THE $(\alpha+2\beta)$-INEQUALITY ON A TORUS

YURI BILU

ABSTRACT

A theorem of Macbeath asserts that $\underline{\mu}(A+B) \geqslant \min(1, \underline{\mu}(A)+\underline{\mu}(B))$ for any subsets A and B of a finite-dimensional torus. We conjecture that, when the obvious exceptions are excluded, a stronger inequality

$$\underline{\mu}(A+B) \geqslant \min(1, \underline{\mu}(A)+\underline{\mu}(B)+\min(\underline{\mu}(A), \underline{\mu}(B)))$$

holds, and we prove this conjecture under some technical restrictions.

1. *Introduction*

Let A and B be subsets of the torus $\mathbb{T}^r = \mathbb{R}^r/\mathbb{Z}^r$ and let

$$A+B = \{a+b : a \in A, b \in B\}.$$

Throughout the paper we use the notation

$$\alpha = \underline{\mu}(A), \quad \beta = \underline{\mu}(B), \quad \gamma = \mu(A+B), \tag{1}$$

where μ is the normalized Haar measure on $\mathbb{T}^r$ and $\underline{\mu}$ the corresponding inner measure. (Recall that by definition $\underline{\mu}(A) = \sup \mu(F)$ over all closed $F \subset A$.) Macbeath [**15**] proved that

$$\gamma \geqslant \min(1, \alpha+\beta) \tag{2}$$

(for the one-dimensional torus, (2) was established earlier by Raikov [**21**]). The result of Macbeath is sometimes called the $(\alpha+\beta)$-*inequality*, by analogy with the classical $(\alpha+\beta)$-theorems of Mann and Kneser on the addition of integer sequences [**16**, **12**, **17**, **9**, **19**].

The $(\alpha+\beta)$-inequality was extended to second countable connected compact abelian groups by Shields [**26**], to connected locally compact abelian groups by Kneser [**13**], and to unimodular connected locally compact groups by Kemperman [**11**]. Recently an new and elegant proof of Kemperman's result was found by Ruzsa [**24**].

In the present paper we restrict ourselves to the case of a torus, asking a different question: can (2) be strengthened? Simple examples show that, in general, the answer is 'no'.

EXAMPLE 1.1. Let $\chi : \mathbb{T}^r \to \mathbb{T}$ be a non-zero character and I, J intervals on $\mathbb{T}$ of length α and β, respectively. Putting $A = \chi^{-1}(I)$ and $B = \chi^{-1}(J)$, we obtain equality in (2). (An *interval of length* $\lambda \leqslant 1$ on the one-dimensional torus $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ is the projection of an interval in $\mathbb{R}$ of length λ.)

Thus, one may hope to improve on (2) only after having excluded certain 'extremal' cases. We suggest the following conjecture (*the* $(\alpha+2\beta)$-*inequality*).

Received 24 November 1995; revised 24 April 1996 and 31 October 1997.

1991 *Mathematics Subject Classification* 11B99.

CONJECTURE 1.2. Let A and B be subsets of $\mathbb{T}^r$ and α, β, γ defined as in (1). Suppose that

$$\alpha \geqslant \beta \quad \text{and} \quad \gamma < 1. \tag{3}$$

Then either

$$\gamma \geqslant \alpha + 2\beta \tag{4}$$

or there exists a non-zero character $\chi : \mathbb{T}^r \to \mathbb{T}$ and closed intervals $I, J \subseteq \mathbb{T}$ such that

$$\begin{gathered} \chi(A) \subseteq I, \quad \chi(B) \subseteq J, \\ \text{length}(I) \leqslant \gamma - \beta, \quad \text{length}(J) \leqslant \gamma - \alpha. \end{gathered} \tag{5}$$

As a particular case, we quote a conjecture of Macbeath [**15**]: if $\alpha, \beta > 0$ and $\gamma = \alpha + \beta < 1$, then $A = \chi^{-1}(I) \setminus M$ and $B = \chi^{-1}(J) \setminus M$, where χ, I, J are as in Example 1.1 and M is a set of measure 0.

It is easy to see that the inequalities in (5) cannot be improved, and closed intervals cannot be replaced by open.

NOTATION. Here and below the subscript $\mathbb{T}$ indicates the projection from $\mathbb{R}$ to $\mathbb{T}$.

EXAMPLE 1.3. Put

$$A_1 = ([0, \alpha] \cup \{\alpha + \beta - \varepsilon\})_{\mathbb{T}}, \quad B_1 = ([0, \beta] \cup \{2\beta - \varepsilon\})_{\mathbb{T}}$$

with $0 < \varepsilon < \beta \leqslant \alpha \leqslant 1/3$. Further, let χ be an arbitrary non-zero character, $A = \chi^{-1}(A_1)$ and $B = \chi^{-1}(B_1)$. Then $\gamma = \alpha + 2\beta - \varepsilon < \alpha + 2\beta$, but for any non-zero character χ' the sets $\chi'(A)$ and $\chi'(B)$ are not contained in open intervals of length $\gamma - \beta$ and $\gamma - \alpha$, respectively; this is obvious for $\chi' = \chi$, and an easy exercise for $\chi' \neq \chi$.

In this paper we confirm Conjecture 1.2, and, in particular, the conjecture of Macbeath in the case when α is small enough and the ratio α/β is not too large. The precise formulation of our result is as follows.

THEOREM 1.4. *For any $\tau \geqslant 1$ there exists a constant $c(\tau) > 0$ such that the conjecture is valid with* (3) *replaced by*

$$\tau^{-1}\alpha \leqslant \beta \leqslant \alpha \leqslant c(\tau). \tag{6}$$

In the important particular case when $A = B$ we obtain the following.

COROLLARY 1.5. *There exists an absolute constant $c > 0$ with the following property. Let $A \subset \mathbb{T}^r$ and suppose that $\alpha = \underline{\mu}(A) \leqslant c$ and $\gamma = \underline{\mu}(A + A) < 3\alpha$. Then there exists a non-zero character $\chi : \mathbb{T}^r \to \mathbb{T}$ such that $\chi(A)$ is a subset of a closed interval of length $\gamma - \alpha$.*

The one-dimensional case of Corollary 1.5 was obtained by Moskvin, Freiman and Yudin [**18**, Lemma 2]. Our argument can be regarded as a development of their method. In particular, like them we make an essential use of Freiman's fundamental theorem on the addition of finite sets, quoted here as Lemma 2.2.4 (see the proof of Proposition 3.3). Some new ideas were needed for extending the argument to arbitrary dimension and distinct summands; for the latter purpose we used a result of Ruzsa [**25**], based on the ideas of Plünnecke [**20**].

In Section 2 we collect miscellaneous auxiliary facts to be used in the argument. In Section 3 we prove Lemma 3.1, which can be considered as a crude version of Theorem 1.4. The proof of Theorem 1.4 occupies Section 4.

2. *Auxiliary material*

2.1. *Convex bodies*

In this subsection $S \subset \mathbb{R}^s$ is a *symmetric convex body*, that is, a convex bounded set, symmetric with respect to the origin, and containing a neighbourhood of the origin.

The *S-norm* on $\mathbb{R}^s$ is defined by $\|\underline{x}\|_S = \inf\{\lambda : \lambda^{-1}\underline{x} \in S\}$. The *S-norm of a linear functional* $\phi : \mathbb{R}^s \to \mathbb{R}$ is $\|\phi\|_S = \sup\{|\phi(\underline{x})| : \|\underline{x}\|_S \leqslant 1\}$. The kth successive minimum λ_k is the smallest λ with the following property: there exist linearly independent $e_1, \dots, e_k \in \mathbb{Z}^s$ such that $\|e_i\|_S \leqslant \lambda$. Recall the second inequality of Minkowski:

$$2^s/s! \leqslant \lambda_1 \cdots \lambda_s \operatorname{Vol} S \leqslant 2^s.$$

Let Γ be a lattice in $\mathbb{R}^s$. We say that S is Γ-*thick* if the set $S \cap \Gamma$ generates a finite index subgroup of Γ. We shall say simply *thick* instead of $\mathbb{Z}^s$-*thick*.

