Arch. Math. 98 (2012), 133–142

0003-889X/12/020133-10
published online February 2, 2012
DOI 10.1007/s00013-011-0345-z

Archiv der Mathematik

New upper bounds for the Davenport and for the Erdős–Ginzburg–Ziv constants

M. N. Chintamani, B. K. Moriya, W. D. Gao, P. Paul, and R. Thangadurai

Abstract. Let G be a finite abelian group (written additively) of rank r with invariants $n_1, n_2, \ldots, n_r$, where n_r is the exponent of G. In this paper, we prove an upper bound for the Davenport constant $\mathsf{D}(G)$ of G as follows; $\mathsf{D}(G) \leq n_r + n_{r-1} + (c(3)-1)n_{r-2} + (c(4)-1)n_{r-3} + \cdots + (c(r)-1)n_1 + 1$, where $c(i)$ is the Alon–Dubiner constant, which depends only on the rank of the group $\mathbb{Z}_{n_r}^i$. Also, we shall give an application of Davenport's constant to smooth numbers related to the Quadratic sieve.

Mathematics Subject Classification (2010). Primary 11B75; Secondary 20K01.

Keywords. Finite abelian groups, Davenport constant, Lattice point problem.

1. Introduction. Let G be a finite abelian group written additively. By the structure theorem, we know that $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ where the n_i's are integers satisfying $1 < n_1 | n_2 | \cdots | n_r$, and n_r is the *exponent* (denoted by $\exp(G)$) of G, and r is the *rank* of G. Also, $n_1, n_2, \ldots, n_r$ are called the *invariants* of G. Let

$$\mathsf{D}^*(G) = 1 + \sum_{i=1}^{r}(n_i - 1).$$

The *Davenport constant* for the finite abelian group G, denoted by $\mathsf{D}(G)$, is defined to be the least positive integer t such that any sequence of t elements of G contains a non-empty subsequence whose sum is zero in G. Such a subsequence is called a *zero-sum subsequence*.

It is trivial to see that $\mathsf{D}^*(G) \leq \mathsf{D}(G) \leq |G|$ and the equality holds if and only if $G = \mathbb{Z}_n$, the cyclic group of order n. Olson [17] proved that $\mathsf{D}(G) = \mathsf{D}^*(G)$ for all finite abelian groups of rank 2 and for all p-groups. It is also

Birkhäuser

known that $\mathsf{D}(G) > \mathsf{D}^*(G)$ for infinitely many groups (See for instance, [13]). The best known upper bound is due to Emde Boas and Kruswjik [6, Theorem 7.1, p. 19], Meshulam [15], Alford et al. [1] and Rath et al. [19] which is as follows

$$\mathsf{D}(G) \leq \exp(G)\left(1 + \log \frac{|G|}{\exp(G)}\right). \tag{1.1}$$

We do have the following conjectures.

Conjecture 1. (1) $\mathsf{D}(G) = \mathsf{D}^*(G)$ *for all* G *with rank* $r = 3$ *or* $G = \mathbb{Z}_n^r$ *(See* [9]*);*
(2) $\mathsf{D}(G) \leq \sum_{i=1}^{r} n_i$ *(See for instance,* [16]*).*

Concerning Conjecture 1(1), we refer to the most recent articles by Schmid [21, Section 4.1], Girard [14, Proposition 2.1] and Geroldinger et al. [12].

We shall follow the notations as given in [8] (One may also refer to [11,22]). For a non-empty subset I of natural numbers and a finite abelian group G, let $\mathsf{s}_I(G)$ denote the smallest $l \in \mathbb{N} \cup \{\infty\}$ such that every sequence S over G of length $|S| \geq l$ has a zero-sum subsequence of length in I.

