A GENERALIZATION OF DAVENPORT’S CONSTANT 
AND ITS ARITHMETICAL APPLICATIONS

BY
FRANZ HALTER-KOCH (GRAZ)

1. For an additively written finite abelian group $G$, Davenport’s constant $D(G)$ is defined as the maximal length $d$ of a sequence $(g_1, \ldots, g_d)$ in $G$ such that $\sum_{j=1}^{d} g_j = 0$, and $\sum_{j\in J} g_j \neq 0$ for all $\emptyset \neq J \subset \{1, \ldots, d\}$. It has the following arithmetical meaning:

Let $K$ be an algebraic number field, $R$ its ring of integers and $G$ the ideal class group of $R$. Then $D(G)$ is the maximal number of prime ideals (counted with multiplicity) which can divide an irreducible element of $R$. This fact was first observed by H. Davenport (1966) and worked out by W. Narkiewicz [8] and A. Geroldinger [4].

For a subset $Z \subset R$ and $x > 1$ we denote by $Z(x)$ the number of principal ideals $(\alpha)$ of $R$ with $\alpha \in Z$ and $(R : (\alpha)) \leq x$. If $M$ denotes the set of irreducible integers of $R$, then it was proved by P. Rémond [12] that, as $x \to \infty$,

$$M(x) \sim Cx(\log x)^{-1}(\log \log x)^{D(G) - 1},$$

where $C > 0$ depends on $K$; the error term in this asymptotic formula was investigated by J. Kaczorowski [7].

If an element $\alpha \in R \setminus (R^\times \cup \{0\})$ has a factorization $\alpha = u_1 \cdot \ldots \cdot u_r$ into irreducible elements $u_j \in R$, we call $r$ the length of that factorization and denote by $L(\alpha)$ the set of all lengths of factorizations of $\alpha$. For $k \geq 1$, we define sets $M_k$ and $M'_k$ (depending on $K$) as follows:

$M_k$ consists of all $\alpha \in R \setminus (R^\times \cup \{0\})$ for which $\max L(\alpha) \leq k$ (i.e., $\alpha$ has no factorization of length $r > k$);

$M'_k$ consists of all $\alpha \in R \setminus (R^\times \cup \{0\})$ for which $\min L(\alpha) \leq k$ (i.e., $\alpha$ has a factorization of length $r \leq k$).

If $G = \{0\}$, then $M_k = M'_k$ for all $k$; in the general case, we have $M_1 = M'_1 = M$ and $M_k \subset M'_k$ for all $k$.

In this paper, we generalize the results of Rémond and Kaczorowski and obtain asymptotic formulas for $M_k(x)$ and $M'_k(x)$. To do this, we shall define a sequence of combinatorial constants $D_k(G)$ ($k \geq 1$) generalizing $D(G) = D_1(G)$, and we shall obtain the following result.
Theorem. For $x \geq e^e$ and $q \in \mathbb{Z}$, $0 \leq q \leq c_0 \frac{\sqrt{\log x}}{\log \log x}$, we have

$$M_k(x) = \frac{x}{\log x} \left[ \sum_{\mu=0}^{q} \frac{W_\mu(\log \log x)}{(\log x)^\mu} + O\left( (c_1 q)^q \frac{(\log \log x)^{D_k(G)}}{(\log x)^q} \right) \right]$$

and

$$M'_k(x) = \frac{x}{\log x} \left[ \sum_{\mu=0}^{q} \frac{W'_\mu(\log \log x)}{(\log x)^\mu} + O\left( (c_1 q)^q \frac{(\log \log x)^{kD(G)}}{(\log x)^q} \right) \right],$$

where $c_0$, $c_1$ are positive constants, and $W_\mu, W'_\mu \in \mathbb{C}[X]$ are polynomials such that $\deg W_\mu \leq D_k(G)$, $\deg W'_\mu \leq kD(G)$, $\deg W_0 = D_k(G) - 1$, $\deg W'_0 = kD(G) - 1$, and $W_0, W'_0$ have positive leading coefficients.