LEMMA 2.1.1 (Mahler). *Let $\lambda_1, \dots, \lambda_s$ be the successive minima of S. Then there exists a basis $e_1, \dots, e_s$ of $\mathbb{Z}^s$ such that*

$$\lambda_i \leqslant \|e_i\|_S \leqslant \max(1, i/2)\,\lambda_i \quad \text{for } 1 \leqslant i \leqslant s. \tag{7}$$

Proof. See [**3**, Chapter 8, Corollary of Theorem 7]. Actually, it is proved there that there exists a basis with $\|e_i\|_S \leqslant \max(1, i/2)\,\lambda_i$. However, we may assume that $\|e_1\|_S \leqslant \dots \leqslant \|e_s\|_S$, rearranging $e_1, \dots, e_s$ if necessary. Then $\|e_i\|_S \geqslant \lambda_i$ by the definition of successive minima.

Any basis with this property will be referred to as a *Mahler's basis for S*. Similarly one defines Mahler's bases for S of an arbitrary lattice Γ.

REMARK 2.1.2. It is natural to make the following remark, though it is irrelevant to the topic of this paper. We do not know whether $\max(1, i/2)$ in Mahler's lemma can be improved, but it certainly cannot be replaced by 1, because, starting from dimension 3, there exist thick symmetric convex bodies containing no basis of the integral lattice. Here is a simple example in dimension 3: put

$$a_1 = (0, 1, 1), \quad a_2 = (1, 0, 1), \quad a_3 = (1, 1, 0),$$

and let S be the convex hull of $\{\pm a_1, \pm a_2, \pm a_3\}$. Then S contains no integral points except the origin and $\pm a_1, \pm a_2, \pm a_3$, and the lattice generated by a_1, a_2, a_3 has index 2 in $\mathbb{Z}^3$. Similar examples can be constructed in the higher dimensions.

ASSUMPTION. All implicit constants in this subsection depend only on the dimension s.

PROPOSITION 2.1.3. *Let $e_1, \dots, e_s$ be a Mahler basis for S and let*

$$\underline{x} = x_1 e_1 + \cdots + x_s e_s.$$

Then

$$x_i \ll \lambda_i^{-1} \|\underline{x}\|_S \quad \text{for } 1 \leqslant i \leqslant s. \tag{8}$$

Proof. Assuming that the basis $e_1, \dots, e_s$ is orthonormal, we write $(\underline{x}, e_i)$ instead of x_i. We have to prove that $\beta_i \lambda_i \ll 1$, where $\beta_i = \max\{(\underline{x}, e_i)/\|\underline{x}\|_S : \underline{x} \in \mathbb{R}\}$.

Fix i and find $a_i \in \mathbb{R}^s$ satisfying $\|a_i\|_S = 1$ and $(a_i, e_i) = \beta_i$. Denote by S_i the convex hull of $2s$ points, two of them being $\pm a_i$ and the remaining $2(s-1)$ are $\pm e_j/\|e_j\|_S$, where $j \neq i$. Clearly, $S_i \subseteq S$. Consequently,

$$\operatorname{Vol} S \geqslant \operatorname{Vol} S_i = \frac{2^s \beta_i \|e_i\|_S}{s! \|e_1\|_S \cdots \|e_s\|_S} \gg \frac{\beta_i \lambda_i}{\lambda_1 \cdots \lambda_s} \gg \beta_i \lambda_i \operatorname{Vol} S,$$

whence $\beta_i \lambda_i \ll 1$, as desired.

PROPOSITION 2.1.4. *Let S be thick. Then*

$$\operatorname{Vol} S \ll |S \cap \mathbb{Z}^s| \ll \operatorname{Vol} S. \tag{9}$$

Proof. If $x_1 e_1 + \cdots + x_s e_s \in S$ then $|x_i| \leqslant \beta_i$, where the β_i were defined in the previous proof. Therefore

$$|S \cap \mathbb{Z}^s| \leqslant (2\beta_1 + 1) \cdots (2\beta_s + 1).$$

Since S is thick, $\lambda_i \leqslant 1$. Therefore $\beta_i \gg \lambda_i^{-1} \geqslant 1$, whence $2\beta_i + 1 \ll \beta_i$. We obtain

$$|S \cap \mathbb{Z}^s| \ll \beta_1 \cdots \beta_s \ll (\lambda_1 \cdots \lambda_s)^{-1} \ll \operatorname{Vol} S.$$

Further, if $\max_i |x| \|e_i\|_S \leqslant (2s)^{-1}$ then $\underline{x} = x_1 e_1 + \cdots + x_s e_s \in S$, because $\|\underline{x}\|_S \leqslant 1/2$. Therefore

$$|S \cap \mathbb{Z}^s| \geqslant \prod_{i=1}^{s} [2(2s\|e_i\|_S)^{-1} + 1] \gg (\|e_1\|_S \cdots \|e_s\|_S)^{-1} \gg (\lambda_1 \cdots \lambda_s)^{-1} \gg \operatorname{Vol} S.$$

The proposition is proved.

REMARK 2.1.5. Note that the assumption 'S is thick' is needed only for the second inequality in (9).

Actually, much more precise estimates for the number of lattice points are available. See [**8**, Section 3.1] and references there.

2.2. *Addition of finite sets*

We quote here some results on the addition of finite sets of integers, to be used in our argument.

ASSUMPTION. In this subsection A and B are finite sets of integers.

We denote by $\min A$ and $\max A$ the minimal and the maximal element and put

$$\begin{gathered} l(A) = \max A - \min A, \quad m(A) = \max\{|a| : a \in A\}; \\ \gcd(A) \text{ denotes the greatest common divisor of the elements of } A. \end{gathered} \tag{10}$$

LEMMA 2.2.1 (Ruzsa). *If $|A + B| \leqslant \sigma |B|$ then $|A + A| \leqslant \sigma^3 |B|$.*

Proof. Ruzsa [**23**, Lemma 3.3] proves that, if $|A+B| \leqslant \sigma|B|$, then for any positive integers k and l we have

$$\left|(\underbrace{A+\cdots+A}_{k})-(\underbrace{A+\cdots+A}_{l})\right| \leqslant \sigma^{k+l}|B|.$$

In particular, $|A+A-A| \leqslant \sigma^3|B|$, which yields $|A+A| \leqslant \sigma^3|B|$.

Ruzsa utilizes the graph-theoretic method of Plünnecke [**20**] (see also [**22**, **19**]).

LEMMA 2.2.2 (Freiman). *Suppose that* $0 \in A \cap B$ *and* $\gcd(A \cup B) = 1$. *Then*
(a) *if* $l(B) \leqslant l(A) \leqslant |A|+|B|-3$, *then* $|A+B| \geqslant l(A)+|B|$;
(b) *if* $\max(l(A), l(B)) \geqslant |A|+|B|-2$, *then* $|A+B| \geqslant |A|+|B|+\min(|A|,|B|)-3$.

Proof. See Freiman [**4**]. Simpler proofs were recently suggested by Steinig [**28**], Lev and Smeliansky [**14**, Theorem 2] and Hamidoune [**10**]. See also Stanchescu [**27**].

PROPOSITION 2.2.3. *Suppose that* $0 \in A \cap B$. *Then*
(a) *if* $\gcd(A) = \gcd(B) = 1$ *and* $\max(l(A), l(B)) \leqslant |A|+|B|-3$, *then* $|A+B| \geqslant l(A)+|B|$ (*and* $|A+B| \geqslant l(B)+|A|$ *by symmetry*);
(b) *if* $\gcd(A \cup B) = 1$, *but* $\gcd(B) > 1$, *then* $|A+B| \geqslant |A|+2|B|-2$.

Proof. (a) Without restricting generality we may assume that $\min B = 0$. Put

$$a = \max A, \quad B' = B \cap [0, l(A)], \quad B'' = B \setminus B'.$$

Then the sets A and B' meet the condition of Lemma 2.2.2(a), whence $|A+B'| \geqslant l(A)+|B'|$.

Further, the sets $A+B'$ and $a+B''$ are disjoint: any element of the former is smaller than any element of the latter. Therefore

$$|A+B| \geqslant |A+B'|+|a+B''| \geqslant l(A)+|B'|+|B''| = l(A)+|B|.$$

(b) See [**14**, Lemma 2].

LEMMA 2.2.4 (Freiman). *Suppose that* $0 \in A$ *and* $|A+A| \leqslant \sigma|A|$, *where* σ *is a positive real number. Then there exist an integer* $s \leqslant c_1(\sigma)$, *a thick symmetric convex body* $S \subset \mathbb{R}^s$ *and a homomorphism* $\phi: \mathbb{Z}^s \to \mathbb{Z}$ *such that* $\operatorname{Vol} S \leqslant c_2(\sigma)|A|$ *and* $\phi(S \cap \mathbb{Z}^s) \supseteq A$.

