. We note that Bill

† That is, a measure that gives measure zero to any single point.

Parry, to whose memory this paper is dedicated, has provided another, related but distinct, proof of Rudolph's theorem [**8**].

In this paper, we give an effective version of the Rudolph–Johnson theorem, and use it (among other things) to obtain effective versions of Furstenberg's theorem, in particular giving an estimate on the rate in (1.1a) in terms of the Diophantine properties of $x$.

1.2. By a straightforward application of the ergodic decomposition, the Rudolph–Johnson theorem is equivalent to the following, which avoids any assumptions regarding ergodicity.

THEOREM 1.3. (Rudolph–Johnson theorem) *Let $\mu$ be a probability measure on $\mathbb{R}/\mathbb{Z}$ invariant under $t_a$ and $t_b$ for $a, b$ multiplicatively independent. Suppose that*

$$h_\mu(t_a) = \eta \log a.$$

*Then*

$$\mu \geq \eta\lambda, \tag{1.3a}$$

*i.e. for any measurable $A \subset \mathbb{R}/\mathbb{Z}$, $\mu(A) \geq \eta\lambda(A)$.*

Linear combinations of Lebesgue measure and measures supported on rationals show that (1.3a) is sharp. We recall that, in this context, the ergodic theoretic entropy† $h_\mu(t_a)$ is simply

$$h_\mu(t_a) = \lim_{n\to\infty} H_\mu(\mathcal{P}_{a^n}),$$

where $\mathcal{P}_{a_n}$ is the partition of $\mathbb{R}/\mathbb{Z}$ into $a^n$ intervals $[0, 1/a^n), [1/a^n, 2/a^n), \ldots$ and $H_\mu(\mathcal{P}) = -\sum_{P\in\mathcal{P}} \mu(P) \log \mu(P)$ the Shannon entropy of a partition $\mathcal{P}$.

We prove the following effective version of Theorem 1.3.

THEOREM 1.4. (Effective Rudolph–Johnson theorem) *Let $a, b$ be multiplicatively independent, and $\mu$ an arbitrary probability measure on $\mathbb{R}/\mathbb{Z}$ satisfying the entropy condition*

$$H_\mu(\mathcal{P}_N) \geq \rho \log N \quad \text{for some } \rho > 0,\ N > N_0(a, b).$$

*Let $\delta \leq \rho/20$ and let $f \in C^1(\mathbb{R}/\mathbb{Z})$ be a non-negative function. Then there is an integer $m = a^s b^t < N$ so that*

$$[m.\mu](f) \geq (\rho - 3\delta)\lambda(f) - \kappa_1 \log(N)^{-\kappa_2\delta} \|f'\|_2 \tag{1.4a}$$

*with $\kappa_1, \kappa_2$ depending only on $a, b$.*

We give two proofs for this theorem: the first based on Host's (not explicitly effective) proof of Rudolph's theorem [**6**] when $a, b$ are relatively prime, and a second, related but different proof, which works in the general multiplicative independent case. Where applicable, the first proof is slightly more informative; in particular, when $a, b$ are relatively prime one can take $\kappa_2 = 1/2$.

Note that here and below we have not attempted to optimize the exponents occurring, the quality of the results being measured rather in the number of logs.

† Also known as the Kolmogorov–Sinai entropy or (somewhat confusingly) the metric entropy.

https://doi.org/10.1017/S0143385708000898 Published online by Cambridge University Press

1.5. It is interesting to compare this result, or more precisely its implications regarding $t_a$,$t_b$-invariant subsets of $N^{-1}\mathbb{Z}/\mathbb{Z}$, with the results of Bourgain [**3**] and Bourgain, Glibichuk and Konyagin [**2**]. Applying Theorem 1.4 to the measure $\mu = |S|^{-1} \sum_{x \in S} \delta_x$ where $S \subset N^{-1}\mathbb{Z}/\mathbb{Z}$ is $t_a$,$t_b$-invariant we get the following corollary.

COROLLARY 1.6. *Let $N$ be an integer greater than or equal to some $N_0(a, b)$, with $(N, ab) = 1$. Suppose that $S \subset N^{-1}\mathbb{Z}/\mathbb{Z}$ with $|S| > N^{\rho}$. Then for any subinterval $J \subset \mathbb{R}/\mathbb{Z}$ there is an $m = a^s b^t < N$ so that the proportion of $m.S$ inside $J$ satisfies*

$$\frac{|m.S \cap J|}{|S|} \geq \rho\lambda(J) - \kappa_3 \frac{\log\log\log N}{\log\log N}.$$

*Moreover, the set*

$$\{m.s \mid m = a^s b^t < N,\ s \in S\}$$

*is* $(\log N)^{-\kappa_2 \rho/100}$*-dense.*

(For the first statement, apply Theorem 1.4 with $\delta = (\log\log\log N)/(10\kappa_2 \log\log N)$ and suitable test function $f$ supported on $J$ with $\lambda(f) \geq \lambda(J) - \delta$ and $\|f'\|_\infty < \delta^{-1}$. For the second statement, use $\delta = \rho/10$, $J$ an interval with $\lambda(J) = \log N^{-\kappa_2\rho/100}$ and a test function $f$ supported on $J$ with $\lambda(f) \geq \lambda(J)/2$ and $\|f'\|_\infty < \lambda(J)^{-1}$.)

When the multiplicative subgroup generated by $a$, $b$ in $\mathbb{Z}/N\mathbb{Z}$ is of order $N^{\alpha}$ and if, for example, $S$ is $t_a$, $t_b$ invariant, the papers [**2**] (for $N$ prime) and [**3**] (for general $N$) imply much sharper results, e.g. that $S$ has no gaps of size $N^{-c_1}$ and that $|S \cap J|/|S| \geq \rho\lambda(J) - N^{-c_2}$ for some $c_1$, $c_2$ depending on $a$, $b$, $\alpha$ but not $N$.

1.7. We deduce from Theorem 1.4 effective versions of Furstenberg's theorem. We begin by giving a quantification of (1.1a).

THEOREM 1.8. *Let $a$, $b$ be multiplicative independent. Suppose $\alpha \in \mathbb{R}/\mathbb{Z}$ is irrational and Diophantine-generic: there exists $k$ so that*

$$|\alpha - p/q| \geq q^{-k}, \quad q \geq 2,\ p, q \in \mathbb{Z}.$$

*Then $\{a^s b^t \alpha \mid s, t \leq N\}$ is $(\log\log N)^{-\kappa_6}$-dense in $\mathbb{R}/\mathbb{Z}$ for constants $\kappa_6 = \kappa_6(a, b)$ and for $N \geq N_0(k, a, b)$.*

Here we say that $S \subset \mathbb{R}/\mathbb{Z}$ is $\varepsilon$-dense if any $x \in \mathbb{R}/\mathbb{Z}$ has distance at most $\varepsilon$ from $S$.

1.9. It follows from Furstenberg's classification of closed $t_a$,$t_b$-invariant sets that for any given $\varepsilon > 0$ there are only finitely many rationals whose orbit under $t_a$, $t_b$ fails to be $\varepsilon$-dense. It can be effectivized as follows.

THEOREM 1.10. *Let $a$, $b$ be multiplicatively independent and $(ab, N) = 1$. Then for any $m \in (\mathbb{Z}/N\mathbb{Z})^{\times}$ the set*

$$\left\{ a^k b^l . \frac{m}{N} \;\middle|\; 0 < k, l < 3 \log N \right\}$$

*is $\kappa_7(\log\log\log N)^{-\kappa_2/100}$-dense with $\kappa_7$ depending only on $a$, $b$ and $\kappa_2$ as in Theorem 1.4 (in particular, if $(a, b) = 1$, an absolute constant, otherwise a constant depending only on $a$, $b$).*

https://doi.org/10.1017/S0143385708000898 Published online by Cambridge University Press

## 2. *Notation and preliminaries*

2.1. We use $\mathbb{N}$ to denote the set $\{0, 1, 2, \dots\}$ and $\mathbb{Z}^+ = \{1, 2, \dots\}$. As is customary $A \subset B$ allows $A = B$; when $B$ is a group we use $A < B$ to denote that $A$ is a subgroup of $B$ (again, $A = B$ is allowed). If $\mu$ is a measure on $\mathbb{R}/\mathbb{Z}$ and $m \in \mathbb{Z}^+$, we denote by $m.\mu$ the pushforward of $\mu$ by $x \mapsto mx$. Sometimes it will be convenient to denote the map $x \mapsto mx$ by $t_m$.

