Davenport Constant for Semigroups

Guoqing Wang* Weidong Gao †

August 27, 2007

Abstract

Let G be a finite commutative semigroup. The Davenport constant of G is the smallest integer d such that, every sequence S of d elements in G contains a subsequence T ($\neq S$) with the same product of S. Let $R = Z_{n_1} \oplus \cdots \oplus Z_{n_r}$. Among other results, we determine $D(R^{\times}) - D(U(R))$, where $R^{\times}$ is the multiplicative semigroup of R and $U(R)$ is the group of units of R.

Key Words: semigroup, Davenport constant, reducible sequence, homogeneous subsequence.

1 Introduction

Let G be a finite abelian group. The Davenport constant $D(G)$ of G is defined as the smallest integer $d \in \mathbb{N}$ such that, every sequence S of d elements in G contains a nonempty subsequence with product 1. $D(G)$ was first introduced by H. Davenport in 1965. Since then a huge variety of interesting work concerning $D(G)$ has been aroused (For e.g., see [1-13]). For its historical comments the reader is referred to [6]. In this paper, we first give a natural generalization of $D(G)$ to any finite commutative semigroup G, then we determine $D(R^{\times}) - D(U(R))$ as mentioned in the abstract (see Theorem 1.3 below). The relative Davenport constant for semigroups is also investigated (see the final section 3).

Since G was often considered as the multiplicative semigroup of a ring in this paper, we write G multiplicatively. Let $\mathcal{F}(G)$ be the free commutative monoid, multiplicatively written, with basis G. To avoid confusing with sequences, we denote by $*$ the operator symbol of G. Let $S = g_1 \cdots g_k \in \mathcal{F}(G)$ be a sequence of elements in G (repetition allowed). Denote $\pi(S)$ by the product $g_1 * \cdots * g_k \in G$. By λ we denote the empty

*Institute of Mathematics, Dalian University of Technology, Dalian, 116024, P.R. China
†Center for Combinatorics, LPMC, Nankai University, Tianjin, 300071, P.R. China

sequence. If G has the identity 1, then we adopt the convention that $\pi(\lambda) = 1$. Let T be a subsequence of S. We call T a *proper subsequence* of S if $T \neq S$. We call S is *reducible* if $\pi(T) = \pi(S)$ for some proper subsequence T (Note that, T is probably the empty sequence λ if G has the identity element 1 and $\pi(S) = 1$). Otherwise, we call S is *irreducible*.

Definition 1.1 *Let G be a finite commutative semigroup. Define the Davenport constant $D(G)$ of G as the smallest integer $d \in \mathbb{N}$ such that, every sequence S of d elements in G is reducible.*

For any finite abelian group G, we can formulate $D(G)$ in various ways. For example, we can first define $d(G)$ to be the maximal length of a sequence in G which contains no nonempty subsequence with product 1 and let $D(G) = d(G) + 1$ (see [7], Definition 2.8.12).

Let R be a finite commutative ring with identity 1. Let $R^\times = R \setminus \{0\}$ be the multiplicative semigroup of R, and let $U(R)$ be the group of units of R. Then, $U(R)$ is a subsemigroup of $R^\times$. So we have

Proposition 1.2 *If R is a finite commutative ring with identity then $D(U(R)) \leq D(R^\times)$.*

Let Z_n denote the residual class ring modulo n, and let $Z_{n_1} \oplus \cdots \oplus Z_{n_r}$ be the direct sum of $Z_{n_1}, \ldots, Z_{n_r}$. Our main result in this paper is the following

Theorem 1.3 *If $R = Z_{n_1} \oplus \cdots \oplus Z_{n_r}$ then $D(R^\times) = D(U(R)) + P_2$, where $P_2 = \#\{1 \leq i \leq r : 2 \parallel n_i\}$.*

Remark 1.4 *If G is a finite abelian group, and if H is a proper subgroup of G, then it is well known that $D(G) > D(H)$. Theorem 1.3 shows that the result above is not true for semigroups in general.*

2 Proof of Theorem 1.3

Lemma 2.1 *([7], Lemma 6.1.3) Let G be a finite abelian group, and H be a subgroup of G. Then, $D(G) \geq D(G/H) + D(H) - 1$.*

Lemma 2.2 *Let $r \geq 1$, and let $n_1, \ldots, n_r$ be positive integers. Let $i \in \{1, \ldots, r\}$, and let p be a prime divisor of n_i. Let $m_i = n_i/p$, let $R_1 = Z_{n_1} \oplus \cdots \oplus Z_{n_r}$ and let $R_2 = Z_{n_1} \oplus \cdots \oplus Z_{n_{i-1}} \oplus Z_{m_i} \oplus Z_{n_{i+1}} \oplus \cdots \oplus Z_{n_r}$. If $p^2 \mid n_i$, then $D(U(R_2)) \leq D(U(R_1)) - p + 1$. If $p \parallel n_i$, then $D(U(R_2)) \leq D(U(R_1)) - p + 2$.*