Proof. This is a fundamental result of Freiman [**5**, **6**]. A different (and simpler) proof was recently suggested by Ruzsa [**25**]. See also [**19**] for an exposition of Ruzsa's proof, and [**1**] for a proof close to Freiman's original.

The following proposition is a useful complement to Lemma 2.2.4.

PROPOSITION 2.2.5. *In Lemma* 2.2.4 *the convex body* S *can be chosen so that* $\|\phi\|_S = m(A)$.

Proof. Put $S' = S \cap \{x \in \mathbb{R}^s : \phi(x) \leqslant m(A)\}$. Obviously, $\phi(S' \cap \mathbb{Z}^s) \supseteq A$ but we cannot directly replace S by S' since the latter may be not thick.

Thus, let $\mathscr{L}$ be the subspace of $\mathbb{R}^s$ spanned by $S' \cap \mathbb{Z}^s$. Put $S'' = S' \cap \mathscr{L}$ and $\Gamma = \mathbb{Z}^s \cap \mathscr{L}$. Then by Proposition 2.1.4

$$\frac{\mathrm{Vol}_{\mathscr{L}}(S'')}{\det \Gamma} \ll |S'' \cap \Gamma| \leqslant |S \cap \mathbb{Z}^s| \ll \mathrm{Vol}\, S \ll |A|,$$

where all implicit constants depend only on σ. Obviously, S'' is Γ-thick and $\|\phi''\|_{S''} = m(A)$, where $\phi'' = \phi|_{\mathscr{L}}$. Identifying $\mathscr{L}$ with $\mathbb{R}^{\dim \mathscr{L}}$ and Γ with $\mathbb{Z}^{\dim \mathscr{L}}$, we obtain the result.

3. *The main lemma*

It is well known that the following three properties of a set $A \subseteq \mathbb{T}^r$ are equivalent:

(J1) $\mu(\partial A) = 0$, where ∂A is the boundary of A;

(J2) the indicator function of A (which is 1 on A and 0 outside A) is Riemann integrable;

(J3) for any infinite sequence $\{a_k\}_{k \in \mathbb{Z}}$ uniformly distributed on $\mathbb{T}^r$ we have

$$\lim_{N \to \infty} \frac{|\{k \in \mathbb{Z} : a_k \in A \text{ and } |k| \leqslant N\}|}{2N} = \mu(A).$$

Sets with any of these properties are usually called *Jordan-measurable*. For brevity, we refer to them as *Jordan sets*.

The goal of this section is the following lemma.

LEMMA 3.1. *Let $A \subset \mathbb{T}^r$ be a non-empty open Jordan set with $\mu(A) = \alpha$. Assume that $A + A$ is also a Jordan set, and that $\mu(A + A) \leqslant \sigma\mu(A)$, where σ is a positive real number. Then there exists a non-zero character χ such that $\chi(A)$ lies in an interval of length $O(\alpha^{c_1})$, where $c_1 = c_1(\sigma) > 0$ and the constant implied by the $O(\ldots)$ depends only on σ.*

For any $\theta \in \mathbb{T}^r$ and $A \subset \mathbb{T}^r$ put

$$\mathscr{B}(\theta, A) = \{n \in \mathbb{Z} : \theta n \in A\}.$$

For any $N > 0$ we also put

$$\mathscr{B}(\theta, A, N) = \mathscr{B}(\theta, A) \cap (-N, N).$$

For $\eta \in \mathbb{T}$ and $\varepsilon > 0$ we write

$$\mathscr{B}(\eta, \varepsilon) = \mathscr{B}(\eta, [-\varepsilon, \varepsilon]_{\mathbb{T}}), \quad \mathscr{B}(\eta, \varepsilon, N) = \mathscr{B}(\eta, [-\varepsilon, \varepsilon]_{\mathbb{T}}, N).$$

REMARK 3.2. Sets $\mathscr{B}(\theta, A)$ with an open A are called *Bohr sets*; they generate Bohr's topology on $\mathbb{Z}$. An efficient application of Bohr sets to additive problems was recently given by Ruzsa [**25**]. See also [**7**, **2**].

Call an element θ of $\mathbb{T}^r$ *generic* if it does not belong to a proper closed subgroup of $\mathbb{T}^r$. In these terms the theorems of Kronecker and Weyl can be expressed as follows:

(Kronecker) *if θ is generic in $\mathbb{T}^r$ and A is an open subset of $\mathbb{T}^r$, then $\theta\mathscr{B}(\theta, A)$ is dense in A,*

(Weyl) *if θ is generic in $\mathbb{T}^r$ and A is a Jordan subset of $\mathbb{T}^r$, then $\mathbf{d}\mathscr{B}(\theta, A) = \mu(A)$.*

(Recall that the *asymptotic density* $\mathbf{d}X$ of a set $X \subset \mathbb{Z}$ is $\lim_{N\to\infty}(2N)^{-1}|X\cap(-N,N)|$, provided that the limit exists.)

For the proof of Lemma 3.1 we may assume, preserving generality, that $0_{\mathbb{T}^r}\in A$.

ASSUMPTIONS. Until the end of this section, A is an open Jordan subset of $\mathbb{T}^r$, such that $A+A$ is also a Jordan set, and

$$\mu(A)=\alpha, \quad \mu(A+A)\leqslant\sigma\alpha, \quad 0_{\mathbb{T}^r}\in A.$$

In this section constants implied by $\ll, \gg$ and $O(\ldots)$ depend only on σ.

PROPOSITION 3.3. *Let $\theta\in\mathbb{T}^r$ be generic. For any $N\geqslant N_0$ (where $N_0>0$ depends on A and θ) there exist $\eta=\eta(N)\in\mathbb{T}$ and $\varepsilon=\varepsilon(N)>0$ such that*

$$\mathscr{B}(\theta,A,N)\subseteq\mathscr{B}(\eta,\varepsilon), \tag{11}$$

$$\alpha\ll\varepsilon\ll\alpha^{c_1}, \tag{12}$$

where $c_1=c_1(\sigma)>0$. Moreover, for any $X, N\geqslant N_0$ we have

$$|\mathscr{B}(\eta(N),2\varepsilon(N),X)|\ll\alpha^{c_1}X. \tag{13}$$

Proof. For any $N>0$ put $N^*=\max\mathscr{B}(\theta,A,N)$. Since A is open,

$$\gcd(\mathscr{B}(\theta,A,N))=1 \quad\text{and}\quad N\leqslant 2N^*, \tag{14}$$

when N is large enough. By the theorem of Weyl, for all sufficiently large N we have

$$|\mathscr{B}(\theta,A,N)|\geqslant\tfrac{1}{2}\alpha N, \quad |\mathscr{B}(\theta,A+A,2N)|\leqslant 3\mu(A+A)\,N. \tag{15}$$

Now define N_0 so that (14) and (15) hold for all $N\geqslant N_0$, and assume that $N\geqslant N_0$ in the sequel. By (15)

$$|\mathscr{B}(\theta,A,N)+\mathscr{B}(\theta,A,N)|\leqslant|\mathscr{B}(\theta,A+A,2N)|\leqslant 6\sigma|\mathscr{B}(\theta,A,N)|.$$

Since $0_{\mathbb{T}^r}\in A$, we have $0\in\mathscr{B}(\theta,A,N)$. By Lemma 2.2.4 together with Proposition 2.2.5, there exist an integer $s\ll 1$, a thick symmetric convex body $S\subset\mathbb{R}^s$ and a homomorphism $\phi:\mathbb{Z}^s\to\mathbb{Z}$ such that

$$\operatorname{Vol}S\ll|\mathscr{B}(\theta,A,N)|\ll\alpha N, \quad \phi(S\cap\mathbb{Z}^s)\supseteq\mathscr{B}(\theta,A,N), \quad \|\phi\|_S\leqslant N. \tag{16}$$

Since $\gcd(\mathscr{B}(\theta,A,N))=1$, the homomorphism ϕ is surjective.

If $s=1$ then $\phi:\mathbb{Z}\to\mathbb{Z}$ is either the identity map or the negation. In both the cases $S\supseteq[-N^*,N^*]$, whence

$$N\leqslant 2N^*\leqslant\operatorname{Vol}S\ll\alpha N.$$

Thus, $\alpha\gg 1$, and the assertion is trivial with $\varepsilon=1/2$ and any $\eta\in\mathbb{T}$.