2.2. For any $N \in \mathbb{Z}^+$, we will use $\mathcal{P}_N$ to denote the partition of $\mathbb{R}/\mathbb{Z}$ into $N$ equal intervals, i.e. $[0, 1/N) \cup [1/N, 2/N) \cup \cdots \cup [1 - 1/N, 1)$. For $a \in \mathbb{Z}^+$, $n_1, n_2 \in \mathbb{N}$, we let

$$\mathcal{P}_a^{[n_1,n_2)} = \bigvee_{k=n_1}^{n_2-1} t_{a^k}^{-1}(\mathcal{P}_a),$$

where $\mathcal{P} \vee \mathcal{Q}$ denotes the common refinement $\{P \cap Q \mid P \in \mathcal{P}, Q \in \mathcal{Q}\}$ of two partitions $\mathcal{P}, \mathcal{Q}$. In particular $\mathcal{P}_a^{[0,n)} = \mathcal{P}_{a^n}$.

2.3. Let $\mu$ be a measure on $\mathbb{R}/\mathbb{Z}$ and $\mathcal{P} = \{P_1, P_2, \dots, P_N\}$ a finite partition of $\mathbb{R}/\mathbb{Z}$. We will use the notation

$$\mu(\mathcal{P}) = (\mu(P_1), \dots, \mu(P_N)).$$

The entropy $H_\mu(\mathcal{P})$ is defined to be

$$H_\mu(\mathcal{P}) = \sum_{P \in \mathcal{P}} -\mu(P) \log \mu(P).$$

Suppose that a partition $\mathcal{P}$ as above refines a partition $\mathcal{Q}$. For each $Q \in \mathcal{Q}$ with $\mu(Q) > 0$, let $\mu_Q$ be the probability measure $\mu(Q)^{-1}\mu|_Q$. The conditional entropy $H_\mu(\mathcal{P}|\mathcal{Q})$ is given by

$$H_\mu(\mathcal{P}|\mathcal{Q}) = H_\mu(\mathcal{P}) - H_\mu(\mathcal{Q}) = \sum_{Q \in \mathcal{Q}} \mu(Q) H_{\mu_Q}(\mathcal{P}),$$

where the latter sum is taken over those $Q$ with $\mu(Q) > 0$. If $\mathcal{P}$ does not necessarily refine $\mathcal{Q}$, we may still define $H_\mu(\mathcal{P}|\mathcal{Q}) := H_\mu(\mathcal{P} \vee \mathcal{Q}|\mathcal{Q})$.

More generally, for any $p > 1$ define the *$\ell^p$-entropy* by

$$H_\mu^p(\mathcal{P}) = \frac{-\log \|\mu(\mathcal{P})\|_p}{1 - 1/p}.$$

This quantity is also often called the Rényi entropy. The function $H_\mu^p(\mathcal{P})$ is non-increasing in $p$, with $\lim_{p \downarrow 1} H_\mu^p(\mathcal{P}) = H_\mu(\mathcal{P})$†.

Finally, if $\mu$ is a measure on a finite set $S$ and we use the notation above without specifying a partition $\mathcal{P}$, we shall mean to take the partition of $S$ into singletons. In particular, in this context,

$$\|\mu\|_p = \left(\sum_{s \in S} |\mu(\{s\})|^p\right)^{1/p}, \quad H_\mu = -\sum\nolimits_{s \in S} \mu(\{s\}) \log \mu(\{s\}).$$

† For this reason it is sometimes convenient to extend the definition of $H_\mu^p$ also to $p = 1$ by setting $H_\mu^1(\mathcal{P}) = H_\mu(\mathcal{P})$.

https://doi.org/10.1017/S0143385708000898 Published online by Cambridge University Press

2.4. We shall repeatedly use the following facts:
(i) $H_\mu(\mathcal{P}) \le \log(\#\mathcal{P})$, with $\#\mathcal{P}$ denoting the number of elements of the partition $\mathcal{P}$†;
(ii) $H_\mu(\mathcal{P} \vee \mathcal{Q}) = H_\mu(\mathcal{P}) + H_\mu(\mathcal{Q} \mid \mathcal{P}) \le H_\mu(\mathcal{P}) + H_\mu(\mathcal{Q})$.

2.5. Let $\mu$ be a probability measure on a finite set $S$. As we have already remarked $H_\mu^p$ is monotonically non-increasing in $p$, and one may certainly have a measure $\mu$ with $H_\mu^1 = H_\mu$ large but $H_\mu^p$ small for any fixed $p > 1$: indeed simply take $\mu$ the measure that gives measure $\frac{1}{2}$ to some $s_0 \in S$ and divide the remaining measure uniformly on $S \setminus \{s_0\}$.

The following lemma allows us to 'upgrade' the ordinary ($H_\mu$) entropy to $l^p$-entropy, but at a price: at the price of replacing $\mu$ by a measure $\nu$ that is dominated by a certain constant (depending on $H_\mu$) times $\mu$.

LEMMA 2.6. *Let $\mu$ be a probability measure on a finite set $S$, with $|S| = N$ and $H_\mu = \rho \log N$. Let $\log 2/\log N < \delta \le \rho/2$. Then there is a probability measure $\nu$ such that $\mu \ge (\rho - \delta)\nu$ and $\|\nu\|_2^2 \le 4\rho^{-1}N^{-\delta}$.*

*Proof.* Put $\mu(\{s\}) = w_s$. Put $S_1 = \{s \in S \mid w_s < 2N^{-\delta}\}$, $S_2 = S \setminus S_1$, and for $i = 1, 2$ let $\nu_i = (1/\mu(S_i))\mu|_{S_i}$. Then, denoting by $\cdot$ the partition of $S$ into singletons,

$$\begin{aligned}\rho \log N = H_\mu &= H_\mu(\{S_1, S_2\}) + H_\mu(\cdot \mid \{S_1, S_2\}) \\ &= H_\mu(\{S_1, S_2\}) + \mu(S_1)H_{\nu_1} + \mu(S_2)H_{\nu_2} \\ &\le \mu(S_1)\log N + \delta\mu(S_2)\log N + \mu(S_1)\log 2,\end{aligned}$$

as $\nu_1$ is a measure supported on at most $N$ elements, hence $H_{\nu_1} \le \log N$; $\nu_2$ is supported on at most $N^\delta/2$ elements and $H_{\nu_2} \le \delta \log N - \log 2$; finally, $H_\mu(\{S_1, S_2\}) \le \log 2$. Thus

$$\mu(S_1) \ge \frac{\rho - \delta}{1 - \delta + \log 2/\log N} > \rho - \delta.$$

The claim now follows by taking $\nu = \nu_1$ and observing that

$$\|\nu\|_2^2 \le \|\nu\|_\infty \le 2\mu(S_1)^{-1}N^{-\delta} \le 4\rho^{-1}N^{-\delta}. \qquad \square$$

We need the following variant of Lemma 2.6.

LEMMA 2.7. *Let $\mu$ be a probability measure on some space $X$, and let $\mathcal{P}$, $\mathcal{Q}$ be finite partitions of $X$. Assume that $H_\mu(\mathcal{P} \mid \mathcal{Q}) = \rho \log |\mathcal{P}|$. Let $0 \le \delta \le \rho/2$. Then we can find probability measures $\nu_1, \ldots, \nu_k$ and weights $w_1, \ldots, w_k$ such that:*
(i) *each $\nu_i$ is supported on a single atom of $\mathcal{Q}$;*
(ii) *$\mu \ge \sum_i w_i\nu_i$ and $\sum_i w_i \ge (\rho - \delta)$; and*
(iii) *$\sum_i w_i \|\nu_i(\mathcal{P})\|_2^2 \le 2|\mathcal{P}|^{-\delta}$.*

*Proof.* Similarly to §2.6, set $\mathcal{S}_1$ to be those $A \in \mathcal{P} \vee \mathcal{Q}$ for which

$$\frac{\mu(A)}{\mu(Q)} < 2|\mathcal{P}|^{-\delta} \quad \text{where } A \subset Q \in \mathcal{Q},$$

and $\mathcal{S}_2$ to be all the other members of $\mathcal{P} \vee \mathcal{Q}$.