When $I = \mathbb{N}$, then we see that $\mathsf{s}_{\mathbb{N}}(G) = \mathsf{D}(G)$. When $I = \{1, 2, \ldots, m\}$, we denote $\mathsf{s}_I(G)$ by $\mathsf{s}_{\leq m}(G)$. Also, when $I = \{\exp(G)\}$, then the constant $\mathsf{s}_{\{\exp(G)\}}(G)$ is nothing but the well-known constant $\mathsf{s}(G)$ in the literature. Clearly,

$$\mathsf{D}(G) \leq \mathsf{s}_{\leq \exp(G)}(G) \leq \mathsf{s}(G) - \exp(G) + 1. \tag{1.2}$$

Alon and Dubiner [2] proved that $\mathsf{s}(\mathbb{Z}_n^r) \leq cn$ for some positive constant c which depends only on r. We define the smallest positive real number $c(r)$ depending only on r such that

$$\mathsf{s}(\mathbb{Z}_n^r) \leq c(r)n \quad \text{for all } n \geq 2. \tag{1.3}$$

Then, we have $c(1) \leq 2$ (due to Erdős et al. [5]), $c(2) \leq 4$ (due to Reiher [20]) and $c(r)$ can be defined inductively as,

$$c(r) \leq 256(r \log_2 r + 5)c(r-1) + (r+1), \tag{1.4}$$

for all $r \geq 3$. In particular, $c(3) \leq 9994$. We call $c(r)$ as Alon–Dubiner constants. From (1.2) and (1.3), we get

$$\mathsf{s}_{\leq n}(\mathbb{Z}_n^r) \leq \mathsf{s}(\mathbb{Z}_n^r) - n + 1 \leq (c(r) - 1)n + 1. \tag{1.5}$$

Conjecture 2. (*Gao* [10]) *We have,* $c(3) \leq 9$.

In this article, we prove the following main theorem.

Theorem 1.1. *Let* G *be any finite abelian group of rank* r *with invariants* $n_1, n_2, \ldots, n_r$. *Then*

$$\mathsf{D}(G) \leq n_r + n_{r-1} + (c(3) - 1)n_{r-2} + (c(4) - 1)n_{r-3} + \cdots + (c(r) - 1)n_1 + 1.$$

Theorem 1.1 is the extension of the result of Balasubramanian and Bhowmik [3]. Also Theorem 1.1 is towards the Conjecture 1(2).

Theorem 1.2. *Let $n \geq 2$ be any integer, and let $\omega(n)$ denote the number of distinct prime factors of n. Then*

$$\mathsf{D}(\mathbb{Z}_n^r) \leq r^{\omega(n)}(n-1)+1.$$

Theorem 1.3. *Let $n = 3^\alpha p^\ell$ be any integer such that $p \geq 3$ be any prime number. Then*

$$3n-2 \leq \mathsf{D}(\mathbb{Z}_n^3) \leq 3n + 3^{\alpha+1} - 7.$$

In particular, when $\alpha = 1$, then we get,

$$3n-2 \leq \mathsf{D}(\mathbb{Z}_n^3) \leq 3n+2.$$

Remark 1.4. (a) Let $n \geq \exp(\prod_{\ell \mid \omega(n), \ell \neq 1} \Phi_\ell(r))$ where $\Phi_k(X)$ denotes the k^{th} cyclotomic polynomial. Then Theorem 1.2 improves the bound (1.1). In particular, for all integers $n = p^\ell q^m \geq \exp(r+1)$ where $p \neq q$ are primes, Theorem 1.2 does improve the known bound (1.1).

(b) When $r = 3$ and $n = q^k p^\ell$ for any primes $p \neq q$ in Theorem 1.2, we get $\mathsf{D}(\mathbb{Z}_n^3) \leq 9n-8$. Theorem 1.3 improves this result, when $n = 3^\alpha p^\ell$, where $p \neq 3$.

Along the same lines of the proof of Theorem 1.1, we can prove the following Theorem for $\mathsf{s}(G)$ and $\mathsf{s}_{\leq \exp(G)}(G)$.