Proof. Let C_n denote the cyclic group of n elements. Note that $U(R_2)$ is a subgroup of $U(R_1)$, and $U(R_1)/U(R_2) \simeq U(Z_{n_i})/U(Z_{m_i}) \simeq C_p$ or C_{p-1} according to $p^2|n_i$ or not. Now the lemma follows from Lemma 2.1. □

Let $r \geq 1$, and $n_1, \ldots, n_r$ be positive integers. For each $i \in \{1, \ldots, r\}$, let κ_i denote the canonical projection from $\bigoplus_{i=1}^{r} Z_{n_i}$ onto Z_{n_i} given by

$$\kappa_i(a_1, \ldots, a_i, \ldots, a_r) = a_i, \forall (a_1, \ldots, a_i, \ldots, a_r) \in \bigoplus_{i=1}^{r} Z_{n_i},$$

and ι_i denote the canonical injection from Z_{n_i} to $\bigoplus_{i=1}^{r} Z_{n_i}$ given by

$$\iota_i(a_i) = (1, \ldots, 1, a_i, 1, \ldots, 1), \forall a_i \in Z_{n_i}.$$

Let $S = g_1 \cdots g_k$ be a sequence of elements in $\bigoplus_{i=1}^{r} Z_{n_i}$. A subsequence T of S is called homogeneous if $\gcd(\kappa_i(\pi(T)), n_i) = \gcd(\kappa_i(\pi(S)), n_i)$ for every $i \in \{1, \ldots, r\}$.

Lemma 2.3 *Let $r \geq 1$, and $n_1, \ldots, n_r$ be positive integers. Let $R = \bigoplus_{i=1}^{r} Z_{n_i}$ and let S be a sequence of elements in $R^\times$. Let $t_i = \gcd(\kappa_i(\pi(S)), n_i)$ for every $i \in \{1, \ldots, r\}$. Then S is reducible if and only if there exists a proper homogeneous subsequence T of S such that ST^{-1} contains a nonempty subsequence W with $\pi(W) - 1_R \in (\frac{n_1}{t_1}, \ldots, \frac{n_r}{t_r})R = \bigoplus_{i=1}^{r} \frac{n_i}{t_i} Z_{n_i}$.*

Proof. Suppose that S is reducible. Then S contains a proper subsequence T such that $\pi(T) = \pi(S)$. Let $W = ST^{-1}$. Let $\mathbf{h} = (\frac{\kappa_1(\pi(T))}{t_1}, \ldots, \frac{\kappa_r(\pi(T))}{t_r})$ and $\mathbf{t} = (t_1, \ldots, t_r)$. Since $\mathbf{t} * \mathbf{h} = \pi(T) = \pi(S) = \pi(T) * \pi(W) = \mathbf{t} * \mathbf{h} * \pi(W)$, it follows that $(\mathbf{h} * \pi(W) - \mathbf{h}) * \mathbf{t} = 0_R$, and so $(\mathbf{h} * \pi(W) - \mathbf{h}) \in (\frac{n_1}{t_1}, \ldots, \frac{n_r}{t_r})R$, or

$$\mathbf{h} * (\pi(W) - 1_R) \in (\frac{n_1}{t_1}, \ldots, \frac{n_r}{t_r})R.$$

Since $t_i = \gcd(\kappa_i(\pi(S)), n_i) = \gcd(\kappa_i(\pi(T)), n_i)$, we have $\gcd(\frac{\kappa_i(\pi(T))}{t_i}, \frac{n_i}{t_i}) = 1$ for every $i \in \{1, \ldots, r\}$. Therefore, $\pi(W) - 1_R \in (\frac{n_1}{t_1}, \ldots, \frac{n_r}{t_r})R$.

Conversely, suppose that T is a proper homogeneous subsequence of S such that ST^{-1} contains a nonempty subsequence W with $\pi(W) - 1_R \in (\frac{n_1}{t_1}, \ldots, \frac{n_r}{t_r})R$. Put $T_0 = SW^{-1}$. Since T is contained in T_0, we see that $t_i \mid \kappa_i(\pi(T_0))$ for $i = 1, \ldots, r$. It follows that $\pi(T_0) * (\pi(W) - 1_R) = 0_R$, and so $\pi(T_0) = \pi(T_0) * \pi(W) = \pi(S)$. □

For any positive integer $t > 1$, write $t = p_1 \cdots p_\ell$ where $p_1, \ldots, p_\ell$ are primes (not necessarily distinct). Define $\Omega(t) = \ell$ the number of prime factors of t. For convenience, let $\Omega(1) = 0$.

