Annales Mathematicae Silesianae 16 (2003)

Prace Naukowe Uniwersytetu Śląskiego nr 2142, Katowice

SPERNER TYPE THEOREMS FOR GENERALIZED DIVISORS

ŠTEFAN PORUBSKÝ

Abstract. The extensions of the well-known Sperner's result on antichains of subsets of a given finite set for divisors of a positive integers are shown to hold also for sets of regular systems of divisors of elements of arithmetical semigroups.

1. Introduction

The original result ($k=2$ in the following result of P. Erdős) of E. Sperner [12] on the maximal number of subsets of a given set no one of which is included in the other has been generalized in many directions. One of them proved by P. Erdős [3] says:

If in $\mathcal{F} = \{A_1, \ldots, A_n\} \subset 2^S$, the power set of a set S of cardinality $|S| = t < \infty$, there is no chain of length k, then

$$n \leqslant \textit{sum of } k-1 \textit{ largest binomial coefficients } \binom{t}{i}$$

and this is sharp.

One of the first novelties in these set generalizations has been brought (again the case $k=2$ below) by De Bruijn, Van Ebbenhorst Tengbergen and Kruyswijk [2] who proved a corresponding result for subsets of divisors of a given positive integer. Motivated by a close connection between the subsets

Received: 22.10.2002.

AMS (1991) subject classification: Primary 05A05, 11B75, 11N80.

Key words and phrases: generalized integer, arithmetical semigroup, Narkiewicz's regular system of divisors, Sperner system, symmetric chain.

The author was supported by the Grant Agency of the Czech Republic, Grant # 201/01/0471.

of a finite sets and the subsets of divisors of a square–free positive integer various interesting links between both topic were found. E.g. Schönheim [11] proved:

If in $\mathcal{D} = \{h_1, \ldots, h_n\} \subset D(N)$, *the set of all divisors of* $N = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, *there is no chain of length* k, *then*

$$n \leqslant \textit{sum of } k-1 \textit{ largest numbers } \tau_i(N)$$

and this is sharp.

Here $d(n)$ denotes the degree of n, that is, the total number of prime divisors of n, and $\tau_\beta(N) = \#\{h : h|N, d(h) = \beta\}$. The reader is referred to [5] for more details about further generalizations and comments.

In [10] the author proposed a further generalization in the sense that the positive integers were replaced by elements of an arithmetical semigroup and the sets of divisors by the so–called regular systems of divisors. To make the paper self–contained we repeat some basic definitions for the convenience of the reader in the next section.

2. Regular systems of divisors

Let G denote a free commutative semigroup relative to a multiplication operation denoted by juxtaposition, with identity element 1_G and with at most countably many generators P_G. Such a semigroup will be called (cf. [7]) **arithmetical semigroup** if in addition a real–valued **norm** $|\cdot|$ is defined on G such that

(i) $|1_G| = 1, |a| > 1$ for all $a \in G$,
(ii) $|ab| = |a| \cdot |b|$ for all $a, b \in G$,
(iii) the set $\{a \in G : |a| \leqslant x\}$ is finite for all real numbers x.

The elements of G are called **generalized integers**. The free semigroup structure of G substitutes the multiplicative structure of positive integers. The analytical part of the theory of arithmetical semigroups based on the existence of the norm mapping $|\cdot|$ will play rather peripheral role mainly because most of our reasoning will be based on the divisibility relation induced by the multiplication in G where each element of G being uniquely representable as a product of generators of G has only a finite number of divisors, what replaces requirement (iii) in our arguments.

The standard terms like **divisor** are defined between generalized integers in the expected way, by saying that an element $b \in G$ divides $a \in G$, in symbols $b|a$, if there exists a $c \in G$ such that $a = bc$. The set of all divisors of $a \in G$ will be denoted by $D(a)$. The elements of the set P_G of all generators of G will be called **primes**.

Besides the set $\mathbb{N}$ of positive integers the most typical prototypes of arithmetical semigroups are:

EXAMPLE 1. $G = G_K$, the semigroup of all non–zero integral ideals in a given algebraic number field K of degree $n = [K : \mathbb{Q}]$ over rationals $\mathbb{Q}$ with the usual norm function $|\mathfrak{a}| = \mathrm{card}(\mathcal{O}_K/\mathfrak{a})$.

EXAMPLE 2. $G = \mathcal{A}$ the category of all finite Abelian groups with the usual direct product operation and the norm $|A| = \mathrm{card}(A)$. Fundamental Theorem on finite Abelian groups shows that $\mathcal{A}$ is free and that the generators are the cyclic groups of prime–power order.

It is well–known that if $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals in a number field K then the relation $\mathfrak{a}|\mathfrak{b}$ is equivalent to $\mathfrak{a}\supset\mathfrak{b}$. Thus in this case any divisibility relation can be converted in turn to a set–inclusion form and vice verse. This remains true also for the factor–rings of algebraic integers with respect to a proper ideal. Thus the reformulation of the problem in the framework of arithmetical semigroups shows perhaps more naturally the mentioned connections between the set–theoretic and divisor version.