Remarks. 1) For $k = 1$, this is [7, Theorem 1].

2) For $G = \{0\}$, we shall see that $D_k(G) = k$, and we rediscover [9, Ch. IX, § 1, Corollary 1].

3) In another context, the number $M'_k(x)$ was studied in [6].

The main part of this paper is devoted to the definition and the investigation of the invariants $D_k(G)$ and is of purely combinatorial nature. Only in the final section shall we present a proof of the above Theorem using the work of Kaczorowski.

2. Let $G$ be an additively written finite abelian group. We denote by $\mathcal{F}(G)$ the (multiplicatively written) free abelian semigroup with basis $G$. In $\mathcal{F}(G)$, we use the concept of divisibility in the usual way: $S' \mid S$ if $S = S'S''$ for some $S'' \in \mathcal{F}(G)$. Every $S \in \mathcal{F}(G)$ has a unique representation

$$S = \prod_{g \in G} g^{v_g(S)}$$

with $v_g(S) \in \mathbb{N}_0$; we call

$$\sigma(S) = \sum_{g \in G} v_g(S) \in \mathbb{N}_0$$

the size and

$$\iota(S) = \sum_{g \in G} v_g(S) \cdot g \in G$$

the content of $S$. The semigroup

$$\mathcal{B}(G) = \{ B \in \mathcal{F}(G) \mid \iota(B) = 0 \} \subset \mathcal{F}(G)$$

is called the block semigroup of $G$; we set $\mathcal{B}(G)' = \mathcal{B}(G) \setminus \{1\}$ where $1 \in \mathcal{F}(G)$ denotes the unit element. Every $B \in \mathcal{B}(G)'$ has a factorization $B = B_1 \cdots B_r$ into irreducible blocks $B_i \in \mathcal{B}(G)'$; again, we call $r$ the length
of the factorization and denote by \( L(B) \) the set of all lengths of factorizations of \( B \) in \( \mathcal{B}(G) \). Obviously, \( B \) is irreducible if and only if \( L(B) = \{1\} \), and \( D(G) = \max\{\sigma(B) \mid B \in \mathcal{B}(G)' \} \) is irreducible.

Now we define, for \( k \geq 1 \),
\[
D_k(G) = \sup\{\sigma(B) \mid B \in \mathcal{B}(G)', \max L(B) \leq k\}.
\]
Obviously, \( D_1(G) = D(G) \), and we shall see in a moment that \( D_k(G) < \infty \) for all \( k \geq 1 \).

**Proposition 1.** Let \( G \) be a finite abelian group and \( k \in \mathbb{N} \).

(i) \( kD(G) = \max\{\sigma(B) \mid B \in \mathcal{B}(G)', \min L(B) \leq k\} = \max\{\sigma(B) \mid B \in \mathcal{B}(G)', k \in L(B)\} \).

(ii) \( D_k(G) \leq kD(G) < \infty \).

(iii) \( D_k(G) = \max\{\sigma(B) \mid B \in \mathcal{B}(G)', \max L(B) = k\} \).

(iv) \( D_k(G) \) is the smallest number \( d \in \mathbb{N} \) with the property that, for every \( S \in \mathcal{F}(G) \) with \( \sigma(S) \geq d \), there exist blocks \( B_1, \ldots, B_k \in \mathcal{B}(G)' \) such that \( B_1 \cdot \ldots \cdot B_k \mid S \).

(v) If \( B \in \mathcal{B}(G) \) is a block satisfying \( \sigma(B) > kD(G) \), then there exist blocks \( B_1, B_{k+1} \in \mathcal{B}(G)' \) such that \( B = B_1 \cdot \ldots \cdot B_{k+1} \).

(vi) If \( G_1 \subsetneq G \) is a proper subgroup, then \( D_k(G_1) < D_k(G) \).

