11. Mathematikertreffen, Zagreb-Graz
D. Butković, D. Gronau,
H. Kraljević, O. Röschel (Eds.)
Grazer Math. Ber., ISSN 1016–7692
Bericht Nr. 348 (2005), 41-64

Half-factorial sets in finite abelian groups: a survey

Wolfgang Alexander Schmid*

Abstract

A monoid is called half-factorial if every non-unit element has a factorization into irreducible elements and the length of such a factorization is uniquely determined by the element. A subset of an abelian group is called a half-factorial set if the monoid of all zero-sum sequences in the set is a half-factorial monoid. In this survey recent results on half-factorial sets in finite abelian groups are discussed, with an emphasize on results that concern the maximal possible cardinality of half-factorial sets. These results are complemented with some conjectures and speculations. Moreover, it is sketched how these results are motivated by and can be applied to problems in (commutative) algebra, in particular in the study of Krull monoids and thus Dedekind domains, and in algebraic number theory.

1 Introduction

The study of half-factorial sets in (finite) abelian groups is motivated by and can be applied to arithmetical problems in Krull monoids, thus in particular in Dedekind domains and in the rings of integers of algebraic number fields. First, we present some (informal) definitions and examples. Then, we sketch this connection and mention a further application of half-factorial sets. In Sections 2 and 3 we give complete definitions and explain this connection in detail.

A monoid, as a domain, is called factorial, if every non-unit has an essentially unique factorization into irreducible elements (atoms). That is, if $a = u_1 \cdot \ldots \cdot u_l$ and $a = u'_1 \cdot \ldots \cdot u'_{l'}$ are factorizations of a into atoms, then $l = l'$ and there exists a permutation τ such that for each $1 \le i \le l$ the elements u_i and $u'_{\tau(i)}$ are associates. We call l the length of the factorization. A monoid is called half-factorial if every non-unit has a factorization into atoms and the length of such a factorization is uniquely determined by the element.

*Supported by the Fonds zur Förderung der wissenschaftlichen Forschung P16770-N12.

Mathematics Subject Classification 2000: Primary 20K01, Secondary 11R27, 13F05.

Keywords and phrases: block monoid, half-factorial, zero-sum sequence, factorization, Krull monoid, Dedekind domain.

If D is a Dedekind domain, or more generally a Krull domain, then the multiplicative monoid $(D \setminus \{0\}, \cdot)$ is a Krull monoid. It is well known that the ring of integers of an algebraic number field is factorial if and only if its class group is trivial. The analogous statement for Krull monoids is true as well. The class group is viewed as a measure for the deviation of the ring from factoriality.

A first result on half-factoriality, without already using this term, is due to L. Carlitz [2]. He proved that the ring of integers of an algebraic number field is half-factorial if and only if its class group has at most two elements (cf. Theorem 3.2). In contrast to the aforementioned result on factoriality, this result does not have an exact analog for Krull monoids. On the one hand, every Krull monoid whose class group has at most two elements is half-factorial. On the other hand, indeed for every finite abelian group G there exists a half-factorial Krull monoid, even a Dedekind domain, whose class group is isomorphic to G. Krull monoids with infinite class group exist as well. In particular, it is known that every finitely generated group and every Warfield group is isomorphic to the class group of some half-factorial Krull monoid (see [19]).

Answering a question of W. Narkiewicz (cf. [40]), L. Skula [50] and A. Zaks [53] gave a characterization of half-factorial Krull monoids (cf. Theorem 4.1). In [53] the term "half-factorial" was initially used. Meanwhile, the study of half-factorial domains and monoids is a main subject in non-unique factorization theory, and this characterization result has become a key tool in it. We refer to the articles by S.T. Chapman and J. Coykendall [5], S.T. Chapman, M. Freeze, and W.W. Smith [6] (where also generalizations of the concept "half-factorial" are discussed), and J. Coykendall [10], the references given there, and the recent articles [19, 34]. For an exposition of non-unique factorization theory in general see for instance the collections [1] and [4].

Whether a Krull monoid is half-factorial just depends on its class group and the subset of classes containing primes. Note that this subset can be almost arbitrary for general Krull monoids, the only condition is that it generates the class group (as a monoid). In contrast, it is well known that every class in the class group of the ring of integers of an algebraic number field contains primes (that is, prime ideals); and the aforementioned result of L. Carlitz makes use of this property.

Thus, to decide whether a Krull monoid is half-factorial, it suffices to decide this for some (auxiliary) Krull monoid with isomorphic class group and subset of classes containing primes.

The following class of auxiliary monoids, called block monoids, has been introduced by W. Narkiewicz [39]. Let $(G, +, 0)$ be an abelian group and $G_0 \subset G$. Let $S = (g_1, \ldots, g_n)$ be a (finite) sequence in G_0; sequences that just differ in the ordering of the terms are identified, so an alternative common name for a sequence, in the present sense, is "multiset". If $\sum_{i=1}^{n} g_i = 0 \in G$, then S is called a zero-sum sequence. The set of all sequences in G_0, with concatenation as operation, is a monoid; and the subset of zero-sum sequences is a submonoid. This submonoid is called the block monoid over G_0, and is denoted by $\mathcal{B}(G_0)$.

A block monoid is itself a Krull monoid. If H is a Krull monoid with class group G and subset of classes containing primes $G_0 \subset G$, then the arithmetic of H and $\mathcal{B}(G_0)$ are

strongly connected. Indeed, various arithmetical invariants of H and $\mathcal{B}(G_0)$ are equal. In particular, H is half-factorial if and only if $\mathcal{B}(G_0)$ is half-factorial; more generally, all invariants defined via lengths of factorizations are equal (cf. Theorem 3.1). However, note that in general the class group of $\mathcal{B}(G_0)$ is different from G.

Now, a subset $G_0 \subset G$ of an abelian group is called half-factorial if the block monoid $\mathcal{B}(G_0)$ is a half-factorial monoid.

In this survey we focus on results on half-factorial sets in finite abelian groups. We emphasizes those results that concern the problem of determining the maximal cardinality $\mu(G)$ of a half-factorial set in a finite abelian group G. And, we discuss the according inverse problem, that is the problem to describe the structure of half-factorial sets with cardinality $\mu(G)$. The problem of determining $\mu(G)$ was explicitly raised by W. Narkiewicz [39] and originated in investigations on counting functions of algebraic integers with certain factorization properties. Asymptotic formulae for these functions involve the constant $\mu(G)$ and a constant that depends on the structure of half-factorial sets with cardinality $\mu(G)$ (see Subsection 3.2 for further details and references).

The survey is organized as follows. In Section 2 we discuss, in more detail, some basic definitions, in particular those of Krull monoids, block monoids, and half-factorial sets. Having these at hand, we explain more concisely, in Section 3, how results on half-factorial sets relate to the problem of half-factoriality of Krull monoids, and how they can be applied to and are motivated by investigations on certain counting functions. In Section 4 we state the characterization result of L. Skula and A. Zaks, and moreover various consequences of it, which are frequently used tools. In Section 5 we discuss the concept of weakly half-factorial sets, and results on half-factorial sets that can be obtained by applying results on weakly half-factorial sets. In the remaining three sections we discuss results for specific types of groups, namely elementary p-groups, cyclic groups, and p-groups, respectively. We hardly present proofs; but for some results, where it seems useful for the further discussion, we give (brief) outlines of the proofs.

2 Preliminaries

In this section we summarize terminology and definitions that we need in the remainder of this survey. In particular, we explain the notions of Krull monoids and block monoids. The terminology and notation we use is fairly standard in non-unique factorization theory, cf. for instance the surveys [29, 7].

Throughout, we denote by $\mathbb{Z}$ the integers, by $\mathbb{N}$ and $\mathbb{N}_0$ the positive and non-negative integers, respectively, and by $\mathbb{P} \subset \mathbb{N}$ the prime numbers; by $[m, n] = \{z \in \mathbb{Z} \colon m \le z \le n\}$ we denote the interval of integers.

2.1 Monoids and factorizations

A monoid H is a commutative cancellative semigroup with identity element $1_H \in H$, and we use multiplicative notation throughout. The subgroup of units (invertible elements)

of H is denoted by $H^\times$. A quotient group of H is denoted by $\mathsf{q}(H)$.

