HALF-FACTORIAL SETS IN ELEMENTARY p-GROUPS

WOLFGANG A. SCHMID

ABSTRACT. Let G be an abelian group. A subset G_0 of G is called half-factorial, if the block monoid over G_0 is a half-factorial monoid. In this article we investigate half-factorial sets in elementary p-groups. In particular, we determine the half-factorial subsets of elementary 3-, 5- and 7-groups. Moreover, we investigate minimal non-half-factorial sets (sets that are not half-factorial, but every proper subset is half-factorial) in elementary p-groups.

1. INTRODUCTION

Let G be an abelian group and $G_0 \subset G$. Then G_0 is called half-factorial, if the block monoid $\mathcal{B}(G_0)$ is a half-factorial monoid. A main reason for the relevance of this notion is that if D is a Krull domain (monoid) with divisor class group G and $G_0 \subset G$ denotes the set of classes containing prime divisors, then D is half-factorial if and only if $G_0 \subset G$ is a half-factorial set. However, there are also other applications of half-factorial sets. For example the asymptotic behavior of certain counting functions in algebraic number fields depends on the maximal cardinality of half-factorial sets in the class group (and the structure of these sets) cf. [7].

Another type of sets that is studied along with half-factorial sets are minimal non-half-factorial sets, i.e., sets that are not half-factorial but each proper subset is half-factorial. These sets play a crucial role in investigations on distances in sets of lengths cf. [5] and [14]. For more information on the applications of half-factorial sets, we refer to [4] and the references given there.

In this article we shall be interested in half-factorial and minimal non-half-factorial sets in elementary p-groups (i.e. finite dimensional vector spaces over $\mathbb{F}_p$ the field with p elements). In particular, we study $\mu(G)$, the maximal cardinality of a half-factorial set in G, a constant introduced by J. Śliwa (cf. [16, Lemma 1]). The problem of determining $\mu(G)$ for arbitrary (finite) abelian groups is wide open (cf. [4] for several results). Even in case G is a cyclic group the value of $\mu(G)$ is not known (cf. [10] for recent results on half-factorial sets in cyclic groups). However, if G is cyclic of prime power order, then not only $\mu(G)$ is known but even the structure of all half-factorial sets (this result was obtained in slightly different formulations by various authors cf. Proposition 3.4.1 for the result and [4, Corollary 5.4] for a proof and detailed references).

1991 *Mathematics Subject Classification.* 11B, 13F05, 20K99.

Key words and phrases. sets of lengths, half-factorial, factorization, abelian groups.

This work was supported by ÖAD Amadée 2003-2004, Projekt 05/2003.

If G is an elementary p-group with $\mathsf{r}(G) = r$, then

$$1 + \lfloor \frac{r}{2} \rfloor p + 2(\frac{r}{2} - \lfloor \frac{r}{2} \rfloor) \le \mu(G) \le 1 + \frac{r}{2}p,$$

thus if r is even or $p = 2$, then $\mu(G) = 1 + \frac{r}{2}p$ ([9, Theorem 8]). Moreover, if $p = 2$, then the structure of half-factorial sets is known ([12, Problem II]).

We will determine the structure of half-factorial sets with (maximal) cardinality $\mu(G)$ in elementary p-groups with even rank (cf. Theorem 3.1). Moreover, we will investigate the structure of half-factorial and minimal non-half-factorial sets in elementary $3, 5$ and 7-groups (cf. Proposition 6.2, 6.3 and 6.5). Combining these results with known ones, we give a result on $\mu(G)$ and the structure of minimal non-half-factorial sets in elementary p-groups where the rank or the exponent is small (cf. Theorem 3.2).

2. Preliminaries

In this section we fix notations and recall some results, in particular for monoids and abelian groups. The notations mostly will be consistent with the usual ones in factorization theory (cf. the survey articles [11] and [2] in [1]).

Let $\mathbb{R}$ denote the real numbers, $\mathbb{Q}$ the rational numbers, $\mathbb{Z}$ the integers, $\mathbb{N}$ the set of positive integers, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ and $\mathbb{P} \subset \mathbb{N}$ the set of prime numbers. For $p \in \mathbb{P}$ let $\mathbb{F}_p$ denote the field with p elements. For $m, n \in \mathbb{Z}$ we set $[m, n] = \{z \in \mathbb{Z} \mid m \le z \le n\}$.

For a set M we denote by $|M| \in \mathbb{N}_0 \cup \{\infty\}$ its cardinality. For $x \in \mathbb{R}$ let $\lceil x \rceil = \min\{z \in \mathbb{Z} \mid x \le z\}$ and $\lfloor x \rfloor = \max\{z \in \mathbb{Z} \mid x \ge z\}$.

A monoid H is a commutative cancellative semigroup with identity element ($1_H = 1 \in H$) and we usually use multiplicative notation.

Let H be a monoid. We denote by $H^\times$ the group of invertible elements of H. Let $H_1, H_2 \subset H$ be submonoids. Then we write $H = H_1 \times H_2$, if for each $a \in H$, there exist uniquely determined $b \in H_1$ and $c \in H_2$, such that $a = bc$.

An element $u \in H \setminus H^\times$ is called irreducible (or an atom), if for all $a, b \in H$, $u = ab$ implies $a \in H^\times$ or $b \in H^\times$. We denote by $\mathcal{A}(H) \subset H$ the set of atoms. H is called atomic, if every $a \in H \setminus H^\times$ has a factorization into a product of atoms.

Let $a \in H \setminus H^\times$ and $a = u_1 \cdot \ldots \cdot u_k$ be a factorization of a into atoms $u_1, \ldots, u_k \in \mathcal{A}(H)$. Then k is called the length of the factorization. The monoid H is called half-factorial monoid, if it is atomic and for every $a \in H \setminus H^\times$ any two factorizations of a into atoms have the same length.

Let G be an additively written abelian group and $G_0 \subset G$ a subset. Then $\langle G_0 \rangle < G$ denotes the subgroup generated by G_0, where $\langle \emptyset \rangle = \{0\}$.

The set G_0 (respectively its elements) is called independent, if $0 \notin G_0$, $\emptyset \ne G_0$ and given distinct elements $e_1, \ldots, e_r \in G_0$ and $m_1, \ldots, m_r \in \mathbb{Z}$, then $\sum_{i=1}^r m_i e_i = 0$ implies that $m_1 e_1 = \cdots = m_r e_r = 0$. If we say that $\{e_1, \ldots, e_r\}$ is independent, then we will assume that the elements $e_1, \ldots, e_r$ are distinct.

An element $g \in G$ is called torsion element, if there exists some $n \in \mathbb{N}$ such that $ng = 0$. If g is a torsion element, then we denote by $\mathrm{ord}(g) = \min\{n \in \mathbb{N} \mid ng = 0\}$

its order. G is called abelian torsion group, if all elements of G are torsion elements. For $n \in \mathbb{N}$ let C_n denote a cyclic group with n elements.

Let $p \in \mathbb{P}$, then we call G elementary p-group, if there exists some $r \in \mathbb{N}$ such that $G \cong C_p^r$. We denote by $\exp(G) = p$ the exponent of G and by $\mathsf{r}(G) = r$ the rank of G. Clearly, elementary p-groups are torsion groups and each non-zero element has order p. An elementary p-group is in a natural way a vector space over the field $\mathbb{F}_p$. Elements are independent if and only if they are linearly independent over $\mathbb{F}_p$, subgroups are subspaces and the rank equals the dimension as $\mathbb{F}_p$ vector space. A main advantage when dealing with elementary p-groups instead of arbitrary (finite) abelian groups is that each generating set contains an independent generating set (a basis).

Let $\mathcal{F}(G_0)$ denote the free abelian monoid with basis G_0. An element $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G_0)$ is called a sequence in G_0. It has a uniquely determined representation $S = \prod_{g \in G_0} g^{\mathsf{v}_g(S)}$ where $\mathsf{v}_g(S) \in \mathbb{N}_0$ for each $g \in G_0$ and $\mathsf{v}_g(S) = 0$ for all but finitely many. For $g \in G_0$ we call $\mathsf{v}_g(S)$ the multiplicity of g in S. A sequence T is called subsequence of S, if T divides S (in $\mathcal{F}(G_0)$). We denote by

- $|S| = l \in \mathbb{N}_0$ the length of S.
- $\mathsf{k}(S) = \sum_{i=1}^{l} \frac{1}{\mathrm{ord}(g_i)}$ the cross number of S.
- $\sigma(S) = \sum_{i=1}^{l} g_i \in G$ the sum of S.

Note that the sequence 1, the identity element of $\mathcal{F}(G_0)$, has length 0, cross number 0 and sum $0 \in G$. If we consider $|\cdot|$, v_g, σ and k as maps from $\mathcal{F}(G_0)$ to $(\mathbb{N}_0, +)$, G and $(\mathbb{Q}_{\geq 0}, +)$ respectively, then these maps define monoid-homomorphisms.

The sequence S is called a zero-sum sequence (a block), if $\sigma(S) = 0$, and S is called zero-sumfree, if $\sigma(T) \neq 0$ for all subsequences $1 \neq T$ of S. A zero-sum sequence $1 \neq S$ is called minimal zero-sum sequence, if for each proper subsequence T (i.e. with $T \neq S$), T is zero-sumfree. The empty sequence is the only zero-sum sequence that is zero-sumfree, but it is not a minimal zero-sum sequence.

The set $\mathcal{B}(G_0)$ consisting of all zero-sum sequences in G_0 is a submonoid of $\mathcal{F}(G_0)$, called the block monoid over G_0. It is an atomic monoid (in fact even a Krull monoid cf. [2, Section 2.1.d]) and its atoms are just the minimal zero-sum sequences. If $G_1 \subset G_0$, then $\mathcal{B}(G_1) \subset \mathcal{B}(G_0)$ is a submonoid. For ease of notation, we will write $\mathcal{A}(G_0)$ instead of $\mathcal{A}(\mathcal{B}(G_0))$.

Next we repeat the definitions of the main objects of this article.

Definition 2.1. Let G be an abelian group and $G_0 \subset G$.

(1) G_0 is called half-factorial, if $\mathcal{B}(G_0)$ is a half-factorial monoid.
(2) G_0 is called minimal non-half-factorial, if G_0 is not half-factorial and each $G_1 \subsetneq G_0$ is half-factorial.
(3) If G is finite, then $\mu(G) = \max\{|G_0'| \mid G_0' \subset G \text{ half-factorial}\}$.

If G is an infinite abelian group, then there exists some infinite half-factorial subset (cf. [4, Proposition 3.4] and [8] for further results on half-factorial sets in

infinite groups). The main tool for investigations on half-factorial sets in abelian torsion groups is the following result obtained independently by several authors (cf. [15, Theorem 3.1], [16, Lemma 2] and [18, Proposition 1]). A proof in the terminology of this article can be found in [2, Proposition 5.4].

