Maximal sets of numbers not containing $k+1$ pairwise coprime integers

Rudolf Ahlswede and Levon H. Khachatrian

Fakultät für Mathematik
Universität Bielefeld
Postfach 100 131

33501 Bielefeld
Germany

Abstract For positive integers k, n let $f(n, k)$ be the maximal cardinality of subsets of integers in the interval $< 1, n >$, which don't have $k+1$ pairwise coprimes. The set $\mathbb{E}(n, k)$ of integers in $< 1, n >$, which are divisible by one of the first k primes, certainly does not have $k+1$ pairwise coprimes.

Whereas we disproved in [1] an old conjecture of Erdös ([4], [5], [6], [7]) by showing that the equality

$$f(n, k) = |\mathbb{E}(n, k)| \tag{1}$$

does **not** always hold, we prove here that (1) holds for every k and all relative to k sufficiently large n .

1. Introduction

We continue our work of [1], in which an old conjecture of Erdös [4] was disproved. There also some cases were settled in the positive and related questions were investigated. For further related work we refer to [8], [9], [10], [11], and [14]. While restating now the conjecture of Erdös in its original form and its general form of [7], we also introduce our notation and some basic definitions. Here we follow [1] as closely as possible.
$\mathbb{N}$ denotes the set of positive integers and $\mathbb{P} = \{p_1, p_2, \dots\} = \{2, 3, 5, \dots\}$ denotes the set of all primes.

For two numbers $u, v \in \mathbb{N}$ we write $u|v$ iff u divides v, (u, v) stands for the largest common divisor of u and v, $[u, v]$ is the smallest common multiple of u and v. The numbers u and v are called coprimes, if $(u, v) = 1$.

We are particularly interested in the sets

$$\mathbb{N}_s = \{u \in \mathbb{N} : (u, \prod_{i=1}^{s-1} p_i) = 1\} \tag{1.1}$$

and

$$\mathbb{N}_s(n) = \mathbb{N}_s \cap < 1, n >, \tag{1.2}$$

where for $i \leq j$, $< i, j >$ equals $\{i, i+1, \dots, j\}$.

Erdös introduced in [4] (and also in [5], [6], [7], [9]) $f(n, k, s)$ as the largest integer r for which an

$$A \subset \mathbb{N}_s(n), \quad |A| = r, \tag{1.3}$$

exists with no $k+1$ numbers in A coprimes.

Certainly the set

$$\mathbb{E}(n, k, s) = \{u \in \mathbb{N}_s(n) : u = p_{s+i}\, v \ \text{ for some } \ i = 0, 1, \dots, k-1\} \tag{1.4}$$

does not have $k+1$ coprimes.

The case $s = 1$, in which we have $\mathbb{N}_1(n) =< 1, n >$, is of particular interest.

Conjecture 1.

$$f(n, k, 1) = |\mathbb{E}(n, k, 1)| \quad \textit{for all} \ \ n, k \in \mathbb{N}.$$

It seems that this conjecture of Erdös appeared for the first time in print in his paper [4] of 1962.

General Conjecture.

$$f(n, k, s) = |\mathbb{E}(n, k, s)| \quad \textit{for all} \ \ n, k, s \in \mathbb{N}.$$

Erdös mentions in [7] that he did not succeed in settling the case $k = 1$. We focus on this special case by calling it

Conjecture 2.

$$f(n,1,s) = |\mathbb{E}(n,1,s)| \quad \textit{for all} \quad n,s \in \mathbb{N}.$$

Notice that

$$\mathbb{E}(n,1,s) = \{u \in \mathbb{N}_1(n) : p_s \ |u; p_1, \dots, p_{s-1} \nmid u\}.$$

Whereas in [1] Conjecture 1 was disproved for $k = 212$, Conjecture 2 was almost settled with the following result.

Theorem 2 ([1]). *For every* $s \in \mathbb{N}$ *and* $n \geq \prod_{i=1}^{s-1} p_i/(p_{s+1} - p_s)$,

$$f(n,1,s) = |\mathbb{E}(n,1,s)|$$

and the optimal configuration is unique.