† Indeed, the same equality holds for $H_\mu^p$ for every $p$, with equality if and only if all the parts of $\mathcal{P}$ are assigned equal measure.

https://doi.org/10.1017/S0143385708000898 Published online by Cambridge University Press

For any $Q \in \mathcal{Q}$ set $\mathcal{S}_1^Q = \{A \in \mathcal{S}_1 \mid A \subset Q\}$, $w_Q = \mu(\bigcup \mathcal{S}_1^Q)$ and $\nu_Q = (1/w_Q)\mu|_{\cup \mathcal{S}_1^Q}$. As in Lemma 2.6,

$$\mu\left(\bigcup \mathcal{S}_1\right) = \sum_{Q \in \mathcal{Q}} w_Q \geq \rho - \delta$$

and

$$\|\nu_Q(\mathcal{P})\|_2^2 = \|\nu_Q(\mathcal{P} \vee \mathcal{Q})\|_2^2 \leq \|\nu_Q(\mathcal{P} \vee \mathcal{Q})\|_\infty \leq \frac{2\mu(Q)|\mathcal{P}|^{-\delta}}{w_Q}.$$

Summing over $Q \in \mathcal{Q}$, we get

$$\sum_Q w_Q \|\nu_Q(\mathcal{P})\|_2^2 \leq 2|\mathcal{P}|^{-\delta} \sum_Q \mu(Q) = 2|\mathcal{P}|^{-\delta}. \qquad \square$$

2.8. Let now $\mu$ be a probability measure on $\mathbb{R}/\mathbb{Z}$. The following lemma shows that, if $N$ and $M$ are comparable, the entropies $H_\mu(\mathcal{P}_N)$ and $H_\mu(\mathcal{P}_M)$ are essentially the same.

LEMMA 2.9. *Let $\mu$ be a probability measure on $\mathbb{R}/\mathbb{Z}$, and $N < M$ positive integers. Then*

$$H_\mu(\mathcal{P}_M) - \log(\lceil M/N \rceil + 1) \leq H_\mu(\mathcal{P}_N) \leq H_\mu(\mathcal{P}_M) + \log 2.$$

*Proof.* Let $\mathcal{P} = \mathcal{P}_N \vee \mathcal{P}_M$. Then any atom of $\mathcal{P}_M$ is a union of at most two element $\mathcal{P}$ and hence

$$H_\mu(\mathcal{P}_N) \leq H_\mu(\mathcal{P}) = H_\mu(\mathcal{P}_M) + H_\mu(\mathcal{P} \mid \mathcal{P}_M) \leq H_\mu(\mathcal{P}_M) + \log 2.$$

The reverse inequalities obtain similarly, by observing that any atom of $\mathcal{P}_N$ is a union of at most $\lceil M/N \rceil + 1$ elements of $\mathcal{P}$. $\square$

2.10. We will use $\alpha_1, \alpha_2, \ldots$ to denote constants. The dependence of these constants on all parameters depends on the context. We will use the superscript $\alpha_1{}^{\text{abs}}$ the first time $\alpha_1$ is used to denote that it is an absolute constant, and use e.g. $\alpha_1(N, \neg\delta)$ to denote that $\alpha_1$ depends on $N$ but not on $\delta$. (Hopefully the dependence of $\alpha_1$ on any other conceivable parameter will be clear from the context; unless otherwise stated, and unless one of the parameters in the exponent is preceded by a $\neg$ sign, the assumption is that $\alpha_1$ does not depend on any other parameter.) The indexing of these constants is reset every section. Similarly we have $\kappa_1, \kappa_2, \ldots$ (numbering is consequtive throughout the paper), $c_1, c_2, \ldots$ (reset every subsection). All our constants will be effective: i.e. in principle one can write an explicit formula for how they depend on all parameters. As is often customary, '$a < \alpha_2 b$' is a shorthand for 'There exists some constant $\alpha_2 > 0$ so that $a < \alpha_2 b$'. We will also use the notation $\ll$ when we would like to keep the constant implicit; this implicit constant will always be absolute and effective.

As usual in analytic arguments, $e(x) := e^{2\pi i x}$. For any measure $\nu$ on $\mathbb{R}/\mathbb{Z}$ let $\widehat{\nu}(n) = \nu(e(nx))$ denote its Fourier transform; occasionally, the notation $\nu^\wedge(n)$ will be typographically friendlier.

https://doi.org/10.1017/S0143385708000898 Published online by Cambridge University Press

## 3. *Proof of the effective Rudolph theorem*

3.1. In this section we prove an effective version of the Rudolph–Johnson theorem for $a$, $b$ relatively prime. A related, but different, argument will be given in the next section that works in the general case.

THEOREM 3.2. (Effective Rudolph theorem) *Let $a$, $b$ be relatively prime integers, and $\mu$ an arbitrary probability measure on $\mathbb{R}/\mathbb{Z}$ satisfying the entropy condition*

$$H_\mu(\mathcal{P}_N) \geq \rho \log N \quad \text{for some } \rho > 0,\ N > N_0(a, b).$$

*Let*

$$\frac{10}{\log_a T} \leq \delta \leq \frac{\rho}{20}, \quad a^{20/\delta} \leq T \leq \frac{\delta}{4} \log_b(N), \quad f \in C^1(\mathbb{R}/\mathbb{Z}) \text{ non-negative}. \tag{3.2a}$$

*Then there exist integers $s$, $t$, $0 \leq s \leq (1-\delta)\log_a(N)$, $0 \leq t \leq T$, satisfying*

$$[a^s b^t.\mu](f) \geq (\rho - 3\delta)\lambda(f) - \kappa_8 T^{-\delta/2}\|f'\|_2$$

*with $\kappa_8$ depending only on $a$, $b$, and $\|f'\|_2 = (\int_0^1 |f'|^2\,dx)^{1/2}$.*

Note that if $\kappa_8$ is bigger than some absolute constant, the bound above becomes trivial if $\delta \geq 10/\log_a T$ and hence the lower bound on $\delta$ in (3.2a) is immaterial.

LEMMA 3.3. *Let $a$, $b$ be relatively prime. Then there is some $\alpha_1 = \alpha_1(a, b)$ so that for every $r > \alpha_1$ the multiplicative subgroup $S_b < (\mathbb{Z}/a^r\mathbb{Z})^*$ generated by $b$ satisfies*

$$S_b > 1 + a^{\alpha_1}(\mathbb{Z}/a^r\mathbb{Z}). \tag{3.3a}$$

*Proof.* By elementary number theory, the group of elements in $(\mathbb{Z}/a^r\mathbb{Z})^*$ congruent to 1 modulo $a^3$ is cyclic; moreover, all its subgroups are of the form

$$\{x \in (\mathbb{Z}/a^r\mathbb{Z}) \mid x \equiv 1 \bmod \underline{m}\}, \tag{3.3b}$$

where $a^3$ divides $\underline{m}$ and $\underline{m}$ divides $a^r$. (To verify this assertion, one may use exponential and logarithm maps, defined via power series, to reduce the question to the corresponding statement in the *additive* group of $(\mathbb{Z}/a^r\mathbb{Z})$, where it is obvious; if $a$ is odd, one could even replace $a^3$ by $a$.)

Let $\varphi(a^3)$ be the size of $(\mathbb{Z}/a^3\mathbb{Z})^*$. The subgroup generated by $b^{\varphi(a^3)}$ is of the form (3.3b); clearly, $\underline{m} \leq b^{\varphi(a^3)}$. We take $\alpha_1 = \lceil a^3 \log_a b \rceil$. □

3.4. Note that Lemma 3.3 is essentially equivalent to the following: for any prime $p$ and integer $b$ not divisible by $p$ we have that

$$|b^k - 1|_p \geq p^{-\log_b k + \alpha_1} = p^{\alpha_1} k^{-\log p/\log b}.$$

LEMMA 3.5. *Let $(a, b) = 1$ and $\gamma \in \mathbb{R}/\mathbb{Z}$ arbitrary. Let $\mu$ be a probability measure on $\gamma + a^{-\ell}\mathbb{Z}/\mathbb{Z}$, and let $S_b < (\mathbb{Z}/a^\ell\mathbb{Z})^*$ be the multiplicative group generated by $b$. Then for any smooth $f$,*

$$\frac{1}{\#S_b} \sum_{\xi \in S_b} |[\xi.\mu](f) - \lambda(f)|^2 \leq \alpha_2 \|f'\|_2^2 \|\mu\|_2^2,$$

*with $\alpha_2 = \alpha_2(a, b)$, and $f'$ the derivative of $f$.*

https://doi.org/10.1017/S0143385708000898 Published online by Cambridge University Press

Here, and in the proof that follows, we enclose the measure $\xi.\mu$ in square brackets for typographical clarity.