Two elements $a, b \in H$ are called associates if there exists a unit $\epsilon \in H^\times$ such that $a = \epsilon b$. A monoid is called reduced if its subgroup of units is trivial. $H_{\red} = H/H^\times$ denotes the reduced monoid associated to H. Frequently, it is advantageous to study factorization properties of H in the associated reduced monoid.

An element $a \in H \setminus H^\times$ is called an atom (or irreducible) if a has no non-trivial divisors, that is $a = bc$ with $b, c \in H$ implies $b \in H^\times$ or $c \in H^\times$. The subset of atoms of H is denoted by $\mathcal{A}(H)$. An element $p \in H \setminus H^\times$ is called prime if $p \mid bc$ with $b, c \in H$ implies $p \mid b$ or $p \mid c$. The subset of primes of H is denoted by $\mathcal{P}(H)$. Every prime is an atom, that is, $\mathcal{P}(H) \subset \mathcal{A}(H)$.

The monoid H is called atomic if every $a \in H \setminus H^\times$ is the product of (finitely many) atoms, and it is called factorial if every $a \in H \setminus H^\times$ is the product of (finitely many) primes. If $a = p_1 \cdot \ldots \cdot p_l$ with primes $p_1, \ldots, p_l \in \mathcal{P}(H)$, then this is (essentially) the unique way to factor a into atoms; more precisely, if $a = u_1 \cdot \ldots \cdot u_{l'}$ with atoms $u_1, \ldots, u_{l'} \in \mathcal{A}(H)$, then $l = l'$ and there exists a permutation τ of $[1, l]$ such that p_i and $u_{\tau(i)}$ are associates for each $i \in [1, l]$. Thus, in a factorial monoid every non-unit has an essentially unique factorization into atoms. H is factorial if and only if it is atomic and $\mathcal{A}(H) = \mathcal{P}(H)$.

If $a = u_1 \cdot \ldots \cdot u_l$ with atoms $u_1, \ldots, u_l \in \mathcal{A}(H)$, then l is called the length of the factorization of a. For $a \in H \setminus H^\times$ the set

$$\mathsf{L}_H(a) = \{l \in \mathbb{N} \colon a \text{ has a factorization of length } l\} \subset \mathbb{N}$$

is called the set of lengths of a and for $a \in H^\times$ set $\mathsf{L}_H(a) = \{0\}$. Note that in general sets of lengths can be infinite. An atomic monoid is called a bounded factorization monoid (BF-monoid), if $\mathsf{L}_H(a)$ is a finite set for each $a \in H$.

A monoid H is half-factorial if $|\mathsf{L}_H(a)| = 1$ for every $a \in H$, that is, if each $a \in H \setminus H^\times$ has a factorization into atoms and all factorizations of a have the same length.

2.2 Free monoids and Krull monoids

A monoid is called free if it is factorial and reduced. For a set P let $\mathcal{F}(P)$ denote the free abelian monoid with basis P, that is, $\mathcal{F}(P)$ is the set of commutative formal products

$$\{\prod_{p \in P} p^{v_p} \colon v_p \in \mathbb{N}_0 \text{ and } v_p = 0 \text{ for almost all } p \in P\}.$$

Let H be a monoid and F be a free monoid. A monoid homomorphism $\varphi : H \to F$ is called a divisor homomorphism if

$$a \mid_H b \text{ if and only if } \varphi(a) \mid_F \varphi(b).$$

A divisor homomorphism $\varphi : H \to F$ with the property that for every $f \in F$ there exists a set $\{a_1, \ldots, a_n\} \subset H$ such that

$$f = \gcd(\{\varphi(a_1), \ldots, \varphi(a_n)\})$$

is called a divisor theory. (Since F is a free monoid, every non-empty subset has a unique greatest common divisor.)

A monoid H is called a Krull monoid if it posses a divisor theory. The divisor theory of a Krull monoid is unique up to isomorphisms. There are several other characterizations of Krull monoids (see [30, Chapters 22 and 23]). We only mention the following two:

- A monoid is a Krull monoid if and only if it posses a divisor homomorphism.
- A monoid is a Krull monoid if and only if it is is completely integrally closed and v-noetherian.

Krull monoids are atomic and even BF-monoids. Let H be a Krull monoid and $\varphi : H \to F$ a divisor theory. The class group of H is defined as $\mathsf{Cl}(H) = \mathsf{q}(F)/\mathsf{q}(\mathrm{im}(\varphi))$, that is, the quotient group of F modulo the quotient group of $\mathrm{im}(\varphi)$. As usual, we use additive notation for the class group. For $f \in F$ we denote by $[f] \in \mathsf{Cl}(H)$ the class containing f, and the subset $\{[p] \colon p \in \mathcal{P}(F)\} \subset \mathsf{Cl}(H)$ is referred to as the set of classes containing primes. As mentioned in the Introduction, a Krull monoid is factorial if and only if $|\mathsf{Cl}(H)| = 1$.

2.2.1 Examples of Krull monoids

The notion of Krull monoids allows a unified treatment of quite different structures. The main examples of Krull monoids are:

- Multiplicative monoids of Krull domains, thus in particular Dedekind domains and rings of integers of algebraic number fields.
- Block monoids, that is the monoids of zero-sum sequences of subsets of abelian groups (see Subsection 2.4).
- Monoids of certain isomorphy classes of modules under direct sum composition (see for example [12, 13]).

In the theory of non-unique factorizations in an integral domain, almost always, only the multiplicative monoid of this integral domain is of relevance. More precisely, if units are negligible, then even only the associated reduced monoid of non-zero principal ideals is responsible for the arithmetical properties of the integral domain.

We mention that the connection among the notions "Krull domain" and "Krull monoid" is closer than already stated. It was proved by U. Krause [36] that a domain D is a Krull domain if and only if its multiplicative monoid $(D \setminus \{0\}, \cdot)$ is a Krull monoid.

2.3 Some notation for finite abelian groups

In this subsection, we fix some notation for finite abelian groups.

Throughout, let $(G, +, 0)$ be a finite abelian group. For a subset $G_0 \subset G$ we denote by $\langle G_0 \rangle$ the subgroup generated by G_0. A subset $G_0 \subset G \setminus \{0\}$ is called independent if, for $m_g \in \mathbb{Z}$,

$$\sum_{g \in G_0} m_g g = 0 \text{ implies } m_g g = 0 \text{ for all } g \in G_0.$$

If we say that a set $\{e_1, \ldots, e_s\}$ is independent, we tacitly assume that the e_i's are distinct. For $g \in G$ we denote by $\mathrm{ord}(g) \in \mathbb{N}$ the order of the element.

For $n \in \mathbb{N}$, let C_n denote a cyclic group with n elements. Suppose $|G| > 1$. Then there exist uniquely determined integers $1 < n_1 | \ldots | n_r$ such that

$$G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}.$$

We denote by $\mathsf{r}(G) = r$ the rank of G and by $\exp(G) = n_r$ the exponent of G. In case $|G| = 1$, we set $\mathsf{r}(G) = 0$ and $\exp(G) = 1$.

The group G is called elementary if $\exp(G)$ is squarefree, and it is called a p-group if $\exp(G) = p^k$ for some $p \in \mathbb{P}$ and $k \in \mathbb{N}$. Thus, elementary p-group means $\exp(G) = p \in \mathbb{P}$.

2.4 Sequences and block monoids

In this subsection, we recall the definitions of sequences and block monoids, in a more formal way than in the Introduction, and some additional terminology.

Let $(G, +, 0)$ be an abelian group and $G_0 \subset G$. An element $S \in \mathcal{F}(G_0)$ is called a sequence in G_0. We refer to the divisors (in $\mathcal{F}(G_0)$) of S as subsequences of S.

For a sequence $S = \prod_{g \in G_0} g^{v_g}$, we denote by

- $|S| = \sum_{g \in G_0} v_g$ its length.
- $\sigma(S) = \sum_{g \in G_0} v_g g \in G$ its sum.
- $\mathsf{k}(S) = \sum_{g \in G_0} \frac{v_g}{\mathrm{ord}(g)}$ its cross number.

Then, $|\cdot| : \mathcal{F}(G_0) \to \mathbb{N}_0$, $\sigma : \mathcal{F}(G_0) \to G$, and $\mathsf{k} : \mathcal{F}(G_0) \to \mathbb{Q}_{\ge 0}$ are monoid homomorphisms. The kernel of σ is called the block monoid over G_0. It is denoted by $\mathcal{B}(G_0)$.

