REMARKS ON GROUP RINGS AND THE DAVENPORT CONSTANT

WEIDONG GAO AND YUANLIN LI

ABSTRACT. Let $D(G)$ be the Davenport constant of a finite abelian group G, defined as the smallest positive integer d such that every sequence of d elements in G contains a nonempty subsequence with sum zero the identity of G. In this short note, we use group rings as a tool to characterize the Davenport constant.

1. INTRODUCTION

Let G be an additively written finite abelian group. Let $\mathcal{F}(G)$ be the free abelian monoid over G, multiplicatively written, with basis G. The elements of $\mathcal{F}(G)$ are called sequences over G. Let $S = g_1 \cdot \ldots \cdot g_t \in \mathcal{F}(G)$. We call S a *zero-sum sequence* if $\sum_{i=1}^{t} g_i = 0$. We call S a *minimal zero-sum sequence* if S is a nonempty zero-sum sequence and contains no proper zero-sum subsequence. We call S a *zero-sumfree sequence* if S contains no nonempty zero-sum subsequence. The Davenport constant of G, denoted by $D(G)$, is defined to be the smallest positive integer d such that every sequence of d elements in G contains a nonempty zero-sum subsequence. The problem of finding $D(G)$ was proposed by H. Davenport in 1966, and he also pointed out that $D(G)$ is connected to algebraic number theory in the following way. Let K be an algebraic number field and G be its class group. Then $D(G)$ is the maximal number of prime ideals (counting multiplicity) that can occur in the decomposition of an irreducible integer in K. It plays an important role in unique factorization theory in algebraic number theory. Furthermore, the Davenport constant is also connected with graph theory, classical number theory and coding theory, and the study of $D(G)$ has attracted a great deal of attention (See for example, [1], [2], [4], [7], [9], [10], and [13]). The exact value of $D(G)$ has been determined only for a few classes of groups, such as finite abelian p-groups, abelian groups of rank not exceeding 2, and certain very special abelian groups of rank 3 (See for example, [3], [4], [6],[11], and [12]).

The first author was supported in part by the Natural Science Foundation of China and the second author was supported in part by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada.

In this paper, we use group rings as a tool to investigate $D(G)$. In Section 2, we give a new characterization of $\mathsf{D}(G)$. Perhaps, this characterization will be helpful in estimating $D(G)$.

Let $\mathbf{R}$ be a commutative ring with unity. The group algebra $\mathbf{R}G$ of group G over the ring $\mathbf{R}$ is a free $\mathbf{R}$-module with basis $\{X^g \mid g \in G\}$ (built with a symbol X).

Let $\mathsf{d}(G)$ denote the maximal length of a zero-sumfree sequence over G. Then $\mathsf{d}(G)+1$ is the Davenport constant of G.

For a field $\mathbf{F}$, let $\mathsf{d}(G,\mathbf{F})$ denote the largest integer $l \in \mathbb{N}$ having the following property:

There is some sequence $S = g_1 \cdot \ldots \cdot g_l$ of length l over G such that

$$(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_l) \neq 0 \in \mathbf{F}G \quad \text{for all} \quad a_1, \ldots, a_l \in \mathbf{F}^\times .$$

Then it is easy to see that $\mathsf{d}(G) \le \mathsf{d}(G,\mathbf{F})$. Define $\overline{d}(G) = \min_{\mathbf{F}}\{d(G,\mathbf{F})\}$. Clearly, $D(G) \le \overline{d}(G)+1$. For any finite abelian p-group G or finite cyclic group G, the equality $D(G) = \overline{d}(G)+1$ was confirmed by J.E. Olson [11], and by the first author and A. Gerlodinger [5], respectively. However, we do not know any other finite abelian group G for which $D(G) = \overline{d}(G)+1$ holds. In the final section 3, we will show that $D(G) = \overline{d}(G)+1$ holds for $G = C_2 \oplus C_{2n}$.

Our notations about group rings follow those of [8]. Throughout this paper, let G be a finite abelian group and let $\mathbf{F}$ be a field.

2. A NEW CHARACTERIZATION OF THE DAVENPORT CONSTANT $\mathsf{D}(G)$

It is well-known that the Davenport constant $\mathsf{D}(G)$ can be characterized by several equivalent conditions:

- $\mathsf{D}(G) = \max\{|S| \mid S \in \mathcal{F}(G) \text{ is a minimal zero-sum sequence}\}$.
- $\mathsf{D}(G)$ is the smallest integer l such that every sequence $S \in \mathcal{F}(G)$ of length $|S| \ge l$ has a non-empty zero-sum subsequence.
- $\mathsf{D}(G) = \mathsf{d}(G)+1$.