Now suppose that $s\geqslant 2$. Since $\phi:\mathbb{Z}^s\to\mathbb{Z}$ is surjective, $\phi(e_0)=1$ for some $e_0\in\mathbb{Z}^s$. Prolong ϕ by linearity to a linear functional on $\mathbb{R}^s$ and put

$$\mathscr{L}=\ker\phi, \quad \Gamma=\mathscr{L}\cap\mathbb{Z}^s, \quad S_0=S\cap\mathscr{L}.$$

Let $e_1,\ldots,e_{s-1}$ be a Mahler basis for S_0 with respect to the lattice Γ. Obviously, $e_0,e_1,\ldots,e_{s-1}$ is a basis of $\mathbb{Z}^s$.

We have $\phi(x_0e_0+\ldots x_{s-1}e_{s-1})=x_0$. Define $\psi:\mathbb{R}^s\to\mathbb{R}$ by

$$\psi(x_0e_0+x_1e_1+\ldots x_{s-1}e_{s-1})=x_1$$

(recall that $s\geqslant 2$). Since $e_0,e_1,\ldots,e_{s-1}$ is a basis of $\mathbb{Z}^s$, we have $\psi(\underline{x})\in\mathbb{Z}$ for any $\underline{x}\in\mathbb{Z}^s$.

Let ψ_0 be the restriction of ψ to $\mathscr{L}$ and let $\underline{v} \in S \cap \mathbb{Z}^s$ be such that $\phi(\underline{v}) = N^*$. Put $\varepsilon = 3\|\psi_0\|_{S_0}$ and $\eta' = \psi(\underline{v})/N^*$. Then

$$\|\eta'\phi - \psi\|_S \leqslant \varepsilon. \tag{17}$$

Indeed, fix $\underline{x} \in \mathbb{R}^s$ and put $\underline{y} = (\phi(x)/N^*)\underline{v}$. Then $\underline{y} - \underline{x} \in \mathscr{L}$ and $\|\underline{y}\|_S \leqslant 2\|\underline{x}\|_S$ because

$$|\phi(\underline{x})| \leqslant \|\phi\|_S \|\underline{x}\|_S \leqslant N\|\underline{x}\|_S \leqslant 2N^*\|\underline{x}\|_S.$$

(recall that $\|\phi\|_S \leqslant N$ by (16)). We obtain

$$|(\eta'\phi - \psi)(x)| = |\psi(\underline{y} - \underline{x})| = |\psi_0(\underline{y} - \underline{x})| \leqslant \|\psi_0\|_{S_0} \|\underline{y} - \underline{x}\|_{S_0} \leqslant \tfrac{1}{3}\varepsilon \|\underline{y} - \underline{x}\|_S \leqslant \varepsilon |\underline{x}|_S,$$

which proves (17).

Put $\eta = \eta'_{\top}$. We have to establish (11)–(13).

Proof of (11). Fix $n \in \mathscr{B}(\theta, A, N)$. There exists $\underline{x} \in S \cap \mathbb{Z}^s$ such that $\phi(\underline{x}) = n$. By (17)

$$|\eta' n - \psi(x)| = |(\eta'\phi - \psi)(x)| \leqslant \varepsilon \|\underline{x}\|_S \leqslant \varepsilon.$$

Since $\psi(\underline{x}) \in \mathbb{Z}$, we obtain $n \in \mathscr{B}(\eta, \varepsilon)$.

Proof of (12). Redefine the inner product on $\mathbb{R}^s$ to make the basis $e_0, e_1, \ldots, e_{s-1}$ orthonormal. The restriction of this inner product to $\mathscr{L}$ induces a Lebesgue measure on $\mathscr{L}$, which will be denoted by $\mathrm{Vol}_{\mathscr{L}}$. Since $e_1, \ldots, e_{s-1}$ is an orthonormal basis of $\mathscr{L}$, we have $\det \Gamma = 1$.

The volume of the convex hull of S_0 and $\pm\underline{v}$ is $2s^{-1}N^* \mathrm{Vol}_{\mathscr{L}} S_0$. Since this convex hull is contained in S, we have $\alpha N \gg \mathrm{Vol}\, S \gg N \mathrm{Vol}_{\mathscr{L}} S_0$. Hence $\mathrm{Vol}_{\mathscr{L}} S_0 \ll \alpha$. Now by Proposition 2.1.3, for any $\underline{x} \in \mathscr{L}$ we have

$$|\psi_0(\underline{x})|/\|\underline{x}\|_{S_0} \ll \lambda_1^{-1} \ll (\mathrm{Vol}_{\mathscr{L}} S_0)^{1/(s-1)} \ll \alpha^{1/(s-1)} \ll \alpha^{c_1},$$

where λ_1 is the first successive minimum of S_0 with respect to Γ. This shows that $\varepsilon \ll |\psi_0|_{S_0} \ll \alpha^{c_1}$.

We now prove that $\varepsilon \gg \alpha$. For any $T > 0$ let Σ_T be the domain in $\mathbb{R}^2$ defined by the inequalities $|x| \leqslant T$ and $|\eta' x - y| \leqslant \varepsilon$. By (16) and (17), for any $\underline{x} \in S \cap \mathbb{Z}^s$ the point $(\phi(\underline{x}), \psi(\underline{x}))$ belongs to $\Sigma_N \cap \mathbb{Z}^2$. Since S is thick, so is Σ_N. By Proposition 2.1.4,

$$\alpha N \ll |\mathscr{B}(\theta, A, N)| \leqslant |\mathscr{B}(\eta, \varepsilon, N)| \leqslant |\Sigma_N \cap \mathbb{Z}^2| \ll \mathrm{Vol}\, \Sigma_N = 2\varepsilon N,$$

which proves that $\varepsilon \gg \alpha$.

Proof of (13). Now let Σ_T be the domain in $\mathbb{R}^2$ defined by the inequalities $|x| \leqslant T$ and $|\eta' x - y| \leqslant 2\varepsilon$. If Σ_X is thick, then by Proposition 2.1.4

$$|\mathscr{B}(\eta, 2\varepsilon, X)| \leqslant |\Sigma_X \cap \mathbb{Z}^2| \ll \mathrm{Vol}\, \Sigma_X = 8\varepsilon X \ll \alpha^{c_1} X,$$

as wanted.

Now suppose that Σ_X is not thick. Put $Y = \min\{T : \Sigma_T \text{ is thick}\}$. Then there is a line Λ in $\mathbb{R}^2$ such that $\Sigma_T \cap \mathbb{Z}^2 \subset \Lambda$ for any positive $T < Y$; in particular, $\Sigma_X \cap \mathbb{Z}^2 \subset \Lambda$. Since Σ_N is thick, $Y \leqslant N$.

For any $n \in \mathscr{B}(\eta, \varepsilon, Y)$, the vertical line $x = n$ intersects Λ inside the strip $|\eta' x - y| \leqslant \varepsilon$ (the intersection point is (n, m), where m is the nearest integer to $\eta' n$). In particular, this is the case for $n = Y^*$, because

$$Y^* = \max \mathscr{B}(\theta, A, Y) \in \mathscr{B}(\theta, A, N) \cap (-Y, Y) \subset \mathscr{B}(\eta, \varepsilon, Y).$$

Since $Y > X \geqslant N_0$, we have $Y \leqslant 2Y^*$, whence the vertical line $x = Y$ intersects Λ inside the strip $|\eta' x - y| \leqslant 2\varepsilon$. It follows that for any positive $T \leqslant Y$ we have $\mathscr{B}(\eta, 2\varepsilon, T) = \mathrm{H} \cap (-T, T)$, where H is the projection of $\Lambda \cap \mathbb{Z}^2$ on the first coordinate.

Let a be the positive generator of H. If $X < a$ then $\mathscr{B}(\eta, 2\varepsilon, X) = \{0\}$ and there is nothing to prove. If $X \geqslant a$ then

$$\frac{|\mathscr{B}(\eta, 2\varepsilon, X)|}{X} = \frac{|\mathrm{H} \cap (-X, X)|}{X} \ll \frac{|\mathrm{H} \cap (-Y, Y)|}{Y} \leqslant \frac{|\Sigma_Y \cap \mathbb{Z}^2|}{Y} \ll \frac{\mathrm{Vol}\,\Sigma_Y}{Y} = 8\varepsilon \ll \alpha^{c_1}.$$

This completes the proof of (13) and of Proposition 3.3.

