What is the Davenport Constant?

Austin Antoniou

26 June 2018

The Davenport constant is a combinatorial invariant of finite abelian groups which has now been fruitfully studied for over five decades by mathematicians with diverse backgrounds and motivations. Herein we discuss the basics of the Davenport constant, including some classical results and some of its connections to factorization theory.

We will begin by stating all the necessary definitions and notation, recall some notions from multiplicative ideal theory, then proceed to summarize some of the highlights of the study of the Davenport constant.

1 Preliminaries

1.1 Notation: Groups

Let G be an additively-written finite abelian group. Recall that we may write G according to its *invariant factor decomposition*, that is, as a product

$$G = C_{n_1} \times \cdots \times C_{n_r}$$

where C_n denotes the cyclic group of order n and $n_1, \ldots, n_r$ are positive integers satisfying $n_1 > 1$ and $n_1 | \cdots | n_r$.

- $|G|$ is the order of G.
- $\mathrm{rank}(G) = r$ is the *rank* of G (which is well-defined since the invariant decomposition is unique).
- $\exp(G) = n_r$ is the *exponent* of G.

Each of these quantities can be thought of as a useful measure of the "size" of G, depending on the circumstance.

1.2 Notation: Sequences

Denote by $\mathcal{F}(G)$ the *free abelian monoid* over G. $\mathcal{F}(G)$ consists of all (unordered) formal words in the elements of G, and words are multiplied by concatenation. We call the elements of $\mathcal{F}(G)$ *sequences* over G, and the identity element $\emptyset$ is called the empty sequence (If the reader prefers, the elements of $\mathcal{F}(G)$ can be thought of as multisets, with the operation of union).

Let $S = g_1 \cdots g_\ell \in \mathcal{F}(G)$.

- $|S| = \ell$ is the *length* of S.

- $\sigma(S) = g_1 + \cdots + g_\ell \in G$ is the *sum* of S.
- T is a *subsequence* of S if there is some $S' \in \mathcal{F}(G)$ with $S = TS'$; we write $T|S$ and $ST^{-1} = S'$.
- $\Sigma(S) = \{\sigma(T) : T|S, T \neq \emptyset\}$ is the *set of subsums* of S.
  - S is a *zero-free sequence* if $0 \notin \Sigma(S)$.
  - S is a *zero-sum sequence* if $\sigma(S) = 0$.
  - S is a *minimal zero-sum sequence* if $\sigma(S) = 0$ but $\sigma(T) \neq 0$ for all proper subsequences $T|S$.

1.3 The Main Problem(s)

Let G be a finite abelian group. The **Davenport constant** of G is

$$D(G) = \inf\{\ell \in \mathbb{N} : S \in \mathcal{F}(G), |S| = \ell \Rightarrow 0 \in \Sigma(S)\}$$

A closely-related quantity which often appears in the literature is the *small Davenport constant*:

$$d(G) = \sup\{\ell \in \mathbb{N} : \exists S \in \mathcal{F}(G), |S| = \ell \text{ and } 0 \notin \Sigma(S)\}$$

$d(G)$ is the length of a longest zero-free sequence over G, and satisfies the relation $d(G)+1 = D(G)$. We may observe that, if S is a zero-free sequence, then $T = S(-\sigma(S))$ is a minimal zero-sum sequence. Conversely, if T is a minimal zero-sum sequence and $g|T$ then $S = g^{-1}T$ is a zero-free sequence. This allows us to make the more modern formulation of the Davenport constant, namely:

$$D(G) = \sup\{|S| : S \in \mathcal{F}(G) \text{ is a minimal zero-sum sequence}\}$$

Problem 1.1 (Direct Davenport Problem). *Given a finite abelian group G, what is the exact value of $D(G)$?*

Problem 1.2 (Inverse Davenport Problem). *If S is a longest minimal zero-sum sequence over G (of length $D(G)$), what is the structure of S?*

2 Motivation from Ring Theory

Before taking any steps to solve the problems posed above, we should first visit the historical motivation for studying $D(G)$. Harold Davenport first introduced his constant at the 1966 Conference in Group Theory and Number Theory at The Ohio State University to help further the study of factorization in algebraic number rings. At this point, it was well-known that a number ring D need not be a unique factorization domain (UFD). However, D is a Dedekind domain, meaning that its nonzero fractional ideals form a group and we can study the ideal class group $\text{Cl}(D) = F(D)/\text{Prin}(D)$ (defined in detail below).