Lemma 2.2. *Let G be an abelian torsion group and $G_0 \subset G$. Then G_0 is half-factorial if and only if $\mathsf{k}(A) = 1$ for each $A \in \mathcal{A}(G_0)$.*

Since the sequence 0 is the only minimal zero-sum sequence in which 0 occurs with positive multiplicity, it follows that if G is an elementary p-group, then statement $\mathsf{k}(A) = 1$ for each $A \in \mathcal{A}(G_0)$ is equivalent to $|A| = p$ for each $A \in \mathcal{A}(G_0) \setminus \{0\}$ (cf. [9, Lemma 1]).

By Lemma 2.2 it is obvious that subsets of half-factorial sets are half-factorial. Next we summarize several properties of half-factorial sets that will be used frequently in the sequel and can also be obtained using Lemma 2.2.

Lemma 2.3. *Let G be an abelian torsion group.*

1. *Independent sets are half-factorial.*
2. *$G_0 \subset G$ is half-factorial if and only if $G_0 \cup \{0\}$ is half-factorial.*
3. *Let $G = G' \oplus G''$, $G'_0 \subset G'$ and $G''_0 \subset G''$. Then $G'_0 \cup G''_0$ is half-factorial if and only if G'_0 and G''_0 are half-factorial. In particular, if G is finite, then $\mu(G) \ge \mu(G') + \mu(G'') - 1$.*
4. *Let G be an elementary p-group and $G_0 \subset G$ be half-factorial with $|G_0| = \mu(G)$. Then $\langle G_0 \rangle = G$.*

Proof. 1.,2. and 3. are proved in [4, Lemma 3.1]. 4. was obtained in [9, 13, Lemma 1]. □

Note that 4. does not hold in general cf. [4, Corollary 6.5] for an example.

By Lemma 2.3.3 it is sufficient to study half-factorial sets that cannot be decomposed into sets that lie in different direct summands of the group. Since every subset of an elementary p-group can be decomposed into such sets, this simplifies the investigation of half-factorial sets considerably. To make this statement precise we recall the notions of components, decomposable and indecomposable sets (cf. [13] in particular Definition 3.8 and Proposition 3.10).

Let $G_0 \subset G$ be a subset of torsion elements. G_0 is decomposable, if G_0 has a partition $G_0 = G_1 \dot\cup G_2$ with non-empty sets G_1, G_2, such that $\langle G_0 \rangle = \langle G_1 \rangle \oplus \langle G_2 \rangle$ (equivalently $\mathcal{B}(G_0) = \mathcal{B}(G_1) \times \mathcal{B}(G_2)$). Otherwise G_0 is indecomposable. A non-empty subset $G_1 \subset G_0$ is called a component of G_0, if $\langle G_0 \rangle = \langle G_1 \rangle \oplus \langle G_0 \setminus G_1 \rangle$.

Proposition 2.4. [13, Proposition 3.10] *Let G be an abelian group and $G_0 \subset G$ a non-empty and finite subset of torsion elements. Then 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*

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

Remark 2.5. By Lemma 2.3 and Proposition 2.4 it follows immediately that if G is an abelian group and $G_0 \subset G$ a non-empty and finite subset of torsion elements then

- G_0 is half-factorial if and only if each indecomposable component of G_0 is half-factorial.
- G_0 is indecomposable if G_0 is minimal non-half-factorial.

By Lemma 2.3.1 we know that independent sets are half-factorial, in fact they are even factorial (cf. [13, Proposition 3.3]). Thus it is natural to investigate sets that consist of independent elements and one additional element. This property together with a certain minimality condition leads to the definition of simple sets (cf. [13, Section 4]).

Definition 2.6. Let G be an abelian group. A non-empty set $G_0 \subset G \setminus \{0\}$ of torsion elements is called simple, if there exist some $g \in G_0$ such that $G_0 \setminus \{g\}$ is independent, $g \in \langle G_0 \setminus \{g\}\rangle$, but $g \notin \langle G_1\rangle$ for any $G_1 \subsetneq G_0 \setminus \{g\}$.

We give a brief summary of results on simple sets in elementary p-groups.

Lemma 2.7. [13, Lemma 4.4] *Let G be an elementary p-group.*

(1) *Let $G_1 \subset G$ be independent, $g \in G \setminus G_1$ and $G_0 = G_1 \cup \{g\}$. Then the following conditions are equivalent:*
   (a) *G_0 is indecomposable.*
   (b) *G_0 is simple.*

   In particular, if G_0 is minimal non-half-factorial, then G_0 is simple.
(2) *Let $G_0 \subset G$ be simple. Then for every $h \in G_0$ the set $G_0 \setminus \{h\}$ is independent, $h \in \langle G_0 \setminus \{h\}\rangle$ and $h \notin \langle G_1\rangle$ for every $G_1 \subsetneq G_0 \setminus \{h\}$.*
(3) *Every simple set is either half-factorial or minimal non-half-factorial.*

Proposition 2.8. *Let G be an elementary p-group, $G_0 \subset G$ a simple set and $g \in G_0$ such that $G_1 = G_0 \setminus \{g\}$ is independent, say $G_1 = \{e_1, \ldots, e_r\}$. Then $g = -\sum_{i=1}^r b_i e_i$ with uniquely determined $b_i \in [1, p-1]$. For every $j \in \mathbb{N}$ there exists some uniquely determined minimal (with respect to divisibility) block $W_j = W_j(G_1, g) \in \mathcal{B}(G_0)$ with $\mathsf{v}_g(W_j) = j$, namely*

$$W_j = g^j \prod_{i=1}^r e_i^{v_i}$$

where $v_i \in [0, p-1]$ with $v_i \equiv jb_i \bmod p$ for each $i \in [1, r]$. In particular, $W_1 = g\prod_{i=1}^r e_i^{b_i}$ and $W_p = g^p$. Moreover, for $\mathcal{A}(G_0)$ the following holds:

$$\{W_1, W_p\} \cup \{e_i^p \mid i \in [1, r]\} \subset \mathcal{A}(G_0) \subset \{W_j \mid j \in [1, p]\} \cup \{e_i^p \mid i \in [1, r]\}.$$

For proofs and further results on simple sets cf. [13, Section 4], in particular Theorem 4.7.

3. Main Results

In this section we state the two main results of this article and we recall known results that will settle several special cases.

Theorem 3.1. *Let G be an elementary p-group with even rank r and $G_0 \subset G$ a half-factorial set with maximal size $|G_0| = \mu(G)$. Then there exist independent elements $e_1, \ldots, e_r \in G$, such that*

$$G_0 = \dot{\bigcup}_{i=1}^{\frac{r}{2}} \{je_{2i-1} + (p+1-j)e_{2i} \mid j \in [1,p]\} \cup \{0\}.$$

Theorem 3.2. *Let G be an elementary p-group such that $\exp(G) \le 7$ or $\mathsf{r}(G) = r \le 2$.*

1. *If $G_0 \subset G$ is minimal non-half-factorial, then G_0 is simple.*
2. *$\mu(G) = 1 + \lfloor \frac{r}{2} \rfloor p + 2(\frac{r}{2} - \lfloor \frac{r}{2} \rfloor)$.*

In Section 6 we will also describe explicitly the structure of half-factorial sets in such elementary p-groups.

There is known no elementary p-group in which the assertions of Theorem 3.2 do not hold.

Next we state a result on half-factorial and minimal non-half-factorial sets in elementary 2-groups that was obtained in [12, Problem II], for convenience we give a proof.

Proposition 3.3. *Let G be an elementary 2-group and $G_0 \subset G \setminus \{0\}$ a non-empty set.*

1. *The following statements are equivalent:*
   (a) *G_0 is half-factorial.*
   (b) *G_0 is independent.*
2. *The following statements are equivalent:*
   (a) *G_0 is minimal non-half-factorial.*
   (b) *G_0 is simple.*

Proof. Let $G_0 \subset G \setminus \{0\}$ and $e_1, \ldots, e_r \in G_0$ independent elements that generate $\langle G_0 \rangle$.

1. By Lemma 2.3.1 it suffices to prove that (a) implies (b). Suppose that G_0 is half-factorial and assume to the contrary that there exists some $g \in G_0 \setminus \{e_1, \ldots e_r\}$. Clearly $g = \sum_{i \in I} e_i$ with some $I \subset [1,r]$ and $|I| \ge 2$. We get $A = g \prod_{i \in I} e_i \in \mathcal{A}(G_0)$ and $\mathsf{k}(A) = \frac{|I|+1}{2} > 1$, hence by Lemma 2.2 G_0 is not half-factorial.

2. Let G_0 be a simple set. Then G_0 is not independent hence by 1. G_0 is not half-factorial and by Lemma 2.7.3 it is minimal non-half-factorial.

Conversely, let G_0 be minimal non-half-factorial. Then 1. implies that there exists some $g \in G_0 \setminus \{e_1, \ldots e_r\}$. Since $g \in \langle e_1, \ldots, e_r \rangle$, we infer by 1. that $\{g, e_1, \ldots, e_r\}$ is not half-factorial, hence $G_0 = \{g, e_1, \ldots, e_r\}$. Since G_0 is minimal non-half-factorial, G_0 is indecomposable and thus simple by Lemma 2.7.1. □

The following result describes the structure of half-factorial and minimal non-half-factorial sets for cyclic groups of prime power order. The first part of this result was obtained in different formulations by various authors (cf. [4, Corollary 5.4] and the references given there), the second part was first obtained in [6, Proposition 6].

Proposition 3.4. *Let G be a cyclic group of prime power order, $G_0 \subset G$ a non-empty set and $g \in G_0$ a generating element of $\langle G_0 \rangle$ with $\mathrm{ord}(g) = p^k$.*

1. *G_0 is half-factorial if and only if $G_0 \subset \{p^i g \mid i \in [0,k]\}$.*
2. *If G_0 is minimal non-half-factorial, then G_0 is simple and the converse holds for $|G| = p$.*

The rest of this article is mainly devoted to the proofs of Theorem 3.1 and Theorem 3.2. Note that for elementary 2-groups and cyclic groups all assertions have been settled by Proposition 3.3 and Proposition 3.4.

4. Auxiliary Results

Several results of this section will be important tools in the proofs of the main results. However, some investigations (e.g., Proposition 4.11) go beyond the needs of these proofs and give further insight in the structure of half-factorial sets in elementary p-groups.

We fix some notation. Until the end of the article, let G be an elementary p-group for some odd prime $p \in \mathbb{P}$. Let

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid x = \frac{z}{s} \text{ with } z, s \in \mathbb{Z} \text{ and } p \nmid s\}$$

denote the localization of $\mathbb{Z}$ at $(p) = p\mathbb{Z}$. Then

$$\pi_p : \begin{cases} \mathbb{Z} \hookrightarrow \mathbb{Z}_{(p)} & \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \\ z & \mapsto z + p\mathbb{Z}_{(p)} \end{cases}$$

is an epimorphism with $\ker(\pi_p) = p\mathbb{Z}$. For $z \in \mathbb{Z}$ with $p \nmid z$ let $z^{-1} \in \mathbb{Z}_{(p)}$ denote its multiplicative inverse, and for $z \in \mathbb{Z}_{(p)}$ let $[z]_p \in [0, p-1]$ be defined by $z + \mathbb{Z}_{(p)} = [z]_p + \mathbb{Z}_{(p)}$.