PROPOSITION 3.4. *As in Proposition* 3.3, *let θ be generic. Then there exist $\eta \in \mathbb{T}$ and a positive $\varepsilon \ll \alpha^{c_1}$ such that $\mathscr{B}(\theta, A) \subseteq \mathscr{B}(\eta, \varepsilon)$ and $\mathbf{d}\mathscr{B}(\eta, \varepsilon) \ll \alpha^{c_1}$.*

Proof. For all $N \geqslant N_0$, let $\eta(N)$ and $\varepsilon(N)$ be the quantities defined in Proposition 3.3. There is a sequence $N_j \to \infty$ such that the sequences $\{\eta_j\}$ and $\{\varepsilon_j\}$ converge (where we write $\eta_j = \eta(N_j)$ and $\varepsilon_j = \varepsilon(N_j)$). Denote by η and ε the corresponding limits. Then $\alpha \ll \varepsilon \ll \alpha^{c_1}$, in particular $\varepsilon > 0$.

Further, fix $n \in \mathscr{B}(\theta, A)$. Then $n\eta_j \in [-\varepsilon_j, \varepsilon_j]_{\mathbb{T}}$ for all sufficiently large j. Therefore $n\eta \in [-\varepsilon, \varepsilon]_{\mathbb{T}}$, which proves that $\mathscr{B}(\theta, A) \subseteq \mathscr{B}(\eta, \varepsilon)$.

To estimate the asymptotic density of $\mathscr{B}(\eta, \varepsilon)$, fix $X \geqslant N_0$. For sufficiently large j we have $N_j \geqslant X$ and $\varepsilon_j \geqslant \varepsilon/\sqrt{2}$. Also, for any $n \in \mathscr{B}(\eta, \varepsilon, X)$ we have $n\eta_j \to n\eta \in [-\varepsilon, \varepsilon]_{\mathbb{T}}$, whence

$$n\eta_j \in [-\varepsilon\sqrt{2}, \varepsilon\sqrt{2}]_{\mathbb{T}} \subseteq [-2\varepsilon_j, 2\varepsilon_j]_{\mathbb{T}}$$

when j is large enough. Thus, $\mathscr{B}(\eta, \varepsilon, X) \subset \mathscr{B}(\eta_j, 2\varepsilon_j, X)$ for all sufficiently large j. By (13),

$$\frac{|\mathscr{B}(\eta, \varepsilon, X)|}{X} \leqslant \frac{|\mathscr{B}(\eta_j, 2\varepsilon_j, X)|}{X} \ll \alpha^{c_1}.$$

Sending X to infinity, we obtain $\mathbf{d}\mathscr{B}(\eta, \varepsilon) \ll \alpha^{c_1}$. The proposition is proved.

Proof of Lemma 3.1. Fix a generic $\theta \in \mathbb{T}^r$ and let η and ε be from Proposition 3.4.

CLAIM 1. *If η is not generic in $\mathbb{T}$ then $\alpha \gg 1$.*

Proof. If η is not generic, then it belongs to the torsion of $\mathbb{T}$, say, $m\eta = 0$ for some non-zero $m \in \mathbb{Z}$. In this case $\mathscr{B}(\eta, \varepsilon)$ is a union of several complete residue classes $\bmod m$. Since A is open, $\mathscr{B}(\theta, A)$ intersects all residue classes $\bmod m$. Therefore $\mathscr{B}(\eta, \varepsilon) = \mathbb{Z}$. This yields $\alpha \gg 1$ since $\mathbf{d}\mathscr{B}(\eta, \varepsilon) \ll \alpha^{c_1}$.

To simplify notation, put $I = [-\varepsilon, \varepsilon]_{\mathbb{T}}$.

CLAIM 2. *If (θ, η) is generic in $\mathbb{T}^r \times \mathbb{T}$, then $\alpha \gg 1$.*

Proof. Suppose that (θ, η) is generic. Then $\mathbf{d}\mathscr{B}((\theta, \eta), A \times I) = 2\varepsilon\mu(A)$ by the theorem of Weyl. On the other hand, since $\mathscr{B}(\theta, A) \subseteq \mathscr{B}(\eta, \varepsilon)$, we have

$$\mathscr{B}((\theta, \eta), A \times I) = \mathscr{B}(\theta, A),$$

whence $\mathbf{d}\mathscr{B}((\theta, \eta), A \times I) = \mu(A)$. Thus, $2\varepsilon = 1$, which yields $\alpha \gg 1$.

The assertion of Lemma 3.1 is trivial when $\alpha \gg 1$. Hence we may assume that η is generic but (θ, η) is not. Since (θ, η) is not generic, there exist a character $\chi: \mathbb{T}^r \to \mathbb{T}$ and an integer m, not both zero, such that $\chi(\theta) = m\eta$. Moreover, both χ and m are non-zero, because both η and θ are generic. We define the pair (χ, m) in a unique way requiring that m is positive and as small as possible.

CLAIM 3. *If $m > 1$ then $\alpha \gg 1$.*

Proof. Let Δ be the subgroup of $\mathbb{T}^r \times \mathbb{T}$ consisting of (x, y) satisfying $\chi(x) = my$. Then $(\theta, \eta) \in \Delta$, and by the minimality of m, the element (θ, η) is generic in Δ.

Denote by $\pi_1: \Delta \to \mathbb{T}^r$ and $\pi_2: \Delta \to \mathbb{T}$ the projections to the first and second coordinate, respectively. Put $U = \pi_1^{-1}(A)$. Then $\mathscr{B}(\theta, A) = \mathscr{B}((\eta, \theta), U)$. By the theorem of Kronecker, $(\eta, \theta)\mathscr{B}(\theta, A)$ is dense in U. It follows that $\eta\mathscr{B}(\theta, A)$ is dense in $\pi_2(U)$. On the other hand, $\eta\mathscr{B}(\theta, A) \subseteq \eta\mathscr{B}(\eta, \varepsilon) \subset I$. Therefore $\pi_2(U) \subset I$.

For any $x \in \pi_2(U)$ we have $x + Z_m \subset \pi_2(U)$, where $Z_m < \mathbb{T}$ is the cyclic subgroup of order m. If $m > 1$ then the set $x + Z_m$ is not contained in an interval shorter than $1 - m^{-1} \geqslant 1/2$. Consequently, $2\varepsilon \geqslant 1/2$, whence $\alpha \gg 1$.

Thus, we may assume that $m = 1$, whence $\chi(\theta) = \eta$. It follows that $\chi(\theta\mathscr{B}(\theta, A)) \subseteq \eta\mathscr{B}(\eta, \varepsilon) \subset I$. Again by the theorem of Kronecker, $\theta\mathscr{B}(\theta, A)$ is dense in A, and we obtain finally $\chi(A) \subseteq I$. The lemma is proved.

4. *Proof of Theorem* 1.4

To begin, we fix some conventions. In this section $A, B \subset \mathbb{T}^r$. We define α, β and γ as in (1) and fix $\tau \geqslant 1$. We put $C = A \cup B$. We assume that

$$\tau^{-1}\alpha \leqslant \beta \leqslant \alpha, \quad \gamma < \alpha + 2\beta.$$

We can assume that $0_{\mathbb{T}^r} \in A \cap B$, translating A and B if necessary. Further, if $\beta = 0$ then trivially $\gamma \geqslant \alpha + 2\beta$. Therefore $\gamma > \alpha \geqslant \beta > 0$.

All constants implied by the symbols $\ll$, $\gg$ and $O(\ldots)$ depend only on τ.

4.1. *Open Jordan sets*

In this subsection we assume that the sets A, B, $A + A$, $A + B$ and $B + B$ are open Jordan sets. Then C and $C + C$ are open Jordan sets as well. As in Section 3, fix a generic $\theta \in \mathbb{T}^r$.