The equivalence of all these definitions is easy to check, details can be found in [6, Section 5.1]. It is the aim of this section to derive a further characterization of $\mathsf{D}(G)$ which could be useful when working with group algebras.

We fix the following notation. For an element $f \in \mathbf{F}G$ and all $g \in G$, let $\mathsf{c}_g(f) \in \mathbf{F}$ be defined by

$$f = \sum_{g \in G} \mathsf{c}_g(f) X^g .$$

Lemma 2.1. *Let* $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ *be a sequence and suppose that there exist* $a_1, \ldots, a_{l-1} \in \mathbf{F}$ *such that*

$$c_0\Big(\prod_{i=1}^{l-1}(X^{g_i} - a_i)\Big) \neq (-1)^{l-1}\prod_{i=1}^{l-1} a_i .$$

Then there exist some $a_l \in \mathbf{F}$ *such that*

$$c_0\Big(\prod_{i=1}^{l}(X^{g_i} - a_i)\Big) \neq (-1)^{l}\prod_{i=1}^{l} a_i .$$

Proof. Let $c = (-1)^{l-1} a_1 a_2 \cdots a_{l-1}$. Write

$$\prod_{i=1}^{l-1}(X^{g_i} - a_i) = \sum_{g \in G} \alpha_g X^g, \alpha_g \in \mathbf{F}.$$

Then $\alpha_0 \neq c$. Let $a_l \in \mathbf{F}$. Then
$c_0((X^{g_l} - a_l)\prod_{i=1}^{l-1}(X^{g_i} - a_i)) = c_0((X^{g_l} - a_l)\sum_{g \in G} \alpha_g X^g) = \alpha_{-g_l} - a_l \alpha_0$.
So, it suffices to choose a_l so that

$$\alpha_{-g_l} - a_l \alpha_0 \neq -a_l c.$$

This is equivalent to

$$a_l(\alpha_0 - c) \neq \alpha_{-g_l}.$$

Since $\alpha_0 - c \neq 0$, it is a unit in $\mathbf{F}$. Clearly we can choose a_l so that $a_l \neq \frac{\alpha_{-g_l}}{\alpha_0 - c}$. This completes the proof. □

Theorem 2.2. *Let* $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ *be a sequence. Then the following statements are equivalent:*

(a) *There exist* $a_1, \ldots, a_l \in \mathbf{F}$ *such that* $c_0(\prod_{i=1}^{l}(X^{g_i} - a_i)) \neq (-1)^l \prod_{i=1}^{l} a_i$.

(b) S *is not zero-sumfree.*

In particular, the Davenport constant $\mathsf{D}(G)$ *is the smallest integer* $l \in \mathbb{N}$ *having the following property:*

> *For every sequence* $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ *of length* l *there exist* $a_1, \ldots, a_l \in \mathbf{F}$ *such that*
>
> $$c_0\Big(\prod_{i=1}^{l}(X^{g_i} - a_i)\Big) \neq (-1)^{l}\prod_{i=1}^{l} a_i .$$

Proof. It suffices to prove the equivalence of (a) and (b).

If there are l elements $a_1, a_2, \cdots, a_l \in \mathbf{F}$ (repetition allowed) such that the $c_0(\prod_{i=1}^{t}(X^{g_i} - a_i)) \neq (-1)^t a_1 a_2 \cdots a_l$, clearly S contains a nonempty zero-sum subsequence.

Next assume that S contains a nonempty zero-sum subsequence. Without loss of generality, we may assume that $T = g_1 \cdot \ldots \cdot g_k$ is a minimal zero-sum subsequence. Then $c_0(\prod_{j=1}^{k}(X^{g_j} - a_j)) = 1 + (-1)^k a_1 a_2 \cdots a_k \neq (-1)^k a_1 a_2 \cdots a_k$. By Lemma 2.1, we can find $a_{k+1}, \cdots, a_l$ inductively, such that $c_0(\prod_{i=1}^{l}(X^{g_i} - a_i)) \neq (-1)^t a_1 a_2 \cdots a_l$. □

3. On $d(G)$ and $\overline{d}(G)$

The question of when $D(G) = \overline{d}(G) + 1$ is investigated in this section. We are able to show that this equality holds when $G = C_2 \oplus C_{2n}$.