Proof of Theorem 1.3.

Choose an arbitrary sequence S in $R^\times$ of length $D(U(R))+P_2$. Let $t_i = \gcd(\kappa_i(\pi(S)), n_i)$ for $i = 1, \ldots, r$. Let $R_0 = Z_{\frac{n_1}{t_1}} \oplus \cdots \oplus Z_{\frac{n_r}{t_r}}$ and let ϕ be the canonical epimorphism from R onto R_0.

If $\pi(S) \in U(R)$ then S is a sequence in $U(R)$ of length $\geq D(U(R))$. Therefore, S is reducible. Otherwise, $\pi(S) \notin U(R)$. We can choose a homogeneous subsequence T of S and of length at most $\sum\limits_{i=1}^{r} \Omega(t_i)$. Since $\phi(\pi(ST^{-1})) \in U(R_0)$, it follows that $\phi(ST^{-1})$ is a subsequence in $U(R_0)$. Applying lemma 2.2 repeatedly, we have $|\phi(ST^{-1})| = |ST^{-1}| \geq |S| - \sum\limits_{i=1}^{r} \Omega(t_i) = D(U(R)) + P_2 - \sum\limits_{i=1}^{r} \Omega(t_i) \geq D(U(R_0))$. It follows that ST^{-1} contains a nonempty subsequence W such that $\pi(\phi(W)) = 1_{R_0}$, or, equivalently, $\pi(W) - 1_R \in \ker(\phi) = (\frac{n_1}{t_1}, \ldots, \frac{n_r}{t_r})R$. Using lemma 2.3, we have that S is reducible, which implies that $D(R^\times) \leq D(U(R)) + P_2$.

Next, we shall provide an example to show that $D(R^\times) \geq D(U(R)) + P_2$. We can assume without loss of generality that $\{1 \leq i \leq r : 2 \parallel n_i\} = [1, P_2]$. Let $m_i = n_i/2$ for each $i \in [1, P_2]$, and let $m_i = n_i$ for each $i \in [P_2+1, r]$. Let $R_1 = Z_{m_1} \oplus \cdots \oplus Z_{m_r}$. Then, $U(R_1) \simeq U(R)$. Let φ be the canonical epimorphism from R onto R_1. Choose a sequence W in $U(R_1)$ of length $D(U(R_1)) - 1 = D(U(R)) - 1$ such that W contains no nonempty subsequence V with $\pi(V) = 1_{R_1}$. Note that φ induces a homomorphism $\widetilde{\varphi} : \mathcal{F}(R^\times) \to \mathcal{F}(R_1^\times)$. Let $\widetilde{W} \in \mathcal{F}(R^\times)$ such that $\widetilde{\varphi}(\widetilde{W}) = W$, and

$$S = \widetilde{W} \cdot \prod_{i=1}^{P_2} \iota_i(2).$$

Applying lemma 2.3, we have that S is irreducible, which implies that $D(R^\times) \geq |S|+1 = D(U(R_1)) + P_2 = D(U(R)) + P_2$. This completes the proof. □

3 Relative Davenport constant

M. Skalba formulated the relative Davenport constant in finite abelian groups in [13] as follows. Let G be a finite abelian group. For every $g \in G$, let $D_g(G)$ denote the greatest integer $d \in \mathbb{N}$ with the following property that there exists a sequence $S \in \mathcal{F}(G)$ of length d and of product g which contains no nonempty, proper subsequence with product 1. The constant $D_g(G)$ is called the relative Davenport constant.

In this section, we shall give the version of relative Davenport constant in semigroups.

Definition 3.1 *Let G be a finite commutative semigroup. For any element g of G, we define $D_g(G)$, the relative Davenport constant of G with respect to g, as the greatest integer $d \in \mathbb{N}$ with the property that there exists a sequence S with $\pi(S) = g$ and of d elements in G, which contains no empty, proper subsequence T such that $\pi(T) = \pi(S)$.*

Note that if g is not unity 1, then $D_g(G)$ is the greatest integer $d \in \mathbb{N}$ such that there exists an irreducible sequence S in G with $\pi(S) = g$ and of length d.