PROPOSITION 4.1.1. *For sufficiently large N we have the inequality*

$$|\mathscr{B}(\theta, C, N) + \mathscr{B}(\theta, C, N)| \geqslant \tfrac{1}{5}\mu(C + C)\, N. \tag{18}$$

Proof. Since $C + C$ is Jordan and $\mu(C + C) > 0$, there exists a closed Jordan set $F \subset C + C$ such that $\mu(F) \geqslant \frac{1}{2}\mu(C + C)$. Since $\theta\mathscr{B}(\theta, C)$ is dense in C, we have

$$F \subset C + C \subseteq \bigcup_{n \in \mathscr{B}(\theta, C)} (\theta n + C).$$

Since F is compact, for some $N_0 > 0$ we have

$$F \subset \bigcup_{n \in \mathscr{B}(\theta, C, N_0)} (\theta n + C). \tag{19}$$

Now pick $n\in\mathscr{B}(\theta,F)$. By (19), there exists $n_1\in\mathscr{B}(\theta,C,N_0)$ such that $n\theta-n_1\theta\in C$. Then $n-n_1\in\mathscr{B}(\theta,C)$ and $|n-n_1|\leqslant|n|+N_0$. Therefore for any $N>N_0$ we have

$$\mathscr{B}(\theta,F,N-N_0)\subseteq\mathscr{B}(\theta,C,N-N_0)+\mathscr{B}(\theta,C,N)\subseteq\mathscr{B}(\theta,C,N)+\mathscr{B}(\theta,C,N). \quad (20)$$

On the other hand, since F is Jordan, for sufficiently large N we have

$$|\mathscr{B}(\theta,F,N-N_0)|\geqslant\tfrac{1}{2}\mu(F)\,(N-N_0)\geqslant\tfrac{1}{5}\mu(C+C)\,N, \quad (21)$$

and the result follows from (20) and (21).

PROPOSITION 4.1.2. *There exists a non-zero character $\chi:\mathbb{T}^r\to\mathbb{T}$ such that $\chi(C)\subseteq[-\varepsilon,\varepsilon]_{\mathbb{T}}$, where $0<\varepsilon\ll\alpha^{c_2}$. Here c_2 is a positive constant, depending on τ.*

Proof. For sufficiently large N we have

$$\begin{aligned}&|\mathscr{B}(\theta,A,N)|\geqslant\tfrac{1}{2}\alpha N,\quad |\mathscr{B}(\theta,B,N)\geqslant\tfrac{1}{2}\beta N,\\ &|\mathscr{B}(\theta,A+B,2N)|\leqslant 3\gamma N,\quad |\mathscr{B}(\theta,C,N)|\leqslant 2\mu(C)\,N.\end{aligned} \quad (22)$$

Now fix N such that (18) and (22) hold. Then

$$\begin{aligned}|\mathscr{B}(\theta,A,N)+\mathscr{B}(\theta,B,N)|&\leqslant|\mathscr{B}(\theta,A+B,2N)|\leqslant 3(\alpha+2\beta)\,N\\ &\leqslant\begin{cases}(6+3\tau)\,\beta N\ll|\mathscr{B}(\theta,B,N)|,\\ 9\alpha N\qquad\ \ll|\mathscr{B}(\theta,A,N)|.\end{cases}\end{aligned}$$

By Lemma 2.2.1

$$|\mathscr{B}(\theta,A,N)+\mathscr{B}(\theta,A,N)|\ll|\mathscr{B}(\theta,B,N)|,\quad |\mathscr{B}(\theta,B,N)+\mathscr{B}(\theta,B,N)|\ll|\mathscr{B}(\theta,A,N)|.$$

Hence

$$\begin{aligned}\mu(C+C)\,N&\ll|\mathscr{B}(\theta,C,N)+\mathscr{B}(\theta,C,N)|\\ &\leqslant|\mathscr{B}(\theta,A,N)+\mathscr{B}(\theta,A,N)|+|\mathscr{B}(\theta,A,N)+\mathscr{B}(\theta,B,N)|\\ &\quad+|\mathscr{B}(\theta,B,N)+\mathscr{B}(\theta,B,N)|\\ &\ll|\mathscr{B}(\theta,A,N)|+|\mathscr{B}(\theta,B,N)|\\ &\ll|\mathscr{B}(\theta,C,N)|\\ &\ll\mu(C)\,N.\end{aligned}$$

Thus, $\mu(C+C)\ll\mu(C)$. By Lemma 3.1, there exists a non-zero character χ such that $\chi(C)$ lies in an interval of length $O(\mu(C)^{c_2})$, where $c_2=c_2(\tau)>0$. Since $0_{\mathbb{T}^r}\in C$, we may assume this interval to be of the form $[-\varepsilon,\varepsilon]_{\mathbb{T}}$, where $\varepsilon\ll\mu(C)^{c_2}\ll\alpha^{c_2}$. This proves the proposition.

A character χ is *primitive* if $\ker\chi$ is connected. Any non-zero character χ can be uniquely presented as $q\chi_0$, where χ_0 is primitive and $q=q(\chi)$ a positive integer (it is equal to the number of components of $\ker\chi$).

By Proposition 4.1.2, there exists a positive $\varepsilon\ll\alpha^{c_2}$ such that $\chi(C)\subseteq[-\varepsilon,\varepsilon]_{\mathbb{T}}$ for some non-zero character χ. However, there can be several characters with this property; choose one with the *minimal value of* $q(\chi)$.

By a *coordinate system* on $\mathbb{T}^r$ we mean a system of closed one-dimensional subgroups $\mathbb{T}_1,\dots,\mathbb{T}_r$, such that $\mathbb{T}^r=\mathbb{T}_1\oplus\cdots\oplus\mathbb{T}_r$, where for any $\mathbb{T}_i$ an isomorphism $\mathbb{T}_i\cong\mathbb{T}$ is fixed. Given a coordinate system, we write an element of $\mathbb{T}^r$ as $(x_1,\dots,x_r)$, where $x_i\in\mathbb{T}$.

Write our character as $\chi = q(\chi)\chi_0$, and fix a coordinate system such that none of $\mathbb{T}_1, \dots, \mathbb{T}_r$ is a subgroup of $\ker \chi_0$. Then $\chi_0(x_1, \dots, x_r) = v_1 x_1 + \cdots v_r x_r$, where $v_1, \dots, v_r$ are non-zero integers with $\gcd(v_1, \dots, v_r) = 1$.

As in [**15**], let $P_1, \dots, P_r$ be distinct odd primes, all greater than $q = q(\chi)$, and let Z_{P_i} be the cyclic subgroup of $\mathbb{T}_i$ of order P_i. Then $G = Z_{P_1} \oplus \cdots \oplus Z_{P_r}$ is a cyclic subgroup of $\mathbb{T}^r$ of order $P = P_1 \dots P_r$. By the construction, $G \cap \ker \chi_0 = 0$, and even $G \cap \ker \chi = 0$, since $\gcd(P, q) = 1$. Therefore χ maps G isomorphically onto the cyclic group $Z_P < \mathbb{T}$.

For any $X \subset \mathbb{T}^r$ define a set of integers $\tilde{X}$ as follows:

$$\tilde{X} = \{k \in \mathbb{Z} : |k| < P/2 \text{ and } (k/P)_{\mathbb{T}} \in \chi(X \cap G)\}.$$

Obviously, $|\tilde{X}| = |X \cap G|$. It is important to notice that $|x| \leqslant \varepsilon P$ for any $x \in \tilde{C}$.

PROPOSITION 4.1.3. *If $P_1, \dots, P_r$ are sufficiently large then* $\gcd(\tilde{C}) = 1$.

Proof. Since C is open and contains the origin, it also contains the r points

$$(0_{\mathbb{T}}, \dots, 0_{\mathbb{T}}, (1/P_i)_{\mathbb{T}}, 0_{\mathbb{T}}, \dots, 0_{\mathbb{T}}) \quad \text{for } 1 \leqslant i \leqslant r,$$

provided that the P_i are large enough. Therefore $\chi(C \cap G) \supseteq \{qv_1/P_1, \dots, qv_r/P_r\}_{\mathbb{T}}$. When the P_i are large enough we have $|qv_i P/P_i| < P/2$, whence

$$\tilde{C} \supseteq \{qv_1 P/P_1, \dots, qv_r P/P_r\}.$$

It follows that $d = \gcd(\tilde{C})$ divides q, because the v_i are distinct from zero and $\gcd(v_1, \dots, v_r) = 1$.