In words: a random translate of $\mu$ by $\xi \in S_b$ is uniformly distributed if the '$l^2$-entropy' $\log(1/\|\mu\|_2)$ is large.

*Proof.* It follows from (3.3a) of Lemma 3.3 that, for any $s \in a^{-\ell}\mathbb{Z}/\mathbb{Z}$, $0 \neq n \in \mathbb{Z}$,

$$\left|\sum_{\xi \in S_b} e(n\xi s)\right| \leqslant \begin{cases} 0 & \text{if } a^{\alpha_1} ns \not\equiv 0 \bmod 1, \\ \#S_b & \text{otherwise} \end{cases} \tag{3.5a}$$

(note that $S_b$ implicitly depends on $\ell$).

Recall that $\widehat{\nu}$ denotes the Fourier transform of a measure $\nu$ on $\mathbb{R}/\mathbb{Z}$. Set $w_s = \mu(\{s+\gamma\})$ for $s \in a^{-\ell}\mathbb{Z}/\mathbb{Z}$. Then

$$\begin{aligned} \frac{1}{\#S_b}\sum_{\xi \in S_b} |[\xi.\mu]^\wedge(n)|^2 &= \frac{1}{\#S_b}\sum_{\xi \in S_b}\left|\sum_s w_s e(n\xi(s+\gamma))\right|^2 \\ &= \frac{1}{\#S_b}\sum_{s,s'} w_s w_{s'} \sum_{\xi \in S_b} e(\xi n(s-s')) \\ &\underset{(3.5a)+C-S}{\leq} \#\{s'' \in \mathbb{Z}/a^\ell\mathbb{Z} \mid a^{\alpha_1} ns'' \equiv 0 \bmod 1\} \sum_s w_s^2 \\ &\leq a^{\alpha_1} \gcd(a^\ell, n)\|\mu\|_2^2, \end{aligned} \tag{3.5b}$$

with $\gcd(a^\ell, n)$ the greatest common divisor of $a^\ell$ and $n$ (and C–S shorthand for Cauchy–Schwarz).

Expanding $f$ in a Fourier series $f(x) = \sum \widehat{f}(n)e(nx)$; in particular $\widehat{f}(0) = \lambda(f)$. Then

$$\begin{aligned} \frac{1}{\#S_b}\sum_{\xi \in S_b} |[\xi.\mu](f) - \lambda(f)|^2 &= \frac{1}{\#S_b}\sum_{\xi \in S_b}\left|\sum_{n\neq 0} \widehat{f}(n)[\xi.\mu]^\wedge(n)\right|^2 \\ &\underset{C-S}{\leq} \left(\frac{1}{\#S_b}\sum_{\xi \in S_b}\sum_{n\neq 0} n^{-2}|[\xi.\mu]^\wedge(n)|^2\right)\left(\sum_n n^2|\widehat{f}(n)|^2\right) \\ &\underset{(3.5b)}{\leq} \|f'\|_2^2\|\mu\|_2^2 a^{\alpha_1}\left(\sum_{n\neq 0}\frac{\gcd(a^\ell, n)}{n^2}\right). \end{aligned}$$

The constants $\sum_{n\neq 0} n^{-2}\gcd(a^\ell, n)$ can be explicitly evaluated as follows:

$$\sum_{n\neq 0}\frac{\gcd(a^\ell, n)}{n^2} \leq \sum_{d|a^\ell}\sum_{\substack{n\neq 0 \\ d|n}} dn^{-2} \leq \frac{\pi^2}{3}\frac{a}{\phi(a)}$$

with $\phi(\cdot)$ the Euler totient function. This establishes Lemma 3.5 with

$$\alpha_2 = \frac{\pi^2}{3}\frac{a^{\alpha_1+1}}{\phi(a)},$$

$\alpha_1$ as in (3.3a). □

https://doi.org/10.1017/S0143385708000898 Published online by Cambridge University Press

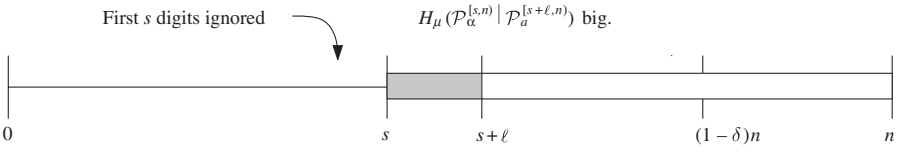


FIGURE 1. $\mu$ and $s$ (relatively prime case).

LEMMA 3.6. *Suppose given* $\rho > 0$ *and a measure* $\mu$ *on* $a^{-n}\mathbb{Z}/\mathbb{Z}$ *so that* $H_\mu \geq \rho n \log a$. *Let* $\delta \leq \rho/10$. *For any* $10/\delta \leq \ell \leq \delta n$, *there exists* $s \leq (1-\delta)n$ *so that*

$$[a^s.\mu] \geq \nu := \sum w_i \nu_i,$$

*where*

(i) *each* $\nu_i$ *is a probability measure supported on a translate of* $a^{-\ell}\mathbb{Z}/\mathbb{Z}$;
(ii) *the* $w_i$ *are non-negative and satisfy* $\sum w_i \geq \rho - 2\delta$; *and*
(iii) $\nu_i$ *and* $w_i$ *satisfy* $\sum_i w_i \|\nu_i\|_2^2 < 2a^{-\ell\delta}$.

*Proof.* Expand using §2.4.(ii), noting the fact that $\mathcal{P}_a^{[0,n)}$ induces the partition of $a^{-n}\mathbb{Z}/\mathbb{Z}$ into singletons:

$$\begin{aligned} H_\mu = {} & H_\mu(\mathcal{P}_a^{[0,n)} | \mathcal{P}_a^{[\ell,n)}) + H_\mu(\mathcal{P}_a^{[\ell,n)} | \mathcal{P}_a^{[2\ell,n)}) + \cdots \\ & + H_\mu(\mathcal{P}_a^{[(m-1)\ell,n)} | \mathcal{P}_a^{[m\ell,n)}) + H_\mu(\mathcal{P}_a^{[m\ell,n)}), \end{aligned}$$

with $m = \lfloor n/\ell \rfloor$. Now $H_\mu(\mathcal{P}_a^{[m\ell,n)}) \leq \ell \log a$. From this we deduce that there is $0 \leq s \leq n - \ell$ so that

$$H_\mu(\mathcal{P}_a^{[s,n)} | \mathcal{P}_a^{[s+\ell,n)}) \geq \frac{(\rho n - \ell)\log a}{m} \geq (\rho - \delta)\ell \log a.$$

We refer to Figure 1 for a graphical description of this. To help decode the picture, notice that $P_a^{[x,y)}$ is precisely the partition of [0, 1], whereupon two numbers lie in the same part if their $a$-ary expansions coincide between digits $x$ and $y$.

To simplify notation, we replace for the remainder of this proof $\mu$ with $[a^s.\mu]$ and $n$ with $n - s$; thus by our choice of $s$ we have that

$$H_\mu(\mathcal{P}_a^{[0,n)} | \mathcal{P}_a^{[\ell,n)}) \geq (\rho - \delta)\ell \log a. \tag{3.6a}$$

The lemma now follows by applying Lemma 2.7 to $\mu$ with $\mathcal{P} = \mathcal{P}_a^{[0,\ell)}$, $\mathcal{Q} = \mathcal{P}_a^{[\ell,n)}$ and $\rho' = \rho - \delta$. □

3.7. Lemmas 3.5 and 3.6 together easily imply the following weak form of the quantitative Rudolph theorem; we will later see how this weaker statement can be massaged to give the stronger version given by Theorem 3.2. The only significant difference between the two versions is that in Proposition 3.8 the measure $\mu$ is assumed to be supported on the finite set $a^{-n}\mathbb{Z}/\mathbb{Z}$.