Let $G = \text{Cl}(D)$. The first observation to make about the class group is that $|G| = 1$ exactly when D is a PID, which implies that D is a UFD.

In 1960, Carlitz addressed the next case: $|G| = 2$ (see [2]). He showed that if $|G| = 2$ then D is a half factorial domain (HFD), meaning that each element of D has a unique *length* of irreducible factorization. That is, a given element may have several different factorizations into products of irreducible elements, but each of these products is of the same length.

From here, the question emerges: what precise statements can be made about the factorization of elements in D when G is any abelian group?

2.1 Details of the Ideal Class Group

Recall that a domain D is a *Dedekind domain* if every ideal of D has a unique factorization into prime ideals; that is, for any nonzero ideal $I \subseteq D$, there are prime ideals $P_1, \ldots, P_k \subseteq D$ such that $I = P_1 \cdots P_k$.

Let K denote the field of fractions of D. A *fractional ideal* of D is a D-module $I \subseteq K$ such that $dI \subseteq D$ for some element $d \in D$. For a nonzero fractional ideal I, we can define $I^{-1} = \{a \in K : aI \subseteq D\}$; this is an inverse to I in the sense that $II^{-1} = I^{-1}I = D$.

Thus the set $F(D)$ of nonzero fractional ideals of D forms a group. Then, letting $\operatorname{Prin}(D)$ denote the group of nonzero principal ideals of D, we define the **ideal class group** of D by

$$\operatorname{Cl}(D) = F(D)/\operatorname{Prin}(D).$$

2.2 A Measure of Non-Uniqueness

For a domain D, denote by $\mathcal{A}(D)$ the set of irreducible elements (or *atoms*) of D. We mentioned above that the order of the ideal class group indicates (for small groups, at least) that the lengths of factorizations of elements of D are controlled in some sense. We now develop the notion of elasticity to help make this precise.

Given a nonzero element $x \in D$, let

$$\mathsf{L}(x) = \{\ell \in \mathbb{N} : \exists a_1, \ldots, a_\ell \in \mathcal{A}(D), x = a_1 \cdots a_\ell\}$$

be the *set of (factorization) lengths* of x. We define the *elasticity* of x to be $\rho(x) = \frac{\sup L(x)}{\inf L(x)}$ and the **elasticity** of D to be

$$\rho(D) = \sup_{x \neq 0} \rho(x).$$

Observe that $\rho(D) = 1$ if and only if D is a half-factorial domain.

2.3 Elasticity and the Davenport Constant

With all of this in place, we can make a formal statement which ties the unruliness of factorization in a Dedekind domain D to the Davenport constant of $\operatorname{Cl}(D)$.

Theorem 2.1. *Let D be a Dedekind domain which is not a UFD and let G be the ideal class group of D.*

1. *$\rho(D) \leq \frac{D(G)}{2}$ (see [1, Corollary 2.3]).*
2. *$\rho(D) = \frac{D(G)}{2}$ if G is finite and each ideal class in G contains a prime of D (see [14, Proposition 1]).*

3 Investigating the Davenport Constant

Even now, the question of determining Davenport constant of a finite abelian group remains mostly open. However, the elementary steps toward this goal, in addition to being highly instructive, exemplify top-quality mathematics.

3.1 Determining $D(G)$: Early Results

We should first make sure that our goal is sensible; that is, ensure that $D(G)$ is finite under reasonable circumstances.