Theorem 1.5. *Let G be a finite abelian group of rank r. Then*

$$\mathsf{s}(G) \leq c(1)n_r + c(2)n_{r-1} + \cdots + c(r)n_1$$

and

$$\mathsf{s}_{\leq \exp(G)}(G) \leq (c(1)-1)n_r + (c(2)-1)n_{r-1} + \cdots + (c(r)-1)n_1 + 1.$$

More recently, Fan et al. [7] have focused on $\mathsf{s}(\mathbb{Z}_n^r)$ for higher ranks.

Given integers $r, n \geq 2$. A subset F of $\mathbb{N}$ is called a *factor base* if $F = \{p_1, p_2, \ldots, p_r\}$, where the p_i's are distinct prime numbers. An integer $N > 1$ is said to be *smooth* with respect to F if all the prime divisors of N are the members of F.

In Quadratic sieve [18], to factor a given integer N with a factor base F, one needs to know how many smooth integers are needed to produce two squares x^2 and y^2 such that $x^2 \equiv y^2 \pmod{N}$. It is well-known that if we can find $|F|+1 = r+1$ number of smooth integers with respect to factor base F, then we can find two squares which are equivalent modulo N. More generally, for any given integer $n \geq 2$, if we want to produce two nth powers of integers which are equivalent modulo N, how many smooth numbers with respect to F we need to have?

By $c(n,r)$, we denote the least positive integer t such that for any sequence U of smooth integers with respect to F, of cardinality at least t has a non-empty subsequence T such that the product of all the terms of T is an nth power of some integer. It is well-known that $c(2,r) = r+1$. We prove the following theorem,

Theorem 1.6. *For all integers $n \geq 2$ and $r \geq 2$, we have $c(n,r) = \mathsf{D}(\mathbb{Z}_n^r)$.*

Remark 1.7. Since

$$\mathsf{D}(\mathbb{Z}_{p^\ell}^r) = \mathsf{D}^*(\mathbb{Z}_{p^\ell}^r) = 1 + r(p^\ell - 1)$$

for any prime p and any integer $\ell \geq 1$, we see that

$$c(p^\ell, r) = 1 + r(p^\ell - 1).$$

2. Preliminaries.

Proposition 2.1. *Let p be a prime number, and let $n_1, n_2, \ldots, n_r > 1$ be integers such that $p^k | n_1 | n_2 | \cdots | n_r$. Let $m > 1$ be the unique integer such that*

$$(m-1)\mathsf{D}(\mathbb{Z}_{p^k}^r) \leq \mathsf{s}_{\leq p^k}(\mathbb{Z}_{p^k}^r) < m\mathsf{D}(\mathbb{Z}_{p^k}^r).$$

Let

$$h := \begin{cases} \mathsf{D}(\mathbb{Z}_{\frac{n_1}{p^k}} \oplus \cdots \oplus \mathbb{Z}_{\frac{n_r}{p^k}}) & \text{if } n_1 \neq p^k, \\ \mathsf{D}(\mathbb{Z}_{\frac{n_2}{p^k}} \oplus \cdots \oplus \mathbb{Z}_{\frac{n_r}{p^k}}) & \text{if } n_1 = p^k, n_2 \neq p^k, \\ \cdots & \cdots \\ \mathsf{D}(\mathbb{Z}_{\frac{n_r}{p^k}}) & \text{if } n_1 = n_2 = \cdots = n_{r-1} = p^k, n_r \neq p^k. \end{cases}$$

Then we have,

$$\mathsf{D}(\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}) \leq \begin{cases} (h-m+1)p^k + \mathsf{s}_{\leq p^k}(\mathbb{Z}_{p^k}^r) & \text{if } h \geq m-1, \\ \mathsf{s}_{\leq p^k}(\mathbb{Z}_{p^k}^r) & \text{otherwise.} \end{cases}$$

Furthermore, if $\mathsf{s}_{\leq p^k}(\mathbb{Z}_{p^k}^r) - (m-1)\mathsf{D}(\mathbb{Z}_{p^k}^r) \geq p^k$, then we have

$$\mathsf{D}(\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}) \leq (h-m)p^k + \mathsf{s}_{\leq p^k}(\mathbb{Z}_{p^k}^r),$$

provided $h \geq m-1$.