In the group case, if a finite Abelian group $H = A \times B$ is the direct product of groups A and B, then A can be understood as a subgroup (and thus also a subset) of B. In the converse direction it is interesting to note that Kertézs [6] proved that every subgroup of a general group G is its direct factor if and only if G is the direct product of cyclic groups of prime order, that is if it is of squarefree order (and clearly Abelian), and we have again a formally different demonstration that De Bruijn et al. implies Sperner.

In the introduction mentioned modification of the divisibility notion is due to Narkiewicz [9] who considered the case of $G = \mathbb{N}$, the set of positive integers. Its extension to arithmetical semigroups is immediate: Let A be a mapping from the arithmetical semigroup G into the set of subsets of G such that $A(a)$ is a subset of the set $D(a)$ of all divisors of $a \in G$. The system

$$\{A(a) : a \in G\} \tag{1}$$

will be called the **system of A–divisors**, the elements of $A(a)$ are called the **A–divisors of a**. If $d \in A(a)$, we shall write $d|_A a$ to distinguish between the A–divisibility and the usual divisibility.

The system of D–divisors is connected with the well–known Dirichlet convolution. The second most known example is the system of unitary divisors defined by

$$U(a) = \{d \in G : d|a, (d, a/d) = 1_G\}$$

and is connected with the so called unitary convolution (cf. [1]).

The system (1) will be called **regular system of divisors** (or **regular system of A–divisors**) provided:

(a) $d \in A(a) \Rightarrow a/d \in A(a)$
(b) if $(a,b) = 1_G$ then $A(ab) = A(a) \cdot A(b)$, where $A \cdot B = \{a'b' : a' \in A, b' \in B\}$
(c) $\{1_G, a\} \subset A(a)$ for all a
(d) the statement "$d \in A(a)$ and $a \in A(b)$" is equivalent to "$d \in A(b)$ and $a/d \in A(b/d)$"
(e) for all prime powers p^k, $k \in \mathbb{N}$, there exists a positive integer v such that
$$A(p^k) = \{1_G, p^v, p^{2v}, \ldots, p^{rv} = p^k\},$$
and moreover $p^v \in A(p^{2v})$, $p^{2v} \in A(p^{3v})$, $\ldots$, $p^{(r-1)v} \in A(p^k)$.
Note that these conditions, as stated here, are not independent.

The divisor v of k is called the **type of** p^k and it will be denoted by $t_A(p^k)$ in what follows.

The next result can be proved for general arithmetical semigroups using the same ideas as in [8, Corollary 4.2] for $\mathbb{N}$.

LEMMA 3. *Let* (1) *be a regular system of divisors and* $p \in P_G$, *and* $\alpha \geqslant \beta \geqslant 1$ *two integers. If* $A(p^\alpha) \cap A(p^\beta) \neq \{1_G\}$ *then* $t_A(p^\alpha) = t_A(p^\beta)$, *and* $A(p^\beta)$ *consists of the* $(\beta/t_A(p^\alpha) + 1)$ *elements of the smallest norm in* $A(p^\alpha)$.

An element $a \in G$, $a \neq 1_G$, is called A–**primitive** if $A(a) = \{1_G, a\}$. The D–primitive elements are the primes $p \in P_G$, while the U–primitive elements are the all powers $p^k, k \in \mathbb{N}$, of prime elements $p \in P_G$. An element m which is a product of distinct A–primitive elements will be called **A–squarefree.**

COROLLARY 4. *If* p^λ *is of type* v, *then* p^v *is* A*-primitive.*

PROOF. Would we have $p^\alpha \in A(p^v)$ with $0 < \alpha < v$, i.e. $p^\alpha \in A(p^v)$ and $p^v \in A(p^\lambda)$, then (d) implies that $p^\alpha \in A(p^\lambda)$ which is not true. Hence $A(p^v) = \{1_G, p^v\}$, as claimed. □

Property (b) immediately implies that:

LEMMA 5. *If* $n \in G$ *is* A*–primitive then* $n = p^\alpha$ *for some* $p \in P_G$ *and* $\alpha \geqslant 1$.

Note that regular systems of A–divisors are completely determined by the sets $A(p^\alpha)$ for all $p \in P_G$ and all $\alpha \geqslant 1$. On the other hand, a regular system of divisors is not *uniquely* determined by its primitive elements. There are different systems of distinct regular systems of divisors having the same set of primitive elements (cf. [9, p. 87] or [8, p. 160]).

LEMMA 6 ([8, Exercise 4.5]). *Let A be a regular system of divisors. If p is a prime and p^α is the highest power of p that divides an element $m \in G$ then $p^\alpha \in A(m)$. Furthermore, if $p^\beta \in A(m)$ then $p^\beta \in A(p^\alpha)$.*

PROOF. The statements are direct consequences of properties (a) and (c). □

If $a, b \in G$ then the A–**greatest common divisor** $(a, b)_A$ is the common A–divisor of a and b that is divisible by any other common A–divisor of a and b. Two elements $a, b \in G$ are A–**relatively prime** if, and only if, $A(a) \cap A(b) = \{1_G\}$.