We start with some results that will be used frequently in the sequel. Lemma 4.1 was proved in [16, Lemma 1] (cf. also [17, 5.]) and Proposition 4.2.2 in [9, Lemma 1]. In [4, Lemma 3.6] similar results are obtained, without the condition, that the order of the elements is prime.

Lemma 4.1. *Let $r \in \mathbb{N}$, $\{e_1, \ldots, e_r\} \subset G$ independent and $g = -\sum_{i=1}^r b_i e_i$ with $b_i \in [0, p-1]$ for each $i \in [1, r]$. If $\{g, e_1, \ldots, e_r\}$ is half-factorial, then $\sum_{i=1}^r b_i = p - 1$.*

Proof. Clearly, $W_1 = g \prod_{i=1}^r e_i^{b_i}$ is an atom with cross number

$$\mathsf{k}(W_1) = \frac{1}{p} + \sum_{i=1}^r \frac{b_i}{p}.$$

From Lemma 2.2 we have $\mathsf{k}(W_1) = 1$, which implies the assertion. □

Proposition 4.2. *Let $r \in \mathbb{N}$, $\{e_1, \ldots, e_r\} \subset G$ independent and $g = -\sum_{i=1}^r b_i e_i$ with $b_i \in [0, p-1]$ for each $i \in [1, r]$. Further let $b_1 \neq 0$ and $h = -\sum_{i=1}^r b_i' e_i \neq 0$, with $b_i' \in [0, p-1]$ for each $i \in [1, r]$. Then*

$$h = -c_1 g - \sum_{i=2}^{r} c_i e_i$$

with $c_1 = [-b_1^{-1} b_1']_p \in [0, p-1]$ and $c_i = [c_1 b_i + b_i']_p \in [0, p-1]$ for each $i \in [2, r]$ and we have:

1. *If $\{g, h, e_1, \ldots, e_r\}$ is half-factorial, then $\sum_{i=1}^r c_i = p - 1$.*
2. *If $\{g, h, e_1, \ldots, e_r\}$ is half-factorial and $b_1 = b_1'$, then $g = h$.*
3. *If $\sum_{i=1}^r c_i \neq p-1$, then there exists a simple subset of $\{g, h, e_1, \ldots, e_r\}$ that is minimal non-half-factorial. In particular, $\sum_{i=1}^r c_i \neq p - 1$, if $b_1 = b_1'$ and $g \neq h$.*

Proof. That $h \in \langle g, e_2, \ldots, e_r \rangle$ and the values of the c_i's follows by linear algebra.

1. Since $\{g, e_2, \ldots, e_r\}$ is independent, we can apply Lemma 4.1 with the set $\{h\} \cup \{g, e_2, \ldots, e_r\}$ and obtain the assertion.

2. Since $b_1 = b_1'$, we get $c_1 = p - 1$ and by 1. this gives $c_2 = \cdots = c_r = 0$, hence $g = h$.

3. As in 1. we apply Lemma 4.1 with the set $\{h\} \cup \{g, e_2, \ldots, e_r\}$ and obtain that $\{h\} \cup \{g, e_2, \ldots, e_r\}$ is not half-factorial. Thus there exists some minimal non-half-factorial subset, which is simple by Lemma 2.7.1. If $b_1 = b_1'$, then $c_1 = p - 1$ and since $g \neq h$ there exists some $j \in [2, r]$ with $c_j \neq 0$. □

4.1. **Simple Half-factorial Sets.** In this subsection we investigate simple half-factorial sets. Throughout the whole subsection, let $r \geq 2$, $\{e_1, \ldots, e_r\} \subset G$ independent and $G_0 = \{g, e_1, \ldots, e_r\}$ a simple half-factorial set, where $g = -\sum_{i=1}^r b_i e_i$ with $b_i \in [1, p-1]$ for each $i \in [1, r]$.

Next we state an easy lemma on certain functions that we will use frequently in the sequel.

Lemma 4.3. *Let $c, d, e \in \mathbb{R}$ with $c > 0$ and let $m, n \in \mathbb{N}$ with $m < n$. Further let*

$$f : \begin{cases} \mathbb{R}_{>0} & \to \mathbb{R} \\ x & \mapsto \frac{c}{x} + dx + e \end{cases}.$$

Then

$$\max\{f(x) \mid x \in [m, n]\} = \max\{f(m), f(n)\}.$$

Proof. Without restriction we assume $e = 0$. Since $c > 0$, we may assume $c = 1$.

Assume to the contrary there exists some $k \in [m+1, n-1]$ with

$$f(k) = \max\{f(x) \mid x \in [m, n]\} > \max\{f(m), f(n)\}.$$

Without restriction let k be minimal with this property. We get $f(k-1) < f(k)$ and $f(k+1) \le f(k)$, hence

$$\frac{1}{k-1} + d(k-1) < \frac{1}{k} + dk$$

and

$$\frac{1}{k+1} + d(k+1) \le \frac{1}{k} + dk.$$

We add up the two inequalities and get $\frac{1}{k-1} + \frac{1}{k+1} + 2dk < \frac{2}{k} + 2dk$, which implies

$$\frac{2}{k - \frac{1}{k}} < \frac{2}{k},$$

a contradiction. □

Lemma 4.4. *For each $j \in [1, r]$*

$$\sum_{i=1}^{r} [b_j^{-1} b_i]_p = p - [b_j^{-1}]_p.$$

Proof. Without restriction we may suppose $j = 1$. We apply Proposition 4.2 with $h = -\sum_{i=1}^{r} b_i' e_1 = e_1$. Then $h = -c_1 g - \sum_{i=2}^{r} c_i e_i$ with $c_1 = [b_1^{-1}]_p$ and $c_i = [b_1^{-1} b_i]_p$ for each $i \in [2, r]$. Since $G_0 = \{g, h, e_1, \ldots, e_r\}$ is half-factorial, Proposition 4.2.1 implies that $\sum_{i=1}^{r} c_i = p - 1$ hence

$$\sum_{i=1}^{r} [b_1^{-1} b_i]_p = 1 + \sum_{i=2}^{r} c_i = 1 - c_1 + (p-1) = p - [b_1^{-1}]_p.$$

□

Next we give an example of a simple set $G_0' = \{g, e_1, \ldots, e_r\}$ which is not half-factorial but

$$\sum_{i=1}^{r} b_i = p - 1 \text{ and } \sum_{i=1}^{r} [b_j^{-1} b_i]_p = p - [b_j^{-1}]_p$$

for each $j \in [1, r]$. Thus the conditions derived in Lemma 4.1 and Lemma 4.4 are not sufficient to characterize half-factoriality.

Example 4.5. Let $p = 19$, $r = 3$ hence $\langle e_1, e_2, e_3 \rangle \cong (\mathbb{Z}/19\mathbb{Z})^3$ and let $G_0' = \{-8e_1 - 5e_2 - 5e_3, e_1, e_2, e_3\}$. Then G_0' is simple, $\sum_{i=1}^{r} b_i = 8 + 5 + 5 = p - 1$,

$$[8^{-1}8]_{19} + [8^{-1}5]_{19} + [8^{-1}5]_{19} = 1 + 3 + 3 = 19 - [8^{-1}]_{19}$$

and

$$[5^{-1}8]_{19} + [5^{-1}5]_{19} + [5^{-1}5]_{19} = 13 + 1 + 1 = 19 - [5^{-1}]_{19}.$$

However,

$$W_3 = g^3 e_1^5 e_2^{15} e_3^{15} \in \mathcal{A}(G_0')$$

and $\mathsf{k}(W_3) = 2$, hence G_0' is not half-factorial.

Lemma 4.6. *Let $b_1 \ge \cdots \ge b_r$, $b_1 > 1$ and $k = \lfloor \frac{p}{b_1} \rfloor$.*

(1) $k = \lfloor \frac{p}{b_k} \rfloor$ *and if* $k < r$, *then* $k < \lfloor \frac{p}{b_{k+1}} \rfloor$.
(2) $r + 2 \le k + b_k$.

Proof. 1. Since $b_1 > 1$ we get $k + 1 = \lceil \frac{p}{b_1} \rceil$. Using the notation of Proposition 2.8, we consider the block $W_{k+1} = g^{k+1} \prod_{i=1}^{r} e_i^{[(k+1)b_i]_p} \in \mathcal{B}(G_0)$. We assert that W_{k+1} is an atom. This follows by [13, Theorem 4.7 and Corollary 4.9], yet for convenience we give a proof.

Clearly, $e_i^p \nmid W_{k+1}$ thus, by Proposition 2.8, it suffices to show that $W_j \nmid W_{k+1}$ for each $j \in [1, k]$. By definition of k it is obvious that $W_j = W_1^j$ for each $j \in [1, k]$ and it remains to verify that $W_1 \nmid W_{k+1}$. Again by definition of k we get $\mathsf{v}_{e_1}(W_{k+1}) = (k+1)b_1 - p < b_1 = \mathsf{v}_{e_1}(W_1)$, which implies $W_1 \nmid W_{k+1}$ and thus W_{k+1} is an atom.

Since G_0 is half-factorial we obtain by Lemma 2.2 that $|W_{k+1}| = p$. We set $s = \max\{i \in [1, r] \mid k = \lfloor \frac{p}{b_i} \rfloor\}$. Clearly, $[(k+1)b_i]_p = (k+1)b_i - p$, if $i \in [1, s]$ and $[(k+1)b_i]_p = (k+1)b_i$, if $i \in [s+1, r]$. We get

$$p = |W_{k+1}| = k + 1 + \sum_{i=1}^{r} [(k+1)b_i]_p = k + 1 + \sum_{i=1}^{r} (k+1)b_i - sp = (k+1)p - sp,$$

where the last equality follows from Lemma 4.1 and the fact that G_0 is half-factorial. This gives $k = s$ and the result is obvious from the definition of s.

2. Since G_0 is half-factorial, we get $\sum_{i=1}^{r} b_i = p - 1$. From this we get

$$\sum_{i=1}^{k} b_i = p - 1 - \sum_{k+1}^{r} b_i \le p - 1 - r + k.$$

Moreover,

$$\sum_{i=1}^{k} b_i \ge \sum_{i=1}^{k} b_k = kb_k = \lfloor \frac{p}{b_k} \rfloor b_k > p - b_k,$$

hence we get $p - b_k < p - 1 - r + k$ and $r + 2 \le k + b_k$. □

Proposition 4.7. *For* r *we have:*

(1) $r \le p - 1$.
(2) $r \notin [\frac{p+1}{2}, p - 2]$.
(3) *If* $p \ge 13$, *then* $r \ne \frac{p-3}{2}$.

Proof. 1. By Lemma 4.1 we have $r \le \sum_{i=1}^{r} b_i = p - 1$.