Proof. If $G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ is a p-group, then it is known that $\mathsf{D}(G) = \mathsf{D}^*(G)$. So, we assume that G is not a p-group and hence $n_i \neq p^k$ for some $i \leq r$. Let ℓ be an integer defined as

$$\ell = \begin{cases} (h-m+1)p^k + \mathsf{s}_{\leq p^k}(\mathbb{Z}_{p^k}^r) & \text{if } h \geq m-1, \\ \mathsf{s}_{\leq p^k}(\mathbb{Z}_{p^k}^r) & \text{otherwise.} \end{cases}$$

Let $\Phi : G \longrightarrow \mathbb{Z}_{p^k}^r$ be the canonical homomorphism. Let $S = a_1 a_2 \cdots a_\ell$ be a sequence of elements of G of length ℓ.

Assume that $h < m-1$. Then, clearly,

$$h\mathsf{D}(\mathbb{Z}_{p^k}^r) < (m-1)\mathsf{D}(\mathbb{Z}_{p^k}^r) \leq \mathsf{s}_{\leq p^k}(\mathbb{Z}_{p^k}^r).$$

Therefore, there are pairwise disjoint subsets $A_1, A_2, \ldots, A_h$ of $\{1, 2, \ldots, \ell\}$ such that

$$\sum_{i \in A_j} \Phi(a_i) = \Phi\left(\sum_{i \in A_j} a_i\right) = 0,$$

for each $j = 1, 2, \ldots, h$. That is, for each j, we have $\sum_{i \in A_j} a_i \in \mathrm{Ker}(\Phi)$. Since $h = \mathsf{D}(\mathrm{Ker}(\Phi))$, there exists a subset $A \subset \{1, 2, \ldots, h\}$ such that

$$\sum_{j \in A} \sum_{f \in A_{i_j}} a_f = 0 \quad \text{in } G.$$

Now, we assume that $h \geq m - 1$. Since $\ell \geq \mathsf{s}_{\leq p^k}(\mathbb{Z}_{p^k}^r)$, then, we can extract $h - m + 1$ disjoint zero-sum subsequences $\Phi(B_1), \Phi(B_2), \ldots, \Phi(B_{h-m+1})$ of $\Phi(S)$ such that the length of each B_i is at most p^k. The length of the remaining sequence S', which is obtained by deleting all the elements of $\Phi(B_i)$ from $\Phi(S)$, is at least

$$\ell - (h - m + 1)p^k \geq \mathsf{s}_{\leq p^k}(\mathbb{Z}_{p^k}^r) \geq (m - 1)\mathsf{D}(\mathbb{Z}_{p^k}^r).$$

Therefore, there are $m-1$ disjoint zero-sum subsequences say $\Phi(B_{h-m+2}), \ldots, \Phi(B_h)$ of $\Phi(S)$. Note that the sum of the elements of B_i lies in the kernel of Φ which is a proper subgroup H with $\mathsf{D}(H) = h$, which proves the proposition. □

Corollary 2.2. *Let $p \geq 3$ be a prime number, and let n_1, n_2 and n_3 be integers such that $p^k | n_1 | n_2 | n_3$. Let*

$$h := \begin{cases} \mathsf{D}(\mathbb{Z}_{\frac{n_1}{p^k}} \oplus \mathbb{Z}_{\frac{n_2}{p^k}} \oplus \mathbb{Z}_{\frac{n_3}{p^k}}) & \text{if } n_1 \neq p^k, \\ \mathsf{D}(\mathbb{Z}_{\frac{n_2}{p^k}} \oplus \mathbb{Z}_{\frac{n_3}{p^k}}) & \text{if } n_1 = p^k, n_2 \neq p^k, \\ \mathsf{D}(\mathbb{Z}_{\frac{n_3}{p^k}}) & \text{if } n_1 = n_2 = p^k, n_3 \neq p^k. \end{cases}$$