The next elementary result will be applied later:

LEMMA 7. *Let A be a regular system of divisors. If $d|_A m_1 m_2$ and $(m_1, m_2) = 1_G$ then*

$$(d, m_1)_A (d, m_2)_A = d.$$

PROOF. Let p^α be the highest power of a prime A–dividing d. Then (d) implies that $p^\alpha|_A m_1 m_2$, and consequently $p|m_1 m_2$. Since $(m_a, m_1) = 1$, either $p|m_1$ or $p|m_2$. Let $p|m_1$, and let p^β be the highest power of p dividing m_1. Clearly, p^β is also the highest power of p dividing $m_1 m_2$. Lemma 6 shows that $p^\alpha|_A p^\beta$. Consequently, $p^\alpha|_A m_1$, i.e. $p^\alpha|_A (d, m_1)_A$, and the proof is finished. □

REMARK 8. In the above lemma it is not possible to replace the condition $(m_1, m_2) = 1_G$ by $(m_1, m_2)_A = 1_G$. To see this, take a power of a prime p^α such that $t_A(p^\alpha) = v > 1$. Then $(p, p^{\alpha-1})_A = 1_G$. Would be this not true, then $(p, p^\alpha)_A = p$, i.e. $t_A(p^{\alpha-1}) = 1$ and consequently $p^v \in A(p^{\alpha-1})$ and Lemma 3 implies the impossible equality $t_A(p^{\alpha-1}) = t_A(p^\alpha)$. Thus if $d = p^v$ we have $(p^v, p)_A = 1_G$ and also $(p^v, p^{v-1})_A = 1_G$, i.e. $p^v \neq (p^v, p)_A (p^v, p^{v-1})_A$.

3. A–degree and A–chains

Unless contrary is stated A will always be supposed to be a regular systems of divisors. Let $m \in G$. If

$$m = p_1^{\lambda_1} p_2^{\lambda_2} \dots p_k^{\lambda_k} \tag{2}$$

is the decomposition of m into primes, then the **A–degree** $d_A(m)$ of $m \neq 1_G$ is defined by

$$d_A(m) = \sum_{i=1}^{k} \frac{\lambda_i}{t_A(p_i^{\lambda_i})},$$

where $t_A(p^k)$ is the type of p^k, and $d_A(1_G) = 0$.

LEMMA 9. *If $a|_A b$ and $b = ac$, where c is A–primitive, then $d_A(b) = d_A(a) + d_A(c)$.*

PROOF. If c is A–primitive then Lemma 5 implies $c = p^\beta$ for some p and $\beta \geqslant 1$, i.e. $b = ap^\beta$. Since $a \in A(b)$, property (a) yields that $p^\beta = b/a \in A(b)$. If p^α is the highest power dividing b then Lemma 6 shows that $p^\beta \in A(p^\alpha)$. Property (a) applied to p^β and p^α implies $p^{\alpha-\beta} \in A(p^\alpha)$.

If $\alpha - \beta = 0$ then the proof is finished. Suppose therefore that $\alpha > \beta$. Lemma 3 implies that $t_A(p^\alpha)$ divides each of the exponents α, β and $\alpha - \beta$ and that $t_A(p^\alpha) = t_A(p^{\alpha-\beta}) = t_A(p^\beta)$. Consequently, for the contribution of powers of p to the degrees of a and b, we get

$$\frac{\alpha}{t_A(p^\alpha)} = \frac{\alpha-\beta}{t_A(p^\alpha)} + \frac{\beta}{t_A(p^\alpha)} = \frac{\alpha-\beta}{t_A(p^{\alpha-\beta})} + \frac{\beta}{t_A(p^\beta)},$$

and the proof is finished. □

Note that in the previous lemma the assumptions that $b = ac$ and c is A–primitive does not imply that also $a|_A b$ as the Remark 8 shows for $b = p^\alpha$ and $c = p$ provided $t_A(p^\alpha) > 1$.

An **A–chain** (of length h) is a sequence $d_1, \ldots, d_h$ of elements of G such that $d_i|_A d_{i+1}$ for all $1 \leqslant i < h$.

LEMMA 10. *If $a|_A b$ then there exists an A–chain $a = d_1, \ldots, d_h = b$ of elements of G such that d_{i+1}/d_i is A–primitive for all $1 \leqslant i < h$.*

PROOF. Let p^α and p^β denote the highest power of a fixed prime p which divides a and b, resp. Lemma 6 shows that $p^\beta \in A(b)$, and similarly $p^\alpha \in A(a)$. Since $p^\alpha \in A(a)$ and $a \in A(b)$, property (d) implies $p^\alpha \in A(b)$. Due to property (b) the relation $p^\alpha \in A(b)$ can hold only if $p^\alpha \in A(p^\beta)$. Lemma 3 shows that $t_A(p^\alpha) = t_A(p^\beta)$ provided both α, β are positive. If v denotes this common value and $\alpha < \beta$ then

$$a, ap^v, ap^{2v}, \ldots, ap^{\beta-\alpha}$$

is the subchain of the constructed A–chain corresponding to the prime p dividing both a and b. If $p \nmid a$, i.e. $\alpha = 0$, then the construction above works with $v = t_A(p^\beta)$. If $\alpha = \beta$ the subchain corresponding to p is empty. □

COROLLARY 11. *If $a|_A b$ then $d_A(a) \leqslant d_A(b)$. More precisely, $d_A(b) = d_A(a) + d_A(b/a)$.*