**Proof.** (i) If \( B \in \mathcal{B}(G)' \) is a block such that \( \min L(B) \leq k \), then there exists a factorization \( B = B_1 \cdot \ldots \cdot B_l \) into irreducible blocks \( B_j \in \mathcal{B}(G)' \) of length \( l \leq k \), and therefore
\[
\sigma(B) = \sum_{j=1}^{l} \sigma(B_j) \leq D(G) \leq kD(G).
\]

Hence it is sufficient to prove that there exists a block \( B \in \mathcal{B}(G) \) such that \( \sigma(B) = kD(G) \) and \( k \in L(B) \). But if \( B_0 \in \mathcal{B}(G)' \) is an irreducible block with \( \sigma(B_0) = D(G) \), then \( B = B_0 \cdot \cdot \cdot \) has the required property.

(ii) follows immediately from (i) and the definition of \( D_k(G) \).

(iii) Let \( l \) be the maximal length of a factorization of a block \( B \in \mathcal{B}(G)' \) with \( \max L(B) \leq k \) and \( \sigma(B) = D_k(G) \). If \( l < k \), then the block \( \overline{B} = B \cdot \cdot \cdot 0 \) satisfies \( \sigma(\overline{B}) = D_k(G) + 1 \) and \( \max L(\overline{B}) = l + 1 \leq k \), which contradicts the definition of \( D_k(G) \).

(iv) In order to prove that \( D_k(G) \) has the indicated property, let \( S \in \mathcal{F}(G) \) be such that \( \sigma(S) \geq D_k(G) \), set \( q = -\iota(S) \in G \) and consider the block \( S_q \in \mathcal{B}(G)' \). Since \( \sigma(S_q) > D_k(G) \), the block \( S_q \) has a factorization of length \( \nu > k \), say \( S_q = B_1 \cdot \ldots \cdot B_{\nu} \) with irreducible \( B_j \in \mathcal{B}(G)' \) and \( v_q(B_j) > 0 \). This implies \( B_1 \cdot \ldots \cdot B_{\nu} \mid S \), as asserted.

In order to prove that \( D_k(G) \) is minimal with this property, let \( B \in \mathcal{B}(G) \) be a block satisfying \( \sigma(B) = D_k(G) \) and \( \max L(B) = k \), according to (iii). If \( B = \prod_{j=1}^{d} g_j \) and \( d < D_k(G) \), then the element \( S_d = \prod_{j=1}^{d} g_j \in \mathcal{B}(G)' \).
\( \mathcal{F}(G) \) cannot be divisible by a product of \( k \) blocks, for this would imply \( \max L(B) \geq k + 1 \).

(v) If \( B = g_1 \cdot \ldots \cdot g_n \) with \( \nu > kD(G) \) then, by (iv), there exist blocks \( B_1, \ldots, B_k \in \mathcal{B}(G)' \) such that \( B_1 \cdot \ldots \cdot B_k \mid g_1 \cdot \ldots \cdot g_\nu - 1 \), and therefore the assertion follows.

(vi) By (iii), there exists a block \( B = g_1 \cdot \ldots \cdot g_N \in \mathcal{B}(G_1) \) such that \( N = \sigma(B) = D_k(G_1) \) and \( \max L(B) = k \). We pick an element \( g \in G \setminus G_1 \) and assume that \( D_k(G_1) \geq D_k(G) \). By (iv), there exist blocks \( B_1, \ldots, B_k \in \mathcal{B}(G)' \) such that \( B_1 \cdot \ldots \cdot B_k \mid g_1 \cdot \ldots \cdot g_N - g \); this implies \( B_1, \ldots, B_k \in \mathcal{B}(G_1)' \), and therefore there exists a block \( B_k+1 \in \mathcal{B}(G_1)' \) such that \( B = B_1 \cdot \ldots \cdot B_k B_k+1 \), a contradiction. \( \blacksquare \)

3. The precise value of \( D(G) \) is known only for some special types of abelian groups [2], [3]; see [5] for a survey. In the following proposition we collate those results which we shall either use or generalize in the sequel.

For \( n \geq 1 \), let \( C_n \) be the cyclic group of order \( n \).