Then, we have

$$\mathsf{D}(\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \mathbb{Z}_{n_3}) \leq (h - 3)p^k + \mathsf{s}_{\leq p^k}(\mathbb{Z}_{p^k}^3).$$

Proof. By the result (due to Edel et al. [4]), we know that $\mathsf{s}_{\leq n}(\mathbb{Z}_n^3) \geq 8n - 7$, for all odd integer n. Therefore, the integer m is ≥ 3 in Proposition 2.1. Since $8p^k - 7 - 2\mathsf{D}(\mathbb{Z}_{p^k}^3) = 8p^k - 7 - 2(3p^k - 2) = 2p^k - 3 \geq p^k$, by Proposition 2.1, we get the result. □

Proposition 2.3. *Let G be a non-cyclic abelian group. If H be any subgroup of G, then*

$$\mathsf{D}(G) \leq (\mathsf{D}(G/H) - 1)\mathsf{D}(H) + 2.$$

Proof. Clearly, for any integer $m > 1$, we have

$$\mathsf{D}(G) \leq \mathsf{s}_{\leq m}(G/H) + m(\mathsf{D}(H) - 1).$$

By choosing $m = \mathsf{D}(G/H) - 1$ and by noting that $\mathsf{s}_{\leq (\mathsf{D}(G)-1)}(G) = \mathsf{D}(G) + 1$, we get the desired result. □

3. Proof of Theorems.

Proof of Theorem 1.1. Given that G is a finite abelian group of rank r. We prove the upper bound by the induction on r. When $r \leq 2$, the result of Olson [17] implies that

$$\mathsf{D}(G) = \mathsf{D}^*(G) \leq n_2 + n_1,$$

and hence the theorem follows. So, we assume the result for some $r = k \geq 3$ and we shall prove the result for $r = k + 1$.
If $n_1 = n_2 = \cdots = n_r$, then, by (1.5),

$$\mathsf{D}(G) \leq \mathsf{s}_{\leq \exp(G)}(G) = \mathsf{s}_{\leq n_1}(\mathbb{Z}_{n_1}^r) \leq (c(r) - 1)n_1 + 1.$$

Therefore, the result is true. Hence we assume that $n_r > n_1$. Let

$$H = \mathbb{Z}_{n_1}^r \text{ and } K \cong G/H \cong \mathbb{Z}_{\frac{n_r}{n_1}} \oplus \cdots \oplus \mathbb{Z}_{\frac{n_2}{n_1}}.$$

Let $\varphi : G \to H$ be a canonical homomorphism from G onto H. Then, $\mathrm{Ker}(\varphi) = K$. Let S be a sequence of elements of G of length

$$|S| = n_r + n_{r-1} + (c(3) - 1)n_{r-2} + \cdots + (c(r) - 1)n_1 + 1.$$

Since $\mathsf{s}_{\leq n_1}(H) \leq (c(r) - 1)n_1 + 1$, we can find disjoint subsequences $S_1, S_2, \ldots, S_\ell$ of S, where

$$\ell = \frac{n_r}{n_1} + \frac{n_{r-1}}{n_1} + (c(3) - 1)\frac{n_{r-2}}{n_1} + \cdots + (c(r-1) - 1)\frac{n_2}{n_1} + 1,$$

such that $1 \leq |S_i| \leq n_1$ for every $i = 1, 2, \ldots, \ell$ and $\sigma(\varphi(S_i)) := \varphi(\sum_{a \in S_i} a)$ $= 0$ in H. Therefore, $\sigma(S_1), \sigma(S_2), \ldots, \sigma(S_\ell) \in \mathrm{Ker}(\varphi) = K$. Since the rank of K is $r - 1$, by the induction hypothesis, we have