Let $\tau_{A,\beta}(m)$ denote the number of A–divisors of m of A–degree β. For later convenience put $\tau_{A,\beta}(m) = 0$ for $\beta < 0$ or $\beta > d_A(m)$. This number satisfies many identities similar to those for binomial coefficients. For instance, if m is A–squarefree then

$$\tau_{A,\beta}(m) = \binom{d_A(m)}{\beta}.$$

The formula

$$\sum_{i=0}^{d_A(m)} \tau_{A,i}(m) = \prod_{i=1}^{k} \left(\frac{\lambda_i}{t_A(p_i^{\lambda_i})} + 1 \right),$$

extends the well–known one $\sum_{i=1}^{n} \binom{n}{i} = 2^n$, and actually says nothing else as that each A–divisor of m has a degree. Another identity

$$\sum_{\beta=0}^{r} \tau_{A,\beta}(d_a(m_2))\tau_{A,r-\beta}(d_a(m_1)) = \tau_{A,r}(d_a(m_1 m_2)) \tag{3}$$

provided $(m_1, m_1) = 1_G$ and $d_A(m_1) \geqslant d_A(m_2)$ is the algebraic form of the fact that A–divisors of $m_1 m_2$ of a given degree r are products of A–divisors of m_1 and m_2 of A–degrees summing up to the A–degree of $m_1 m_2$.

4. Symmetric A–chains

An A–chain $d_1, \ldots, d_h$ of A–divisors of $m \in G$ will be called a **symmetric A–chain** if:

(c) the A–degree of d_1 equals the A–degree of m/d_h,

(cc) if $h > 1$ then the quotient d_{i+1}/d_i is A–primitive for all $1 \leqslant i < h$.

The notion of the symmetric chain was introduced by De Bruijn, van Ebbenhorst Tengbergen, and Kruyswijk in [2] for the case $G = \mathbb{N}$ and $A = D$. The next result as well as its proof technique goes back to the corresponding Theorem 2 in this paper.

THEOREM 12. *The set of A-divisors of an element $m \in G$ can be completely divided into a number of disjoint symmetric A-chains.*

PROOF. The proof can be done by induction on the number $\omega_G(m)$ of distinct prime divisors of m. Let $m = m_1 p^\lambda$ with $p \nmid m_1$ and $A(p^\lambda) = \{1_G, p^v, p^{2v}, \ldots, p^{rv} = p^\lambda\}$. The main ingredient of the proof is the construction of symmetric A-chains for m from those for m_1. Given a symmetric A-chain $d_1, d_2, \ldots, d_h$ of A-divisors of m_1 we can generate a sequence of disjoint symmetric A-chains for m as follows:

$$d_1, d_1 p^v, \ldots, d_1 p^{rv}, d_2 p^{rv}, \ldots, d_h p^{rv},$$

$$d_2, d_2 p^v, \ldots, d_2 p^{(r-1)v}, d_3 p^{(r-1)v}, \ldots, d_h p^{(r-1)v}$$

etc. The last one being

$$d_{r+1}, \ldots, d_h$$

if $h \geqslant r+1$, or

$$d_h, \ldots, d_h p^{(r+1-h)v}$$

if $h \leqslant r+1$. □

The next result can be reconstructed using ideas of the proof of Theorem 1 of [2]. Its connections to Theorem 19 are immediate.

LEMMA 13. *Let $m \in G$. Then the number of symmetric A-chains in which the set of A-divisors of m splits is $\tau_{A,\lfloor d_A(m)/2 \rfloor}(m)$.*

COROLLARY 14. *We have $\tau_{A,0}(m) \leqslant \tau_{A,1}(m) \leqslant \tau_{A,2}(m) \leqslant \ldots \leqslant \tau_{A,\lfloor d_A(m)/2 \rfloor}(m)$.*

LEMMA 15. *If a symmetric A-chain contains an A-divisor of degree*
(s) $s \leqslant d_A(m)/2$ then the chain under question contains at least $d_A(m) - 2s$ other A-divisors of degree $> s$,
(ss) $s \geqslant d_A(m)/2$ then the chain under question contains at least $2s - d_A(m)$ other A-divisors of degree $< s$.

PROOF. Let our symmetric A-chain be $t_1, \ldots, t_k$ and let $d_A(t_1) \leqslant s = d_A(t_i) \leqslant d_A(t_h)$ for some index $i \in \{1, \ldots, k\}$. We know that the values $d_A(t_i)$ increase by 1 when the index i increases by 1. Thus
(s) the all terms of the chain of degree $> s$ are those between t_{i+1} and t_k including the bounds. They are $d_A(t_k) - d_A(t_i)$ in number. The condition

(c) implies that $d_A(t_k) = d_A(m) - d_A(t_1)$, and since $d_A(t_1) \leqslant d_A(t_i) = s$, the result follows. [1]
(ss) in this case all the terms of the chain of degree $< s$ are those between t_1 and t_{i-1} including them. Their number is $d_A(t_i) - d_A(t_1) = s - (d_A(m) - d_A(t_k)) \geqslant 2s - d_A(m)$. □

An extension of another property of symmetric A–chains used in the proof of Lemma 13 leads to the following observation:

LEMMA 16. *If t_1 is the initial element of a symmetric A–chain of length h then h and $d_A(m)$ are of opposite parity and $d_A(t_1) = (d_A(m) + 1 - h)/2$.*

PROOF. The definition implies that if $t_1, \ldots, t_h$ is a symmetric A–chain then $d_A(t_h) = d_A(m) - d_A(t_1)$. On the other hand, we know that the values $d_A(t_i)$ increase by 1 when the index i increases by 1. Thus $d_A(t_h) = d_A(t_1) + h - 1$, i.e. $2d_A(t_1) = d_A(m) + 1 - h$. Since the numbers occurring in the last equality are integers the statement follows.