The embedding $\mathcal{B}(G_0) \hookrightarrow \mathcal{F}(G_0)$ is a divisor homomorphism, and thus $\mathcal{B}(G_0)$ is a Krull monoid. However, in general this embedding is not a divisor theory and possibly $G \ncong \mathsf{Cl}(\mathcal{B}(G_0))$ or even $\langle G_0 \rangle \ncong \mathsf{Cl}(\mathcal{B}(G_0))$. Yet, under certain, not too restrictive, conditions $\mathcal{B}(G_0) \hookrightarrow \mathcal{F}(G_0)$ is a divisor theory, G is the class group of $\mathcal{B}(G_0)$ and G_0 is the set of classes containing primes; in particular, $\mathcal{B}(G) \hookrightarrow \mathcal{F}(G)$ is a divisor theory if and only if $|G| \ne 2$ (see [27]).

Clearly, $\mathcal{B}(G_0)$ is atomic. The atoms of $\mathcal{B}(G_0)$ are the minimal zero-sum sequences in G_0, that is, zero-sum sequences such that no proper non-trivial subsequence is a zero-sum sequence. For notational convenience the set of atoms of $\mathcal{B}(G_0)$ is denoted just by $\mathcal{A}(G_0)$.

Now, we recall the main definition of this survey.

Definition 2.1 Let G be an abelian group. A subset $G_0 \subset G$ is called a half-factorial set if $\mathcal{B}(G_0)$ is a half-factorial monoid. For G a finite abelian group, let

$$\mu(G) = \max\{|G_0| \colon G_0 \subset G \text{ half-factorial}\}.$$

3 Applications of half-factorial sets

In this section we explain, in more detail, how half-factorial sets are related to half-factorial Krull monoids, and how half-factorial sets can be applied in the study of the counting functions mentioned in the Introduction, in particular we discuss the significance of the constant $\mu(G)$ in this context.

3.1 Transfer and block homomorphisms

First, we recall the notion of transfer homomorphisms; it has been introduced by F. Halter-Koch [29], also see [21] for recent developments. A monoid homomorphism $\theta : H \to B$ is called a transfer homomorphism if

- $B = \theta(H)B^\times$ and $\theta^{-1}(B^\times) = H^\times$, and
- if $u \in H$, $b_1, b_2 \in B$ and $\theta(u) = b_1 b_2$, then there exist $u_1, u_2 \in H$ such that $u = u_1 u_2$ and $\theta(u_i)$ is associated to b_i for $i \in [1, 2]$.

An important property of transfer homomorphisms is that they preserve sets of lengths, more precisely (see [29]): Let $\theta : H \to B$ be a transfer homomorphism. Then

$$\mathsf{L}_H(a) = \mathsf{L}_B(\theta(a)),$$

for every $a \in H$.

Let H be a Krull monoid and $\varphi : H \to \mathcal{F}(P)$ a divisor theory. Further, let $G_0 \subset \mathsf{Cl}(H)$ denote the set of classes containing primes and $\pi : \mathcal{F}(P) \to \mathcal{F}(G_0)$ the homomorphism defined by $p \mapsto [p]$.

Then $\beta = \pi \circ \varphi$ is called the block homomorphism of H. Since elements of H are mapped to the zero-class, it follows that $\mathrm{im}\beta \subset \mathcal{B}(G_0)$ and indeed the following holds.

Theorem 3.1 *Let H be a Krull monoid and $G_0 \subset \mathsf{Cl}(H)$ the set of classes containing primes. Then*

$$\beta : H \to \mathcal{B}(G_0)$$

is a (surjective) transfer homomorphism. In particular, H is a half-factorial monoid if and only if G_0 is a half-factorial set.

The origins of this theorem can be traced back to W. Narkiewicz [39], subsequent formalizations and generalizations are mainly due to A. Geroldinger and F. Halter-Koch, see for instance [17], the surveys [29, 7], or [20].

Thus, the problem of deciding whether a Krull monoid is half-factorial, and more generally the problem of determining the sets of lengths of its elements, can be transferred to the associated block monoid and thus to a question on zero-sum sequences in abelian groups. In particular, having this machinery at hand, the theorem of L. Carlitz [2] on half-factorial rings of integers can be obtained quite easily. We state its generalization due to L. Skula [50] and A. Zaks [53, 54].

Theorem 3.2 *Let H be a Krull monoid such that every class contains a prime. Then H is half-factorial if and only if $|\mathsf{Cl}(H)| \le 2$.*

Clearly, by Theorem 3.1 this result is equivalent to the statement: An abelian group is a half-factorial set if and only if $|G| \le 2$.

The general approach of this survey is to investigate the block monoid $\mathcal{B}(G_0)$ for some subset $G_0 \subset G$ of some finite abelian group, without having in mind any specific monoid or domain that actually has G as class group and G_0 as set of classes containing primes. This approach is justified by realization results asserting that for every abelian group G and every subset $G_0 \subset G$ that generates G as a monoid there actually exists a Krull monoid (in fact even a Dedekind domain) with class group isomorphic to G such that G_0 corresponds to the set of classes containing primes; see [9], the book [14], and [26, 50, 27, 25] for generalizations and refinements.

3.2 Applications in algebraic number theory – asymptotic of counting functions

In this subsection, we discuss the significance of half-factorial sets for quantitative results in the arithmetic of algebraic number fields. It has been a main motivation for research on half-factorial sets.

Let R be the ring of integers of an algebraic number field. Then R is a Dedekind domain (hence a Krull monoid) with finite class group G and every class contains infinitely many primes.

In the sixties W. Narkiewicz [38] started a systematic investigation of problems of the following type (also see [40, Chapter 9] and the references there). Let $\mathcal{Z} \subset R$ be a subset defined by some phenomenon of non-unique factorization. Determine the asymptotic of the counting function

$$\mathcal{Z}(x) = |\{aR \colon a \in \mathcal{Z}, \mathcal{N}(a) \le x\}|, \quad x \to \infty.$$

We specifically discuss the functions $\mathcal{G}_k(x)$, for $k \in \mathbb{N}$, defined by the sets

$$\mathcal{G}_k(R) = \{a \in R \setminus \{0\} \colon |\mathsf{L}(a)| \le k\}.$$

(Note that by Theorem 3.2 these functions are only of actual interest if $|G| \ge 3$.) It is known that (see [51] and [18])

$$\mathcal{G}_k(x) \sim Cx(\log x)^{-1+\mu(G)/|G|}(\log\log x)^{\psi_k(G)},$$

where $\mu(G)$ denotes, as defined in Subsection 2.4, the maximal cardinality of a half-factorial set in G and $\psi_k(G)$ depends only on k and the structure of half-factorial sets with cardinality $\mu(G)$. For other counting functions of this type similar results are known, but instead of problems related to half-factorial sets other (combinatorial) problems arise, see [28] for a unified approach.

We briefly outline how this result is obtained and emphasize in what way the exponents arise. Let $\mathcal{G}_k(G) = \{B \in \mathcal{B}(G) \colon |\mathsf{L}(B)| \le k\}$ and let $\beta : R \setminus \{0\} \to \mathcal{B}(G)$ denote the block homomorphism. Then $\mathcal{G}_k(R) = \beta^{-1}(\mathcal{G}_k(G))$. Now, there are two main steps to determine the asymptotic formula for $\mathcal{G}_k(x)$.

First, for $G_0 \subset G$ and $S \in \mathcal{F}(G \setminus G_0)$, let $\Omega(G_0, S) = S \cdot \mathcal{F}(G_0) \cap \mathcal{B}(G)$. It is known that if $\Omega(G_0, S) \ne \emptyset$, then

$$|\{a \in H \colon \beta(a) \in \Omega(G_0, S)\}| \sim \begin{cases} Cx(\log x)^{-|G\setminus G_0|/|G|}(\log\log x)^{|S|} & \text{if } G_0 \ne \emptyset \\ Cx(\log x)^{-1}(\log\log x)^{|S|-1} & \text{if } G_0 = \emptyset \end{cases}$$

for some $C > 0$, see [51] and [33] for more precise asymptotic results.