Now write $\tilde{C} = \{dn_1, \dots, dn_k\}$. Then $|dn_i/P| \leqslant \varepsilon$, whence

$$(q/d)\chi_0(C \cap G) = \{n_1/P, \dots, n_k/P\}_{\mathbb{T}} \subset [-\varepsilon/d, \varepsilon/d]_{\mathbb{T}}.$$

We may assume $P_1, \dots, P_r$ to be so large that $\chi_0(C)$ is contained in the (ε/q)-neighbourhood of $\chi_0(C \cap G)$. It follows that $(q/d)\chi_0(C)$ is contained in the (ε/d)-neighbourhood of $(q/d)\chi_0(C \cap G)$, that is, $(q/d)\chi_0(C) \subseteq [-2\varepsilon/d,\ 2\varepsilon/d]$. From the minimality of q we conclude that $d = 1$. The proposition is proved.

PROPOSITION 4.1.4. *If $\varepsilon < 1/4$ then* $\tilde{A} + \tilde{B} \subseteq \widetilde{A+B}$.

Proof. If $a \in \tilde{A}$ and $b \in \tilde{B}$ then obviously $((a+b)/P)_{\mathbb{T}} \in \chi((A+B) \cap G)$. Since $|a| \leqslant \varepsilon P$ and $|b| \leqslant \varepsilon P$, we have $|a+b| \leqslant 2\varepsilon P < P/2$, whence $a+b \in \widetilde{A+B}$. The proposition is proved.

Since $\varepsilon \ll \alpha^{c_2}$, we have $\varepsilon < \frac{1}{4}$ when $\alpha \leqslant c_3(\tau)$. We shall assume this in the sequel. It is worth noting that this is the single point in the whole argument where we need the extra condition $\alpha \leqslant c_3(\tau)$.

Let $\delta > 0$ be so small that $\gamma + 5\delta < \alpha + 2\beta$; if $\alpha > \beta$ then we require in addition that $\alpha - \delta > \beta + \delta$. Assume that P_i are so large that

$$\delta P \geqslant 3, \quad \left|\frac{|A \cap G|}{P} - \alpha\right| \leqslant \delta, \quad \left|\frac{|B \cap G|}{P} - \beta\right| \leqslant \delta, \quad \left|\frac{|(A+B) \cap G|}{P} - \gamma\right| \leqslant \delta, \qquad (23)$$

and

(*) for any $x \in A$ (respectively, B) there exists $x' \in A \cap G$ (respectively, $B \cap G$) such that $\chi(x - x') \in [-\delta, \delta]_{\mathbb{T}}$.

We can also assume that $|\tilde{B}| \leqslant |\tilde{A}|$. Indeed, if $\beta < \alpha$ then $\beta+\delta < \alpha-\delta$, which yields $\tilde{B} < \tilde{A}$ by (23) (recall that $|\tilde{A}| = |A \cap G|$ and $|\tilde{B}| = |B \cap G|$). If $\alpha = \beta$ then the assertion is symmetric in A and B, and we can interchange them if it happens that $|\tilde{B}| > |\tilde{A}|$.

By Proposition 4.1.3 we have $\gcd(\tilde{A} \cup \tilde{B}) = 1$. Since $0_{\mathbb{T}^r} \in A \cap B$, we have $0 \in \tilde{A} \cap \tilde{B}$. Since $\tilde{A}+\tilde{B} \subseteq \widetilde{A+B}$, we have

$$|\tilde{A}+\tilde{B}| \leqslant |\widetilde{A+B}| \leqslant (\gamma+\delta)P < ((\alpha-\delta)+2(\beta-\delta)-\delta)P \leqslant |\tilde{A}|+2|\tilde{B}|-3.$$

Hence $\gcd(\tilde{A}) = \gcd(\tilde{B}) = 1$ by Proposition 2.2.3(b), and

$$\max(l(\tilde{A}), l(\tilde{B})) \leqslant |\tilde{A}|+|\tilde{B}|-3$$

by Lemma 2.2.2(b). It follows now from Proposition 2.2.3(a) that

$$l(\tilde{A}) \leqslant |\tilde{A}+\tilde{B}|-|\tilde{B}| \leqslant (\gamma-\beta+2\delta)P, \quad l(\tilde{B}) \leqslant |\tilde{A}+\tilde{B}|-|\tilde{A}| \leqslant (\gamma-\alpha+2\delta)P.$$

Therefore $\chi(A \cap G)$ is contained in an interval of length $\gamma-\beta+2\delta$. By (*), $\chi(A)$ is a subset of an interval of length $\gamma-\beta+4\delta$. Sending δ to zero, we conclude that $\chi(A)$ is contained in an interval of length $\gamma-\beta$. Similarly $\chi(B)$ is a subset of an interval of length $\gamma-\alpha$. This completes the proof of Theorem 1.4 in the case when A and B are open Jordan sets.

4.2. *Closed sets*

We begin with a very simple lemma.

LEMMA 4.2.1. *Let X be a subset of $\mathbb{T}^r$ with $\mu(X) > 0$. Then for any fixed $\lambda < 1$ there exist only finitely many characters $\chi: \mathbb{T}^r \to \mathbb{T}$ such that $\mu(\chi(X)) \leqslant \lambda$.*

Proof. We use induction in r. Thus, put $r = 1$ and let $X \subseteq \mathbb{T}$ have positive measure. Fix a density point x of X and find $\varepsilon > 0$ such that any open interval I which contains x and is of length at most ε satisfies $\mu(I \cap X) > \lambda\mu(I)$.

Any character $\chi: \mathbb{T} \to \mathbb{T}$ is the multiplication by an integer $v = v(\chi)$. If $|v| \geqslant \varepsilon^{-1}$ then we have an interval I of length v^{-1} such that $\mu(I \cap X) > \lambda\mu(I)$. The character χ maps I faithfully onto $\mathbb{T}$, whence $\mu(\chi(X)) \geqslant \mu(\chi(I \cap X)) > \lambda$. Thus, $\mu(\chi(X)) \leqslant \lambda$ yields $|v(\chi)| < \varepsilon^{-1}$, which proves the lemma in the case $r = 1$.

Now consider arbitrary $r > 1$ and present $\mathbb{T}^r$ as $\mathbb{T}^{r-1} \times \mathbb{T}$. By the theorem of Fubini, there exists $x \in \mathbb{T}^r$ such that $\mu(X \cap (x+\mathbb{T}^{r-1})) > 0$ and $\mu(X \cap (x+\mathbb{T})) > 0$. (Here we denote by μ the normalized Lebesgue measures on $x+\mathbb{T}^{r-1}$ and $x+\mathbb{T}$, respectively.) Translating X, we may assume that $x = 0_{\mathbb{T}^r}$. By induction, there are finitely many possibilities for the restrictions $\chi|_{\mathbb{T}^{r-1}}$ and $\chi|_{\mathbb{T}}$. Hence there are finitely many possibilities for χ. The lemma is proved.

In this subsection A and B are closed sets. Fix an epimorphism $\mathbb{R}^r \to \mathbb{T}^r$ and denote by $O_\varepsilon \subset \mathbb{T}^r$ the image of the open ball in $\mathbb{R}^r$ having centre in the origin and radius ε. Obviously, O_ε is an open Jordan set.

Since A and B are closed, so is $F = A+B$. Therefore

$$F = \bigcap_{\varepsilon > 0} (F+O_\varepsilon),$$

and similarly for A and B. Pick $\delta > 0$ such that $\gamma+\delta < \alpha+2\beta$ and $\alpha > \beta+\delta$ in the case $\alpha > \beta$. Let $\varepsilon = \varepsilon(\delta)$ be such that

$$\mu(B+O_\varepsilon) \leqslant \beta+\delta, \quad \mu(F+O_{2\varepsilon}) \leqslant \gamma+\delta.$$

Since A is compact, its open covering $\bigcup_{a\in A}(a+O_\varepsilon)$ has a finite subcovering. Arguing similarly with B, we obtain finite subsets $\hat{A}\subset A$ and $\hat{B}\subset B$ such that $A\subset A' := \hat{A}+O_\varepsilon$ and $B\subset B' := \hat{B}+O_\varepsilon$. Both A' and B' are open Jordan sets (each of them is a union of finitely many translates of O_ε), and so are the sets $A'+A'$, $A'+B'$ and $B'+B'$ (which are unions of finitely many translates of $O_{2\varepsilon}$). We can assume that $\mu(A')\geqslant\mu(B')$: if $\alpha>\beta$, this follows from $\alpha>\beta+\delta$; if $\alpha=\beta$, then interchange A and B if necessary.