COROLLARY 17. *If h is the length of a symmetric A–chain for $m \in G$, then*

$$h \in \{d_A(m) + 1, d_A(m) - 1, d_A(m) - 3, \ldots\} \cap \mathbb{N}.$$

To the proof only note that the largest length $d_A(m) + 1$ is really realizable and starts at 1_G and ends at m. If $m = p^\lambda$ then this is the only symmetric A–chain, which shows that not each h in the above interval is realizable.

LEMMA 18. *Let $m \in G$. If $h \in \mathbb{N}$ and $d_A(m)$ have the opposite parity, then the number of mutually disjoint symmetric A–chains of length h of the A–divisors of an element $m \in G$ is given by the formula*

$$\tau_{A,(d_A(m)+1-h)/2}(m) - \tau_{A,(d_A(m)-1-h)/2}(m).$$

PROOF. We shall proceed by induction on $d_A(m)$. If $d_A(m) = 1$ then $m \in P_G$ and we have only one symmetric chain of length 2. Suppose that the formula of the lemma holds for all admissible h and for each $m \in G$ with $d_A(m) < k$ and $k > 1$ a positive integer. Consider an m with $d_A(m) = k > 1$.

[1] The reason for the assumption $s \leqslant d_A(m)/2$ is that in the opposite case the statement of the lemma is empty for $d_A(m) - 2s$ is negative.

Let p^k be the highest power of a prime dividing m and let $v = t_A(p^k)$ be its type. Then $k = rv$, and let $m = np^k$.

To count the number of mutually disjoint symmetric A–chains of length h we shall use the construction employed in the proof of Theorem 12. Suppose that we took a symmetric A–chain of length f for n. Taking into account the final remark in the proof of this theorem consider two possibilities $f \geqslant r+1$ or $f < r+1$. In the first case the longest symmetric A–chain for m which we obtain using the procedure of the proof of Theorem 12 has length $f+r$, the next to the right has length $f+r-2$, etc. and the shortest one has length $f-r$, i.e. we obtain symmetrical A–chains for m having lengths

$$f+r-2i \qquad \text{for} \qquad i = 0,1,2,\dots,r.$$

If $f < r+1$ we get chains of length $f+r$, $f+r-2$, ..., $r+2-f$, i.e.

$$r+f-2i \qquad \text{for} \qquad i = 0,1,2,\dots,f-1.$$

Since $f-1 < r$ in the later case, we can sum up both cases saying: with every symmetric A–chain of length f for n we can generate a symmetric A–chain for m of length

$$h = f+r-2i$$

for every $i = 0,1,\dots,r$ provided $h \geqslant 0$. In other words, if for $h \geqslant 0$ we have

$$f = h-r+2i \tag{4}$$

for some $i \in \{0,1,\dots,r\}$, then we can associate with each symmetric A–chain of length f for n a symmetric A–chain of length h for m. The induction hypothesis shows that the total number of symmetric A–chains for n is

$$\tau_{A,(d_A(n)+1-f)/2}(n) - \tau_{A,(d_A(n)-1-f)/2}(n).$$

Plugging (4) for f and summing up for $i \in \{0,1,\dots,r\}$ we get

$$\begin{aligned}
&\big(\tau_{A,(d_A(n)+1-(h-r+2.0))/2}(n) - \tau_{A,(d_A(n)-1-(h-r+2.0))/2}(n)\big)\\
&\quad + \big(\tau_{A,(d_A(n)+1-(h-r+2.1))/2}(n) - \tau_{A,(d_A(n)-1-(h-r+2.1))/2}(n)\big) + \dots +\\
&\quad + \big(\tau_{A,(d_A(n)+1-(h-r+2.r))/2}(n) - \tau_{A,(d_A(n)-1-(h-r+2.r))/2}(n)\big)
\end{aligned}$$

and the result follows for $d_A(n) + r = d_A(m)$. □

The above proof can be used to demonstrate the comment after Corollary 17 once again: If $m = p_1^{\alpha_1} p_2^{\alpha_2}$, $p_1 \neq p_2$, $v_1 = t_A(p_1^{\alpha_1})$ and $v_2 = t_A(p_2^{\alpha_2})$

with $v_1 > v_2$ then only lengths $(v_1+1)+v_2, (v_2+1)+v_2-2, \ldots, (v_1+1)+v_2-2v_2$ are realizable. This sequence does not contain the length 1.

5. Sperner type theorems

The preliminaries for the proof of next result are already behind us (cf. proof of [2, Theorem 1] for details).