And, it is known that the set $\mathcal{G}_k(G)$ can be written as a finite union of Ω-sets, say

$$\mathcal{G}_k(G) = \bigcup_{i=1}^{n} \Omega(G_i, S_i)$$

with $G_i \subset G$ and $S_i \in \mathcal{F}(G \setminus G_i)$. This already yields that

$$\mathcal{G}_k(x) \sim C'x(\log x)^A(\log\log x)^B$$

with $A = -1 + m/|G|$, where $m = \max\{|G_i| \colon i \in [1, n]\}$, and, provided some G_i is non-empty, $B = \max\{|S_i| \colon |G_i| = m\}$.

Since $\mathcal{B}(G_0) \subset \mathcal{G}_k(G)$ if and only if G_0 is half-factorial, it can be shown that $m = \mu(G)$ and $\psi_k(G)$ is the maximal $t \in \mathbb{N}$ with the property that there exists a half-factorial set $G_0 \subset G$ with $|G_0| = \mu(G)$ and a sequence $S \in \mathcal{F}(G \setminus G_0)$ with $|S| = t$ such that $\emptyset \ne \Omega(G_0, S) \subset \mathcal{G}_k(G)$; see [18].

These counting functions were also studied for other structures, namely in abstract settings, for holomorphy rings in functions fields over finite fields [31], and for non-principal orders [22]. In all these cases, a similar asymptotic formula holds and the invariant $\mu(G)$ appears as the exponent of the logarithmic factor.

A very recent contribution to this subject is due to M. Radziejewski [44]. He investigated oscillations of $\mathcal{G}_k(x)$ about its main term and, among others, proved the existence of oscillations under the assumption that $\psi_k(G) > 0$. For $k \ge 2$ and arbitrary G it was subsequently proved by M. Radziejewski and the author [46] that in fact $\psi_k(G) > 0$ holds. Also, the positivity of $\psi_1(G)$ was proved for several types of groups; yet only for groups where one has some understanding of the structure of half-factorial sets with maximal cardinality in G.

4 General results on half-factorial sets

From this section on we present the subject of half-factorial sets in a purely group theoretical setting. Throughout, let G denote an, additively written, finite abelian group. First, we state the already mentioned characterization result for half-factorial sets, due to L. Skula [50] and A. Zaks [53, 54], and then various frequently used results on half-factorial sets.

Theorem 4.1 *A subset $G_0 \subset G$ is a half-factorial set if and only if*

$$\mathsf{k}(A) = 1 \text{ for each } A \in \mathcal{A}(G_0).$$

This characterization is the key tool in investigations of half-factorial sets in finite abelian groups. By Theorem 3.1 it provides a characterization of half-factorial Krull monoids with finite class group. For a characterization of arbitrary half-factorial monoids see [35].

Next, we collect a variety of auxiliary results that can be proved using the characterization result, details and further results of this flavor can be found in [15].

1. The set $G_0 \subset G$ is half-factorial if and only if $G_0 \cup \{0\}$ is half-factorial. In particular, if G_0 is a half-factorial set with maximal cardinality $|G_0| = \mu(G)$, then $0 \in G_0$.

2. Independent sets are half-factorial. (Indeed, they are even factorial, that is the block monoid over an independent set is a factorial monoid.) Thus, every finite abelian group has a half-factorial generating set. (As indicated in the Introduction, the problem to decide whether this is also true for infinite abelian groups is open; for recent results see [19].)

3. Subsets of half-factorial sets are half-factorial. In particular, if $G' \subset G$ is a subgroup, then $\mu(G') \le \mu(G)$.

4. Let $G = G' \oplus G''$. If $G'_0 \subset G'$ and $G''_0 \subset G''$ are half-factorial sets, then $G'_0 \cup G''_0$ is a half-factorial set. In particular, $\mu(G) \ge \mu(G') + \mu(G'') - 1$.

In view of 3., we point out the result due to W. Gao and A. Geroldinger [15] that there exist finite abelian groups G for which no half-factorial set with maximal cardinality generates the group; in particular, in this case there exists a proper subgroup $G' \subsetneq G$ with $\mu(G') = \mu(G)$. We discuss this surprising result in more detail in Section 8. For now we only mention a result in the converse direction.

Theorem 4.2 ([15]) *If G is cyclic or elementary, then every maximal, with respect to inclusion, half-factorial subset is a generating set.*

It is clear that every half-factorial set with maximal cardinality is maximal with respect to inclusion, yet the converse is in general not true; cf. Section 6 for examples.

In the following lemma subsets that consist of independent elements and one or two additional elements are considered. Among others, this lemma is an essential tool in the proofs of the results given in Section 6.

Lemma 4.3 ([15]) *Let $\{e_1, \ldots, e_r\} \subset G$ an independent set with $\mathrm{ord}(e_1) = \cdots = \mathrm{ord}(e_r) = n$, and let $g = -\sum_{i=1}^r b_i e_i$ and $g' = -\sum_{i=1}^r b_i' e_i$ with $b_i, b_i' \in [0, n-1]$ and $\mathrm{ord}(g) = \mathrm{ord}(g')$. Further, let $G_0 \subset G$ be a half-factorial set with $\{g, e_1, \ldots, e_r\} \subset G_0$.*

1. *$\sum_{i=1}^r b_i = n - \gcd\{n, b_1, \ldots, b_r\}$.*
2. *Assume $g' \in G_0$. Then $b_i = b_i'$ and $\mathrm{ord}(b_i e_i) = \mathrm{ord}(g)$ for some $i \in [1, r]$ implies $g = g'$.*

We emphasize that 1. is in general only a necessary condition.

Outline of proof. The result is proved by applying the condition $\mathsf{k}(A) = 1$ to suitable atoms of $\mathcal{B}(G_0)$. For instance, the sequence $A' = g \prod_{i=1}^r e_i^{b_i}$ is an atom. Since $\mathrm{ord}(g) = n/\gcd\{n, b_1, \ldots, b_r\}$, the condition $\mathsf{k}(A') = 1$ is equivalent to the first statement. □

We end this section by mentioning that for groups with $|G| \le 95$ all half-factorial subsets have been determined (computationally) by M. Radziejewski [45].

5 Half-factorial sets via weakly half-factorial sets

The notion of a weakly half-factorial set was introduce, using different terminology, by J. Śliwa [52] as a tool to investigate half-factorial sets. In this section, among others, we state a recent result on weakly half-factorial sets (cf. Theorem 5.3) and some results on half-factorial sets that can be obtained by applying this result.

Definition 5.1 Let G be a finite abelian group. A subset $G_0 \subseteq G$ is called weakly half-factorial if $\mathsf{k}(A) \in \mathbb{N}$ for each atom $A \in \mathcal{A}(G_0)$; and

$$\mu_0(G) = \max\{|G_0| : G_0 \subseteq G \text{ weakly half-factorial}\}.$$

Since half-factorial sets are characterized as those sets $G_0 \subset G$ for which $\mathsf{k}(A) = 1$ for each atom $A \in \mathcal{A}(G_0)$, every half-factorial set is weakly half-factorial and $\mu(G) \le \mu_0(G)$.

Weakly half-factorial sets are in general easier to investigate than half-factorial ones, mainly because of the following characterization in terms of characters of the group (see [52] and also [15]).

Lemma 5.2 *Let G be a finite abelian group with $\exp(G) = n$. A subset $G_0 \subseteq G$ is weakly half-factorial if and only if there exists a character $\chi : G \to \mathbb{Z}/n\mathbb{Z}$ such that*

$$G_0 \subset \{g \in G : \chi(g) = \frac{n}{\mathrm{ord}(g)} + n\mathbb{Z}\}.$$

For instance, this characterization almost directly yields that $\mu_0(C_p^r) = 1 + p^{r-1}$, since it implies that all non-zero elements of a weakly half-factorial set are contained in the same affine hyperplane.

Very recently, M. Radziejewski and the author [47] determined $\mu_0(G)$ and the structure of weakly half-factorial sets with maximal cardinality for arbitrary finite abelian groups (previously, this was already known for groups of the form C_n^r by a result of W. Gao and A. Gerolginger [15]).