The following easy observation will be helpful in the proof of Theorem 3.3.

Lemma 3.1. *Let $S = g_1 \cdot \ldots \cdot g_t \in \mathcal{F}(G)$, and let $k_1, \cdots, k_t$ be some positive integers. If there exist $a_1, \cdots, a_t \in \mathbf{F}^\times$ such that $(X^{g_1} - a_1) \cdots (X^{g_t} - a_t) = 0 \in \mathbf{F}G$, then $(X^{k_1 g_1} - a_1^{k_1}) \cdots (X^{k_t g_t} - a_t^{k_t}) = 0 \in \mathbf{F}G$.*

For $n \in \mathbb{N}$, let $\mu_n(F) = \{\zeta \in F \mid \zeta^n = 1\} \subset F^\times$ denote the group of n-th roots of unity of F. Then $\mu_n(F)$ is a cyclic subgroup of $F^\times$. If $\exp(G) = n$, then $\mathrm{Hom}(G, F^\times) = \mathrm{Hom}(G, \mu_n(F))$, and F is called a *splitting field* of G if $|\mu_n(F)| = n$. Clearly, if F is a splitting field of G, then $\mathrm{char}(\mathbf{F}) \nmid \exp(G)$.

Lemma 3.2. *Let $S = g_1 \cdot \ldots \cdot g_t \in \mathcal{F}(G)$ be a sequence with $ord(g_1) \leq \cdots \leq ord(g_t)$. Let $\mathbf{F}$ a splitting field of G and let $m_i = ord(g_i)$ for $i = 1, \cdots, t$. If $[(1 - \frac{1}{m_1}) \cdots (1 - \frac{1}{m_{t-\ell}})|G|] \leq \ell$ holds for some non-negative integer $\ell < t$, then there exist nonzero elements $c_1, \cdots, c_t$ of $\mathbf{F}$ such that the product*

$$(X^{g_1} - c_1) \cdots (X^{g_t} - c_t) = 0 \in \mathbf{F}G.$$

Therefore, $\overline{d}(G) \leq t$.

Proof. This lemma follows immediately from Lemma 5.5.3 and Proposition 5.5.4.2 in [6]. □

Theorem 3.3. *Let $G = C_2 \oplus C_{2n}$ with $n \geq 2$ and suppose that $\mathbf{F}$ is a splitting field of G. Then the equality $d(G) = d(G, \mathbf{F})$ holds, and therefore, $D(G) = \overline{d}(G) + 1$.*

Proof. As observed in the introduction, we clearly have $\mathsf{d}(G) \leq \mathsf{d}(G, F)$. Thus it remains to prove the reverse inequality. Since $\mathsf{d}(G) = 2n$ (see [6, Theorem 5.8.3]), we have to show that $\mathsf{d}(G, F) \leq 2n$. Let $S = g_1 \cdot \ldots \cdot g_{2n+1} \in \mathcal{F}(G)$. We will prove that there are $a_1, \ldots, a_{2n+1} \in \mathbf{F}^\times$ such that

$$(X^{g_1} - a_1)(X^{g_2} - a_2) \cdots (X^{g_{2n+1}} - a_{2n+1}) = 0 \in \mathbf{F}G. \tag{3.1}$$

Then by definition of $\mathrm{d}(G,F)$ it follows that $\mathrm{d}(G,F) < |S| = 2n+1$, and we are done.

We now prove Equation (3.1). If S contains an element of order 2, we may assume that $ord(g_1) = 2$. Since $[(1 - \frac{1}{ord(g_1)})|G|] = 2n$, (3.1) follows from Lemma 3.2 with $t = 2n+1$ and $\ell = 2n$. Thus we may assume that S contains no element of order 2.