After the presentation of these results on his 80th birthday at a conference in his honour Erdös conjectured that with finitely many exceptions "Erdös sets" are optimal or, in other terminology, that for every $k \in \mathbb{N}$ $f(n,k,1) \neq |\mathbb{E}(n,k,1)|$ occurs only for finitely many n .

We call this Conjecture 1 * . Analogously we speak of Conjecture 2 * (which is settled in the affirmative by Theorem 2 of [1]) and of the General * Conjecture, which is established in this paper.

Actually the main step is the proof of Conjecture 1 * . It can easily be extended to the general case with a bulk of notation. To simplify notation we write in the case $s = 1$ $\mathbb{N}(n) \triangleq \mathbb{N}_1(n),\ f(n,k) \triangleq f(n,k,1)$ and $\mathbb{E}(n,k) \triangleq \mathbb{E}(n,k,1)$.
We climed the mountain to Conjecture 1 * in 3 steps by going through a series of weaker conjectures of increasing strength:

Conjecture 1A.
The infinite Erdös set

$$\mathbb{E}(\infty,k) = \{mp_i : 1 \leq i \leq k,\ m \in \mathbb{N}\}$$

has maximal (lower) density among subsets of $\mathbb{N}$ *without* $k+1$ *coprimes.*

Conjecture 1B.

$$\lim_{n\to\infty} f(n,k)|\mathbb{E}(n,k)|^{-1} = 1 \quad \textit{for every} \quad k \in \mathbb{N}.$$

A few more definitions and known facts are needed.
For $A \subset \mathbb{N}$ we define

$$A(n) = A \cap < 1, n > \quad \text{and} \quad |A| \text{ as cardinality of } A.$$

We call $\underline{d}A = \varliminf_{n\to\infty} \frac{|A(n)|}{n}$ the lower and $\overline{d}A = \varlimsup_{n\to\infty} \frac{(A(n))}{n}$ the upper asymptotic density of A .
If $dA = \lim_{n\to\infty} \frac{|A(n)|}{n}$ exists, then we call dA the asymptotic density of A .

Erdös sets can be nicely described in terms of sets of multiples. The set of multiples of A is

$$M(A) = \{m \in \mathbb{N} : a|m \text{ for some } a \in A\}$$

and the set of non–multiples of A is

$$N(A) = \mathbb{N} \setminus M(A).$$

Thus $\mathbb{E}(n,k) = M(\{p_1, \dots, p_k\}) \cap <1, n>$ and also for any finite $A = \{a_1, \dots, a_t\} \subset \mathbb{N}$ and $a = \prod_{i=1}^{t} a_i$ $N(A) \cap <1, a>$ the set of integers in $<1, a>$ not divisible by any member of A. Already Dirichlet knew that

$$|N(A) \cap <1, a>| = a \prod_{i=1}^{t} (1 - \frac{1}{a_i}),$$

if the elements of A are pairwise relatively prime.

For general A by inclusion–exclusion

$$|N(A) \cap <1, a>| = a(1 - \sum_{i=1}^{t} \frac{1}{a_i} + \sum_{i<j} \frac{1}{[a_i, a_j]} - \dots)$$

and therefore

$$dN(A) = 1 - \sum_{i=1}^{t} \frac{1}{a_i} + \sum_{i<j} \frac{1}{[a_i, a_j]} - \dots \quad . \tag{1.5}$$

2. The main results

It is convenient to introduce the family $\mathcal{S}(n,k,s)$ of all subsets of $\mathbb{N}_s(n)$ no $k+1$ elements of which are pairwise relatively prime. In case $s = 1$ we also write $\mathcal{S}(n,k)$ and $\mathcal{S}(\infty, k)$ in the unrestricted case $n = \infty$.