Theorem 5.3 *Let $G = \oplus_{i=1}^r C_{n_i}$ with $n_1 \mid \cdots \mid n_r$. Further, let $H = \oplus_{i=1}^{r-1} C_{n_i}$ and $e \in C_{n_r}$ a generating element. Then*

$$\mu_0(G) = \sum_{d \mid n_r} \prod_{i=1}^{r-1} \gcd(n_i, d),$$

and $G_0 \subset G$ is a weakly half-factorial set with maximal cardinality if and only if there exists an automorphism f of G such that

$$f(G_0) = \bigcup_{d \mid n} \{h + \tfrac{\exp(G)}{d} e : h \in H \text{ and } \mathrm{ord}(h) \mid d\}.$$

Moreover, every weakly half-factorial set that generates G and is maximal with respect to inclusion has cardinality $\mu_0(G)$.

A weakly half-factorial subset of G that is maximal with respect to inclusion does not necessarily generate the group, and thus possibly has a cardinality smaller than $\mu_0(G)$. These weakly half-factorial sets were characterized in [47] as well.

It is clear that Theorem 5.3 yields the upper bound

$$\mu(\oplus_{i=1}^r C_{n_i}) \le \sum_{d \mid n_r} \prod_{i=1}^{r-1} \gcd(n_i, d).$$

And, more information on half-factorial sets (for certain groups) can be obtained from it. First, we recall the definition of the cross number of a group. Let G be a finite abelian group, then $\mathsf{K}(G) = \max\{\mathsf{k}(A) \colon A \in \mathcal{A}(G)\}$ denotes the cross number of G.

By the very definition of weakly half-factorial sets and by the characterization of half-factorial sets (cf. Theorem 4.1), it is clear that for groups with $\mathsf{K}(G) < 2$ every weakly half-factorial set is half-factorial. Thus, for groups with $\mathsf{K}(G) < 2$, Theorem 5.3 yields the value of $\mu(G)$, and the structure of half-factorial sets with maximal cardinality. Moreover, by results of U. Krause, C. Zahlten [37] and A. Geroldinger, R. Schneider [24] all groups with $\mathsf{K}(G) < 2$ are known. Indeed, these are precisely the groups occurring in the following corollary.

The results stated in the following corollary were partly well known (for 1. cf. [50, 51, 53, 8, 23, 42] and for special cases of 2. cf. [52, 23, 46]). The approach via weakly half-factorial sets presented in [47] provided a unified proof of these known results and in addition some new results.

Corollary 5.4 *Let $p, q \in \mathbb{P}$ with $p < q$ and $m, n \in \mathbb{N}_0$.*

1. $\mu(C_{p^m q^n}) = \mu_0(C_{p^m q^n}) = (m+1)(n+1)$.
2. $\mu(C_{p^m} \oplus C_{p^{m+n}}) = \mu_0(C_{p^m} \oplus C_{p^{m+n}}) = np^m + \frac{p^{m+1}-1}{p-1}$.
3. $\mu(C_2 \oplus C_{2q^n}) = \mu_0(C_2 \oplus C_{2q^n}) = 3(n+1)$.

And, in each of the cases the structure of half-factorial sets with maximal cardinality is given by Theorem 5.3.

As mentioned above, for all groups not given in Corollary 5.4 actually $\mathsf{K}(G) \geq 2$. Thus, one cannot extend this straightforward way of applying Theorem 5.3 to further classes of groups. However, Theorem 5.3 is also a main tool to determine $\mu(G)$ for further classes of groups; in particular, to obtain the following result that (partly) extends Corollary 5.4.3.

Proposition 5.5 ([47]) *Let $p, q \in \mathbb{P}$ distinct and $G = C_p \oplus C_{pq}$.*

1. *If $q \equiv 1 \pmod{p}$, then $\mu(G) = 2p + 2$.*
2. *If $q \not\equiv 1 \pmod{p}$, then $\mu(G) = 2p + 1$.*

Outline of proof. We note that $\mu_0(C_p \oplus C_{pq}) = 2p + 2$. Thus, in order to prove 1. it suffices to show that a weakly half-factorial set with maximal cardinality is half-factorial. To prove 2., one shows that a weakly half-factorial set with maximal cardinality is not half-factorial, but the set obtained by removing the element with order q from it is half-factorial. □

In Section 7 we encounter an analog of the phenomenon that $\mu(C_p \oplus C_{pq})$ depends on a congruence condition among divisors of the order of the group.

We conclude this section by remarking that for groups with large rank, which implies large cross number, weakly half-factorial sets can be much larger than half-factorial sets; for instance, $\mu_0(C_p^r) = 1 + p^{r-1}$ whereas $\mu(C_p^r) \leq 1 + rp/2$ (cf. Theorem 6.1).

6 Elementary p-groups

Elementary p-groups are a class of groups for which half-factorial sets are relatively well understood. In particular, in this case the value of $\mu(G)$ and the structure of half-factorial sets with maximal cardinality are known (cf. Subsection 6.1). Yet, a complete characterization of all half-factorial sets is only known in special cases (cf. Subsection 6.2).

For an elementary p-group, since every non-zero element has order p, the characterization of a half-factorial set G_0 simplifies to: $|A| = p$ for every $A \in \mathcal{A}(G_0) \setminus \{0\}$.

6.1 Maximal cardinality and the inverse problem

In this subsection we present results on the maximal cardinality of half-factorial sets and the according inverse problem. The following theorem was obtained for groups with even rank by A. Geroldinger and J. Kaczorowski [23] and for odd rank by A. Plagne and the author [41].

Theorem 6.1 *For $p \in \mathbb{P}$ and $r \in \mathbb{N}$,*

$$\mu(C_p^r) = \begin{cases} 2 + \frac{r-1}{2}p & \text{if } r \text{ is odd,} \\ 1 + \frac{r}{2}p & \text{if } r \text{ is even.} \end{cases}$$

The solution of the inverse problem was given in [41] as well.

Theorem 6.2 *There exists an absolute constant $c > 0$ such that for $G_0 \subset C_p^r$ a half-factorial set the following holds: If $|G_0| > \mu(C_p^r) - cp$, then there exists an independent generating set $\{e_1, \ldots, e_r\} \subset C_p^r$, such that*

$$G_0 \subset \bigcup_{i=1}^{\lfloor \frac{r}{2} \rfloor} \{je_{2i-1} + (p+1-j)e_{2i} \colon j \in [1,p]\} \cup \{e_r, 0\}.$$

In particular, if $\mu(G) = |G_0|$, then

$$G_0 = \bigcup_{i=1}^{\lfloor \frac{r}{2} \rfloor} \{je_{2i-1} + (p+1-j)e_{2i} \colon j \in [1,p]\} \cup \{e_r, 0\}.$$

Outline of proofs. To show that the expressions on the right-hand side in Theorem 6.1 is a lower bound and that the set on the right-hand side in Theorem 6.2 is half-factorial, one repeatedly applies 4. of Section 4 and results on p-groups of rank 1 and 2 (cf. 1. and 2. of Corollary 5.4; note however the difference in notation, in order to have a consistent formulation of Theorem 6.2 and Theorem 6.3).

To obtain the upper bounds Lemma 4.3 and further results of this type are main tools. A crucial point of the argument, in particular for the inverse result, is the following: The half-factorial sets that are used to obtain the lower bounds consist, except the

zero-element, of an independent generating set and elements that have two non-zero coordinates with respect to this generating set. And indeed, if G_0 is a half-factorial set for which this is not the case, that is G_0 contains some element that has three or more non-zero coordinates with respect to some independent generating set contained in G_0, then for $|G_0|$ a (considerably) improved upper bound, namely by cp, for some $c > 0$, smaller than the aforementioned lower bounds, can be obtained. □

We point out that the property of elementary p-groups that every subset contains an independent generating set (of the generated subgroup) is crucial for the proof. In Section 8 we see, in more general situations, that for half-factorial sets that contain an independent generating set good estimates for their cardinality are known.

Given the way Theorem 6.1 is stated, a natural question to address is the size of the constant c. In [41] it was noted that Theorem 6.2 holds for "$c = 1/12$" and that it cannot hold, in general, for "c=1"; and some further considerations were made there:

For $p \in \mathbb{P}$ and $r \in \mathbb{N}$, let $c_0(p, r)$ denote the supremum of all $c > 0$ such that the conclusion of Theorem 6.2 holds for the group C_p^r.