PROPOSITION 3.8. *Let* $a, b$ *be relatively prime integers,* $n \in \mathbb{N}$, *and* $\mu$ *a probability measure on* $a^{-n}\mathbb{Z}/\mathbb{Z}$ *satisfying the entropy condition*

$$H_\mu = H_\mu(\mathcal{P}_{a^n}) \geq \rho n \log a \quad \textit{for some } \rho > 0.$$

https://doi.org/10.1017/S0143385708000898 Published online by Cambridge University Press

*Let* $\alpha_3 = \log a/4 \log b$ *and suppose*

$$\frac{10}{\log_a T} \le \delta \le \frac{\rho}{10},\ a^{20/\delta} \le T \le \alpha_3 \delta n,\ \ f \in C^1(\mathbb{R}/\mathbb{Z}) \text{ non-negative}. \tag{3.8a}$$

*Then there exist integers* $s, t,\ 0 \le s \le (1-\delta)n, 0 \le t \le T$ *satisfying*

$$[a^s b^t.\mu](f) \ge (\rho - 2\delta)\lambda(f) - \kappa_9 T^{-\delta/2}\|f'\|_2 \tag{3.8b}$$

*with* $\kappa_9 = \kappa_9(a, b)$.

*Proof.* Set $\ell = \lfloor \log_a T \rfloor$, and let $\nu_i$, $\nu = \sum_i w_i \nu_i$ be as in Lemma 3.6; we recall in particular that each $\nu_i$ is a probability measure on a translate of $a^{-\ell}\mathbb{Z}/\mathbb{Z}$ with $\sum_i w_i \|\nu_i\|_2^2 \le 2a^{-\delta\ell}$. Let $w = \sum_i w_i$. Note that by (3.8a) the conditions $10/\delta \le \ell \le \delta n$ of Lemma 3.6 are satisfied. (To see $\ell \le \delta n$, note that by the upper bound on $T$ given by (3.8a), if $\delta n < \ell$ (hence $\delta n < \log_a T$), $e^{\delta n \log a} \le \delta n \log a/4 \log b$ and by $e^x > x^2/2$ this would imply $\delta n < (2 \log a \log b)^{-1}$ in contradiction to $\alpha_3 \delta n \ge T \ge 2^{20/\delta}$.)

Let $T'$ be the order of $b$ in the multiplicative group $\mathbb{Z}/a^\ell\mathbb{Z}$, and note that $T' < a^\ell \le T$. By Lemma 3.5,

$$\begin{aligned}
\frac{1}{T'}\sum_{t=0}^{T'} |[b^t.\nu](f) - w\lambda(f)| &\le \sum_i w_i \left(\frac{1}{T'}\sum_{t=0}^{T'} |[b^t.\nu_i](f) - \lambda(f)|\right) \\
&\le w^{1/2}\left(\sum_i w_i \left(\frac{1}{T'}\sum_{t=0}^{T'} |[b^t.\nu](f) - \lambda(f)|\right)^2\right)^{1/2} \\
&\le \left(\sum_i w_i \frac{1}{T'}\sum_{t=0}^{T'} |[b^t.\nu](f) - \lambda(f)|^2\right)^{1/2} \\
&\le {\alpha_2}^{1/2}\|f'\|_2 \left(\sum_i w_i \|\nu_i\|_2^2\right)^{1/2} \\
&\le 2{\alpha_2}^{1/2}\|f'\|_2 a^{-\ell\delta/2}.
\end{aligned} \tag{3.8c}$$

Since $[a^s.\mu] \ge \nu$ for some $s \le (1-\delta)n$, equation (3.8c) implies that there are $s \le (1-\delta)n$, $t \le T$ so that

$$[a^s b^t.\mu](f) \ge (\rho - 2\delta)\lambda(f) - \kappa_9 T^{-\delta/2}\|f'\|_2$$

with $\kappa_9 = 2a^{1/2}{\alpha_2}^{1/2}$. □

3.9. We now deduce the effective Rudolph theorem §3.2, from the seemingly weaker Proposition 3.8.

*Proof of Theorem 3.2.* Let the notation be as in the statement of Theorem 3.2. Let $n = \lfloor \log_a N \rfloor$. Define the measure $\mu'$ on $a^{-n}\mathbb{Z}/\mathbb{Z}$ by

$$\mu'\left(\left\{\frac{k}{a^n}\right\}\right) = \mu\left(\left[\frac{k}{a^n}, \frac{k+1}{a^n}\right)\right).$$

By Lemma 2.9.

$$H_{\mu'} = H_\mu(\mathcal{P}_{a^n}) \ge H_\mu(\mathcal{P}_N) - \log(a+1) \ge (n\rho - 2)\log a \ge n(\rho - \delta).$$

https://doi.org/10.1017/S0143385708000898 Published online by Cambridge University Press

Assumptions (3.2a) on $\delta, \rho, T, N$ imply that $\rho' = \rho - \delta$, $T' = T$, $\delta' = \delta$, $n$ satisfy (3.8a). Applying Proposition 3.8 we get that there are $0 \le s \le (1-\delta)\lfloor \log_a N \rfloor$ and $0 \le t \le T$ so that

$$[a^s b^t.\mu'](f) \ge (\rho - 3\delta)\lambda(f) - \kappa_9 T^{-\delta/2}\|f'\|_2. \tag{3.9a}$$

By the choice of $s, t$, $a^s b^t \le N^{1-\delta/2}$ (hence $a^{s-n}b^t \le aN^{-\delta/2}$), hence

$$|[a^s b^t.\mu](f) - [a^s b^t.\mu'](f)| \leqslant \max_{|x-x'|\le aN^{-\delta/2}} |f(x) - f(x')| \le aN^{-\delta/4}\|f'\|_2. \tag{3.9b}$$

As long as $N^{1/2} > \log_b(N)$ (a condition we can use to define $N_0(a,b)$), we have that $T \le N^{1/2}$; hence from (3.9a), there are $s$, $t$ as in Theorem 3.2 so that

$$[a^s b^t.\mu](f) \ge (\rho - 3\delta)\lambda(f) - \kappa_8 T^{-\delta/2}\|f'\|_\infty$$

with $\kappa_8 = \kappa_9 + a$. □

## 4. *Proof of the effective Rudolph–Johnson theorem*

4.1. In this section we present a related, but different, proof of Theorem 3.2 that works for the general case of $a$, $b$ multiplicatively independent, at the (modest) expense of not being able to consider a smaller range for the power of $b$.

Throughout this section we shall denote:

$$\mathcal{S}_{a,b} = \{a^n b^m \mid n, m \ge 0\}.$$

4.2. The following deep result regarding lower bounds on linear forms in two logarithms plays a role analogous to Lemma 3.3 in our second proof of an effective version of the Rudolph–Johnson theorem. The first non-trivial bounds in this direction (which are probably sufficiently good for our purposes) are due to Gelfond and Schneider, with subsequent improvements by Baker and others; the rather precise form we give here (in a much more general form) is due to Baker and Wüstholz [**1**].

THEOREM 4.3. (Baker and Wüstholz [**1**]) *Let $a$, $b$ be multiplicative independent integers. Then for any $k, n \in \mathbb{Z}$*

$$|k/n - \log a/\log b| \ge \exp(-\kappa_{10} \log a \log b \log(1 + |k| + |n|)),$$

*with $\kappa_{10}$ an effective absolute constant (indeed, one can take $\kappa_{10} = 2^{31}$).*

COROLLARY 4.4. *There exist $\kappa_{11}, \kappa_{12} > 0$ depending on $a, b$ so that if we write the elements of $\mathcal{S}_{a,b}$ as $a_1 \le a_2 \le \ldots$, then the gap*

$$a_{k+1} - a_k \le \frac{\kappa_{11} a_k}{(\log a_k)^{\kappa_{12}}}. \tag{4.4a}$$

*Proof.* Let $a_r = a^k b^n$, and for notational convenience assume $a^k > b^n$. We want to show that there is an element $t \in \mathcal{S}_{a,b}$ with

$$a_r \le t \le a_r\left(1 + \frac{\kappa_{11} a_k}{(\log a_k)^{\kappa_{12}}}\right).$$

Let $p/q$ be the last successive continued fraction approximation of $\log a/\log b$ so that

$$q < k \quad \text{and} \quad \log a/\log b < p/q, \tag{4.4b}$$

https://doi.org/10.1017/S0143385708000898 Published online by Cambridge University Press

and let $p'/q'$, $p''$, $q''$ be the next two continued fraction approximations of $\log a/\log b$; as $p''/q''$ is also greater than $\log a/\log b$, $q'' \geq k$. Then

$$\frac{p'}{q'} < \frac{\log a}{\log b} < \frac{p''}{q''} < \frac{p}{q}; \tag{4.4c}$$

as $p/q - p'/q' = 1/qq'$ and $p''/q'' - p'/q' = 1/q''q'$, it follows that

$$0 < p - \frac{\log a}{\log b} q < \frac{1}{q'} \tag{4.4d}$$

$$0 > p' - \frac{\log a}{\log b} q' > -\frac{1}{q''} > -\frac{1}{k}. \tag{4.4e}$$