2. For $p = 3$ the assertion is obvious. Let $p \ge 5$ and assume to the contrary that $r \in [\frac{p+1}{2}, p - 2]$. After a suitable renumeration we may suppose that $b_1 \ge \cdots \ge b_r$. If $b_1 = 1$, then $p - 1 = \sum_{i=1}^{r} b_i = r$, a contradiction. If $b_1 \ge \frac{p+1}{2}$, then $p - 1 = \sum_{i=1}^{r} b_i \ge \frac{p+1}{2} + r - 1 \ge p$, a contradiction. This implies that $b_1 \in [2, \frac{p-1}{2}]$ and we set $k = \lfloor \frac{p}{b_1} \rfloor$. Then Lemma 4.6 implies that $b_k \in [2, \frac{p-1}{2}]$ and

$$\frac{p+5}{2} \le r + 2 \le \lfloor \frac{p}{b_k} \rfloor + b_k \le \frac{p}{b_k} + b_k.$$

Let $f : \mathbb{R}_{>0} \to \mathbb{R}$ be defined via $f(x) = \frac{p}{x} + x$ for every $x \in \mathbb{R}_{>0}$. Then Lemma 4.3 implies that

$$\max\{f(x) \mid x \in [2, \frac{p-1}{2}]\} = \max\{f(2), f(\frac{p-1}{2})\}.$$

However, $f(2) < \frac{p+5}{2}$ and $f(\frac{p-1}{2}) < \frac{p+5}{2}$, a contradiction.

3. Let $p \geq 13$ and assume to the contrary that $r = \frac{p-3}{2}$. After a suitable renumeration we may suppose that $b_1 \geq \cdots \geq b_r$ and arguing as in 2. we infer that $b_1 \in [3, \frac{p+3}{2}]$.

Let $b_1 = \frac{p+3}{2}$. Then $b_2 = \cdots = b_r = 1$ and for $d = [(\frac{p+3}{2})^{-1}]_p$ we consider

$$W_d = g^d e_1^1 \prod_{i=2}^{r} e_i^d.$$

Clearly, W_d is an atom and since $d \in [3, p-2]$, we obtain that $|W_d| > p$ and $\mathsf{k}(W_d) > 1$, a contradiction to G_0 half-factorial.

Let $b_1 = \frac{p+1}{2}$. Then $b_2 = 2$ and $b_3 = \cdots = b_r = 1$. We consider

$$W_{\frac{p+1}{2}} = g^{\frac{p+1}{2}} e_1^{[(\frac{p+1}{2})^2]_p} e_2^1 \prod_{i=3}^{r} e_i^{\frac{p+1}{2}}.$$

$W_{\frac{p+1}{2}}$ is an atom and since $r \geq 3$ we get that $|W_{\frac{p+1}{2}}| > p$, a contradiction.

Let $b_1 \in \{\frac{p-3}{2}, \frac{p-1}{2}\}$. Then $\lfloor \frac{p}{b_1} \rfloor = 2$, hence by Lemma 4.6 we have $b_2 > \frac{p}{3}$. Since $p - 1 - b_1 - b_2 = \sum_{i=3}^{r} b_i$,

$$p - 1 - b_1 - b_2 < p - 1 - \frac{p-3}{2} - \frac{p}{3} = \frac{p}{6} + \frac{1}{2}$$

and $\sum_{i=3}^{r} b_i \geq \frac{p-3}{2} - 2 = \frac{p}{2} - \frac{7}{2}$, we get $\frac{p}{6} + \frac{1}{2} > \frac{p}{2} - \frac{7}{2}$ respectively $p < 12$, a contradiction.

Let $b_1 \in [3, \frac{p-5}{2}]$ and $k = \lfloor \frac{p}{b_1} \rfloor$. If $p = 13$, then either $b_1 = 3$, $k = 4$ and thus $b_4 = 3$ contradicting

$$\sum_{i=1}^{5} b_i = 12$$

or $b_1 = 4$, $k = 3$ and thus $b_3 = 4$ again contradicting $\sum_{i=1}^{5} b_i = 12$.
Therefore suppose $p \geq 17$. Then by Lemma 4.6 $b_k \in [3, \frac{p-5}{2}]$ and $r + 2 = \frac{p+1}{2} \leq \frac{p}{b_k} + b_k$. Let $f : \mathbb{R}_{>0} \to \mathbb{R}$ be defined as in 2. and we have

$$\max\{f(x) \mid x \in [3, \frac{p-5}{2}]\} = \max\{f(3), f(\frac{p-5}{2})\}.$$

However, $f(3) < \frac{p+1}{2}$ and $f(\frac{p-5}{2}) < \frac{p+1}{2}$, a contradiction.

Consequently, we have that all possible choices of b_1 lead to a contradiction, hence $r \neq \frac{p-3}{2}$. □

Remark 4.8. The bound $p \ge 13$ in Proposition 4.7.3 is optimal. For $p = 11$ and $g = -4e_1 - 4e_2 - e_3 - e_4$ the set $\{g, e_1, \ldots, e_4\}$ is half-factorial, since

$$\{ge_1^4e_2^4e_3e_4, g^3e_1e_2e_3^3e_4^3, g^{11}\} \cup \{e_1^{11}, \ldots, e_4^{11}\}$$

is the set of atoms and each has cross number 1.

Now we will give further examples of half-factorial sets that are simple.

Lemma 4.9. *Suppose that $r \mid p-1$. Then*

$$\{-\sum_{i=1}^{r} \frac{p-1}{r} e_i, e_1, \ldots, e_r\} \text{ and } \{re_1 - \sum_{i=2}^{r} e_i, e_1, \ldots, e_r\}$$

are simple and half-factorial sets.

Proof. Clearly, both sets are simple, and it remains to show that they are half-factorial.

Setting $k = \frac{p-1}{r}$, $g = -\sum_{i=1}^{r} ke_i$ and $G_0 = \{g, e_1, \ldots, e_r\}$ we infer that, using the notation of Proposition 2.8,

$$\mathcal{A}(G_0) = \{W_{1+\nu r} \mid \nu \in [0,k]\} \cup \{e_i^p \mid i \in [1,r]\}.$$

This follows by [3, Theorem 2.1] and [13, Theorem 4.7], yet we give a proof.

By Proposition 2.8 it suffices to show that W_j is an atom if and only if $j \in \{1 + \nu r \mid \nu \in [0,k]\}$. Note that $[(1+\nu r)k]_p = k - \nu$ for each $\nu \in [0,k]$ and that $[jk]_p \ge k$ for each $j \in [1,p] \setminus \{1 + \nu r \mid \nu \in [0,k]\}$.

Therefore $W_1 \mid W_j$ for each $j \in [1,p] \setminus \{1 + \nu r \mid \nu \in [0,k]\}$ and W_j is not an atom. Conversely, $W_{1+\nu' r}$ is an atom for each $\nu' \in [0,k]$, since $W_{1+\nu r} \nmid W_{1+\nu' r}$ for each $\nu \in [0, \nu' - 1]$.

Since for every $\nu \in [0,k]$ the atom

$$W_{1+\nu r} = g^{1+\nu r} \prod_{i=1}^{r} e_i^{k-\nu}$$

has cross number $\mathsf{k}(W_{1+\nu r}) = \frac{1}{p}|W_{1+\nu r}| = \frac{1}{p}(1 + \nu r + \sum_{i=1}^{r}(k-\nu)) = 1$, it follows that G_0 is half-factorial.

To consider the second set, we set $g' = re_1 - \sum_{i=2}^{r} e_i$. Since $\{g', e_2, \ldots, e_r\}$ is independent and

$$e_1 = -\frac{p-1}{r} g' - \sum_{i=2}^{r} \frac{p-1}{r} e_i,$$

the set $\{g', e_1, \ldots, e_r\}$ is half-factorial because $\{g, e_1, \ldots, e_r\}$ is half-factorial. □

In the following two results we will investigate properties of sets that have a subset that is simple and half-factorial with large cardinality, i.e. $r = p-1$ respectively $r = \frac{p-1}{2}$.

Proposition 4.10. *Let $r = p-1$ and $G_0 \subset G_0' \subset G$. Further let $r' = \mathsf{r}(\langle G_0' \rangle)$ and $\{e_{r+1}, \ldots, e_{r'}\} \subset G_0'$ a set such that $\langle G_0' \rangle = \langle e_1, \ldots, e_{r'} \rangle$.*

(1) $g = -\sum_{i=1}^{r} e_i$.

(2) *If* $h = -\sum_{i=1}^{r'} b_i' e_i \notin G_0$ *with* $b_i' \in [0, p-1]$ *and* $b_j' \neq 0$ *for some* $j \in [1, r]$, *then* $\{g, h, e_1, \ldots, e_{r'}\}$ *has a simple, minimal non-half-factorial subset.*
(3) *If* G_0 *is not a component of* G_0', *then* G_0' *has a simple, minimal non-half-factorial subset.*
(4) *If* G_0' *is half-factorial, then* G_0 *is an indecomposable component of* G_0'.

Proof. 1. Since $r \mid p-1$ we get by Lemma 4.9 that $\{-\sum_{i=1}^{r} e_i, e_1, \ldots, e_r\}$ is half-factorial and by Lemma 4.1 we have $p - 1 = \sum_{i=1}^{r} b_i \geq r = p - 1$ hence $b_1 = \cdots = b_r = 1$.

2. If $\{h, e_1, \ldots, e_{r'}\}$ is not half-factorial, then there exists a minimal non-half-factorial subset which is simple by Lemma 2.7.1.

Thus we suppose that $\{h, e_1, \ldots, e_{r'}\}$ is half-factorial. Hence $\sum_{i=1}^{r'} b_i' = p-1$ by Lemma 4.1 and since $p-1 = r$ and $h \neq g$ there exists some $k \in [1, r]$ with $b_k' = 0$. After a suitable renumeration we may suppose that $k = 2$ and $b_1' = \max\{b_i' \mid i \in 1, r]\} > 0$. We set $b_i = 0$ for each $i \in [r+1, r']$ and apply Proposition 4.2 with the independent set $\{e_1, \ldots, e_{r'}\}$. We have $h = -c_1 g - \sum_{i=2}^{r'} c_i e_i$ with $c_1 = [-b_1^{-1} b_1']_p = [-b_1']_p = p - b_1'$, $c_i = [p - b_1' + b_i']_p$ for each $i \in [2, r]$ and $c_i = b_i'$ for each $i \in [r+1, r']$. We show that $\sum_{i=1}^{r'} c_i \neq p-1$ and hence by Proposition 4.2.3 there exists a simple, minimal non-half-factorial subset of $\{g, h, e_1, \ldots, e_{r'}\}$.

If $b_1' \leq \frac{p}{2}$, then $\sum_{i=1}^{r'} c_i \geq c_1 + c_2 = p - b_1' + [p - b_1' + b_2']_p = 2(p - b_1') \geq p$. If $b_1' > \frac{p}{2}$, then we have $b_1' > \max\{b_i' \mid i \in [2, r]\}$. Consequently, $[p - b_1' + b_i']_p = p - b_1' + b_i'$ for each $i \in [2, r]$ and

$$\sum_{i=1}^{r'} c_i = (p-1)(p - b_1') + \sum_{i=2}^{r'} b_i'.$$

Since $h \notin G_0$, we get $b_1' \neq p-1$, hence $\sum_{i=1}^{r'} c_i \geq p$.