Theorem 1A.

$$\sup_{A \in \mathcal{S}(\infty,k)} \underline{d}A = d\mathbb{E}(\infty, k) = 1 - \prod_{i=1}^{k} (1 - \frac{1}{p_i}).$$

Theorem 1B.

$$\lim_{n \to \infty} \frac{f(n,k)}{|\mathbb{E}(n,k)|} = 1 \quad \textit{for every} \quad k \in \mathbb{N}.$$

Theorem 1. *For every* $k \in \mathbb{N}$ *there is an* $n(k)$ *such that* $f(n,k) = |\mathbb{E}(n,k)|$ *for all* $n > n(k)$ *and the optimal set is unique.*

After the example of [1] this is the strongest statement one can hope for.

A key tool in the proof of Theorem 1 is a combinatorial result of independent interest. For a subfamily $\mathcal{A} \subset \binom{[m]}{\ell}$, that is a set of ℓ –element subsets of an m –element set, the (lower) shadow $\Delta\mathcal{A}$ is defined by $\Delta\mathcal{A} = \{B \in \binom{[m]}{\ell-1} : B \subset A$ for some $A \in \mathcal{A}\}$ and the (upper) shadow of $B \subset \binom{[m]}{\ell-1})$ is $\delta\mathcal{B} = \{A \in \binom{[m]}{\ell}) : B \subset A$ for some $B \in \mathcal{B}\}$.

With any function $g : \mathcal{A} \to \mathbb{R}^+$ we associate the function $h : \Delta\mathcal{A} \to \mathbb{R}^+$, where $h(B) = \max\limits_{A \in \delta\{B\} \cap \mathcal{A}} g(A)$.

Theorem 2. *Let* $\mathcal{A} \subset \binom{[m]}{\ell}$ *have the property that no* $k+1$ *elements of* $\mathcal{A}$ *are disjoint. Then for any function* $g : \mathcal{A} \to \mathbb{R}^+$ *and its associated function* $h : \Delta\mathcal{A} \to \mathbb{R}^+$ *(defined as above)*

$$\sum_{B \in \Delta\mathcal{A}} h(B) \geq \frac{1}{k} \sum_{A \in \mathcal{A}} g(A).$$

In particular

$$|\Delta\mathcal{A}| \geq \frac{1}{k} |\mathcal{A}|.$$

Eventhough Therem 1A follows now from Theorem 1, we give our original proof, because it is much simpler than that of Theorem 1, which is based on Theorem 2.

It also shows how the ideas developped. The original proof of Theorem 1B is not based on Theorem 2, but since it is rather technical, it is not presented in this paper.

It should be mentioned, however, that Theorem 1B implies

$$\sup_{A \in \mathcal{S}(\infty,k)} \overline{d}A = \sup_{A \in \mathcal{S}(\infty,k)} \underline{d}A = \sup_{A \in \mathcal{S}(\infty,k)} dA.$$

Finally we remark that inspection of our methods and proofs shows that they apply also to the general case of $f(n,k,s)$ for $s > 1$. Only some extra notation is needed. Therefore we just state the results.

Theorem 1'. *For every* $k, s \in \mathbb{N}$ *there exists an* $n(k,s)$ *such that for all* $n \geq n(k,s)$

$$|\mathbb{E}(n,k,s)| = f(n,k,s)$$

and this optimal set is unique.

3. Reduction to left compressed sets

The operation "pushing to the left" is frequently used in extremal set theory, but to our surprise seems not to be as popular in combinatorial number theory, perhaps because its usefullness is less obvious. Anyhow, our first (but not only) idea is to exploit it.

Definition 1. *$A \subset \mathbb{N}_s$ is said to be "left compressed", if for any $a \in A$ of the form*

$$a = p_r^i \cdot a_1, \ (a_1, p_r) = 1$$

and any p_ℓ of the form

$$p_s \le p_\ell < p_r, \ (p_\ell, a_1) = 1$$

it follows that $a^* = p_\ell^i \cdot a_1 \in A$ as well.
For any $n \in \mathbb{N} \cup \{\infty\}$ we denote the family of all left compressed sets from $\mathcal{S}(n,k,s)$ by $\mathcal{C}(n,k,s)$.