Using Theorem 4.3 and (4.4e) we have

$$k^{-1} > \left| p' - \frac{\log a}{\log b} q' \right| > \exp\left( -\frac{1}{\kappa_{12}} \log q' \right)$$

for $\kappa_{12} = (2\kappa_{10} \log a \log b(1 + \log a/\log b))^{-1}$, hence $q' > k^{\kappa_{12}}$. Recall also that we have assumed that $a^k > b^n$, hence $k > \log(a_r)/2\log(a)$. Equation (4.4d) and the inequality $b^x \leq 1 + (b-1)x$ for $x \in [0, 1]$ implies that

$$1 < b^p a^{-q} < 1 + \frac{b-1}{q'}.$$

We conclude that

$$\begin{aligned} a_r &< a^{k-q} b^{n+p} < a_r(1 + (b-1)/q') \\ &< a_r(1 + (b-1)k^{-\kappa_{12}}) \\ &\leq a_r\left(1 + (b-1)\left(\frac{\log a_r}{2\log a}\right)^{-\kappa_{12}}\right), \end{aligned}$$

hence we can take

$$\kappa_{11} = \max((b-1)(2\log a)^{\kappa_{12}}, (a-1)(2\log b)^{\kappa_{12}}). \qquad \square$$

LEMMA 4.5. *Let $\nu$ be a probability measure on $\mathbb{R}/\mathbb{Z}$ and $M \in \mathbb{Z}^+$. Then there is an absolute constant $\alpha_1$ so that for any $0 \neq \xi \in \mathbb{Z}$*

$$M^{-1} \sum_0^{M-1} |[m.\nu]^\wedge(\xi)|^2 \leq 2\alpha_1 |\xi| \|\nu(\mathcal{P}_M)\|_2^2. \tag{4.5a}$$

*Proof.* We first consider the case $\xi = 1$. Number the intervals comprising $\mathcal{P}_M$ as $I_0, \ldots, I_{M-1}$, and for $x \in \mathbb{R}$ we let $\|x\|$ denote the distance of $x$ from $\mathbb{Z}$.

Let $h(m)$ be a non-negative function on $\mathbb{Z}$ so that $h(i) \geq 1/M$ for $0 \leq i \leq M-1$:

$$M^{-1} \sum_0^{M-1} |[m.\nu]^\wedge(1)|^2 \leq \sum_m h(m)[m.\nu]^\wedge(1)^2 = \iint G(x, y)\, d\nu(x)\, d\nu(y) \tag{4.5b}$$

with $G(x, y) = \sum_m h(m) e(m(x-y))$. It is possible to choose the function $h(m)$ so that

$$|G(x, y)| < 5 \min(1, M^{-2}\|x - y\|^{-2}).$$

https://doi.org/10.1017/S0143385708000898 Published online by Cambridge University Press

(Take, for example, $h = 1/M \max(1 - d(m)/M, 0)$, where $d(m)$ is the distance of $m$ to the set $[0, M-1]$, i.e. $d(m) = \min_{0\le i\le M-1} |i - m|$.†) Since for $\ell \neq \ell'$, $\ell' \pm 1$

$$\|x - y\| \ge \frac{1}{2}\left\|\frac{\ell - \ell'}{M}\right\| \quad \text{for } x \in I_\ell,\ y \in I_{\ell'},$$

we have that

$$(4.5b) \le 20\left(\sum_\ell \nu(I_\ell)^2 + \sum_{\ell\neq\ell'} \frac{\nu(I_\ell)\nu(I_{\ell'})}{|\ell - \ell'|^2}\right). \tag{4.5c}$$

By the Frobenius theorem the norm of the quadratic form above is bounded by the row sum of the matrix, which is bounded above by an absolute constant $\alpha_1$. We conclude that

$$M^{-1}\sum_0^{M-1} |[m.\nu]^\wedge(1)|^2 \le \alpha_1 \|\nu(\mathcal{P}_M)\|_2^2. \tag{4.5d}$$

To obtain the required estimate for general $\xi$, apply (4.5d) on $\xi.\nu$ to obtain

$$M^{-1}\sum_0^{M-1} |[m.\nu]^\wedge(\xi)|^2 \le \alpha_1 \|\xi.\nu(\mathcal{P}_M)\|_2^2,$$

and note that

$$\|\xi.\nu(\mathcal{P}_M)\|_2^2 = \|\nu(\xi^{-1}\mathcal{P}_M)\|_2^2 \underset{(*)}{\le} 2|\xi|\|\nu(\xi^{-1}\mathcal{P}_M \vee \mathcal{P}_M)\|_2^2 \le 2|\xi|\|\nu(\mathcal{P}_M)\|_2^2,$$

where the inequality marked by $(*)$ is a consequence of the fact that every atom of $\xi^{-1}\mathcal{P}_M$ intersects at most $2|\xi|$ atoms of $\xi^{-1}\mathcal{P}_M \vee \mathcal{P}_M$. □

LEMMA 4.6. *Let $a, b$ be multiplicative independent integers, and $\mu$ a probability measure, and $s$ a sufficiently large integer ($s > \alpha_2$). Assume that $\mu$ is supported on the interval $[ka^{-s}, (k+1)a^{-s}]$. Let $f \in C^1(\mathbb{R}/\mathbb{Z})$, $\ell < \kappa_{12}\log_a(s)/3$ ($\kappa_{12}$ as in Corollary 4.4). Then there is a subset*

$$R_s \subset S_{a,b} \cap \{1, 2, 3, \dots, a^{s+\ell}\}$$

*(independent of $\mu$, $k$) so that*

$$\frac{1}{\#R_s}\sum_{n\in R_s} |[n.\mu](f) - \lambda(f)|^2 < \alpha_3 \ell \|f'\|_2^2 \|\mu(\mathcal{P}_{a^{s+\ell}})\|_2^2. \tag{4.6a}$$

*Here $\alpha_2$ and $\alpha_3$ depend on $a$, $b$.*

*Proof.* By Corollary 4.4, we can find a subset

$$R_s = \{n_1, \dots, n_{a^\ell}\} \subset S_{a,b} \cap \{1, \dots, a^{s+\ell}\}$$

so that

$$|n_m - ma^s| < \delta a^s \tag{4.6b}$$

† If we took naively $h(m)$ to be the characteristic function of $[0, M-1]$, this would lead to a similar result but with an extra factor of $\log M$; this would not affect our argument in any substantive way.

https://doi.org/10.1017/S0143385708000898 Published online by Cambridge University Press

for $\delta = \kappa_{11}(s \log a)^{-2\kappa_{12}/3}$. Define $\alpha_2$ so that, if $s > \alpha_2$,

$$(s \log a)^{2\kappa_{12}/3} > 10\kappa_{11} \quad \text{and} \quad \delta \le a^{-\ell}.$$

We now estimate, for any $0 \neq \xi \in \mathbb{Z}$,

$$a^{-\ell} \sum_{m=0}^{a^\ell - 1} |(n_m.\mu)^\wedge(\xi)|^2 \le a^{-\ell} \Bigg( \sum_{m=0}^{a^\ell-1} |(ma^s.\mu)^\wedge(\xi)|^2 + \sum_{m=0}^{a^\ell-1} |(ma^s.\mu)^\wedge(\xi) - \theta_m (n_m.\mu)^\wedge(\xi)|^2 \Bigg) \tag{4.6c}$$

where $\theta_m$ are arbitrary complex numbers with $|\theta_m| = 1$. Taking $\theta_m = e(-n_m k a^{-s}\xi)$ we have

$$\begin{aligned} |(ma^s.\mu)^\wedge(\xi) - \theta_m (n_m.\mu)^\wedge(\xi)| &\le \max_{0 \le t \le a^{-s}} |e(ma^s \xi t) - e(n_m \xi t)| \\ &\le |\xi| |m - n_m a^{-s}| \\ &\le a^{-\ell} |\xi|, \end{aligned}$$

and so by Lemma 4.5

$$(4.6c) \le 2\alpha_1 |\xi| \|\mu(\mathcal{P}_{a^{s+\ell}})\|_2^2 + a^{-2\ell}|\xi|^2. \tag{4.6d}$$