3. Suppose G_0 is not a component of G_0'. We assert that there exists some $h = -\sum_{i=1}^{r'} b_i' e_i \in G_0' \setminus G_0$ with $b_i' \in [0, p-1]$ and $b_j' \neq 0$ for some $j \in [1, r]$. Then $\{g, h, e_1, \ldots, e_{r'}\}$ and hence G_0' has a simple, minimal non-half-factorial subset by 2..

Since G_0 is not a component of G_0' we have $G_0 \neq G_0'$ and hence $G_0' \setminus G_0 \neq \emptyset$. Let $h' \in G_0' \setminus G_0$. Clearly, there exist $b_i'(h') \in [0, p-1]$ for every $i \in [1, r']$ such that $h' = -\sum_{i=1}^{r'} b_i'(h') e_i$. Assume that for every $h' \in G_0' \setminus G_0$ we have $b_1'(h') = \cdots = b_r(h') = 0$. This implies that $\langle e_1, \ldots, e_r \rangle \cap \langle G_0' \setminus G_0 \rangle = \{0\}$. Since $\langle G_0 \rangle = \langle e_1, \ldots, e_r \rangle$, we get that G_0 is a component of G_0', a contradiction. Hence there exists some $h \in G_0' \setminus G_0$ and some $j \in [1, r]$ such that $b_j'(h) \neq 0$, which proves the assertion.

4. Since G_0 is simple we get by Lemma 2.7.1 that G_0 is indecomposable. Thus it suffices to show that G_0 is a component of G_0'. Assume to the contrary that G_0 is not a component. Then by 3. there exists some non-half-factorial subset of G_0', a contradiction to G_0' half-factorial. □

Proposition 4.11. *Let $p \geq 13$, $r = \frac{p-1}{2}$ and $G_0 \subset G_0' \subset G$. Further let $r' = \mathsf{r}(\langle G_0' \rangle)$ and $\{e_{r+1}, \ldots, e_{r'}\} \subset G_0'$ a set such that $\langle G_0' \rangle = \langle e_1, \ldots, e_{r'} \rangle$.*

1. *Let $H = \{-\sum_{i=1}^r 2e_i\} \cup \{(r+1)e_\nu - \sum_{i=1}^r e_i \mid \nu \in [1,r]\}$. Then $g \in H$ and $\{h, e_1, \ldots, e_r\}$ is simple and half-factorial for every $h \in H$.*
2. *If $h = -\sum_{i=1}^{r'} b_i' e_i \notin G_0$ with $b_i' \in [0, p-1]$ and $b_j' \neq 0$ for some $j \in [1,r]$, then $\{g, h, e_1, \ldots, e_{r'}\}$ has a simple, minimal non-half-factorial subset.*
3. *If G_0 is not a component of G_0', then G_0' has a simple, minimal non-half-factorial subset.*
4. *If G_0' is half-factorial, then G_0 is an indecomposable component of G_0'.*

Proof. 1. Lemma 4.9 implies that $\{h, e_1, \ldots, e_r\}$ is simple and half-factorial for every $h \in H$.

Recall that $g = -\sum_{i=1}^r b_i$ with $b_i \in [1, p-1]$ and after a suitable renumeration we may suppose that $b_1 \geq \cdots \geq b_r$. Since $\sum_{i=1}^r b_i = p-1$ and $r = \frac{p-1}{2}$ we obtain that $b_1 \in [2, \frac{p+1}{2}]$. If $b_1 = 2$, then $b_2 = \cdots = b_r = 2$ and $g \in H$. If $b_1 = \frac{p+1}{2}$, then $b_2 = \cdots = b_r = 1$ and $g \in H$.

Assume to the contrary that $b_1 \in [3, \frac{p-1}{2}]$. Setting $k = \lfloor \frac{p}{b_1} \rfloor$ we apply Lemma 4.6 and obtain that $b_k \in [3, \frac{p-1}{2}]$ and

$$\frac{p+3}{2} \leq \lfloor \frac{p}{b_k} \rfloor + b_k < \frac{p}{b_k} + b_k.$$

Let $f : \mathbb{R}_{>0} \to \mathbb{R}$ be defined via $f(x) = \frac{p}{x} + x$ for every $x \in \mathbb{R}_{>0}$. Then Lemma 4.3 implies that

$$\max\{f(x) \mid x \in [3, \frac{p-3}{2}]\} = \max\{f(3), f(\frac{p-3}{2})\}.$$

However, $f(3) < \frac{p+3}{2}$ and $f(\frac{p-3}{2}) < \frac{p+3}{2}$. Thus $b_k = \frac{p-1}{2}$, $k = 2$ and $\sum_{i=1}^r b_i > b_1 + b_2 = p-1$, a contradiction. Hence, we have $g \in H$.

2. If $g = -\sum_{i=1}^r 2e_i$, then $e_1 = \frac{p-1}{2}g - \sum_{i=2}^r e_i$, $\{g, e_2, \ldots, e_r\}$ is independent and $\{g, e_1, \ldots, e_r\} = \{\frac{p-1}{2}g - \sum_{i=2}^r e_i, g, e_2 \ldots, e_r\}$. Moreover, $h = -c_1 g - \sum_{i=2}^{r'} c_i e_i$ with suitable $c_i \in [0, p-1]$ and by Proposition 4.2 we obtain $c_1 = [-2^{-1} b_1']_p$ and $c_j = [c_1 2 + b_j']_p$ for each $j \in [2,r]$ hence there exists a $j' \in [1,r]$ such that $c_{j'} \neq 0$. Thus it suffices to consider the case where $g = \frac{p-1}{2}e_1 - \sum_{i=2}^r e_i$.

If $\{h, e_1, \ldots, e_{r'}\}$ is not half-factorial, then there exists a minimal non-half-factorial subset which is simple by Lemma 2.7.1.

Thus we suppose that $\{h, e_1, \ldots, e_{r'}\}$ is half-factorial and decide three cases:

Case 1: $b_i' \neq 0$ for each $i \in [2, r]$. Proposition 4.7, Proposition 4.10.1 and the first part of this Lemma imply that

$$\begin{aligned} h \in &\{-\sum_{i\in I} 2e_i \mid [2,r] \subset I \subset [1,r'] \text{ and } |I| = r\} \cup \\ &\{(r+1)e_\nu - \sum_{i\in I} \mid [2,r] \subset I \subset [1,r'], |I| = r \text{ and } \nu \in I \setminus \{1\}\} \cup \\ &\{-\sum_{i\in I} e_i \mid [2,r] \subset I \subset [1,r'] \text{ and } |I| = p-1\}. \end{aligned}$$

If $h \in \{-\sum_{i\in I} e_i \mid [2,r] \subset I \subset [1,r'] \text{ and } |I| = p-1\}$, then we apply Proposition 4.10.2 with the simple, half-factorial set $\{h, e_i \mid i \in I\}$ and obtain that there exists a simple, minimal non-half-factorial subset of $\{g, h, e_i \mid i \in I\}$.

If $h \in \{(r+1)e_\nu - \sum_{i\in I} e_i \mid [2,r] \subset I \subset [1,r'], |I| = r \text{ and } \nu \in I \setminus \{1\}\}$, then $b_i = b_i' \neq 0$ for some $i \in [2, r]$ and clearly $g \neq h$. Thus by Proposition 4.2.3 there exists a simple, minimal non-half-factorial subset of $\{g, h, e_1, \ldots, e_r\}$.

If $h = -\sum_{i\in I} 2e_i$ with $I = [1, r]$, then by Proposition 4.2 $h = -c_1 g - \sum_{i=2}^{r} c_i e_i$ with $c_1 = [-(\frac{p+1}{2})^{-1}2]_p = p-4$ and $c_i = [(p-4)1+2]_p = p-2$ for each $i \in [2, r]$. Thus $\sum_{i=1}^{r} c_i \neq p-1$ and by Proposition 4.2.3 be obtain again a simple, minimal non-half-factorial subset.

If $h = -\sum_{i\in I} 2e_i$ with $I = [2, r] \cup \{j\}$ and $j \in [r+1, r']$, then $\{h, g, e_1\}$ is independent and $e_j = rh + g + (r+1)e_1 = -(r+1)h - (p-1)g - re_1$. Thus we apply Lemma 4.1 and obtain that the simple set $\{e_j\} \cup \{h, g, e_1\}$ is not half-factorial and hence by Lemma 2.7.3 minimal non-half-factorial.

Case 2: $b_i' = 0$ for each $i \in [2, r]$. Since $b_j' \neq 0$ for some $j \in [1, r]$ we have $b_1' \neq 0$, and since $\{h, e_1, \ldots, e_{r'}\}$ is half-factorial and $h \neq e_1$ we have $b_k' \neq 0$ for some $k \in [r+1, r']$.

We apply Proposition 4.2 with the independent set $\{e_1, \ldots, e_{r'}\}$ and obtain $h = -c_1 g - \sum_{i=2}^{r'} c_i e_i$ with $c_1 = [-(r+1)^{-1} b_1']_p \neq 0$, $c_i = [c_1 b_i + b_i']_p = c_1$ for each $i \in [2, r]$ and $c_i = b_i'$ for each $i \in [r+1, r']$. We consider the independent set $G_1 = \{g, e_2, \ldots, e_r\} \cup \{e_i \mid i \in [r+1, r'] \text{ and } c_i \neq 0\}$, then $\{h\} \cup G_1$ is simple. Since $|G_1| > r = \frac{p-1}{2}$ be obtain, applying Proposition 4.7 and 4.10.1, that either $\{h\} \cup G_1$ is not half-factorial or

$$|G_1| = p-1 \text{ and } h = -\sum_{g' \in G_1} g'.$$

If $\{h\} \cup G_1$ is not half-factorial, we are done since $\{h\} \cup G_1$ is simple and hence minimal non-half-factorial.

Thus we may suppose that $|G_1| = p-1$ and $h = -\sum_{g' \in G_1} g'$. Since $e_1 \in \langle G_1 \rangle$ we infer by Proposition 4.10.2 that $\{e_1\} \cup \{h\} \cup G_1$ has a simple, minimal non-half-factorial subset. Clearly, this set is a subset of $\{g, h, e_1, \ldots, e_{r'}\}$.

Case 3: There exist $\mu, \nu \in [2, r]$, such that $b_\mu' \neq 0$ and $b_\nu' = 0$. After a suitable renumeration we may suppose that $\mu = 2$, $b_2' = \max\{b_i' \mid i \in [2, r]\}$ and $\nu = 3$.

Recall that $b_2 = 1 \neq 0$. Hence we may apply Proposition 4.2, replacing e_2 instead of e_1, and obtain

$$h = -c_1'g - c_2'e_1 - \sum_{i=3}^{r'} c_i'e_i,$$

with $c_1' = [-b_2^{-1}b_2']_p = p - b_2'$, $c_2' = [c_1'b_1 + b_1']_p$, $c_i' = [c_1'b_i + b_i']_p = [p - b_2' + b_i']_p$ for each $i \in [3, r]$ and $c_i' = b_i'$ for each $i \in [r+1, r']$.