Lemma 1. *For $n \in \mathbb{N}$*

$$\max_{A \in \mathcal{S}(n,k,s)} |A| = \max_{A \in \mathcal{C}(n,k,s)} |A| = f(n,k,s).$$

Proof: For any $A \in \mathcal{S}(n,k,s)$ and $p_s \le p_\ell < p_r$ we consider the partition of A

$$A = A^1 \dot\cup A^2 \dot\cup A^0,$$

where

$$\begin{aligned} A^1 &= \{a \in A : a = p_r^i \cdot a_1 (i \ge 1), \ (a_1, p_r p_\ell) = 1; \ p_\ell^i \cdot a_1 \in A\}, \\ A^2 &= \{a \in A : a = p_r^i \cdot a_1 (i \ge 1), \ (a_1, p_r p_\ell) = 1; \ p_\ell^i \cdot a_1 \notin A\}, \\ A^0 &= A \setminus (A^1 \cup A^2). \end{aligned}$$

Define $A_*^2 = \{u \in \mathbb{N}_s : u = p_\ell^i \cdot a_1, \ p_r^i \ a_1 \in A^2\}$ and notice that by our definitions $A_*^2 \subset \mathbb{N}_s(n)$. Consider now $A^* = (A \cup A_*^2) \setminus A^2$ and observe that $|A^*| = |A|$ and also that $A^* \in \mathcal{S}(n,k,s)$.

Finitely many iterations of this procedure to primes $p_s \le p_\ell < p_r$ give the result.

The operation which led from A to A^* can be denoted by $L_{s,\ell,r}$. This is a "left pushing" operation:

$$A^* = L_{s,\ell,r}(A).$$

Moreover, by countably many left pushing operations one can transform every $A \in \mathcal{S}(\infty, s)$ into a left compressed set A' such that

$$|A(n)| \le |A'(n)| \tag{3.1}$$

and therefore also that

$$\underline{d}A \le \underline{d}A', \ \underline{d}A \le \underline{d}A'. \tag{3.2}$$

For the left compressed sets $\mathcal{C}(\infty,k)$ in $\mathcal{S}(\infty,k)$ we have thus shown the following.

Lemma 2.

$$\sup_{B\in\mathcal{S}(\infty,n)} \underline{d}B = \sup_{B\in\mathcal{C}(\infty,n)} \underline{d}B$$

and

$$\sup_{B\in\mathcal{S}(\infty,n)} \overline{d}B = \sup_{B\in\mathcal{C}(\infty,n)} \overline{d}B.$$

Next we mention two useful observations.

Any optimal $B \in \mathcal{S}(n,k,s)$, that is $|B| = f(n,k,s)$, is an "upset":

$$B = M(B) \cap \mathbb{N}_s(n) \tag{3.3}$$

and it is also a "downset" in the following sense:

$$b \in B, b = q_1^{\alpha_1} \cdots q_t^{\alpha_t}, \alpha_i \geq 1 \Rightarrow b' = q_1 \dots q_t \in B. \tag{3.4}$$

Finally we introduce for any $B \subset \mathbb{N}$ the unique primitive subset $P(B)$, which has the properties

$$b_1, b_2 \in P(B) \Rightarrow b_1 \nmid b_2 \text{ and } B \subset M(P(B)). \tag{3.5}$$

We know from (3.4) that for an optimal $B \in \mathcal{S}(n,k,s)$ $P(B)$ consists only of squarefree integers.