Theorem 3.2 *Let $R = Z_{n_1} \oplus \cdots \oplus Z_{n_r}$. For any element $\mathbf{g} = (g_1, \ldots, g_r)$ of $R^\times$, let $t_i = \gcd(g_i, n_i)$ for $i = 1, \ldots, r$. Let $R_0 = Z_{\frac{n_1}{t_1}} \oplus \cdots \oplus Z_{\frac{n_r}{t_r}}$. Then*

$$D_{\mathbf{g}}(R^\times) = \begin{cases} D_{\mathbf{g}}(U(R)) & : \quad \mathbf{g} \in U(R) \\ D(U(R_0)) + \sum\limits_{i=1}^{r} \Omega(t_i) - 1 & : \quad \mathbf{g} \notin U(R) \end{cases}.$$

Proof. Suppose that $\mathbf{g} \in U(R)$. For any sequence S in $R^\times$, if $\pi(S) = \mathbf{g}$, then S must be a sequence in $U(R)$. Thus, it follows that $D_{\mathbf{g}}(R^\times) = D_{\mathbf{g}}(U(R))$.

Suppose that $\mathbf{g} \notin U(R)$, that is, $t_i > 1$ for some $i \in [1, r]$. We can assume without loss of generality that $t_1 > 1$. Let ϕ be the canonical epimorphism from R onto R_0.

For any sequence S of length $D(U(R_0)) + \sum\limits_{i=1}^{r} \Omega(t_i)$ such that $\pi(S) = \mathbf{g}$, similarly as Theorem 1.3, we can prove S is reducible. Thus, we conclude that $D_{\mathbf{g}}(R^\times) \leq D(U(R_0)) + \sum\limits_{i=1}^{r} \Omega(t_i) - 1$.

Next, it suffices to show that $D_{\mathbf{g}}(R^\times) \geq D(U(R_0)) + \sum\limits_{i=1}^{r} \Omega(t_i) - 1$. For each $i \in [1, r]$, let $t_i = p_{i,1} p_{i,2} \cdots p_{i,\Omega(t_i)}$ be the prime factorization of t_i. Let $\mathbf{g_0} = (\frac{g_1}{t_1}, \ldots, \frac{g_r}{t_r})$. Choose a sequence W in $U(R_0)$ of length $D(U(R_0)) - 1$ such that W contains no nonempty subsequence V with $\pi(V) = 1_{R_0}$. Since $\phi(\mathbf{g_0}) \in U(R_0)$, there exists an element $\mathbf{h} \in U(R_0)$ such that $\pi(W) * \mathbf{h} = \phi(\mathbf{g_0})$. For any element $\mathbf{a}$ of W (or $\mathbf{h}$), we can choose an element $\tilde{\mathbf{a}}$ ($\tilde{\mathbf{h}}$) of $U(R)$ such that $\phi(\tilde{\mathbf{a}}) = \mathbf{a}$ ($\phi(\tilde{\mathbf{h}}) = \mathbf{h}$, respectively). Let sequence $\tilde{W} = \prod\limits_{\mathbf{a}|W} \tilde{\mathbf{a}}$. Put $S = \tilde{W} \cdot (\tilde{\mathbf{h}} * \iota_1(p_{1,1})) \cdot \iota_1(p_{1,2}) \cdots \iota_1(p_{1,\Omega(t_1)}) \cdot \prod\limits_{i=2}^{r} \prod\limits_{j=1}^{\Omega(t_i)} \iota_i(p_{i,j})$. Since $\pi(\tilde{W}) * \tilde{\mathbf{h}} - \mathbf{g_0} \in \ker(\phi) = (\frac{n_1}{t_1}, \ldots, \frac{n_r}{t_r})R$, it follows that $\pi(S) = \mathbf{g}$. Applying lemma 2.3, we have that S is irreducible, which implies that $D_{\mathbf{g}}(R^\times) \geq |S| = D(U(R_0)) + \sum\limits_{i=1}^{r} \Omega(t_i) - 1$. This completes the proof. □

Acknowledgement. We would like to thank the referee for his/her very useful suggestion. This work has been supported by the 973 Project, the PCSIRT Project of the Ministry of Education, the Ministry of Science and Technology, and the National Science Foundation of China.

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] V. Dimitrov, *On the strong Davenport constant of nonabelian finite p-groups*, Math. Balkanica **18**(2004) 131–140.

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

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

[7] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory,* Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2005.

[8] A. Geroldinger and R. Schneider, *The cross number of finite abelian groups III*, Discrete Mathematics, **150**(1996) 123-130.

[9] F. Halter-Koch, *A generalization of Davenport's constant and its arithmetical 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 I*, 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 the relative Davenport constant*, Eur. J. Comb. **19**(1998) 221-225.