If $b_2' \leq \frac{p}{2}$, then

$$\sum_{i=1}^{r'} c_i' \geq c_1' + c_3' = (p - b_2') + [p - b_2' + b_3']_p = 2(p - b_2') > p - 1.$$

Thus by Proposition 4.2.3 there exists a simple, minimal non-half-factorial subset of $\{g, h, e_1, \ldots, e_{r'}\}$.

If $p - 3 \geq b_2' > \frac{p}{2}$, then $b_2' > \max\{b_i' \mid i \in [3, r]\}$. Thus $(p - b_2' + b_i') < p$ and $c_i' = [p - b_2' + b_i']_p = p - b_2' + b_i'$ for each $i \in [3, r]$. Consequently,

$$\sum_{i=1}^{r'} c_i' \geq c_1' + \sum_{i=3}^{r} c_i' = (p - b_2') + \sum_{i=3}^{r}(p - b_2' + b_i') \geq 3 + 3(r-2) = 3\frac{p-3}{2} > p - 1$$

and by Proposition 4.2.3 there exist a simple, minimal non-half-factorial subset.

If $b_2' = p - 2$, then $h = 2e_2 - e_l$ with $l \in [1, r'] \setminus \{2\}$. If $l > r$, then

$$h = -e_1 - e_l - 2g - \sum_{i=3}^{r} 2e_i.$$

Thus the set $\{h\} \cup \{e_1, g, e_3, \ldots, e_r, e_l\}$ is simple and since $|\{e_1, g, e_3, \ldots, e_r, e_l\}| = r + 1 = \frac{p+1}{2}$ we obtain by Proposition 4.7.2 that it is not half-factorial. If $l \in [3, r]$, then we apply Proposition 4.2 and obtain a simple, minimal non-half-factorial subset. Suppose that $l = 1$. We note that

$$2r^2 - r = (p-1)\frac{p-1}{2} - \frac{p-1}{2} = (p-2)\frac{p-1}{2} \equiv 1 \bmod p.$$

Thus $e_2 = [r^2]_p h + rg + \sum_{i=3}^{r} re_i = -(p - [r^2]_p) - (r+1)g - (r+1)\sum_{i=3}^{r} e_i$. Since $\{h, g, e_3, \ldots, e_r\}$ is independent and $(r+1)(r-1) > p - 1$ we obtain applying Lemma 4.1 that the simple set $\{e_2\} \cup \{h, g, e_3, \ldots, e_r\}$ is not half-factorial.

Since $h \neq e_2$ we obtain $b_2' \neq p - 1$.

3. and 4. are proved analogously to 3. and 4. in Proposition 4.10. □

5. Large Half-Factorial Sets - Proof of Theorem 3.1

In this section we give the proof for the result on $\mu(G)$ for elementary p-groups mentioned in the introduction (cf. Proposition 5.3). Having this at hand we will be able to prove Theorem 3.1.

The results formulated in this section are mainly reformulations of the proof of Theorem 8 in [9]. Therefore we only give brief or no proofs and refer to [9]

for detailed arguments. An exception is Proposition 5.3.1, since the arguments of this proof are inevitable for the proof of Theorem 3.1. We start with a result on groups with rank less or equal than 2.

Proposition 5.1. *Let $G_0 \subset G$.*

(1) *If $\mathsf{r}(\langle G_0 \rangle) \le 1$, then G_0 is half-factorial if and only if*

$$G_0 \subset \{0, g\} \text{ with some } g \in G.$$

(2) *If $\mathsf{r}(\langle G_0 \rangle) = 2$ and $\{e_1, e_2\} \subset G_0$ independent, then G_0 is half-factorial if and only if*

$$G_0 \subset \{je_1 + (p+1-j)e_2 \mid j \in [1,p]\} \cup \{0\}.$$

Proof. 1. follows immediately by Proposition 3.4.

2. Suppose that $\mathsf{r}(\langle G_0 \rangle) = 2$ and $e_1, e_2 \in G_0$ are independent. By Lemma 4.1 G_0 is a subset of the set on the righthand side. That

$$H = \{je_1 + (p+1-j)e_2 \mid j \in [1,p]\}$$

is half-factorial, is proved in [9, Proof of Theorem 8]. □

Corollary 5.2. (1) *If $\mathsf{r}(G) = 1$, then $\mu(G) = 2$.*

(2) *If $\mathsf{r}(G) = 2$, then $\mu(G) = p + 1$.*

Proposition 5.3. *Let $\mathsf{r}(G) = r$ and let $G_0 \subset G \setminus \{0\}$ be a half-factorial set.*

(1) $|G_0| \le \frac{r}{2}p$.

(2) *If $|G_0| = \frac{r}{2}p$, then there exists an independent subset with r elements. Moreover, if $\{e_1, \ldots, e_r\} \subset G_0$ is independent and $g \in G_0 \setminus \{e_1, \ldots, e_r\}$, then $g = -b_ie_i - b_je_j$ with distinct $i, j \in [1, r]$ and $b_i, b_j \in [1, p-2]$ such that $b_i + b_j = p - 1$.*

(3) *There exists a half-factorial set $G_0' \subset G \setminus \{0\}$ with $|G_0'| = \lfloor \frac{r}{2} \rfloor p + 2(\frac{r}{2} - \lfloor \frac{r}{2} \rfloor)$.*

(4) $1 + \lfloor \frac{r}{2} \rfloor p + 2(\frac{r}{2} - \lfloor \frac{r}{2} \rfloor) \le \mu(G) \le 1 + \frac{r}{2}p$.

(5) *If r is even then $\mu(G) = 1 + \frac{r}{2}p$.*

Proof. 1. Without restriction let $\mathsf{r}(\langle G_0 \rangle) = r$. Let $\{e_1, \ldots, e_r\} \subset G_0$ be an independent set and let $G_1 = G_0 \setminus \{e_1, \ldots, e_r\}$. Lemma 4.1 gives that

$$G_1 = \{-\sum_{i=1}^{r} b_ie_i \in G_1 \mid b_i \in [0, p-2], \text{ at least two of the } b_i\text{'s distinct to } 0\},$$

hence

$$\begin{aligned} |G_1| &\le \frac{1}{2}\sum_{j=1}^{r} |\{-\sum_{i=1}^{r} b_ie_i \in G_1 \mid b_i \in [0, p-2], b_j \ne 0\}| \\ &\le \frac{1}{2}\sum_{j=1}^{r} |\{b_j \in [0, p-2] \mid b_j \ne 0\}| \\ &= \frac{1}{2}r(p-2), \end{aligned}$$

where the second inequality follows again by Proposition 4.2.2. Since $|G_0| = |G_1| + r$, the statement follows.

2. We note that if $|G_0| = \frac{r}{2}p$, then r is even (note that by our general assumption p is odd) and by Lemma 2.3.4 there exists some independent subset of G_0 with r elements.

We use the same notation as in 1.. From 1. we get

$$|G_1| = \frac{1}{2}\sum_{j=1}^{r} |\{-\sum_{i=1}^{r} b_i e_i \in G_1 \mid b_i \in [0, p-2], b_j \neq 0\}|,$$

hence for each $g = -\sum_{i=1}^{r} b_i e_i \in G_1$ exactly two of the b_i's are not equal to 0. Thus $g = -b_i e_i - b_j e_j$ for distinct $i, j \in [1, r]$ and the other conditions follow immediately by Lemma 4.1.

3., 4. and 5. The existence of the half-factorial set G_0' and the lower bound in 4. is obtained by decomposing the group G into subgroups of rank 1 and 2, and applying Lemma 2.3.3 and Corollary 5.2. The upper bound in 4. follows by 1. and if r is even, they are equal which proves 5.. □

Proof of Theorem 3.1. For elementary 2-groups the assertion follows from Proposition 3.3.

Let G be an elementary p-group with $p \in \mathbb{P}$ odd, $r = \mathsf{r}(G)$ even and $G_0 \subset G \setminus \{0\}$ a half-factorial subset with $|G_0| = \mu(G) - 1 = \frac{r}{2}p$. By Proposition 5.3.2 there exists an independent subset $\{e_1, \ldots, e_r\} \subset G_0$, and we have to show that after suitable renumeration

$$G_0 = \dot{\bigcup}_{i=1}^{\frac{r}{2}} \{je_{2i-1} + (p+1-j)e_{2i} \mid j \in [1, p]\} \cup \{0\}.$$

Let $G_1 = G_0 \setminus \{e_1, \ldots, e_r\}$ and $g \in G_1$. By Proposition 5.3.2 we may suppose after renumeration that $g = -b_1 e_1 - b_2 e_2$ with $b_1, b_2 \in [1, p-2]$.

It suffices to prove, that if $h \in G_1$, with $h = -b_1' e_1 - b_j' e_j$ and $b_1', b_j' \in [1, p-1]$, then $j = 2$. Assume to the contrary $j \in [3, r]$. Without restriction we assume $j = 3$. By Proposition 4.2

$$h = -c_1 g - c_2 e_2 - c_3 e_3,$$

with $c_1 = [-b_1' b_1^{-1}]_p$, $c_2 = [c_1 b_2]_p$ and $c_3 = [b_3']_p$. The set $\{g, e_2, \ldots, e_r\} \subset G_0$ is independent and $c_i \in [1, p-1]$ for each $i \in [1, r]$. This contradicts Proposition 5.3.2. □

6. Proof of Theorem 3.2

In this section we give a proof of Theorem 3.2. This theorem determines $\mu(G)$ and the structure of minimal non-half-factorial sets for elementary p-groups with $\mathsf{r}(G) \leq 2$ or $\exp(G) \leq 7$. We will prove several preparatory results.

First we give a result that will settle the case of rank less or equal than 2. In Proposition 3.3 we investigated already elementary 2-groups. Therefore it remains to consider elementary p-groups with $p \in \{3, 5, 7\}$. This will be done in

Proposition 6.2, 6.3 and 6.5, where we describe the structure of half-factorial sets in $3, 5$ and 7-groups in detail.

Proposition 6.1. *Let $G_0 \subset G$ be a minimal non-half-factorial set. If $\mathsf{r}(\langle G_0 \rangle) \le 2$, then G_0 is simple.*

Proof. Suppose that $\mathsf{r}(\langle G_0 \rangle) = 1$. Then Proposition 5.1.1 implies that there exist two distinct non-zero elements, say $g, e \in G_0 \setminus \{0\}$. Again by Proposition 5.1.1, $\{g, e\}$ is not half-factorial, hence $G_0 = \{g, e\}$. Since $\mathsf{r}(\langle G_0 \rangle) = 1$, it follows that $g \in \langle e \rangle$ and G_0 is simple.
Suppose that $\mathsf{r}(\langle G_0 \rangle) = 2$. Then Proposition 5.1.2 implies that G_0 contains two independent elements e_1, e_2 and some element $g = a_1e_1 + a_2e_2$ with $a_1, a_2 \in [1, p]$ and $a_1 \neq p + 1 - a_2$. Again by Proposition 5.1.2, $\{g, e_1, e_2\}$ is not half-factorial hence $G_0 = \{g, e_1, e_2\}$ and G_0 is simple. □

Using the notion of components, we can formulate the result on half-factorial sets of elementary 2-groups (Proposition 3.3) in the following way: A subset G_0 of an elementary 2-group is half-factorial if and only if for each indecomposable component $G_1 \subset G_0$ we have $|G_1| = 1$. In the sequel we will determine the indecomposable components of half-factorial sets in elementary $3, 5$ and 7-groups.