Write $2n = 2^u v$ with $2 \nmid v$. Let $G = C_2 \oplus C_{2n} = \langle x \rangle \oplus \langle y \rangle$ with $\langle x \rangle = C_2$ and $\langle y \rangle = C_{2n}$. Then every element in G is of the form ay or $x + ay$ with $a \geq 0$. Since S contains no element of order 2, for each $g \in S$ either $g = ay$ or $g = x + by$ with $b \in \{1, 2, \cdots, 2n-1\}$. If $g = ay$, then by Lemma 3.1 we can replace g by y. If $g = x + 2^c by$ with b odd, then $g = b(x + 2^c y)$, so by Lemma 3.1 we can replace g by $x + 2^c y$. Furthermore, if $c > u$ then $x + 2^c y = x + (2^c + 2n)y = x + (2^u(2^{c-u} + v))y = (2^{c-u} + v)(x + 2^u y)$ and we can replace $x + 2^c y$ by $x + 2^u y$. Thus we may assume that $g \in \{y, x+y, x+2y, x+4y, \cdots, x+2^u y\}$ holds for every $g \in S$. Let ξ be a primitive $2n$-th root of 1. Then $\{1, \xi, \xi^2, \cdots, \xi^{2n-1}\}$ are all $2n$-th roots of 1. Clearly $\{1, \xi, \xi^2, \cdots, \xi^{2n-1}\} = \{\pm 1, \pm\xi, \pm\xi^2, \cdots, \pm\xi^{n-1}\}$.

The next 4 equations will be used later in the proof.

$$(3.2)\quad \prod_{i=0}^{n-1}(X^y - \xi^i)(X^y + \xi^i) = \prod_{i=0}^{2n-1}(X^y - \xi^i) = X^{2ny} - 1 = X^0 - 1 = 0.$$

$$(3.3)\quad X^{2x} = X^0 = 1.$$

(3.4)
$$(X^x z^a - \eta^a)(X^x z^b + \eta^b) = (z^{a+b} - \eta^{a+b}) + \eta^b X^x z^a - \eta^a X^x z^b = (z - \eta)\alpha,$$

where $z, \eta, \alpha \in \mathbf{F}G$, $a, b \in N$ and $a < b$.

$$(3.5)\quad (X^x z - \eta)(X^x z + \eta) = (z - \eta)(z + \eta),$$

where $z, \eta \in \mathbf{F}G$.

Next, we divide the terms of S into as many as possible disjoint pairs $(z_1, w_1), (z_2, w_2), \cdots, (z_q, w_q)$ such that each pair is of one of the following three forms: $(y, y), (x + 2^r y, x + 2^r y)(0 \leq r \leq u)$ and $(x + 2^s y, x + 2^t y)(1 \leq s < t \leq u)$.

Consider the remaining sequence obtained by deleting $(z_1, w_1, z_2, w_2, \cdots, z_q, w_q)$ from S, and clearly there are only two cases: (1) the remaining sequence is of the form $(y, x + y, x + 2^f y)$ with $1 \leq f \leq u$, or (2) the remaining sequence contains only one term.

Case 1. If the remaining sequence is of the form $(y, x+y, x+2^f y)$, then there are $q = n-1$ pairs (z_i, w_i) of terms from S. We show that there exist $b_1, c_1, b_2, c_2, \cdots, b_{n-1}, c_{n-1} \in \mathbf{F}^\times$ such that $(X^y+1)(X^{x+y}-1)(X^{x+2^f y}+1)\prod_{i=1}^{n-1}(X^{z_i}-b_i)(X^{w_i}-c_i) = 0 \in \mathbf{F}G$. For each pair (z_i, w_i) with $i \in \{1, 2, \cdots, n-1\}$, we choose b_i, c_i in the following way:

(1) If $(z_i, w_i) = (y, y)$, then let $b_i = \xi^i$ and $c_i = -\xi^i = \xi^{n+i}$;

(2) If $(z_i, w_i) = (x+2^r y, x+2^r y)$, then let $b_i = (\xi^i)^{2^r}$ and $c_i = -(\xi^i)^{2^r}$. By (3.5), $(X^{z_i}-b_i)(X^{w_i}-c_i) = (X^{2^r y}-\xi^{i2^r})(X^{2^r y}+\xi^{i2^r}) = (X^y-\xi^i)(X^y+\xi^i)\alpha_i$ where $\alpha_i \in \mathbf{F}G$;

(3) If $(z_i, w_i) = (x+2^s y, x+2^t y)$ with $1 \le s < t \le u$, then let $b_i = (\xi^i)^{2^s}$ and $c_i = -(\xi^i)^{2^t}$. Thus by (3.4), $(X^{z_i}-b_i)(X^{w_i}-c_i) = (X^{2y}-(\xi^i)^2)\alpha_i = (X^y-\xi^i)(X^y+\xi^i)\alpha_i$ where $\alpha_i \in \mathbf{F}G$.