Lemma 3.1. *Let G be a finite abelian group. Then $D(G) \leq |G|$.*

Proof. Suppose $S = g_1 \cdots g_n$ is a sequence over G with $n \geq |G|$. Consider the sums of the subsequences $S_k = g_1 \cdots g_k$ for $k = 1, \ldots, n$. Either $\sigma(S_k) = 0$ for some k, or else $S_j = S_k$ for some $j < k$. Then $\sigma(g_{j+1} \cdots g_k) = \sigma(S_k S_j^{-1}) = \sigma(S_k) - \sigma(S_j) = 0$. In either case, we find that there is a subsequence $T|S$ with $\sigma(T) = 0$. □

The next order of business is securing a reasonable general lower bound as a starting point for closing in on the exact value of $D(G)$ for specific classes of groups. For convenience, if G has invariant factor decomposition $G = C_{n_1} \times \cdots \times C_{n_r}$, we set $D^*(G) = 1 + \sum_{i=1}^{r}(n_i - 1)$.

Lemma 3.2. *Let G be a finite abelian group. Then $D(G) \geq D^*(G)$.*

Proof. To prove this, it is sufficient to construct a zero-free sequence of length $D^*(G) - 1 = \sum_{i=1}^{r}(n_i - 1)$. Writing $G = C_{n_1} \times \cdots \times C_{n_r}$, let $C_{n_i} = \langle e_i \rangle$ for each i. Then set $S = e_1^{n_1-1} \cdots e_r^{n_r-1}$; this is a zero-free sequence of length $D^*(G)$, so we are done. □

Corollary 3.3. *If G is a cyclic group of order n then $D(G) = n$.*

Almost by accident, we have determined the Davenport constant of all cyclic groups. We proceed now to a stunning result of J.E. Olson from 1967 which does the same for finite abelian p-groups.

Theorem 3.4 (Olson, [11])**.** *Let p be a prime and $G = C_{p^{k_1}} \times \cdots \times C_{p^{k_r}}$ be a finite abelian p-group. Then $D(G) = D^*(G)$.*

Proof. Let $S = g_1 \cdots g_n$ be a sequence with $n \geq D^*(G)$. We will consider the group ring $\mathbb{Z}[G] = \mathbb{Z}[\{X^g : g \in G\}]$. Specifically, consider the element $P = \prod_{i=1}^{n}(1 - X^{g_i})$.

First, we examine P from an algebraic viewpoint; our goal is to decompose P in terms of the elements X^{e_i}, where e_i generates the ith factor of G. To this end, Observe that

$$1 - X^{a+b} = (1 - X^a) + X^a(1 - X^b)$$

for any group elements $a, b \in G$. Iteratively rewriting elements in this way, we can express

$$P = \sum_{\alpha} h_\alpha P_\alpha,$$

where the h_α are some elements of G and P_α has the form

$$P_\alpha = (1 - X^{e_1})^{f_1} \cdots (1 - X^{e_r})^{f_r}$$

with f_i nonnegative integers satisfying $f_1 + \cdots + f_r = n$.

Since $n > \sum_{i=1}^{r}(p^{k_i} - 1)$, we must have $f = f_i \geq p^{e_i}$ for some i. Letting $k = k_i$, it then follows that

$$(1 - X^{e_i})^{p_k} \equiv 0 \mod p$$

This tells us that $P_\alpha \equiv 0 \pmod{p}$ for each α, so $P \equiv 0 \pmod{p}$.