Proposition 6.2. *Let G be an elementary 3-group and $G_0 \subset G$ a non-empty subset.*

1. *G_0 is simple and half-factorial if and only if $G_0 = \{-e_1 - e_2, e_1, e_2\}$ with independent elements $\{e_1, e_2\}$.*
2. *There are equivalent:*
   (a) *G_0 is half-factorial.*
   (b) *For each indecomposable component G_1 of G_0 either $|G_1| = 1$ or $G_1 = \{-e_1 - e_2, e_1, e_2\}$, with independent elements $\{e_1, e_2\} \subset G_1$.*
3. *If G_0 is minimal non-half-factorial, then G_0 is simple.*

Proof. 1. Clearly, the considered sets are simple and $\{-e_1 - e_2, e_1, e_2\}$ is half-factorial by Lemma 4.9.

Conversely, let G_0 be simple and half-factorial. Proposition 4.7 implies that $|G_0| = 3$ and by Lemma 4.1 the assertion follows.

2. A set with these indecomposable components is half-factorial, since 1. gives that each indecomposable component is half-factorial (cf. Remark 2.5).
Conversely, let $G_0 \subset G$ half-factorial and let G_1 be an indecomposable component. Either $|G_1| = 1$ or there exists a simple subset $G_2 \subset G_1$ with $|G_2| \ge 2$. By 1. we get that $G_2 = \{-e_1 - e_2, e_1, e_2\}$ with independent elements $\{e_1, e_2\}$, and by Proposition 4.10.4 we get that G_2 is an indecomposable component of G_1, hence $G_2 = G_1$.

3. By Lemma 2.7.3 it suffices to prove that every indecomposable non-half-factorial set has some subset that is simple and non-half-factorial.

Let $G_0 \subset G$ be indecomposable non-half-factorial and let $\{e_1, \ldots, e_r\} \subset G_0$ be a maximal independent set. Let $g \in G_0 \setminus \{e_1, \ldots, e_r\}$. Clearly $g = -\sum_{i=1}^{r} b_i e_i$

with $b_i \in [0,2]$. By 1. we get that either $\{g, e_1, \ldots, e_r\}$ is not half-factorial or $g = -e_i - e_j$ with $i, j \in [1, r]$. In the first case the statement is obvious, hence we may suppose after a suitable renumeration that $g = -e_1 - e_2$. Since G_0 is indecomposable (cf. Remark 2.5) and $\{g, e_1, e_2\} \neq G_0$ we obtain that $\{g, e_1, e_2\}$ is not an indecomposable component of G_0 and the assertion follows applying Proposition 4.10.3. □

Proposition 6.3. *Let G be an elementary 5-group and $G_0 \subset G$ a non-empty subset.*

(1) *G_0 is simple and half-factorial if and only if either*
   - *$G_0 = \{je_1 + (6-j)e_2, e_1, e_2\}$ with independent elements $\{e_1, e_2\}$ and $j \in [2,4]$ or*
   - *$G_0 = \{-e_1 - e_2 - e_3 - e_4, e_1, e_2, e_3, e_4\}$ with independent elements $\{e_1, \ldots, e_4\}$.*

(2) *There are equivalent:*
   (a) *G_0 is half-factorial.*
   (b) *For each indecomposable component G_1 of G_0 either $|G_1| = 1$ or $G_1 \subset \{je_1 + (6-j)e_2 \mid j \in [1,5]\}$ with independent elements $\{e_1, e_2\} \subset G_1$ or $G_1 = \{-e_1 - e_2 - e_3 - e_4, e_1, e_2, e_3, e_4\}$ with independent elements $\{e_1, e_2, e_3, e_4\} \subset G_1$.*

(3) *If G_0 is minimal non-half-factorial, then G_0 is simple.*

Proof. 1. Clearly, the considered sets are simple. By Lemma 4.9 and Proposition 5.1.2 all these sets are half-factorial.
Conversely, let $G_0 \subset G$ be simple and half-factorial. Let $g \in G_0$, such that $G_0 \setminus \{g\} = \{e_1, \ldots, e_r\}$ is independent. By Proposition 4.7 we obtain $r \in \{2, 4\}$ and by Lemma 4.1 the set G_0 has the form as claimed.

2. A set with these indecomposable components is half-factorial, since Proposition 5.1 and Lemma 4.9 give that each indecomposable component is half-factorial (cf. Remark 2.5). Conversely, let $G_0 \subset G$ half-factorial and let G_1 be an indecomposable component. Either $|G_1| = 1$ or there exists a simple subset $G_2 \subset G_1$ with $|G_2| \geq 2$. We choose G_2 such that the cardinality of G_2 is maximal.

By 1. we get that $|G_2| \in \{3, 5\}$. If $|G_2| = 5$, then $G_2 = \{-e_1 - e_2 - e_3 - e_4, e_1, e_2, e_3, e_4\}$ with independent elements $\{e_1, e_2, e_3, e_4\}$. By Proposition 4.10.4 we get $G_2 = G_1$.

Suppose $|G_2| = 3$. Then $G_2 = \{je_1 + (6-j)e_2, e_1, e_2\}$ with independent elements $\{e_1, e_2\}$ and $j \in [2,4]$. We set $h = je_1 + (6-j)e_2$. By Proposition 5.1.2, it remains to prove that $G_1 \subset \langle\{e_1, e_2\}\rangle$. Assume to the contrary there exists some $r \geq 3$ and elements $\{e_3, \ldots, e_r\} \subset G_1$, such that $\{e_1, \ldots, e_r\}$ is independent. For each element $g \in G_1 \setminus \{e_1, \ldots, e_r\}$, we get $g = ke_m + (6-k)e_n$ with $m, n \in [1, r]$ and $k \in [2,4]$. Since G_1 is indecomposable, there exist some $h' \in G_1 \setminus \{e_1, \ldots, e_r\}$ such that $h' = j'e_m + (6-j')e_n$ with $m \in [1,2]$, $n \in [3, r]$ and $j' \in [2,4]$. Without restriction we assume $m = 1$ and $n = 3$. Clearly $\{h', e_2, e_3\} \subset G_1$ is independent and by Proposition 4.2.

$$h' = -c_1 h - c_2 e_2 - c_3 e_3,$$

with $c_1 = [-jj'^{-1}]_p \in [1,4]$, $c_2 = j - 1 \in [1,4]$ and $c_3 = [c_1(j'-1)]_p \in [1,4]$. The set $\{h', h, e_2, e_3\}$ is simple, 1. gives that it is not half-factorial, a contradiction. Consequently, $G_1 \subset \langle\{e_1, e_2\}\rangle$ and $G_1 \subset \{je_1 + (6-j)e_2 \mid j \in [1,5]\}$.

3. It suffices to prove that every indecomposable non-half-factorial set has some subset, which is simple and non-half-factorial. Let $G_0 \subset G$ be indecomposable non-half-factorial and let

$$\{e_1, \dots, e_r\} \subset G_0$$

be a maximal independent set in G_0. Let $g \in G_0 \setminus \{e_1, \dots, e_r\}$. Clearly $g = -\sum_{i=1}^r b_i e_i$ with $b_i \in [0,4]$. We get that either $\{g, e_1, \dots, e_r\}$ is not half-factorial or g is of the form given in 1.. In the first case the statement is obvious. For $g = -e_1 - e_2 - e_3 - e_4$ the statement follows by Proposition 4.10.3. For $g = je_1 + (p+1-j)e_2$ the statement follows by Proposition 4.2.3 and the proof of 2.. □

Lemma 6.4. *Let G be an elementary 7-group, $\{e_1, \dots, e_r\} \subset G$ an independent set and $g = -\sum_{i=1}^r b_i e_i$ with $b_i \in [1,6]$. Then $G_0 = \{g, e_1, \dots, e_r\}$ is half-factorial if and only if*

- *$r = 2$ and $b_1 + b_2 = 6$ or*
- *$r = 3$ and $b_1 = b_2 = b_3 = 2$ or*
- *$r = 3$ and $b_i = 4$, $b_j = b_k = 1$ with $\{i,j,k\} = \{1,2,3\}$ or*
- *$r = 6$ and $b_1 = \dots = b_6 = 1$.*

Proof. Suppose G_0 is half-factorial. By Proposition 4.7.1 we have $r \in [2,6]$.

If $r = 2$ or $r = 6$, then it is obvious by Lemma 4.1, that $b_1, \dots, b_r$ have the values as claimed.

Suppose $r = 3$ and we may assume after a suitable renumeration that $b_1 \geq b_2 \geq b_3$. We need to verify that for $b_1 = 3$, $b_2 = 2$ and $b_3 = 1$ the set G_0 would not be half-factorial. Assume to the contrary $b_1 = 3$, $b_2 = 2$ and $b_3 = 1$. Then we obtain $\sum_{i=1}^3 [b_1^{-1} b_i]_p = 1+3+5 \neq 7-5$, which gives by Lemma 4.4 a contradiction to G_0 half-factorial.

By Proposition 4.7.2 we obtain that, since G_0 is half-factorial, $r \notin [4,5]$.

Conversely, if r and $b_1, \dots, b_r$ are as given by the Lemma, then we obtain by Lemma 4.9 and Proposition 5.1.2 that G_0 is half-factorial. □

Proposition 6.5. *Let G be an elementary 7-group and $G_0 \subset G$ a non-empty subset.*

1. *G_0 is simple and half-factorial if and only if either*
   - *$G_0 = \{je_1 + (8-j)e_2, e_1, e_2\}$ with $\{e_1, e_2\}$ independent and $j \in [2,6]$ or*
   - *$G_0 = \{-2(e_1+e_2+e_3), e_1, e_2, e_3\}$ with $\{e_1, e_2, e_3\}$ independent or*
   - *$G_0 = \{-\sum_{i=1}^6 e_i, e_1, \dots, e_6\}$ with $\{e_1, \dots, e_6\}$ independent.*
2. *There are equivalent:*
   (a) *G_0 is half-factorial.*
   (b) *For each indecomposable component G_1 of G_0 either*
      - *$|G_1| = 1$ or*

- $G_1 \subset \{je_1+(8-j)e_2 \mid j \in [1,7]\}$ *with* $\{e_1, e_2\} \subset G_1$ *independent or*
- $G_1 \subset \{-2(e_1+e_2+e_3), -4(e_1+e_2), e_1, e_2, e_3\}$ *with* $\{e_1, e_2, e_3\} \subset G_1$ *independent or*
- $G_1 = \{-\sum_{i=1}^{6} e_i, e_1, \ldots, e_6\}$ *with* $\{e_1, \ldots, e_6\} \subset G_1$ *independent.*

(3) *If G_0 is minimal non-half-factorial, then G_0 is simple.*

Proof. 1. Clearly, the considered sets are simple. From Lemma 6.4 we get that all the sets are half-factorial.
Conversely, let $G_0 \subset G$ be simple and half-factorial. Let $g \in G_0$ such that $G_0 \setminus \{g\} = \{e_1, \ldots, e_r\}$ is independent. We get $g = -\sum_{i=1}^{r} b_i e_i$ with $b_i \in [1,6]$ for each $i \in [1,r]$. From Lemma 6.4 we get that

- $r = 2$ and $b_1 + b_2 = 6$ or
- $r = 3$ and $b_1 = b_2 = b_3 = 2$ or
- $r = 3$ and $b_i = 4$, $b_j = b_k = 1$ with $\{i,j,k\} = \{1,2,3\}$ or
- $r = 6$ and $b_1 = \cdots = b_6 = 1$.