**Proposition 2.** Let \( G = \bigoplus_{i=1}^d C_{n_i} \) be a finite abelian group with \( 1 < n_d \mid n_{d-1} \mid \ldots \mid n_1 \), and set

\[
M(G) = n_1 + \sum_{i=2}^d (n_i - 1).
\]

(i) \( M(G) \leq D(G) \leq \# G \).

(ii) If either \( d \leq 2 \) or \( G \) is a p-group, then \( M(G) = D(G) \).

**Proof.** [10], [11]; see also [1].

**Proposition 3.** Let \( G \) be a finite abelian group and \( k \in \mathbb{N} \).

(i) If \( G = G' \oplus G'' \), then \( D_k(G) \geq D_k(G') + D(G'') - 1 \).

(ii) If \( G = \bigoplus_{i=1}^d C_{n_i} \) with \( 1 < n_d \mid n_{d-1} \mid \ldots \mid n_1 \), then \( D_k(G) \geq kn_1 + \sum_{i=2}^d (n_i - 1) \).

(iii) \( D_k(C_n) = kn \).

**Proof.** (i) By Proposition 1(iv), there exist elements \( S' \in \mathcal{F}(G') \) and \( S'' \in \mathcal{F}(G'') \) such that \( \sigma(S') = D_k(G') - 1 \), \( S' \) is not divisible by a product of \( k \) blocks from \( \mathcal{B}(G')' \) and \( \sigma(S'') = D(G'') - 1 \), \( S'' \) is not divisible by a block of \( \mathcal{B}(G'')' \). If \( S' = \prod_{j=1}^{D_k(G')-1} g'_j \) and \( S'' = \prod_{j=1}^{D(G'')-1} g''_j \), then the element

\[
S = \prod_{j=1}^{D_k(G')-1} (g'_j, 0) \cdot \prod_{j=1}^{D(G'')-1} (0, g''_j) \in \mathcal{F}(G)
\]

is not divisible by a product of \( k \) blocks of \( \mathcal{B}(G)' \), whence

\[
D_k(G) > \sigma(S) = D_k(G') + D(G'') - 2,
\]
by Proposition 1(iv), as asserted.
(ii) If $G = \langle g_1, \ldots, g_d \rangle$ and $\operatorname{ord}(g_i) = n_i$, then the block
\[ B = g_1^{n_1-1} \cdot (g_1 + \ldots + g_d) \cdot \prod_{j=2}^{d} g_j^{n_j-1} \in \mathcal{B}(G) \]
has a unique factorization into irreducible blocks of length $k$, given by $B = B_1^{k-1} B_0$, where $B_1 = g_1^{n_1}$ and $B_0 = (g_1 + \ldots + g_d) \cdot \prod_{j=1}^{d} g_j^{n_j-1}$. This implies $D_k(G) \geq \sigma(B) = kn_1 + \sum_{j=2}^{d} (n_j - 1)$.
(iii) By Propositions 1 and 2, we have $D_k(C_n) \leq kD(C_n) = kn$, whereas, by (ii), $D_k(C_n) \geq kn$.

4. In this section we generalize the result on groups of rank 2.

**Proposition 4.** Let $G = G_1 \oplus G_2$ be a finite abelian group, $\#G_i = n_i$, $n_2 \mid n_1$ and $k \in \mathbb{N}$. Then
\[ D_k(C_n) \leq kn_1 + n_2 - 1. \]

For the proof of Proposition 4 we need two technical lemmas.

**Lemma 1.** Let $G$ be a finite abelian group, $m \in \mathbb{N}$, $D(G) < 2m$ and $D(G \oplus C_m) < 3m$. Let $t \in \mathbb{N}$ and $S \in \mathcal{F}(G)$ be such that $\sigma(S) \geq D(G \oplus C_m) + (t - 1)m$. Then there exist blocks $B_1, \ldots, B_t \in \mathcal{B}(G)^t$ such that $B_1 \cdot \ldots \cdot B_t \mid S$ and $\sigma(B_i) \leq m$ for all $i \in \{1, \ldots, t\}$.