Then $1/6 \le \liminf_{p\to\infty} c_0(p, r) \le 1$ for odd $r \ge 3$ and $2/3 \le \liminf_{p\to\infty} c_0(p, r) \le 2$ for even $r \ge 4$. It is highly unlikely that equality holds at the lower bounds. Also, there is no good evidence, known to the author, that supports that equality holds at the upper bounds; yet this might be the case.

Moreover, $c_0(p, r) \ge c_0(p, r + 2)$ and

$$c_0(p, 2r) \ge c_0(p, 2r + 1) \ge c_0(p, 2r + 2) - (p - 2)/p$$

for every $r \in \mathbb{N}$. In the following subsection we give the values of $c_0(p, r)$ for $r \le 2$ and for $p \le 7$. Yet, the problem of determining $c_0(p, r)$ in general or, more modestly, to determine for some fixed r the behavior of $c_0(p, r)$ as $p \to \infty$ is open.

6.2 Complete characterization in special cases

The results of the preceding subsection describe the structure of half-factorial sets with (almost) maximal cardinality. Yet, in general there exist half-factorial subsets that are not contained in a half-factorial set with maximal cardinality. For arbitrary elementary p-groups a complete characterization of half-factorial sets is not known.

Let G denote an elementary p-group. In this subsection we present a complete characterization of its half-factorial sets in case $\mathsf{r}(G) \le 2$ or $\exp(G) \le 7$, and a (partial) conjecture for the general case.

6.2.1 Small rank

The case $\mathsf{r}(G) \le 2$ is in fact already settled by the results mentioned in Section 5. We recall that in this case every half-factorial subset is contained in a half-factorial subset with cardinality $\mu(G)$; this set is uniquely determined up to automorphisms of the group. In particular, this yields $c_0(p, 1) = c_0(p, 2) = \infty$ for every prime p.

For $\mathsf{r}(G) \ge 3$, and general exponent, the problem of determining all half-factorial subsets is open. It seems, to the author, that even for $\mathsf{r}(G) = 3$ an explicit characterization of all half-factorial sets could be quite complex. The fact that in this case $\mathsf{K}(G) > 2$ and weakly half-factorial sets can differ considerably from half-factorial ones can be seen as explanation for the seemingly rapid increase in difficulty.

6.2.2 Small exponent

For groups with small exponent Lemma 4.3 yields very restrictive conditions. These conditions can be used, in combination with some more or less ad hoc considerations, to give a complete characterization of all half-factorial sets in case $\exp(G) \le 7$; for $\exp(G) = 2$ this was initially given by W. Narkiewicz [39] and the other cases were given in [49], for $\exp(G) = 3$ a slightly different characterization was obtained independently by M. Radziejewski [43].

To state the result conveniently, we introduce some additional notation (cf. [48]). Let $G_0 \subset G$ be a non-empty subset. The set G_0 is called decomposable, if G_0 has a partition $G_0 = G_0' \dot\cup G_0''$ with non-empty sets G_0' and G_0'' such that $\langle G_0\rangle = \langle G_0'\rangle \oplus \langle G_0''\rangle$; and it is called indecomposable otherwise. There exist a uniquely determined $d \in \mathbb{N}$ and (up to order) uniquely determined indecomposable sets $\emptyset \ne G_1, \ldots, G_d \subset G_0$ such that

$$G_0 = \dot{\bigcup}_{i=1}^{d} G_i \text{ and } \langle G_0\rangle = \oplus_{i=1}^{d} \langle G_i\rangle.$$

Thus, in order to describe all half-factorial subsets, it suffices to determine all indecomposable half-factorial subsets.

Theorem 6.3 *Let G be an elementary p-group, for some $p \in \{2, 3, 5, 7\}$, and $G_0 \subset G$ an indecomposable half-factorial set. (The sets $\{e_1, \ldots, e_n\}$ below are independent.)*

1. *If $p = 2$, then $G_0 = \{g\}$ for some $g \in G$.*
2. *If $p = 3$, then*
   - *$G_0 = \{g\}$ for some $g \in G$ or*
   - *$G_0 = \{je_1 + (4-j)e_2 \colon j \in [1, 3]\}$.*
3. *If $p = 5$, then*
   - *$G_0 = \{g\}$ for some $g \in G$,*
   - *$G_0 \subset \{je_1 + (6-j)e_2 \colon j \in [1, 5]\}$, or*
   - *$G_0 = \{4(e_1 + e_2 + e_3 + e_4), e_1, e_2, e_3, e_4\}$.*
4. *If $p = 7$, then*
   - *$G_0 = \{g\}$ for some $g \in G$,*
   - *$G_0 \subset \{je_1 + (8-j)e_2 \colon j \in [1, 7]\}$,*

- $G_0 \subset \{5(e_1+e_2+e_3), 4(e_1+e_2), e_1, e_2, e_3\}$, *or*
- $G_0 = \{6\sum_{i=1}^{6} e_i, e_1, \ldots, e_6\}$.

It is of course more natural to express the result for $p = 2$ as: $G_0 \subset C_2^r$ is half-factorial if and only if $G_0 \setminus \{0\}$ is independent, which is the way it is stated in [39]. Yet, to have a uniform description for all $p \in \{2, 3, 5, 7\}$, we choose this somewhat artificial description.

We note that Theorem 6.3 yields

- $c_0(2, r) = c_0(3, r) = \infty$ for $r \in \mathbb{N}$.
- $c_0(5, r) = \infty$ for $r = 3$, and $c_0(5, r) = 1$ for $r \geq 4$.
- $c_0(7, 2r+1) = 2/7$ and $c_0(7, 2r+2) = 8/7$ for $r \in \mathbb{N}$.

It seems conceivable to expect that when attempting to extend Theorem 6.3 to further (small) primes one would face only a "natural" increase in complexity, but not a jump in difficulty as for the rank. Indeed, in view of Theorem 6.3 and some other evidence obtained in [49] and [41], the following conjecture could be true.

Conjecture 6.4 For every $p \in \mathbb{P}$ there exists some $R(p) \in \mathbb{N}$ such that for every $r \in \mathbb{N}$ and every indecomposable half-factorial set $G_0 \subset C_p^r$,

$$\mathsf{r}(\langle G_0 \rangle) \leq R(p).$$

In the absence of an example to the contrary, one can hope that the conjecture is even true for $R(p) = p-1$; this would be best possible, since the set $\{-\sum_{i=1}^{p-1} e_i, e_1, \ldots, e_{p-1}\}$ is half-factorial for every p.

However, note that a statement analogous to Conjecture 6.4 cannot hold for arbitrary finite abelian groups. Already in C_4^r there exists, for every $r' \leq r$, an indecomposable half-factorial subset such that the generated subgroup has rank r' (cf. Section 8).

Provided the conjecture is true, the value of $c_0(p, r)$ depends for any (fixed) $p \in \mathbb{P}$ and $r \geq r_0(p)$ just on the parity of r.

7 Cyclic groups

In this section we consider half-factorial subsets of cyclic groups. We recall from Section 5 that, for each $n \in \mathbb{N}$,

$$\mu(C_n) \leq \tau(n),$$

where $\tau(n)$ denotes the number of divisors of n. More precisely, it is known that for every half-factorial set $G_0 \subset C_n$ there exists some generating element $g \in C_n$ such that (cf. Section 5)

$$G_0 \subset \{dg \colon 1 \leq d \mid n\}.$$

In the opposite direction S.T. Chapman [3] showed that any subset of $\{dg\colon 1 \le d \mid n\}$ that contains at most three non-zero elements is half-factorial; and in general "three" is best possible.

Recall that

$$\mu(C_n) = \tau(n)$$

if n is divisible by at most two distinct prime numbers (cf. Corollary 5.4). But, this equality does not hold for all $n \in \mathbb{N}$; indeed A. Zaks [54] showed $\mu(C_{30}) < 8$.

The fact that $G_0 \subset \{dg\colon 1 \le d \mid n\}$ for every half-factorial set, in combination with the characterization result (cf. Theorem 4.1), allows to reduce investigations on half-factorial sets to investigations of sums of the form

$$\sum_{d\in\mathcal{D}} a_d d = kn$$

where $\mathcal{D}$ is a subset of the set of divisors of n and $k, a_d \in \mathbb{N}_0$. Note that $1/\mathrm{ord}(dg) = d/n$ for $1 \le d \mid n$. This lead to the definition of splittable sets in [54] (also cf. [15]), which were then further investigated by P. Erdős and A. Zaks [11].