$$\mathsf{D}(K) \leq \frac{n_r}{n_1} + \frac{n_{r-1}}{n_1} + (c(3) - 1)\frac{n_{r-2}}{n_1} + \cdots + (c(r-1) - 1)\frac{n_2}{n_1} + 1 = \ell$$

and hence, we can find a subsequence T of the sequence $\sigma(S_1)\sigma(S_2)\cdots\sigma(S_\ell)$ whose sum is zero in K. That in turn produces a zero-sum subsequence of S in G. Therefore the result follows. □

Proof of Theorem 1.2. We shall prove this result by induction on $\omega(n)$, the number of distinct prime factors of n. Let $\omega(n) = 1$. Since $n = p^\alpha$, by Olson's Theorem the result is true. We shall assume that the result is true for integers m satisfying $\omega(m) < k$. Let $\omega(n) = k$ and $n = p^\alpha p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where $\alpha, \alpha_i > 0$ are integers.

Set $H = \mathbb{Z}_{n/p^\alpha}^r$. Since p^α divides n, clearly H is a subgroup of $\mathbb{Z}_n^r$. Therefore we have $G/H = \mathbb{Z}_{p^\alpha}^r$. Hence by Proposition 2.3, we get,

$$\begin{aligned}\mathsf{D}(\mathbb{Z}_n^r) &\leq (\mathsf{D}(\mathbb{Z}_{p^\alpha}^r) - 1)\mathsf{D}(H) + 2 = r(p^\alpha - 1)\mathsf{D}(H) + 2 \\ &\leq r(p^\alpha - 1)\left(r^{\omega(n/p^\alpha)}\left(\frac{n}{p^\alpha} - 1\right) + 1\right) + 2 \\ &= r^{\omega(n)}\frac{(p^\alpha - 1)}{p^\alpha}n - (p^\alpha - 1)(r^{\omega(n)} - r) + 2.\end{aligned}$$

To prove the theorem, it is enough to prove that

$$r^{\omega(n)}\frac{(p^\alpha - 1)}{p^\alpha}n - (p^\alpha - 1)(r^{\omega(n)} - r) + 2 \le r^{\omega(n)}(n-1) + 1. \qquad (3.1)$$

Since

$$\frac{r^{\omega(n)}n}{2} > r^{\omega(n)} - (r^{\omega(n)} - r),$$

by a little calculation (3.1) follows. Hence the theorem. □

Proof of Theorem 1.3. Note that $\mathsf{s}_{\le 3}(\mathbb{Z}_3^3) = 17 = 8 \times 3 - 7$ and if $f(p) = \mathsf{s}_{\le p}(\mathbb{Z}_p^3) = 8p - 7$, then $f(p^\alpha) \le 8p^\alpha - 7$. To show this, it is enough to prove that

$$f(p^\alpha) \le (f(p^{\alpha-1}) - 1)p + f(p),$$

which follows easily by arguing similar to the proof of Proposition 2.1 and hence we omit the proof here.

Put $p = 3$ in $f(p^\alpha)$. We get $f(3^\alpha) \le 8\times 3^\alpha - 7$. But we know that $\mathsf{s}_{\le n}(\mathbb{Z}_n^3) \ge 8n - 7$, *for all odd integers* n (see [4]). So $f(3^\alpha) \ge 8 \times 3^\alpha - 7$ and hence we get $f(3^\alpha) = 8 \times 3^\alpha - 7$. Now, apply Corollary 2.2, by putting $n = 3^\alpha p^\ell$ for all primes $p > 3$ to get

$$\mathsf{D}(\mathbb{Z}_n^3) \le (3p^\ell - 5)3^\alpha + 8 \times 3^\alpha - 7 \le 3n + 3^{\alpha+1} - 7.$$

Hence the theorem. □

The proof of Theorem 1.5 is similar to the proof of Theorem 1.1 and hence we omit the proof here.