**Proof.** It suffices to consider the case $t = 1$, for then the general case follows by a trivial induction argument.

Set $N = D(G \oplus C_m) < 3m$, and let $S = g_1 \cdot \ldots \cdot g_\nu \in \mathcal{F}(G)$ be an element with $\nu = \sigma(S) \geq N$. Let $e_m$ be a generator of $C_m$, and consider the element
\[ S' = \prod_{j=1}^{N} (g_j, e_m) \in \mathcal{F}(G \oplus C_m); \]
by Proposition 1(iv) there exists an irreducible block $S'_0 \in \mathcal{B}(G \oplus C_m)^t$ such that $S'_0 \mid S'$, and we may assume that $S'_0 = \prod_{j=1}^{N_0} (g_j, e_m)$ for some $N_0 \leq N$.

Since
\[ t(S'_0) = \left( \sum_{j=1}^{N_0} g_j, N_0 e_m \right) = (0, 0) \in G \oplus C_m, \]
we obtain $S_0 = \prod_{j=1}^{N_0} g_j \in \mathcal{B}(G)$ and $m \mid N_0$, whence $m = N_0$ or $2m = N_0$. If $m = N_0$, the assertion follows with $B = S_0$; if $2m = N_0 > D(G)$, then $S_0$ has a decomposition $S_0 = BB'$ with $B, B' \in \mathcal{B}(G)$ and $\sigma(B) \leq m$, which again implies the assertion. \(\blacksquare\)
Lemma 2. Let $p$ be a prime, $t \in \mathbb{N}$ and $B \in \mathcal{B}(C_p \oplus C_p)$ a block satisfying
\[ \sigma(B) \geq tp. \]
Then there exist blocks $B_1, \ldots, B_t \in \mathcal{B}(C_p \oplus C_p)'$ such that $B = B_1 \ldots B_t$.

Proof. The assertion is true for $t = 1$ and also for $t = 2$, as $D(C_p \oplus C_p) = 2p - 1 < 2p$. Therefore we assume that $t \geq 3$ and $B = g_1 \cdots g_t$ for some $\nu \geq tp$. We apply Lemma 1 with $G = C_p \oplus C_p$, $m = p$ and $S = g_1 \cdots \ldots g_{tp-1}$. Since $\sigma(S) = tp - 1 > (3p - 2) + (t - 3)p = D(C_p \oplus C_p \oplus C_p) + (t - 3)p$, there exist blocks $B_1, \ldots, B_{t-2}, B' \in \mathcal{B}(G)'$ such that $B = B_1 \ldots B_{t-2}B'$ and $\sigma(B') \leq p$ for all $j \in \{1, \ldots, t - 2\}$. This implies
\[ \sigma(B') = \sigma(B) - \sum_{j=1}^{t-2} \sigma(B_j) \geq tp - (t - 2)p = 2p > D(G), \]
whence $B' = B_{t-1}B_t$ with blocks $B_{t-1}, B_t \in \mathcal{B}(G)'$.

Proof of Proposition 4. By induction on $n_2$; if $n_2 = 1$, then $D_k(G) = D_k(G_1) \leq kD(G_1) \leq kn_1$ by Proposition 1(ii) and Proposition 2(i).