THEOREM 19. *Let $d_1, \ldots, d_h$ be a set of A-divisors of $m \in G$ with the property that no d_i is an A-divisor of a d_j with $i \neq j$. Then $h \leqslant \tau_{A,\lfloor d_A(m)/2 \rfloor}(m)$.*

The next results were proved for $G = \mathbb{N}$ and $A = D$ in [11, Theorem 2]. The presented proof follows the ideas used in that paper. If m is A–squarefree we get a result extending original Sperner's one and proved in [3] showing that the result is sharp.

THEOREM 20. *Let $m \in G$ and $\mathcal{D} = \{d_1, \ldots, d_h\}$ be a set of A-divisors of m with the property that $\mathcal{D}$ has no A-subchain of length $\ell + 1$. Then*

$$h \leqslant \text{ sum of } \ell \text{ largest values of } \tau_{A,i}(m).$$

Since any set consisting of A–divisors of a fixed degree cannot contain an A–subchain, the set consisting of the all A–divisors of ℓ distinct degrees does not contain an A–chain of length $\ell + 1$.

PROOF. First note the following two simple properties of $\tau_{A,\beta}(m)$:
(i) if $0 \leqslant \beta \leqslant d_A(m)$ then $\tau_{A,\beta}(m) = \tau_{A,d_A(m)-\beta}(m)$, and
(ii) $\tau_{A,0}(m) \leqslant \tau_{A,1}(m) \leqslant \tau_{A,2}(m) \leqslant \ldots \leqslant \tau_{A,\lfloor d_A(m)/2 \rfloor}(m)$.

Property (i) follows immediately from Corollary 11 and (ii) is Corollary 14.

Properties (i) and (ii) imply that the ℓ largest values of $\tau_{A,\beta}(m)$ correspond to a segment of consecutive values β, say $\beta = i_0, \ldots, i_0 + \ell - 1$, where

$$i_0 \leqslant (d_A(m) - \ell + 2)/2. \tag{5}$$

If the A–degree of each member of $\mathcal{D}$ lies in the interval $\langle i_0, i_0 + \ell - 1\rangle$ we are done. Therefore suppose that the A–degree of at least one member in $\mathcal{D}$ lies outside this interval. We have two possibilities to consider:

a) The minimal degree j of elements in $\mathcal{D}$ satisfies $j < i_0$. Let $\mathcal{D}_j = \{d_1, \ldots, d_k\}$ be the set of all elements of degree j in $\mathcal{D}$. By Theorem 12 each element of $\mathcal{D}_j$ belongs to some symmetric A–chain. Moreover, each symmetric chain contains at most one member of $\mathcal{D}_j$. Let C_v be the symmetric A–chain containing d_v for each $v = 1, \ldots, k$.

Since $j < i_0$ then $j \leqslant (d_A(m) - \ell)/2$ due to (5), i.e.

$$j + \ell \leqslant d_A(m) - j. \tag{6}$$

Lemma 15 (s) shows that each C_v contains at least $d_A(m) - 2j$ divisors of degree $> j$. Since in a symmetric A–chain the degree of members increases by step 1 with the growing index, we have at least one member of degree $j + (d_A(m) - 2j) = d_A(m) - j$ in each C_v. Then (6) implies the existence of a member, say d'_v of degree $j + \ell$ in C_v. The A–subchain of C_v starting with d_v and terminating in d'_v has length $\ell + 1$ and it cannot be completely in $\mathcal{D}$. Let d^*_v be the element of this A–subchain not belonging to $\mathcal{D}$ of the smallest possible degree. Let $\mathcal{D}' = (\mathcal{D} \setminus \mathcal{D}_j) \cup \{d^*_1, \ldots, d^*_h\}$. Since $j + \ell \leqslant i_0 + \ell - 1$, the A–degree of no member in $\mathcal{D}'$ exceeds $i_0 + \ell - 1$. On the other hand, the minimal A–degree of $\mathcal{D}'$ is $> j$. Repeating this procedure we can construct a set of A–divisors having the same cardinality as the original one and satisfying the hypotheses of our theorem until the A–degree of its each member is at least i_0.

b) The minimal degree j of elements in $\mathcal{D}$ satisfies $j > i_0 + \ell - 1$. A similar reduction procedure based on Lemma 15 (ss) leads to a set $\mathcal{D}''$ of A–divisors of m each of which is of degree $\leqslant i_0 + \ell - 1$ and simultaneously $\geqslant i_0$. □

THEOREM 21. *Let $m \in G$ and $m = m_1 m_2$ where $(m_1, m_2) = 1_G$ and $d_A(m_1) \geqslant d_A(m_2)$. Let $\mathcal{D} = \{d_1, d_2, \ldots, d_h\}$ be a set of A–divisors of m such that for no $\{i, j\} \subset \{1, 2, \ldots, h\}$ either*

$$(d_i, m_2)_A = (d_j, m_2)_A \qquad \text{and} \qquad (d_i, m_1)_A |_A (d_j, m_1)_A \tag{7}$$

or

$$(d_i, m_1)_A = (d_j, m_1)_A \qquad \text{and} \qquad (d_i, m_2)_A |_A (d_j, m_2)_A \tag{8}$$

holds. Then

$$h \leqslant \tau_{A, \lfloor (d_A(m_1) + d_A(m_2))/2 \rfloor}(m). \tag{9}$$

PROOF. We shall use Lemma 7 to classify the divisors in $\mathcal{D}$ in groups. Writing $d_i = (d_i, m_1)_A (d_i, m_2)_A$, $i \in \{1, \ldots, h\}$, the grouping will be realized with respect to the A–divisors $(d_i, m_2)_A$ of m_2. We then append each such group to the corresponding A–divisor of m_2 after the all A–divisors of m_2 are split into symmetric A–chain. To the groups appended to A–divisors of each chain we then apply Theorem 20. That this theorem can be applied is guaranteed by the assumptions. More precisely:

Let $b_2, b_2, \ldots, b_l$ be an A–chain of A–divisors of m_2. Define for $i = 1, 2, \ldots, l$

$$\mathcal{G}_i = \{(d, m_1)_A : d \in \mathcal{D}, (d, m_2)_A = b_i\}.$$

Then (7) implies

$$\text{for no } h, k \text{ and } i\text{: } g_h, g_k \in \mathcal{G}_i \text{ and } g_h |_A g_k. \tag{10}$$

Further, if $x \in \mathcal{G}_i \cap \mathcal{G}_j$ for $i \neq j$, then $x = (d', m_1)_A$ and $(d', m_2)_A = b_i$ for some $d' \in \mathcal{D}$, and similarly $x = (d'', m_1)_A$ and $(d'', m_2)_A = b_j$ for some $d'' \in \mathcal{D}$. But (8) implies that either $b_i \not|_A b_j$ or $b_j \not|_A b_i$, what is impossible due to the fact that the b's form an A–chain. That is, we have

$$\mathcal{G}_i \cap \mathcal{G}_j = \emptyset \text{ for } i \neq j \tag{11}$$

Finally, the denial of

$$\bigcup_{i=1}^{l} \mathcal{G}_i \text{ cannot contain a chain of length } l+1 \tag{12}$$

would imply that two elements $(d', m_1)_A$ and $(d'', m_1)_A$ of the chain in the same $\mathcal{G}_i$ contradict (7) since $(d', m_2)_A = (d'', m_2)_A = b_i$, i.e. (12) holds.

To prove (9), as already indicated, partition the set of A–divisors of m_2 into disjoint symmetric A–chains. This can be done due to Theorem 12. If $b_1, \ldots, b_l$ is one such chain of length l associate to it sets $\mathcal{G}_i$ as described above. Since (12), Theorem 20 implies

$$\left| \bigcup_{i=1}^{l} \mathcal{G}_i \right| \leqslant \text{ sum of } l \text{ largest values of } \tau_{A,i}(m_2).$$

If L consists of the positive terms of the decreasing sequence $\{d_A(m_2) + 1, d_A(m_2) - 1, d_A(m_2) - 3, \ldots\}$, then Corollary 17 and Lemma 18 give the estimate

$$h \leqslant \sum_{l \in L} \left[\tau_{A,(d_A(m_2)+1-l)/2}(m_2) - \tau_{A,(d_A(m_2)-1-l)/2}(m_2)\right] \sum_{v=i_0}^{i_0+l-1} \tau_{A,v}(m_1),$$

where i_0 is determined in (5).

For the sake of simplicity suppose that the numbers $d_A(m_1) = 2M_1$, $d_A(m_2) = 2M_2$, $l = 2l_1 - 1$ are even. The other cases can be checked along similar lines. Then the last double sum reduces to the form

$$\sum_{l_1=1}^{M_2+1} [\tau_{A,M_2-l_1+1}(m_2) - \tau_{A,M_2-l_1}(m_2)] \sum_{v=1-l_1}^{l_1-1} \tau_{A,v}(m_1)$$

and this, due to the inner cancellations, to

$$\tau_{A,M_2}(m_2)\tau_{A,M_1}(m_1) + \sum_{i=1}^{M_2} \tau_{A,M_2-i}(m_2)\left(\tau_{A,M_1-i}(m_1) + \tau_{A,M_1+i}(m_1)\right).$$

Using the fact that $\tau_{A,j}(m) = \tau_{A,d_A(m)-j}(m)$, we get finally

$$\begin{aligned} &= \sum_{j=0}^{M_2} \tau_{A,j}(m_2)\tau_{A,M_1+M_2-j}(m_1) + \sum_{j=1}^{M_2} \tau_{A,M_2-j}(m_2)\tau_{A,M_1-M_2+j}(m_1) \\ &= \sum_{j=0}^{M_1+M_2} \tau_{A,j}(m_1 m_2), \end{aligned}$$

as claimed. □

6. A–convex sets

A set S of A–divisors of an $m \in G$ will be called **A–convex** whenever

$$(d_1 \in S, d_2 \in S, d_1|_A d_3|_A d_2) \quad \Rightarrow \quad d_3 \in S.$$

One of the conditions imposed on the regularity of an A–system of divisors (cf. [9] for more details) is that the Möbius function μ_A of an A–convolution should assume only values 0 and -1 at prime powers.[2)] The value of μ_A at $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ is defined by

$$\mu_A(a) = \begin{cases} 1 & \text{if } a = 1_G, \\ (-1)^r & \text{if each } p_i^{\alpha_i} \text{ is } A\text{–primitive for every } i, \\ 0 & \text{if some } p_i^{\alpha_i} \text{ is not } A\text{–primitive.} \end{cases}$$

[2)] Note that, in the case of Dirichlet convolution, that is if $A = D$, the function μ_A is the ordinary Möbius function, while in the case of unitary convolution it is one of the Liouville functions, namely $a \mapsto (-1)^{\omega(a)}$, where $\omega(a)$ denotes the number of distinct prime divisors of $a \in G$.