Proof of Theorem 1.6. To prove $c(n,r) \le \mathsf{D}(\mathbb{Z}_n^r)$, let $\ell = \mathsf{D}(\mathbb{Z}_n^r)$ and let $U = m_1 m_2 \cdots m_\ell$, be a sequence of smooth numbers with respect to F of length ℓ. Therefore, let $m_i = p_1^{e_{i1}} p_2^{e_{i2}} \cdots p_r^{e_{ir}}$, for each $i = 1, 2, \ldots, \ell$, where $e_{ij} \ge 0$ are integers. We associate each m_i to $a_i \in \mathbb{Z}_n^r$ as follows;

$$m_i \mapsto a_i := (e_{i1}, e_{i2}, \ldots, e_{ir}) \pmod n$$

for all $i = 1, 2, \ldots, \ell$. Thus, we get a sequence $S = a_1 a_2 \cdots a_\ell$ of elements of $\mathbb{Z}_n^r$ of length $\ell = \mathsf{D}(\mathbb{Z}_n^r)$. Therefore, there exists a non-empty zero-sum subsequence T' of S in $\mathbb{Z}_n^r$, and let $T' = a_{j_1} a_{j_2} \cdots a_{j_t}$. That is,

$$\sum_{i=1}^{t} e_{j_i k} \equiv 0 \pmod n, \quad \text{for all } k = 1, 2, \ldots, r. \qquad (3.2)$$

Consider the subsequence T of U corresponding to T'. Clearly, $T = m_{j_1} m_{j_2} \cdots m_{j_t}$, and by Eq. (3.2), we get

$$\prod_{m\in T} m = \prod_{k=1}^{r} p_k^{\sum_{i=1}^{t} e_{j_i k}} = \left(\prod_{k=1}^{r} p_k^{l_k}\right)^n,$$

for some integers $l_k \ge 0$, for all $k = 1, 2, \ldots, r$.

To prove $\mathsf{D}(\mathbb{Z}_n^r) \le c(n,r)$, let $\ell = c(n,r)$ and $S = a_1 a_2 \cdots a_\ell$ be a sequence of elements of $\mathbb{Z}_n^r$ of length ℓ, where for each $i = 1, 2, \ldots, \ell$ we have

$$a_i = (e_{i1}, e_{i2}, \ldots, e_{ir}) \in \mathbb{Z}_n^r.$$

Let

$$m_i = p_1^{e_{i1}} p_2^{e_{i2}} \cdots p_r^{e_{ir}},$$

for all $i = 1, 2, \ldots, \ell$. Clearly, the sequence $U = m_1 m_2 \cdots m_\ell$ of integers is a sequence of smooth numbers with respect to F. Since $\ell = c(n, r)$, there exists a non-empty subsequence T of U such that

$$\prod_{a \in T} a = b^n, \quad \text{where } b = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

for some integers $k_i \geq 0$. If we let $T = m_{j_1} m_{j_2} \cdots m_{j_t}$, then the subsequence T' of S corresponding to T will sum upto the identity in $\mathbb{Z}_n^r$. Hence $\mathsf{D}(\mathbb{Z}_n^r) \leq c(n, r)$ and the theorem follows. □

Acknowledgements. We would like to thank the referee for the valuable comments and suggestions which improved the presentation of the paper considerably.

References

[1] W. R. Alford, A. Granville, and C. Pomerance, There are infinitely many Carmichael numbers, Annals of Math. **140** (1994), 703–722.

[2] N. Alon and M. Dubiner, A lattice point problem and additive number theory, Combinatorica, **15** (1995), 301–309.

[3] R. Balasubramanian and G. Bhowmik, Upper bounds for the Davenport constant, Combinatorial number theory, 61–69, de Gruyter, Berlin, 2007.