A way to obtain lower bounds for $\mu(C_n)$, for arbitrary $n \in \mathbb{N}$, is to factor $n = \prod_{i=1}^{r} n_i$, where n_i are prime powers or products of two prime powers, and then to apply 4. of Section 4 to obtain (cf. [23])

$$\mu(C_n) \ge \sum_{i=1}^{r} \mu(C_{n_i}) - (r-1) = \sum_{i=1}^{r} \tau(n_i) - (r-1).$$

Yet, this lower bound in general does not have the same order of magnitude as $\tau(n)$.

Very recently, A. Plagne and the author [42] showed that $\tau(n)$ is indeed the true order of magnitude of $\mu(C_n)$.

Theorem 7.1 *Let $n \in \mathbb{N} \setminus \{1\}$. Then*

$$1 + \frac{1}{2}\tau(n) \le \mu(C_n) \le \tau(n).$$

Outline of proof. Let $m = n/p'$, where p' denotes the largest prime divisor of n, and let $G_0 = \{0\} \cup \{dg\colon 1 \le d \mid m\}$, where $g \in C_n$ is a generating element. Note that $|G_0| = 1 + \tau(m) \ge 1 + \tau(n)/2$. To obtain the lower bound, it suffices to show that G_0 is a half-factorial set, which is the main step in the proof. □

From the outline of the proof it can be seen that if the largest prime divisor of n has multiplicity greater than one, then this construction yields a better lower bound. Moreover, some further improvements can be obtained, for various n, by this method. The point is that it is not essential to take $m = n/p'$, but one can choose any divisor m of n that is not too "large", in a somewhat technical sense given in [42]. Yet, for squarefree numbers the lower bound of the theorem seems to be the limit of this(!) method. However, several other results obtained in [42] suggest that if n is composite

$\mu(C_n)$ might always exceed the lower bound $1 + \tau(n)/2$. Here, we only state a simple result of this type. It is, moreover, another example for the phenomenon that the value of $\mu(G)$ depends on congruence relations among the prime divisors of the order of the group (cf. Proposition 5.5): For $p \in \mathbb{P}$ we have

$$\mu(C_{6p}) = \begin{cases} 7 & \text{if } p \equiv 2 \pmod 3 \\ 8 & \text{if } p \equiv 1 \pmod 3. \end{cases}$$

Other interesting constructions of half-factorial sets in cyclic groups were given by W. Hassler [32]. Among others, he considered the problem when $\{ig\colon i \in [1,k]\} \subset C_n$, for $g \in C_n$ generating, is half-factorial and gave the following criterion.

Theorem 7.2 *Let $k, n \in \mathbb{N}$ with $k \le n$ and $g \in C_n$ a generating element. Then the following conditions are equivalent:*

1. *The set $\{ig\colon i \in [1,k]\} \subset C_n$ is half-factorial.*
2. *$\operatorname{lcm}([1,k])$ divides n.*

8 p-groups

In preceding sections we already stated results on half-factorial subsets of certain p-groups, namely for elementary p-groups and for p-groups with $\mathsf{r}(G) \le 2$. For these groups, among others, the value of $\mu(G)$ is known.

For arbitrary p-groups the problem seems to be significantly more difficult and less is known. However, for the cardinality of generating half-factorial subsets of $C_{p^k}^r$ a good upper bound is known by the following result of W. Gao and A. Geroldinger [15]. For the proof of this result it is essential to know that every generating subset of $C_{p^k}^r$ contains an independent generating subset (see [16]).

Proposition 8.1 *Let $p \in \mathbb{P}$ and $k, r \in \mathbb{N}$, and let $G_0 \subset C_{p^k}^r$ a half-factorial generating set. Then*

$$|G_0| \le 1 + r(p^k - 1).$$

The following proposition gives a complete characterization of the generating half-factorial sets of groups of the form C_4^r.

Proposition 8.2 ([46]) *Let $r \in \mathbb{N}$ and let $G_0 \subset C_4^r$ be a generating set. The set G_0 is half-factorial if and only if there exists an independent generating set $\{e_1, \ldots, e_r\}$, $s, t \in \mathbb{N}_0$ with $r = 3s + t$ and a map f from $[1,t]$ to itself such that*

$$G_0 \subset \{0\} \cup \bigcup_{j=1}^{t} \{e_j, 2e_j, 3e_j + 2e_{f(j)}\} \cup \bigcup_{i=0}^{s-1} \{e_{3i+t+1}, e_{3i+t+2}, e_{3i+t+3}, 3(e_{3i+t+1} + e_{3i+t+2} + e_{3i+t+3})\}.$$

In particular, the maximal cardinality of a generating half-factorial set in C_4^r equals $1 + 3r$.

Moreover, this proposition shows that C_4^r contains indecomposable half-factorial sets of every rank $r' \leq r$; in contrast to the results for elementary p-groups (cf. Section 6). Also, it implies that the bound stated in Proposition 8.1 is best possible, for $p^k = 4$. Indeed, for even r the bound is optimal for any 2-power, which can be seen by repeatedly applying 4. of Section 4 and Corollary 5.4.2 to obtain a generating half-factorial set with cardinality $(2^{k+1} - 1)r/2 - (r/2 - 1) = 1 + r(2^k - 1)$.

It is subject of current research of M. Radziejewski and the author to generalize these results. For instance, to obtain analogous results for other (small) prime powers, and a description for non-generating half-factorial sets in C_4^r as well. Among others, some preliminary results suggest the following: For even r and every $p \in \mathbb{P}$, the half-factorial subset of $C_{p^k}^r$ obtained, as above for $C_{2^k}^r$, by repeatedly applying 4. of Section 4 and Corollary 5.4.2, is a generating half-factorial subset of $C_{p^k}^r$ with, for a generating subset, maximal possible cardinality.

Finally, we state the result, mentioned in Section 4, that asserts the existence of finite abelian groups in which no subset of maximal cardinality generates the group.

Theorem 8.3 ([15]) *Let $p \in \mathbb{P}$ and $k, s \in \mathbb{N}$ with $k \geq 2$ and $p+k \geq 6$. No half-factorial subset of $C_{p^k}^{(p+1)s}$ with maximal cardinality, $\mu(C_{p^k}^{(p+1)s})$, is a generating set.*

Outline of proof. By Proposition 8.1 one has the upper bound $1 + s(p+1)(p^k - 1)$ for the cardinality of a generating half-factorial set in $C_{p^k}^{(p+1)s}$. Thus, in order to prove the theorem, it suffices to construct a half-factorial set whose cardinality exceeds this bound. The crucial step is to obtain such a set in case $s = 1$; the result for $s > 1$ then follows by 4. of Section 4. This is achieved by making use of further results of [15] that yield the existence of a half-factorial set with cardinality $1 + p^{p(k-1)}$; which by the assumptions on p and k is larger than $1 + (p+1)(p^k - 1)$. □

References

[1] Anderson, D.D. (ed.), *Factorization in integral domains*, Lecture Notes in Pure and Appl. Math. *189*, Marcel Dekker Inc., New York 1997.

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

[3] Chapman, S.T., *On the Davenport constant, the cross number, and their application in factorization theory*, in: Anderson, D.F. and Dobbs, D.E. (eds.): *Zero-dimensional commutative rings (Knoxville, TN, 1994)*, Lecture Notes in Pure and Appl. Math. *171*, 167–190, Marcel Dekker Inc., New York 1995.

[4] Chapman, S.T. (ed.), *Arithmetical properties of commutative rings and monoids*, Lecture Notes in Pure and Appl. Math. *241*, CRC Press (Taylor & Francis Group), Boca Raton 2005.

[5] Chapman, S.T. and Coykendall, J., *Half-factorial domains, a survey*, in: Chapman, S.T. and Glaz, S. (eds.): *Non-Noetherian commutative ring theory*, Math. Appl. *520*, 97–115, Kluwer Acad. Publ., Dordrecht 2000.

[6] Chapman, S.T., Freeze, M., and Smith, W.W., *On generalized lengths of factorizations in Dedekind and Krull domains*, in: Chapman, S.T. and Glaz, S. (eds.): *Non-Noetherian commutative ring theory*, Math. Appl. *520*, 117–137, Kluwer Acad. Publ., Dordrecht 2000.