Using (4.6d) we have

$$\begin{aligned} a^{-\ell} \sum_{m=0}^{a^\ell-1} |[n_m.\mu](f) - \lambda(f)|^2 &= a^{-\ell} \sum_{m=0}^{a^\ell-1} \Bigg| \sum_{\xi \neq 0} |[n_m.\mu]^\wedge(\xi)| \widehat{f}(\xi)| \Bigg|^2 \\ &\le a^{-\ell} \|f'\|_2^2 \sum_{m=0}^{a^\ell-1} \Bigg( \sum_{\xi} |\xi|^{-2} |[n_m.\mu]^\wedge(\xi)|^2 \Bigg) \\ &\le \|f'\|_2^2 \Bigg( \sum_{|\xi| < a^\ell} (2\alpha_1 |\xi|^{-1} \|\mu(\mathcal{P}_{a^{s+\ell}})\|_2^2 + 2a^{-2\ell}) + 2a^{-\ell} \Bigg) \\ &\le (4\alpha_1 \log a + 4)\ell \|f'\|_2^2 \|\mu(\mathcal{P}_{a^{s+\ell}})\|_2^2. \end{aligned}$$

□

Note that, by the assumption on the support of $\mu$,

$$\|\mu(\mathcal{P}_{a^{s+\ell}})\|_2^2 = \|[a^s.\mu](\mathcal{P}_{a^\ell})\|_2^2 \ge a^{-\ell}.$$

LEMMA 4.7. *Suppose given $\rho > 0$, $n$ and a measure $\mu$ on $\mathbb{R}/\mathbb{Z}$ so that $H_\mu(\mathcal{P}_{a^n}) \ge \rho n \log a$. Let $\delta \le \rho/10$. For any $10/\delta \le \ell \le \delta n$, there exists $s$ with $\delta n \le s + \ell \le n$ so that*

$$\mu \ge \nu := \sum w_i \nu_i,$$

*where*

(i) *each $\nu_i$ is a probability measure supported on a single $a^{-s}$-interval from $\mathcal{P}_{a^s}$;*
(ii) *the $w_i$ are non-negative and satisfy $\sum w_i \ge \rho - 3\delta$; and*
(iii) *$\nu_i$ and $w_i$ satisfy $\sum_i w_i \|\nu_i(\mathcal{P}_{a^{s+\ell}})\|_2^2 < 2a^{-\ell\delta}$.*

This lemma is proved precisely as Lemma 3.6, with Figure 2 substituting for Figure 1. For example, the first displayed equation of Lemma 3.6 should be replaced in the present context by $H_\mu = H_\mu(\mathcal{P}_a^{[0,\ell)}) + H_\mu(\mathcal{P}_a^{[0,2\ell)} | \mathcal{P}_a^{[0,\ell)}) + H_\mu(\mathcal{P}_a^{[0,3\ell)} | \mathcal{P}_a^{[0,2\ell)}) + \cdots$.

https://doi.org/10.1017/S0143385708000898 Published online by Cambridge University Press

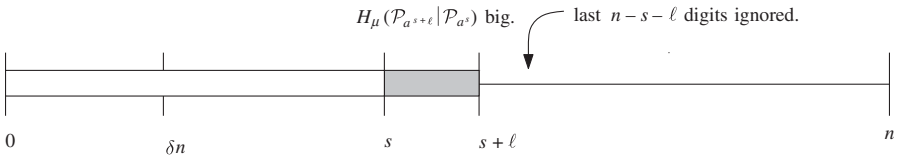


FIGURE 2. $\mu$ and $s$ (general multiplicatively independent case).

4.8. *Proof of Theorem 1.4.* Let $n = \lfloor \log_a N \rfloor$. Then $H_\mu(\mathcal{P}_{a^n}) \geq H_\mu(\mathcal{P}_N) - \log 2a \geq (\rho - \delta)n \log a$. Without loss of generality, we may assume that $\delta \geq 40/\kappa_{12} \log_a(\delta n)$ as otherwise $\log(N)^{-\kappa_2 \delta}$ is bounded from below by some constant that depends only on $a, b$, hence if $\kappa_1$ is chosen to be sufficiently large the right- hand side of (1.4a) is negative. Apply Lemma 4.7 with $\rho' = \rho - \delta$ and $\ell = \kappa_{12} \log_a(\delta n)/4$ to find $s$ with $\delta n \leq s + \ell \leq n$, probability measures $\nu_i$ and weights $w_i$ as in that lemma; in particular

$$w := \sum w_i \geq \rho - 4\delta \quad \text{and} \quad \sum w_i \|\nu_i(\mathcal{P}_{a^{s+l}})\|_2^2 \leq 2a^{-\ell\delta}.$$

Also by appropriate choice of $N_0(a, b)$ we may certainly assume that $\ell < \delta n/2$.

As in Lemma 4.7 set $\nu = \sum w_i \nu_i \leq \mu$. Then

$$\begin{aligned}
\frac{1}{\#R_s} \sum_{m \in R_S} |[m.\nu](f) - w\lambda(f)| &\leq \sum_i w_i \left( \frac{1}{\#R_s} \sum_{m \in R_S} |[m.\nu_i](f) - \lambda(f)| \right) \\
&\leq w^{1/2} \left( \sum_i w_i \left( \frac{1}{\#R_s} \sum_{m \in R_S} |[m.\nu_i](f) - \lambda(f)| \right)^2 \right)^{1/2} \\
&\leq \left( \sum_i w_i \frac{1}{\#R_s} \sum_{m \in R_S} |[m.\nu_i](f) - \lambda(f)|^2 \right)^{1/2} \\
&\underset{(*)}{\leq} {\alpha_3}^{1/2} \ell \|f'\|_2 \left( \sum_i w_i \|\nu_i(\mathcal{P}_{a^{s+l}})\|_2^2 \right)^{1/2} \\
&\leq 2{\alpha_3}^{1/2} \ell \|f'\|_2 a^{-\ell\delta/2}
\end{aligned}$$

where the inequality (*) follows by applying Lemma 4.6 on each $\nu_i$.

As $\ell = \kappa_{12} \log_a(\delta n)/4$,

$$a^{-\ell\delta/2} = (\delta n)^{-\kappa_{12}\delta/8} \leq 10 n^{-\kappa_{12}\delta/8},$$

obtaining

$$\frac{1}{\#R_s} \sum_{m \in R_s} m.\mu(f) \geq w\mu(f) - \kappa_1 \|f'\|_2 \log\log N (\log N)^{-\kappa_{12}\delta/8}$$

for $\kappa_1 = 20\kappa_{12}\alpha_3$. □

## 5. *Deduction of effective Furstenburg theorem*

5.1. Let $\alpha \in \mathbb{R}/\mathbb{Z}$ be an irrational; set $X_N = \{n\alpha \mid n \in \mathcal{S}_{a,b}, n \leq N\} \subset \mathbb{R}/\mathbb{Z}$.

We will assume that we are given an increasing function $F : \mathbb{N} \to \mathbb{R}$ such that $|q\alpha - p| \geq F(q)^{-1}$ for all $p, q \in \mathbb{N}$.

https://doi.org/10.1017/S0143385708000898 Published online by Cambridge University Press

We define functions $F_2$, $F_3$ in terms of $F$ via:

$$\begin{aligned} F_1(x) &= \exp(\exp((2\kappa_{11}x)^{1/\kappa_{12}})), \\ F_2(N) &= 3F_1(N)F \circ F_1(N), \\ F_3(N) &= F_2(a^{N+1}),\ F_4 = a^N F_3(N), \end{aligned} \tag{5.1a}$$

where $\kappa_{12}$, $\kappa_{11}$ is as in Corollary 4.4.

We prove the following refinement of Theorem 1.8.

PROPOSITION 5.2. *Suppose that $K \geq F_4(M)$. Then $X_K$ is $M^{-1/200}$-dense in $\mathbb{R}/\mathbb{Z}$ for sufficiently large $M$ ('sufficiently large' depending on $a$, $b$).*

LEMMA 5.3. *Let $F_2$ be defined as in (5.1a). If $M \geq M_0(a, b)$, then*

$$X_{F_2(M)} - X_{F_2(M)}$$

*is $1/M$-dense in $\mathbb{R}/\mathbb{Z}$.*

*Proof.* The set $\{n \in \mathcal{S}_{a,b} \mid n \leq N\}$ has cardinality at least $c_1(\log N)^2$ for some $c_1 = c_1(a, b)$.

Therefore, for $L \geq L_0(a, b)$ the set $X_L - X_L$ contains an element whose distance $d$ from 0 satisfies $F(L)^{-1} \leq d \leq (\log L)^{-1}$.