If $n_2 > 1$, let $p$ be a prime with $p \mid n_2$ and choose subgroups $G_i' \subset G_i$ ($i = 1, 2$) with $(G_1 : G_i') = p$. Set
\[ t = kn_1/p + n_2/p, \]
and assume that the assertion is true for the subgroup $G' = G_1' \oplus G_2' \subset G$, i.e., $D_k(G') \leq t - 1$. We must prove that every block $B \in \mathcal{B}(G)$ with $\sigma(B) = N \geq kn_1 + n_2$ has a factorization of length $l \geq k + 1$. We set $B = g_1 \cdots g_N$ and consider the canonical epimorphism $\pi : G \to C_p \oplus C_p$ with $\text{ker}(\pi) = G'$. The block $B^* = \pi(g_1) \cdots \pi(g_N) \in \mathcal{B}(C_p \oplus C_p)$ satisfies $\sigma(B^*) = N \geq tp$ and therefore, by Lemma 2, $B^*$ is a product of $t$ blocks from $\mathcal{B}(C_p \oplus C_p)'$. Taking preimages in $G$, we obtain a decomposition $B = S_1 \cdots S_t$ with $S_i \in \mathcal{F}(G)'$ and $i(S_i) = g_i' \in G'$. Since $t > D_k(G')$ and $g_1' \cdots g_t' \in G(G')'$, there exist blocks $B_1', \ldots, B_{k+1}' \in \mathcal{B}(G')'$ with $B_1' \ldots B_{k+1}' \mid g_1' \cdots g_t'$ by Proposition 1(v). Hence there exists a decomposition
\[ \{1, \ldots, t\} = \bigcup_{\nu=1}^{k+1} J_{\nu} \quad \text{(disjoint union)} \]
such that $B_\nu' = \prod_{j \in J_\nu} g_j'$ for all $\nu \in \{1, \ldots, k+1\}$. Putting $B_\nu = \prod_{j \in J_\nu} S_j \in \mathcal{B}(G)$, we obtain $B_1' \ldots B_{k+1}' \mid B$, and therefore $B$ has a factorization of length $l \geq k + 1$.

Proposition 5. If $G = C_{n_1} \oplus C_{n_2}$ with $n_2 \mid n_1$, then $D_k(G) = kn_1 + n_2 - 1$.

Proof. Obvious by Propositions 3 and 4.
5. Proof of the Theorem. Let $K$ be an algebraic number field, $R$ its ring of integers, $G$ the ideal class group, $I$ the semigroup of non-zero ideals and $H$ the subsemigroup of non-zero principal ideals of $R$. We write $G$ additively, and for $J \in I$ we denote by $[J] \in G$ the ideal class of $J$. Let $\theta : I \to \mathcal{F}(G)$ be the unique semigroup homomorphism satisfying $\theta(P) = [P]$ for every maximal $P$ of $R$. For $J \in I$, we have $\theta(J) \in B(G)$ if and only if $J \in H$. If $\alpha \in R \setminus (R^\times \cup \{0\})$, then $L(\alpha) = L(\theta((\alpha)))$.

Let $M_k$ be the set of all blocks $B \in B(G)$ such that $\max L(B) \leq k$, and let $M'_k$ be the set of all blocks $B \in B(G)$ such that $\min L(B) \leq k$. Then

$$M'_k = \{\alpha \in R \setminus (R^\times \cup \{0\}) \mid \theta((\alpha)) \in M_k\}$$

and, by Proposition 1,

$$kD(G) = \max\{\sigma(B) \mid B \in M'_k\}, \quad D_k(G) = \max\{\sigma(B) \mid B \in M_k\}.$$

In particular, the sets $M_k$ and $M'_k$ are finite.

After these observations, the Theorem is an immediate consequence of the following Lemma, due to Kaczorowski [7, Lemma 1].

**Lemma 3.** For $1 \neq S \in \mathcal{F}(G)$, $x \geq e^e$ and $q \in \mathbb{Z}$, $0 \leq q \leq c_0 \frac{\sqrt{\log x}}{\log \log x}$, we have

$$\#\{J \in I \mid (R : J) \leq x, \theta(J) = S\} = \frac{x}{\log x} \left[ \sum_{\mu = 0}^{q} W_\mu \left(\frac{\log \log x}{\log x}\right)^\mu + O\left((c_1 q)^q \left(\frac{\log \log x}{\log x}\right)^{\sigma(S)}\right) \right]$$

with constants $c_0, c_1 \in \mathbb{R}_+$, and polynomials $W_\mu \in \mathbb{C}[X]$ such that $\deg W_\mu \leq \sigma(S)$, $\deg W_0 = \sigma(S) - 1$, and $W_0$ has a positive leading coefficient.

**References**


INSTITUT FÜR MATHEMATIK
KARL-FRANZENS-UNIVERSITÄT
HEINRICHSTRASSE 36
A-8010 GRAZ, AUSTRIA

Reçu par la Rédaction le 14.1.1991