We just showed that for each above pair (z_i, w_i) with $i \in \{1, \cdots, n-1\}$ we can choose a pair (b_i, c_i) of elements in $\mathbf{F}^\times$ such that $(X^{z_i}-b_i)(X^{w_i}-c_i) = (X^y-\xi^i)(X^y+\xi^i)\alpha_i$ where $\alpha_i \in \mathbf{F}G$.

It follows from (3.4) that $(X^{x+y}-1)(X^{x+2^f y}+1) = (X^y-1)\beta$ where $\beta \in \mathbf{F}G$. We now have $(X^y+1)(X^{x+y}-1)(X^{x+2^f y}+1)\prod_{i=1}^{n-1}(X^{z_i}-b_i)(X^{w_i}-c_i) = (X^y+1)(X^y-1)\beta\prod_{i=1}^{n-1}(X^y-\xi^i)(X^y+\xi^i)\alpha_i = (\beta\prod_{i=1}^{n-1}\alpha_i)\prod_{i=0}^{n-1}(X^y-\xi^i)(X^y+\xi^i) = 0$.

Case 2. If the remaining sequence contains only one term, then there are $q = n$ pairs (z_i, w_i) of terms from S. As before, for each pair (z_i, w_i), we can find a pair (b_i, c_i) of elements in $\mathbf{F}^\times$ such that $(X^{z_i}-b_i)(X^{w_i}-c_i) = (X^y-\xi^i)(X^y+\xi^i)\alpha_i$, where $\alpha_i \in \mathbf{F}G$. Therefore, $\prod_{i=1}^{n}(X^{z_i}-b_i)(X^{w_i}-c_i) = (\prod_{i=1}^{n}\alpha_i)\prod_{i=1}^{n}(X^y-\xi^i)(X^y+\xi^i) = 0$.

In all the cases, we showed that (3.1) holds. This completes the proof. □

We are not aware of any example of a finite abelian group G for which the equality $d(G) = \mathsf{d}(G, \mathbf{F})$ fails to hold. We close this paper by making the following conjecture.

Conjecture 3.4. *For every finite abelian group G and every splitting field $\mathbf{F}$ of G, we have $\mathsf{d}(G) = \mathsf{d}(G, \mathbf{F})$.*

ACKNOWLEDGEMENTS

We would like to thank the referee for useful suggestions and comments.

REFERENCES

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

[2] N. Alon, S. Friedland and G. Kalai, *Regular subgraphs of almost regular graphs*, J. Combinatorial Theory B, **37** (1984), 79-91.

[3] S.T. Chapman, M. Freeze, W. Gao and W.W. Smith, *On Davenport's constant of finite abelian groups*, Far East J. Math. Sci., **2** (2002), 47-54.

[4] P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite abelian groups III*, Report ZW-1969-008, Math. Centre Amsterdam.

[5] W.D. Gao and A. Geroldinger, *Group algebras of finite abelian groups and their applications to combinatorial problems*, preprint, 2005.

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

[7] A. Geroldinger and R. Schneider, *On Davenport's constant*, J. Combinatorial Theory A, **61** (1992), 147-152.

[8] R. Gilmer, *Commutative Semigroup Rings*, The University of Chicago Press, 1984.

[9] F. Halter-Koch, *A generalization of Davenport's constant and its arithematical applications*, Colloq. Math., **63** (1992), 203-210.

[10] M. Mazur, *A note on the growth of Davenport's constant*, Manuscr. Math., **74** (1992), 229-235.

[11] J.E. Olson, *A combinatorial problem on finite abelian groups*, J.Number Theory, **1** (1969), 8–10.

[12] J.E. Olson, *A combinatorial problem on finite abelian groups II*, J.Number Theory, **1** (1969), 195–199.

[13] M. Skalba, *On relative Davenport constant*, Eur. J. Comb., **19** (1998), 221-225.

CENTER FOR COMBINATORICS, NANKAI UNIVERSITY, TIANJIN 300071, P.R. CHINA
E-mail address: gao@cfc.nankai.edu.cn

DEPARTMENT OF MATHEMATICS, BROCK UNIVERSITY, ST. CATHARINES, ONTARIO, CANADA L2S 3A1
E-mail address: yli@brocku.ca