Now

$$\mu(A'+B')\leqslant\mu(F+O_{2\varepsilon})\leqslant\gamma+\delta<\alpha+2\beta\leqslant\mu(A')+2\mu(B').$$

Therefore there exists a non-zero character χ mapping A' and B' into intervals of length $\gamma-\beta+\delta$ and $\gamma-\alpha+\delta$, respectively.

Formally, we cannot now send δ to 0, because the character χ depends on δ, so we have to write it as χ_δ. However, by Lemma 4.2.1, there are at most finitely many possibilities for χ_δ. Therefore we have a sequence $\delta_n\to 0$ such that all the χ_{δ_n} are equal to the same character χ. This completes the proof of the theorem in the case when A and B are closed.

4.3. *Arbitrary sets*

Now we make no additional assumptions about A and B. Since the closure $\bar{A}$ is compact, for any $\delta>0$ and any character χ there exists a finite set $A(\chi,\delta)\subset A$ with the following property: *for any $x\in A$ there is $x'\in A(\chi,\delta)$ such that* $\chi(x-x')\in[-\delta,\delta]_{\mathbb{T}}$. Similarly we define $B(\chi,\delta)$.

For every small $\delta>0$ we want to find a non-zero character $\chi=\chi_\delta$ mapping the sets $A(\chi,\delta)$ and $B(\chi,\delta)$ into intervals of length $\gamma-\beta+\delta$ and $\gamma-\alpha+\delta$, respectively. Such a χ would map A and B into intervals of length $\gamma-\beta+3\delta$ and $\gamma-\alpha+3\delta$, respectively, and we would be able to complete the proof using Lemma 4.2.1 in the same manner, as at the end of the previous subsection.

Thus, fix $\delta>0$ so small that $\gamma<\alpha+2\beta-3\delta$ and $\alpha-\delta>\beta$ in the case $\alpha>\beta$. Let $A'\subseteq A$ and $B'\subseteq B$ be closed sets such that $\mu(A')\geqslant\alpha-\delta$ and $\mu(B')\geqslant\beta-\delta$. Again, we may assume that $\mu(A')\geqslant\mu(B')$.

By Lemma 4.2.1, there exist only finitely many characters χ mapping A' into an interval of length $\gamma-\alpha+\delta$. Put

$$A''=A'\cup\left(\bigcup_\chi A(\chi,\delta)\right),$$

the union being over the characters quoted in the previous sentence. Since we added to the set A' only finitely many new elements, the set A'' is closed and $\mu(A'')=\mu(A')$. In the same manner define the set B''.

Since $A''+B''$ is closed, we have

$$\mu(A''+B'')\leqslant\underline{\mu}(A+B)=\gamma<(\alpha-\delta)+2(\beta-\delta)\leqslant\mu(A'')+2\mu(B'').$$

Therefore there exists a non-zero character χ mapping A'' and B'' into intervals of length $\gamma-\beta+\delta$ and $\gamma-\alpha+\delta$, respectively. This χ maps A' into an interval of length $\gamma-\beta+\delta$, whence $A(\chi,\delta)\subset A''$. Thus, χ maps $A(\chi,\delta)$ into an interval of length

$\gamma-\beta+\delta$; by the similar reason it maps $B(\chi,\delta)$ into an interval of length $\gamma-\alpha+\delta$. This completes the proof of Theorem 1.4.

Acknowledgements. I am pleased to thank Gregory Freiman for having initiated this research. Some ideas of this paper came up in our conversation. I also thank Daniel Berend, Seva Lev, and the referee for valuable suggestions.

This work was done during the author's post-doctoral stage at the Max-Planck-Institut für Mathematik. I am grateful to Prof. F. Hirzebruch and MPI für Mathematik for their kind invitation and excellent working conditions. A considerable part of the paper was written when I was visiting Macquarie University, New South Wales, Australia. I am pleased to thank the Mathematical Department of that university, and especially William W. L. Chen and Alfred J. van der Poorten for their generous hospitality.

References

1. Yu. Bilu, 'Structure of sets with small sumsets', Forschungsinst. für Math., ETH Zürich, June 1997, preprint; *Astérisque*, to appear.
2. Yu. Bilu, 'Addition of sets of integers of positive density', *J. Number Theory* 64 (1997) 233–275.
3. J. W. S. Cassels, *An introduction to the geometry of numbers* (Springer, Berlin, 1959).
4. G. A. Freiman, 'Inverse problems in additive number theory VI. On the addition of finite sets III' (Russian), *Izv. Vyss. Učebn. Zaved. Matem.* 28 (1962) 151–157.
5. G. A. Freiman, *Foundations of a structural theory of set addition* (Kazan', 1966); Translation of Mathematical Monographs 37 (American Mathematical Society, Providence, 1973).
6. G. A. Freiman, 'What is the structure of K if $K+K$ is small?, *Number Theory*, *New York* 1984–1985, Lecture Notes in Mathematics 1240 (ed. D. V. Chudnovsky, G. V. Chudnovsky, H. Cohn and M. B. Nathanson; Springer, 1987), 109–134.
7. G. A. Freiman, H. Halberstam and I. Z. Ruzsa, 'Integer sum sets containing long arithmetic progressions', *J. London Math. Soc.* (2) 46 (1992) 193–201.
8. P. Gritzmann and J. M. Wills, 'Lattice points', *Handbook of convex geometry* (ed. P. M. Gruber and J. M. Wills; North-Holland, Amsterdam, 1993) 765–797.
9. H. Halberstam and K. F. Roth, *Sequences* (Springer, New York, 1983).
10. Y. O. Hamidoune, 'On inverse additive problems', preprint EC95/01, Institut Blaise Pascal, Paris, 1995.
11. J. H. B. Kemperman, 'On products of sets in a locally compact group', *Fund. Math.* 45 (1964) 51–68.
12. M. Kneser, 'Abschätzung der asymptotischen Dichte von Summenmengen', *Math. Z.* 58 (1953) 459–484.
13. M. Kneser, 'Summenmengen in lokalkompakten abelschen Gruppen', *Math. Z.* 66 (1956) 88–110.
14. V. F. Lev and P. Y. Smeliansky, 'On addition of two distinct sets of integers', *Acta Arith.* 70 (1995) 85–91.
15. A. M. Macbeath, 'On measure of sum sets II: the sum-theorem for the torus', *Proc. Cambridge Philos Soc.* 49 (1953) 40–43.
16. H. Mann, 'A proof of the fundamental theorem on the density of sums of sets of positive integers', *Ann. Math.* 43 (1942) 523–527.
17. H. Mann, *Addition theorems: the addition theorems of group theory and number theory* (Wiley, New York, 1965).
18. D. A. Moskvin, G. A. Freiman and A. A. Yudin, 'Inverse problems of additive number theory and local limit theorems for lattice random variables', *Number-theoretic studies in the Markov spectrum and in the structural theory of set addition* (Kalinin. Gos. Univ., Moscow, 1973) 148–162.
19. M. B. Nathanson, *Additive number theory: inverse problems and the geometry of sumsets* (Springer, New York, 1996).
20. H. Plünnecke, 'Eine zahlentheoretische Anwendung der Graphentheorie', *J. Reine Angew. Math.* 243 (1970) 171–183.
21. D. A. Raikov, 'On the addition of point-sets in the sense of Shnirelman', *Mat. Sb.* 5 (1939) 425–440.
22. I. Z. Ruzsa, 'An application of graph theory to additive number theory', *Scientia*, *Ser. A* 3 (1989) 97–109.
23. I. Z. Ruzsa, 'Arithmetical progressions and the number of sums', *Period. Math. Hungar.* 25 (1992) 105–111.
24. I. Z. Ruzsa, 'A concavity property for the measure of product sets in groups', *Fund. Math.* 140 (1992) 247–254.

25. I. Z. RUZSA, 'Generalized arithmetic progressions and sumsets', *Acta Math. Hungar.* 65 (1994) 379–388.
26. A. SHIELDS, 'Sur la mesure d'une somme vectorielle', *Fund. Math.* 42 (1955) 57–60.
27. Y. STANCHESCU, 'On addition of two distinct sets of integers', *Acta Arith.* 75 (1996) 191–194.
28. J. STEINIG, 'On Freiman's theorems concerning the sum of two finite sets of integers', preprint, CIRM, Marseilles, 1993; *Astérisque*, to appear.

Mathematisches Institut
Universität Basel
Rheinsprung 21
CH-4051 Basel
Switzerland

E-mail: yuri@math.unibas.ch