Now we interpret P combinatorially:

$$P = \prod_{i=1}^{n}(1 - X^{g_i}) = \sum_{g \in G} N(S, g) X^g$$

where we define

$$N(S, g) = |\{T|S : \sigma(T) = g \text{ and } |T| \text{ is even}\}| - |\{T|S : \sigma(T) = g \text{ and } |T| \text{ is odd}\}|$$

Now, because the X^g are linearly independent over $\mathbb{Z}/(p) \cong \mathbb{F}_p$, $P \cong 0$ implies that $N(S, g) \equiv 0$ for all g. In particular, $N(S, 0) \equiv 0$. We know that there is at least one subsequence of S of even length with sum zero; namely, the empty sequence. Thus, to have the above congruence, there must be another subsequence $T|S$ with $\sigma(T) = 0$. □

This proof leans heavily on the fact that G is a p-group, which enables us to use some elementary vector space techniques over $\mathbb{F}_p$ that would otherwise be unavailable. However, the proof has no dependence on the rank of G. We can use this to more systematically determine the Davenport constant of groups of higher rank. First, we need a new definition and a lemma.

Definition 3.5. Let G be a finite abelian group. The *eta invariant* of G is

$$\eta(G) = \inf\{\ell \in \mathbb{N} : |S| \geq \ell \Rightarrow \text{ there is } T|S \text{ with } \sigma(T) = 0 \text{ and } |T| \leq \exp(G)\}$$

In other words, $\eta(G)$ is the minimal length required for a sequence to have a *short* zero-sum subsequence (in contrast to the ordinary Davenport constant, which omits the "short" requirement).

Lemma 3.6. *Let $G = C_p \times C_p$. Then $\eta(G) = 3p - 2$; that is, if S is a sequence over G of length at least $3p - 2$ then S has a zero-sum subsequence of length at most p.*

Proof. Let $S = x_1 \cdots x_\ell$ be a sequence over C_p^2. We identify C_p^2 with the subgroup of C_p^3 whose elements have third coordinate equal to zero. Consider the modified sequence $T = S + (0, 0, 1)$; that is, $T = (x_1, 1) \cdots (x_\ell, 1)$. Then, since $D(C_p^3) = 3p - 2$ by Theorem 3.4, we know that T has a zero subsequence $U = V + (0, 0, 1)$. Because the third coordinate of each element of T has order p, we know that $|U| = p$ or $2p$.

If $|U| = p$ then V is a short zero sequence over C_p^2 and we need look no further. If $|U| = |V| = 2p > D(C_p^2)$, then V has a zero sequence of length smaller than $2p$; either this subsequence or its complement in V has length smaller than p, and we are done. □

With this in hand, we can determine $D(G)$ for all groups of rank two.

Theorem 3.7 (Olson, [12])**.** *Let $G = C_m \times C_n$ with $m|n$. Then $D(G) = m + n - 1 = D^*(G)$.*

Proof. We induct on the order m of the first cyclic factor. We have already resolved the $m = 1$ case (in which G is cyclic).

In the general case, let S be a sequence over G with $|S| \geq D^*(G)$. Suppose p is a prime divisor of m, hence a prime divisor of n. There is a quotient map $\pi : G \to C_p \times C_p$ whose kernel H is isomorphic to $C_{m/p} \times C_{n/p}$; in other words, there is an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \underbrace{C_{m/p} \times C_{n/p}}_{=H} \arrow[r] & C_m \times C_n \arrow[r, "\pi"] & C_p \times C_p \arrow[r] & 0 \end{tikzcd}$$

Consider the sequence $\pi(S)$ over $C_p \times C_p$. Observe that

$$|\pi(S)| \geq D^*(C_m \times C_n) = m + n - 1 = p\left(\frac{m}{p} + \frac{n}{p} - 3\right) + 3p - 1$$

By the previous lemma, we can remove a subsequence T_0 of S such that $|T_0| \leq p$ and $\sigma(\pi(T_0)) = 0$ (equivalently, $\sigma(T_0) \in H$).

In fact, we can continue to remove disjoint sequences $T_1, \ldots, T_\ell$ in this manner (where $\ell = \frac{m}{p} + \frac{n}{p} - 3$) so that $|T_i| \leq p$ and $\sigma(T_i) \in H$ for each i.