[7] Chapman, S.T. and Geroldinger, A., *Krull domains and monoids, their sets of lengths, and associated combinatorial problems*, in: Anderson, D.D. (ed.): *Factorization in integral domains, (Iowa City, IA, 1996)*, Lecture Notes in Pure and Appl. Math. *189*, 73–112, Marcel Dekker Inc., New York 1997.

[8] Chapman, S.T. and Smith, W.W., *Factorization in Dedekind domains with finite class group*, Israel J. Math. *71* (1990), 65–95.

[9] Claborn, L., *Every abelian group is a class group*, Pacific J. Math. *18* (1966), 219–222.

[10] Coykendall, J., *Extensions of half-factorial domains: a survey*, in: Champman, S.T. (ed.): *Arithmetical Properties of Commutative Rings and Monoids*, Lecture Notes in Pure and Appl. Math. *241*, 46–70, CRC Press (Taylor & Francis Group), Boca Raton 2005.

[11] Erdős, P. and Zaks, A., *Reducible sums and splittable sets*, J. Number Theory *36* (1990), 89–94.

[12] Facchini, A. and Halter-Koch, F., *Projective modules and divisor homomorphisms*, J. Algebra Appl. *2* (2003), 435–449.

[13] Facchini, A. and Wiegand, R., *Direct-sum decompositions of modules with semilocal endomorphism rings*, J. Algebra *274* (2004), 689–707.

[14] Fossum, R.M., *The divisor class group of a Krull domain*, Springer-Verlag, New York 1973.

[15] Gao, W. and Geroldinger, A., *Half-factorial domains and half-factorial subsets of abelian groups*, Houston J. Math. *24* (1998), 593–611.

[16] Gao, W. and Geroldinger, A., *Systems of sets of lengths. II*, Abh. Math. Sem. Univ. Hamburg *70* (2000), 31–49.

[17] Geroldinger, A., *Über nicht-eindeutige Zerlegungen in irreduzible Elemente*, Math. Z. *197* (1988), 505–529.

[18] Geroldinger, A., *Ein quantitatives Resultat über Faktorisierungen verschiedener Länge in algebraischen Zahlkörpern*, Math. Z. *205* (1990), 159–162.

[19] Geroldinger, A. and Göbel, R., *Half-factorial subsets in infinite abelian groups*, Houston J. Math. *29* (2003), 841–858.

[20] Geroldinger, A. and Halter-Koch, F., *Congruence monoids*, Acta Arith. *112* (2004), 263–296.

[21] Geroldinger, A. and Halter-Koch, F., *Transfer principles in the theory of non-unique factorization*, in: Chapman, S.T. (ed.): *Arithmetical Properties of Commutative Rings and Monoids*, Lecture Notes in Pure and Appl. Math. *241*, 114–141, CRC Press (Taylor & Francis Group), Boca Raton 2005.

[22] Geroldinger, A., Halter-Koch, F., and Kaczorowski, J., *Non-unique factorizations in orders of global fields*, J. Reine Angew. Math. *459* (1995), 89–118.

[23] Geroldinger, A. and Kaczorowski, J., *Analytic and arithmetic theory of semigroups with divisor theory*, Sém. Théor. Nombres Bordeaux (2) *4* (1992), 199–238.

[24] Geroldinger, A. and Schneider, R., The cross number of finite abelian groups. II, European J. Combin. *15* (1994), 399–405.

[25] Gilmer, R., Heinzer, W., and Smith, W.W., *On the distribution of prime ideals within the ideal class group*, Houston J. Math. *22* (1996), 51–59.

[26] Grams, A.P., *The distribution of prime ideals of a Dedekind domain*, Bull. Austral. Math. Soc.*11* (1974), 429–441.

[27] Halter-Koch, F., *Halbgruppen mit Divisorentheorie*, Exposition. Math. *8* (1990), 27–66.

[28] Halter-Koch, F., *Chebotarev formations and quantitative aspects of nonunique factorizations*, Acta Arith. *62* (1992), 173–206.

[29] Halter-Koch, F., *Finitely generated monoids, finitely primary monoids, and factorization properties of integral domains*, in: Anderson, D.D. (ed.): *Factorization in integral domains, (Iowa City, IA, 1996)*, Lecture Notes in Pure and Appl. Math. *189*, 31–72, Marcel Dekker Inc., New York 1997.

[30] Halter-Koch, F., *Ideal Systems, an Introduction to Multiplicative Ideal Theory*, Monographs and Textbooks in Pure and Applied Mathematics *211*, Marcel Dekker Inc., New York 1998.

[31] Halter-Koch, F. and Müller, W., *Quantitative aspects of nonunique factorization: a general theory with applications to algebraic function fields*, J. Reine Angew. Math. *421* (1991), 159–188.

[32] Hassler, W., *A note on half-factorial subsets of finite cyclic groups*, Far East J. Math. Sci. (FJMS) *10* (2003), 187–197.

[33] Kaczorowski, J., *Some remarks on factorization in algebraic number fields*, Acta Arith. *43* (1983), 53–68.

[34] Kainrath, F., *On local half-factorial orders*, in: Chapman, S.T. (ed.): *Arithmetical Properties of Commutative Rings and Monoids*, Lecture Notes in Pure and Appl. Math. *241*, 316–324, CRC Press (Taylor & Francis Group), Boca Raton 2005.

[35] Kainrath, F. and Lettl, G., *Geometric notes on monoids*, Semigroup Forum *61* (2000), 298–302.

[36] Krause, U., *On monoids of finite real character*, Proc. Amer. Math. Soc. *105* (1989), 546–554.

[37] Krause, U., and Zahlten, C., *Arithmetic in Krull monoids and the cross number of divisor class groups*, Mitt. Math. Ges. Hamburg *12* (1991), 681–696.

[38] Narkiewicz, W., *On algebraic number fields with non-unique factorization*, Colloq. Math. *12* (1964), 59–68.

[39] Narkiewicz, W., *Finite abelian groups and factorization problems*, Colloq. Math. *42* (1979), 319–330.

[40] Narkiewicz, W., *Elementary and analytic theory of algebraic numbers, third edition*, Springer-Verlag, Berlin 2004.

[41] Plagne, A. and Schmid, W.A., *On large half-factorial sets in elementary p-groups: Maximal cardinality and structural characterization*, Isreal J. Math. *145* (2005), 285–310.

[42] Plagne, A. and Schmid, W.A., *On the maximal cardinality of half-factorial sets in cyclic groups*, Math. Ann. to appear.

[43] Radziejewski, M., *Wybrane zagadnienia teorii funkcji L wraz z zastosowaniami*, PhD Thesis, Adam Mickiewicz University, Poznań 2002.

[44] Radziejewski, M., *On the distribution of algebraic numbers with prescribed factorization properties*, Acta. Arith. *116* (2005), 153–171.

[45] Radziejewski, M., *The ψ_1 conjecture computations*, at M. Radziejewski's home page, `http://www.staff.amu.edu.pl/~maciejr/`.

[46] Radziejewski, M. and Schmid, W.A., *On the asymptotic behavior of some counting functions*, Colloq. Math. *102* (2005), 181–195.

[47] Radziejewski, M. and Schmid, W.A., *Weakly half-factorial sets in finite abelian groups*, submitted.

[48] Schmid, W.A., *Arithmetic of block monoids*, Math. Slovaca *54* (2004), 503–526.

[49] Schmid, W.A., *Half-factorial sets in elementary p-groups*, Far East J. Math. Sci. (FJMS), to appear.

[50] Skula, L., *On c-semigroups*, Acta Arith. *31* (1976), 247–257.

[51] Śliwa, J., *Factorizations of distinct lengths in algebraic number fields*, Acta Arith. *31* (1976), 399–417.

[52] Śliwa, J., *Remarks on factorizations in algebraic number fields*, Colloq. Math. *46* (1982), 123–130.

[53] Zaks, A., *Half factorial domains*, Bull. Amer. Math. Soc. *82* (1976), 721–723.

[54] Zaks, A., *Half-factorial-domains*, Israel J. Math. *37* (1980), 281–302.

Wolfgang A. Schmid
Institut für Mathematik
Karl-Franzens-Universität Graz
Heinrichstraße 36
8010 Graz, Austria
e-mail: *wolfgang.schmid@uni-graz.at*