[4] Y. Edel, et al. Zero-sum problems in finite abelian groups and affine caps, Q. J. Math., **58** (2007), 159–186.

[5] P. Erdős, A. Ginzburg, and A. Ziv, Theorem in the additive number theory, Bull. Res. Council Israel, **10 F**(1961), 41–43.

[6] P. van Emde Boas and D. Kruswjik, A combinatorial problem on finite abelian group III, Z. W. 1969-008 (Math. Centrum, Amsterdam).

[7] Y. Fan, W. Gao, and Q. Zhong, On the Erdős–Ginzburg–Ziv constant of finite abelian groups of high rank, J. Number Theory **131** (2011), 1864–1874.

[8] M. Freeze and W. A. Schmid, Remarks on a generalization of the Davenport constant, Discrete Math. **310** (2010), 3373–3389.

[9] W. D. Gao, On Davenport's constant of finite abelian groups with rank three, Discrete Math., **222** (2000), 111–124.

[10] W. D. Gao and A. Geroldinger, Zero-sum problems in finite abelian groups; a survey, Expo. Math. **24** (2006), 337–369.

[11] A. Geroldinger and F. Halter-Koch, Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory, Pure and Applied Mathematics, Vol. **278**, Chapman & Hall/CRC, 2006.

[12] A. Geroldinger, M. Liebmann, and A. Philipp, On the Davenport constant and on the structure of extremal sequences, Period. Math. Hung.

[13] A. Geroldinger and R. Schneider, On Davenport's constant, J. Combin. Theory, Ser. A, **61** (1992), 147–152.

[14] B. Girard, Inverse zero-sum problems and algebraic invariants, Acta Arith., **135** (2008), 231–246.

[15] R. Meshulam, An uncertainty inequality and zero subsums, Discrete Math., **84** (1990), 197–200.

[16] W. Narkiewicz and J. Śliwa, Finite abelian groups and factorization problems-II, Colloq. Math., **46** (1982), 115–122.

[17] J. E. Olson, A combinatorial problem in finite abelian groups, I and II, J. Number Theory, **1** (1969), 8–10 and 195–199.

[18] C. Pomerance A tale of two sieves. Notices Amer. Math. Soc. **43** (1996), 1473–1485.

[19] P. Rath, K. Srilakshmi, and R. Thangadurai, On Davenport's constant, Int. J. Number Theory, **4** (2008), 107–115.

[20] C. Reiher, On Kemnitz' conjecture concerning lattice-points in the plane., Ramanujan J. **13** (2007), 333–337.

[21] W. Schmid, The inverse problem associated to the Davenport constant for $C_2 \oplus C_2 \oplus C_{2n}$, and applications to the arithmetical characterization of class groups, Electron. J. Comb., **18**, Research Paper 33, (2011).

[22] D. Smertnig, On the Davenport constant and group algebras, Colloq. Math. **121** (2010), 179–193.

M. N. Chintamani and B. K. Moriya
The Institute of Mathematical Sciences,
4th Cross Street, CIT Campus,
Taramani,
Chennai 600 113,
India
e-mail: mchintamani@imsc.res.in

B. K. Moriya
e-mail: bhavinkm@imsc.res.in

W. D. Gao
Center for Combinatorics,
Nankai University,
Tianjin 300071,
China
e-mail: gao@cfc.nankai.edu.cn

P. Paul
C.R. Rao Advanced Institute of Mathematics,
Statistics and Computer Science (AIMSCS),
University of Hyderabad Campus,
Central University Post Office,
Hyderabad 500 046,
AP, India
e-mail: prabal.paul@gmail.com

R. Thangadurai
Harish-Chandra Research Institute,
Chhatnag Road,
Jhunsi, Allahabad 211019,
India
e-mail: thanga@hri.res.in

Received: 6 June 2011

Revised: 13 October 2011