This leaves at least $2p - 1 = D(C_p \times C_p)$ elements in $S \setminus (T_0 \cdots T_\ell)$, so we can find an additional sequence $T'|S \setminus (T_0 \cdots T_\ell)$ with $\sigma(T) \in H$. We can now consider the sequence $S^* = \sigma(T')\sigma(T_0) \cdots \sigma(T_\ell)$ over $H \leq G$; since $|S^*| = \ell + 2 = \frac{m}{p} + \frac{n}{p} - 1 = D(H)$, S^* has a zero sum. Thus $0 \in \sigma(S^*) \subseteq \sigma(S)$, which is what we needed to show. □

3.2 Determining $D(G)$: Beyond Rank 2

The theorems of Olson we have seen suggest the conjecture that $D(G) = D^*(G)$ for all finite abelian groups G. However, the next wave of results, due to P. van Emde Boas and P.C. Baayen, reveal that this is merely wishful thinking. In particular:

Theorem 3.8 (Baayen, [15])**.** *For any $k \geq 1$, the group $G = C_2^{4k} \times C_{4k+2}$ has $D(G) > D^*(G)$.*

The smallest group this theorem yields is $G = C_2^4 \times C_6$. To see the zero-free sequence of length $D^*(G) = 10$ which demonstrates that $D(G) > D^*(G)$, we first write $G \cong C_2^5 \times C_3$. In these coordinates, we may express the sequence as

$$S = \begin{array}{cccccccccc} \begin{pmatrix}1\\0\\0\\0\\0\\1\end{pmatrix} & \begin{pmatrix}0\\1\\0\\0\\0\\1\end{pmatrix} & \begin{pmatrix}0\\0\\1\\0\\0\\1\end{pmatrix} & \begin{pmatrix}0\\0\\0\\1\\0\\1\end{pmatrix} & \begin{pmatrix}0\\0\\0\\0\\1\\1\end{pmatrix} & \begin{pmatrix}0\\1\\1\\1\\1\\1\end{pmatrix} & \begin{pmatrix}1\\0\\1\\1\\1\\1\end{pmatrix} & \begin{pmatrix}1\\1\\0\\1\\1\\1\end{pmatrix} & \begin{pmatrix}1\\1\\1\\0\\1\\1\end{pmatrix} & \begin{pmatrix}1\\1\\1\\1\\0\\1\end{pmatrix} \\ e_1 & e_2 & e_3 & e_4 & e_5 & f_1 & f_2 & f_3 & f_4 & f_5 \end{array}$$

$C_2^4 \times C_6$ has order 96 and rank 5. This raises the question of whether a smaller counterexample exists. This question was answered shortly after Baayen's example was give, in the form of the following theorem.

Theorem 3.9 (Kruyswijk and van Emde Boas, [16])**.** *Let $n \geq 2$ and $k \geq 2$ such that $\gcd(n, k) = 1$ and let $0 \leq \rho \leq n - 1$. If*

$$G = C_n^{(k-1)n+\rho} \times C_{kn}$$

then

(a) $D(G) - D^*(G) \geq \rho$ if $1 \leq \rho \leq n - 1$ and $\rho \not\equiv n \mod k$.

(b) $D(G) - D^*(G) \geq \rho + 1$ if $\rho \leq n - 2$ and $x(n - \rho + 1) \not\equiv n \mod k$ for $x = 1, \ldots, n - 1$.

Applying this result for $n = 3$, $k = 2$, and $\rho = 0$, we get:

Corollary 3.10. *$G = C_3 \times C_3 \times C_3 \times C_6$ satisfies $D(G) > D^*(G)$.*

With these examples, we can refine our original conjecture that $D(G) = D^*(G)$ for all groups G.