The notion of A–convexity has its origin in [2] where also the next result can be found (Theorem 3) if $G = \mathbb{N}$ and $A = D$.

THEOREM 22. *If $\omega_G(m)$ stands for the number of different primes dividing $m \in G$, and S is a A–convex set of A–divisors of m, then*

$$\left|\sum_{d\in S}\mu_A(d)\right| \leqslant \binom{\omega_G(m)}{\lfloor\frac{\omega_G(m)}{2}\rfloor}.$$

PROOF. Since $\mu_A(d) = 0$ when d is not a product of A–primitive elements, we can limit our consideration only to the case when m is a product of distinct A–primitive elements. In this case $\omega_G(m) = d_A(m)$ and the cardinality $\tau_{A,\lfloor d_A(m)/2\rfloor}(m)$ of the set of A–divisors of m of degree $\omega_G(m)/2$ is equal to

$$\tau_{A,\lfloor d_A(m)/2\rfloor}(m) = \binom{\omega_G(m)}{\lfloor\frac{\omega_G(m)}{2}\rfloor}.$$

We saw in the proof of Lemma 13 that this is the number of A–chains into which the set of A–divisors of m can be divided. Let

$$S = S_1 + S_2 + \ldots + S_{\tau_{A,\lfloor d_A(m)/2\rfloor}(m)},$$

where S_i is the subset of the ith chain. However, when d runs over the elements of one chain then $\mu_A(d)$ assumes the values $+1$ and -1 alternately. Hence, $\sum_{d\in S}\mu_A(d) \in \{0,-1,+1\}$. Finally,

$$\left|\sum_{d\in S}\mu_A(d)\right| \leqslant \sum_{i=1}^{\tau_{A,\lfloor d_A(m)/2\rfloor}(m)}\left|\sum_{d\in S_i}\mu_A(d)\right| \leqslant \tau_{A,\lfloor d_A(m)/2\rfloor}(m).$$

□

7. Problem

Regular systems of divisors have their origin in Narkiewicz's paper [9], where he investigated the question under which conditions a convolution of two arithmetical functions f, and g defined on the set of positive integers $\mathbb{N}$

$$(f\circ g)(n) = \sum_{d\in A_n} f(d)g\left(\frac{n}{d}\right)$$

derived from a system $A = \{A_n;\ n \in \mathbf{N}\}$ turns the set of arithmetical functions into a commutative ring with unity and prescribed properties of its inverse.

Theorem 12 shows that the regular system of A–divisors possesses a symmetric chain partition. The question is whether this statement can be inverted:

If the system of A–divisors of each element $m \in G$ possesses a symmetric chain partition then it is regular.

References

[1] E. Cohen, *Arithmetical functions associated with the unitary divisors of an integer*, Math. 74 (1960), 66–80.

[2] N. G. De Bruijn, C. van Ebbenhorst Tengbergen and D. Kruyswijk, *On the set of divisors of a number*, Nieuw Arch. Wisk. 23 (1952), 191–193.

[3] P. Erdős, *On a lemma of Littlewood and Offord*, Bull. Amer. Math. Soc. 51 (1945), 898–902.

[4] P. Erdős, J. Schönheim, *On the set of non pairwise coprime divisors of a number*, in "Combinatorial Theory and its Applications" Vol. 1, pp. 369–376, Coll. Math. Soc. J. Bolayi 2 (P. Erdős, A. Rényi, V.T. Sós eds.), North–Holland, Amsterdam – London 1970.

[5] P. Erdős and J. Schönheim, *Sets versus divisors*, in "Combinatorics, Paul Erdős is Eighty" Vol. 2, pp. 193–212, Bolayi Society Mathematical Studies, 2 (Keszthely, 1993), Budapest 1996.

[6] A. Kertész, *On groups every subgroup of which is a direct summand*, Publ. Math. 2 (1951), 74–75.

[7] J. Knopfmacher, *Abstract Analytic Number Theory*, North–Holland Mathematical Library Vol. 12, North–Holland & American Elsevier, Amsterdam–Oxford–New York 1975.

[8] P. J. McCarthy, *Introduction to Arithmetical Functions*, Springer Verlag, New York 1986.

[9] W. Narkiewicz, *On a class of arithmetical convolutions*, Coll. Math. 10 (1963), 81–94.

[10] Š. Porubský, *Sets of regular systems of divisors of a generalized integer*, Ann. Math. Sil. 12 (1998), 149–156.

[11] J. Schönheim, *A generalization of results of P. Erdős, G. Katona and D.J. Kleitman concerning Sperner's theorem*, J. Combin. Theory 11 (1971), 111–117.

[12] E. Sperner, *Ein Satz über Untermengen einer endlichen Menge*, Math. Zeit. 27 (1928), 544–548.

Institute of Computer Science
Academy of Sciences of the Czech Republic
Pod Vodárenskou věží 2
182 07 Prague 8
Czech Republic

e-mail: stefan.porubsky@cs.cas.cz