It now follows from Corollary 4.4 that, if $L \geq L_1(a, b)$, then

$$K \geq 3.L.F(L) \implies X_K - X_K \text{ is } \frac{2\kappa_{11}}{(\log\log L)^{\kappa_{12}}}\text{-dense;} \tag{5.3a}$$

rephrasing this gives the lemma.

To see (5.3a), note that $d + \mathbb{Z} \in X_L - X_L$. Let $\mathcal{S}_{a,b} = \{a_1 < a_2 < \cdots\}$ and consider the sequence $a_n.d$ for $n_1 \leq n \leq n_2$ with $n_1$ the smallest so that $a_{n_1} > d^{-1/2}$ and $n_2$ the largest so that $a_{n_2} < d^{-1}$.

Then by (4.4a) for $n_1 \leq n \leq n_2$ we have that

$$\frac{a_{n+1}}{a_n} \leq 1 + \frac{2\kappa_{11}}{(\log d)^{\kappa_{12}}} \leq \frac{2\kappa_{11}}{(\log\log L)^{\kappa_{12}}},$$

so there is no gap larger than $2\kappa_{11}(\log\log L)^{-\kappa_{12}}$ in the sequence $a_{n_1}d, \ldots, a_{n_2}d$. Also the smallest element $a_{n_1}d$ is less than or equal to $d^{-1/2} \leq 2\kappa_{11}(\log\log L)^{-\kappa_{12}}$ if $L \geq L_1(a, b)$, and the largest is greater than or equal to $1 - 2\kappa_{11}(\log\log L)^{-\kappa_{12}}$.

Thus, for $L \geq L_1(a, b)$, the set $X_{3.d^{-1}.L} - X_{3.d^{-1}.L}$ is $2\kappa_{11}(\log\log L)^{-\kappa_{12}}$-dense. Note that $3d^{-1}L \leq 3F(L)L$. □

LEMMA 5.4. *For $N \geq N_0(a, b)$ the set $X_{F_3(N)}$ intersects at least $\frac{1}{2}a^{N/2}$ atoms of the partition $\mathcal{P}_{a^N}$.*

*Proof.* By the previous lemma (recalling that $F_3(N) = F_2(a^{N+1})$) $X_{F_3(N)} - X_{F_3(N)}$ is $a^{-N-1}$-dense in $\mathbb{R}/\mathbb{Z}$ if $N$ is sufficiently large (in terms of $a$, $b$). This means that $X_{F_3(N)} - X_{F_3(N)}$ intersects every atom of the partition $\mathcal{P}_{a^N}$.

If $P_1$, $P_2$ are two atoms of $\mathcal{P}_{a^N}$, then $P_1 - P_2 := \{\alpha_1 - \alpha_2 \mid \alpha_j \in P_j\}$ is covered by at most two atoms of $\mathcal{P}_{a^N}$. Therefore, $X_{F_3(N)}$ must intersect at least $\frac{1}{2}a^{N/2}$ atoms of $\mathcal{P}_{a^N}$. □

https://doi.org/10.1017/S0143385708000898 Published online by Cambridge University Press

5.5. *Proof of Proposition 5.2.* By Lemma 5.4, the set $X_{F_3(N)}$ intersects at least $\frac{1}{2}a^{N/2}$ atoms of $\mathcal{P}_{a_N}$.

Let

$$\mathcal{C} = \{P \in \mathcal{P}_{a_N} \mid P \cap X_{F_3(N)} \neq \emptyset\}$$

and for every $P \in \mathcal{C}$ let $x_P$ be a single point in $P \cap X_{F_3(N)}$. Let $\mu = (1/|\mathcal{C}|) \sum_{p\in\mathcal{C}} \delta_{x_P}$.

Then $H_\mu(\mathcal{P}_{a^N}) \geq N \log a/2 - \log 2$. Applying Theorem 1.4 with $\rho = 0.49$, $\delta = 0.1$ and $f$ a suitable test function supported on an arbitrary interval $J$ of size $N^{-\kappa_2/100}$, we get an $m \leq a^N$ in $\mathcal{S}_{a,b}$ so that $m.\mu(J) > 0$, hence $X_{F_4(N)}$ is $N^{-\kappa_2/100}$-dense for $N \geq N_2(a, b)$. □

5.6. The proof of Theorem 1.10 about density of $\{a^k b^l.(m/N) \mid 0 < k, l < \kappa_5 \log N\}$ is very similar.

*Proof of Theorem 1.10. Step 1.* Set for any $M$

$$X_M = \left\{ a^k b^\ell . \frac{m}{N} \;\middle|\; a^k b^\ell < M \right\}. \tag{5.6a}$$

Then there is a $d \in X_N - X_N$ with

$$\frac{1}{N} \leq d < {\alpha_1}^{-1} (\log N)^{-2}.$$

*Step 2.* The set

$$Y = \{a^k b^\ell . d \mid a^k b^\ell < d^{-1}\} \subset X_{N^2} - X_{N^2}$$

is $2\kappa_{11}(\log d)^{-\kappa_{12}}$-dense.

Hence if $M = (\log d)^{\kappa_{12}}/4\kappa_{11}$, we can find a probability measure $\mu$ (constructed similarly to the measure $\mu$ in §5.5) supported on $X_{N^2}$ with $H_\mu(\mathcal{P}_M) \geq \frac{1}{2} \log M - \log 2$.

*Step 3.* Applying Theorem 1.4, we conclude that the set

$$X_{MN^2} = \{m.x \mid m = a^s b^t < M, x \in X_{N^2}\}$$

is $\alpha_2(\log M)^{-\kappa_2/100}$-dense. If $N$ is sufficiently large, $X_{N^2 M} \subset X_{N^3}$, and moreover by definition of $M$ it follows that

$$\alpha_2(\log M)^{-\kappa_2/100} = \alpha_3(\log\log d)^{-\kappa_2/100} \leq \alpha_4(\log\log\log N)^{-\kappa_2/100}. \tag{5.6b}$$

5.7. Note that *if* $X_N - X_N$ contained an element $d$ of size $O(1/N)$ (e.g. if $m = 1$) in the proof outlined above in §5.6 one log can be dropped in (5.6b), yielding a substantially improved estimate.

*Acknowledgements.* This work is closely connected to the work of E.L., P.M. and A.V. with Manfred Einsiedler; in particular Corollary 1.6 is an (effective) analogue of [**4**, Corollary 1.7]. We thank him for numerous discussions on these and related topics. We also thank Peter Varju for careful reading and helpful comments on a preliminary version of this manuscript.

This research has been supported by NSF grants DMS 0627882 (J.B.), DMS 0500205, 0554345 (E.L.) and DMS 0554365 (A.V). A.V. was also supported by the Sloan Foundation and by the Packard Foundation.

## References

**[1]** A. Baker and G. Wüstholz. Logarithmic forms and group varieties. *J. Reine Angew. Math.* **442** (1993), 19–62.

**[2]** J. Bourgain, A. Glibichuk and S. Konyagin. Estimate for the number of sums and products and for exponential sums in fields of prime order. *J. London Math. Soc.* **73** (2006), 380–398.

**[3]** J. Bourgain. Sum-product theorems and exponential sum bounds in residue classes for general modulus. *C. R. Math. Acad. Sci. Paris* **344**(6) (2007), 349–352.

**[4]** M. Einsiedler, E. Lindenstrauss, P. Michel and A. Venkatesh. The distribution of periodic torus orbits on homogeneous spaces *Duke Math. J.* to appear.

**[5]** H. Furstenberg. Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation. *Math. Systems Theory* **1** (1967), 1–49.

**[6]** B. Host. Nombres normaux, entropie, translations. *Israel J. Math.* **91**(1–3) (1995), 419–428.

**[7]** A. S. A. Johnson. Measures on the circle invariant under multiplication by a nonlacunary subsemigroup of the integers. *Israel J. Math.* **77**(1–2) (1992), 211–240.

**[8]** W. Parry. Squaring and cubing the circle—Rudolph's theorem. *Ergodic Theory of* $\mathbf{Z}^d$ *Actions (Warwick, 1993–1994) (London Mathematical Society Lecture Note Series, 228)*. Cambridge University Press, Cambridge, 1996, pp. 177–183.

**[9]** D. J. Rudolph. $\times 2$ and $\times 3$ invariant measures and entropy. *Ergod. Th. & Dynam. Sys.* **10**(2) (1990), 395–406.