Conjecture 3.11. *If G is a finite abelian group of rank 3 then $D(G) = D^*(G)$.*

Conjecture 3.12. *If $n \geq \mathbb{N}$, $r \geq 1$, and $G = C_n^r$ then $D(G) = 1 + r(n - 1) = D^*(G)$.*

Both of these conjectures remain open. After being ignored for several decades, these problems were revisited in the 1990s and early 2000s by a new group of mathematicians. A. Geroldinger, W.D. Gao, and many others with interests in factorization theory or combinatorics lent fresh eyes to zero-sum problems of the flavor of Problem 1.1 (See, for example, [9, 10, 5]) This led to several new results, new techniques, and a renewed interest in algebraic approaches and applications for combinatorial problems on groups.

In the mid 2000s, the focus shifted from determining $D(G)$ for groups G of high rank to determining the exact structure of minimal zero-sum sequences (as in Problem 1.2). This problem was solved completely for groups of rank 2 in a series of papers by A. Geroldinger, W.D. Gao, W. Schmid, C. Reiher, and others [7, 13, 6].

The factorization theory community remains engaged in employing combinatorial viewpoints to better understand various aspects of factorization. The survey [8] gives a friendly introduction to some ways in which researchers are trying to do this.

References

[1] D. D. Anderson and David F. Anderson. Elasticity of factorizations in integral domains. *J. Pure Appl. Algebra*, 80(3):217–235, 1992.

[2] L. Carlitz. A characterization of algebraic number fields with class number two. *Proc. Amer. Math. Soc.*, 11:391–392, 1960.

[3] Scott T. Chapman, Michael Freeze, and William W. Smith. On generalized lengths of factorizations in Dedekind and Krull domains. In *Non-Noetherian commutative ring theory*, volume 520 of *Math. Appl.*, pages 117–137. Kluwer Acad. Publ., Dordrecht, 2000.

[4] Scott T. Chapman and William W. Smith. An inequality concerning the elasticity of Krull monoids with divisor class group $\mathbb{Z}_p$. *Ric. Mat.*, 56(1):107–117, 2007.

[5] W. Gao. On Davenport's constant of finite abelian groups with rank three. *Discrete Math.*, 222(1-3):111–124, 2000.

[6] Weidong Gao, Alfred Geroldinger, and David J. Grynkiewicz. Inverse zero-sum problems. III. *Acta Arith.*, 141(2):103–152, 2010.

[7] Weidong Gao, Alfred Geroldinger, and Wolfgang A. Schmid. Inverse zero-sum problems. *Acta Arith.*, 128(3):245–279, 2007.

[8] Alfred Geroldinger. Sets of lengths. *Amer. Math. Monthly*, 123(10):960–988, 2016.

[9] Alfred Geroldinger, Manfred Liebmann, and Andreas Philipp. On the Davenport constant and on the structure of extremal zero-sum free sequences. *Period. Math. Hungar.*, 64(2):213–225, 2012.

[10] Alfred Geroldinger and Rudolf Schneider. On Davenport's constant. *J. Combin. Theory Ser. A*, 61(1):147–152, 1992.

[11] John E. Olson. A combinatorial problem on finite Abelian groups. I. *J. Number Theory*, 1:8–10, 1969.

[12] John E. Olson. A combinatorial problem on finite Abelian groups. II. *J. Number Theory*, 1:195–199, 1969.

[13] Wolfgang A. Schmid. Inverse zero-sum problems II. *Acta Arith.*, 143(4):333–343, 2010.

[14] Jean-Luc Steffan. Longueurs des décompositions en produits d'éléments irréductibles dans un anneau de Dedekind. *J. Algebra*, 102(1):229–236, 1986.

[15] P. van Emde Boas. A combinatorial problem on finite abelian groups. II. *Math. Centrum Amsterdam Afd. Zuivere Wisk.*, 1969(ZW-007):60, 1969.

[16] P. van Emde Boas and D. Kruyswijk. *A Combinatorial Problem on Finite Abelian Groups III.* Stichting Mathematisch Centrum. Afd. Zuivere Wiskunde. Stichting Mathematisch Centrum, 1969.