If $b_1 + b_2 = 6$, then there exists some $j \in [2,6]$, such that

$$-b_1e_1 - b_2e_2 = je_1 + (8-j)e_2.$$

If $g = -4e_i - e_j - e_k$, we note that $e_i = -2(g + e_j + e_k)$ and since $\{g, e_2, e_3\} \subset G_0$ is independent, we get that G_0 can be written in the given way.

2. Let $G_0 \subset G$ be half-factorial and let G_1 be an indecomposable component. Either $|G_1| = 1$ or there exists some simple set $G_2 \subset G_1$ with $|G_2| \geq 2$. We choose G_2 such that the cardinality of G_2 is maximal. By Lemma 6.4 $|G_2| \in \{3,4,7\}$. If $|G_2| = 7$, then $G_2 = G_1$ by Proposition 4.10.4.

Suppose $|G_2| = 4$. Then we get by 1. that $G_2 = \{g, e_1, e_2, e_3\}$ with $g = -2(e_1 + e_2 + e_3)$ and $\{e_1, e_2, e_3\}$ independent.
We show that $\mathsf{r}(\langle G_1 \rangle) = 3$. Assume to the contrary $\mathsf{r}(\langle G_1 \rangle) = r > 3$. Then there exist elements $\{e_4, \ldots, e_r\} \subset G_1$ such that $\{e_1, \ldots, e_r\}$ is independent and since G_1 is indecomposable, there exists some element $h = -\sum_{i=1}^{r} b_i' e_i \in G_1$ with $b_i' \in [0, p-1]$ for each $i \in [1,r]$ and $b_j' \neq 0$ for some $j \in [1,3]$ and $b_k' \neq 0$ for some $k \in [4,r]$. Let $I = \{i \in [1,r] \mid b_i' \neq 0\}$. Since $\{h\} \cup \{e_i \mid i \in I\}$ is a simple set, we get $|I| \leq 3$. We decide two cases.
Case 1: $|I \cap [1,3]| = 1$. We may suppose $1 \in I$. Applying Proposition 4.2 we get

$$h = -c_1 g - c_2 e_2 - c_3 e_3 - \sum_{i \in I \setminus \{1\}} c_i e_i$$

with $c_i \in [1,6]$ for each i. Consequently, the set $\{h, g, e_2, e_3\} \cup \{e_i \mid i \in I \setminus \{1\}\}$ is a simple set with cardinality $3 + |I| \in \{5,6\}$, a contradiction.
Case 2: $|I \cap [1,3]| = 2$. Without restriction let $I = \{1,2,4\}$. From Lemma 6.4 we get that either $h = -2(e_1+e_2+e_4)$ or $h = -4e_i - e_j - e_k$ with $\{i,j,k\} = \{1,2,4\}$. By Proposition 4.2 we get, that $h = -2(e_1 + e_2 + e_4)$ gives a contradiction. We consider $h = -4e_i - e_j - e_k$. It suffices to consider $i = 1$ and $i = 4$. If $i = 4$,

we get $h = -3g - 6e_3 - 4e_4$, a contradiction by Lemma 6.4. If $i = 1$, we get $h = -3g - 3e_1 - 6e_3 - e_4$, a contradiction.

Consequently, we get $\mathsf r(\langle G_1\rangle) = 3$. Let $h \in G_1 \setminus \{g, e_1, e_2, e_3\}$ with $h = -\sum_{i=1}^3 b_i'e_i'$ and $b_i' \in [0, 6]$. Without restriction we assume $b_1' \ge b_2' \ge b_3'$. If $b_3' \ne 0$, we get by Lemma 6.4 that $b_1' = 4$ and $b_2' = b_3' = 1$. This gives $e_2 = -3g - 2h - e_3$, a contradiction by Lemma 6.4. If $b_3' = 0$, we get by Lemma 4.1 and Proposition 4.2, that either $b_1' = 5$ and $b_2' = 1$ or $b_1' = b_2' = 3$. For $b_1' = 5$ and $b_2' = 1$, we get $h = -g - 3e_2 - 2e_3$, a contradiction by Lemma 6.4. For $b_1' = b_2' = 3$, we get that

$$\{gh^2e_1e_2e_3^2, gh^4e_3^2, g^2he_3^4, g^4h^2e_3\}$$

is the set of all atoms in $\mathcal A(\{g, h, e_1, e_2, e_3\})$ for which the multiplicity of g and of h is positive. All these atoms have cross number 1. Clearly, for each $A \in \mathcal A(\{g, h, e_1, e_2, e_3\})$ with $\mathsf v_g(A) = 0$ or $\mathsf v_h(A) = 0$, we get $\mathsf k(A) = 1$. Thus $\{g, h, e_1, e_2, e_3\}$ is half-factorial by Lemma 2.2. Since neither for $h' = -3(e_1 + e_3)$ nor for $h' = -3(e_2 + e_3)$ the set $\{g, h, h', e_1, e_2, e_3\}$ is half-factorial, we get that $G_1 \subset \{-2(e_1 + e_2 + e_3), -3(e_1 + e_2), e_1, e_2, e_3\}$ with independent elements $\{e_1, e_2, e_3\} \subset G_1$.

Suppose $|G_2| = 3$. From Lemma 6.4 we get that $G_2 = \{g, e_1, e_2\}$ with independent $\{e_1, e_2\}$ and $g = -b_1e_1 - b_2e_2$ and $b_i \in [1, 6]$ for each $i \in [1, 2]$. We prove $\mathsf r(\langle G_1\rangle) = 2$. Assume to the contrary $\mathsf r(\langle G_1\rangle) > 2$. Then there exist elements $e_3, h \in G_1$ such that $\{e_1, e_2, e_3\}$ is independent and $h = -b_j'e_j - b_3'e_3$ with $b_j', b_3' \in [1, 6]$ and $j \in [1, 2]$. We may suppose $j = 1$. By Proposition 4.2, we get

$$h = -c_1g - c_2e_2 - c_3e_3$$

with $c_i \in [1, 6]$ for each i. The set $\{h, g, e_2, e_3\}$ is simple with cardinality 4, a contradiction. Consequently, $\mathsf r(\langle G_1\rangle) = 2$ and $G_1 \subset \{je_1+(p+1-j)e_2 \mid j \in [1, 7]\}$ with independent elements $\{e_1, e_2\} \subset G_1$ by Proposition 5.1.2.

Conversely, every set with these indecomposable components is half-factorial, since Lemma 4.9, Proposition 5.1 and what we proved in the first part gives that each indecomposable component is half-factorial (cf. Remark 2.5).

3. By Lemma 2.7.3 it suffices to prove that every indecomposable non-half-factorial set has a subset that is simple and non-half-factorial. Let $G_0 \subset G$ be indecomposable non-half-factorial and let $\{e_1, \ldots, e_r\} \subset G_0$ be a maximal independent set in G_0. Let $g \in G_0 \setminus \{e_1, \ldots, e_r\}$. Clearly $g = -\sum_{i=1}^r b_ie_i$ with $b_i \in [0, 6]$. We get that either $\{g, e_1, \ldots, e_r\}$ is not half-factorial or g is of the form given in Lemma 6.4. In the first case the statement is obvious. Otherwise the statement follows from Proposition 4.10.3 respectively from the proof of 2.. □

Proof of Theorem 3.2. Let G be an elementary p-group.

If $\mathsf r(G) \le 2$, then the statements are obvious by Lemma 5.1 and Proposition 6.1. If $\exp(G) = 2$, then the statements are obvious by Proposition 3.3.

For $p \in \{3, 5, 7\}$ the first part of the theorem is just Proposition 6.2.3 respectively 6.3.3 and 6.5.3. The statement on $\mu(G)$ follows immediately from the explicit description of the half-factorial sets given in Proposition 6.2.2 respectively 6.3.2 and 6.5.2. □

References

[1] D. D. Anderson. *Factorization in integral domains*. Marcel Dekker, 1997.

[2] S. Chapman and A. Geroldinger. Krull domains and monoids, their sets of lengths and associated combinatorial problems. In *Factorization in integral domains*, volume 189 of *Lecture Notes in Pure Appl. Math.*, pages 73 – 112. Marcel Dekker, 1997.

[3] S.T. Chapman and W.W. Smith. On factorization in block monoids formed by $\{\overline{1}, \overline{a}\}$ in $\mathbb{Z}_n$. *Proc. Edinb. Math. Soc.*, 46:257 –267, 2003.

[4] W. Gao and A. Geroldinger. Half-factorial domains and half-factorial subsets in abelian groups. *Houston J. Math.*, 24:593 – 611, 1998.

[5] W. Gao and A. Geroldinger. Systems of sets of lengths II. *Abhandl. Math. Sem. Univ. Hamburg*, 70:31 – 49, 2000.

[6] A. Geroldinger. On non-unique factorizations into irreducible elements II. volume 51 of *Colloquia Mathematica Societatis Janos Bolyai*, pages 723 – 757. North Holland, 1987.

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

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

[9] A. Geroldinger and J. Kaczorowski. Analytic and arithmetic theory of semigroups with divisor theory. *J. Theorie d. Nombres Bordeaux*, 4:199 – 238, 1992.

[10] W. Hassler. A note on half-factorial set of finite cyclic groups. *Far East Journal of Mathematical Sciences*, 10: 187–198, 2003.

[11] F. Halter-Koch. Finitely generated monoids, finitely primary monoids and factorization properties of integral domains. In *Factorization in integral domains*, volume 189 of *Lecture Notes in Pure Appl. Math.*, pages 73 – 112. Marcel Dekker, 1997.

[12] W. Narkiewicz. Finite abelian groups and factorization problems. *Colloq. Math.*, 17: 319 – 330, 1979.

[13] W. A. Schmid. Arithmetic of Block Monoids. *Mathematica Slovaca*, to appear.

[14] W. A. Schmid. On Differences in Sets of Lengths, submitted.

[15] L. Skula. On c-semigroups. *Acta Arithm.*, 31:247 – 257, 1976.

[16] J. Śliwa. Factorizations of distinct length in algebraic number fields. *Acta Arithm.*, 31; 399 –417, 1976.

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

[18] A. Zaks. Half-factorial domains. *Bull. AMS*, 82:721 – 723, 1976.

Institut für Mathematik, Karl-Franzens-Universität, Heinrichstrasse 36, 8010 Graz, Austria

E-mail address: waschmid@aon.at