Remark 1: We could use also the following concept of left compressedness:

Definition 2. $A \subset \mathbb{N}_s$ *is left compressed, if for any* $a \in A$ *of the form*

$$a = p_i^{\alpha_i} \cdot a_1, \alpha_i \geq 1, (a_1, p_i) = 1$$

it follows that for any p_j , $p_s \leq p_j < p_i$, *in case* $\alpha_i \geq 2$

$$a^* = p_j \cdot p_i^{\alpha_i - 1} a_1 \in A$$

and in case $\alpha_i = 1$

$$a^* = p_j \cdot a_1 \in A, \quad \textit{if } (a_1, p_j) = 1.$$

While the two definitions are different in general, it can be easily seen, that if the considered set $A \subset \mathbb{N}_s$ is also "upset" and "downset", then both definitions of left compressedness coincide.

Besicovitch has shown in the thirties (see [9]) that $M(A)$ need not have a density for general A . Erdös [15] has given a characterisation for sets A for which $dM(A)$ exists.

Here we have the following

Conjectures. *The set of multiples* $M(A)$ *of any left compressed set* A *(in the sense of Definition 2) possesses asymptotic density. We conjecture this even for left compressed sets in the sense of Definition 1.*

Moreover, we think that even a stronger statement is true. For any left compressed set A *in the sense of Definition 1 or 2* dA *exists.*

4. Proof of Theorem 1A

We remind the reader of the abbreviations $f(n,k)$, $\mathbb{E}(n,k)$, $\mathbb{N}(n)$, $\mathcal{S}(n,k)$, $\mathcal{C}(n,k)$ for $f(n,k,1)$, $\mathbb{E}(n,k,1)$, $\mathbb{N}_1(k)$, $\mathcal{S}(n,k,1)$, and $\mathcal{C}(n,k,1)$ resp. We also introduce

$$\mathcal{O}(n,k) = \{B \in \mathcal{S}(n,k) : |B| = f(n,k)\}. \tag{4.1}$$

By the remarks at the end of Section 3 we know that for $A \in \mathcal{O}(n,k)$ we have **properties (I):**

(a) $P(A) \subset \mathbb{N}^*$, the set of squarefree numbers

(b) $A = M(P(A)) \cap \mathbb{N}(n)$.

We also know from Lemma 1 that

(c) $\mathcal{O}(n,k) \cap \mathcal{C}(n,k) \neq \varnothing$.

For infinite sets $A \subset \mathbb{N}$ we choose the lower asymptotic density $\underline{d}A$ as a measure and define

$$\mathcal{O}(\infty,k) = \{A \in \mathcal{S}(\infty,k) : \underline{d}A = \sup_{B \in \mathcal{S}(\infty,k)} \underline{d}B\}, \tag{4.2}$$

which is not automatically non–empty. $\mathcal{C}(\infty,k)$ are the left compressed sets in $\mathcal{S}(\infty,k)$. Again it suffices to look at $A \in \mathcal{C}(\infty,k)$ with the properties

(a) $P(A) \subset \mathbb{N}^*$

(b) $A = M(P(A))$.

Sets of multiples have been studied intensively in the thirties (c.f. Halberstam and Roth [12]).

Let $P(A) = \{a_1, a_2, \dots\}$, where the elements are written in the usual lexicographical (or alternatively in natural) order. It is easy to show (see [12]) that

$$\underline{d}M(P(A)) = \sum_{i=1}^{\infty} b^{(i)}, \tag{4.3}$$

where

$$b^{(i)} = \frac{1}{a_i} - \sum_{j<i} \frac{1}{[a_j, a_i]} + \dots \tag{4.4}$$

is the density of the set $B^{(i)}$ of those integers in $M(P(A))$, which are divisible by a_i and not by $a_1, a_2, \dots,$ or a_{i-1} . We can say more about $b^{(i)}$, if we use the prime number factorization of the squarefree numbers a_i .

Lemma 3. *Let* $a_i = q_1 \dots q_r,\ q_1 < q_2 < \dots < q_r$ *and* $q_j \in \mathbb{P}$ *for* $j = 1,2,\dots,r$. *Then*

(i) $B^{(i)} = \{n \in \mathbb{N} : n = q_1^{\alpha_1} \cdots q_r^{\alpha_r} \cdot q$ *with* $\alpha_j \geq 1,\ (q, \prod_{p \leq q_r} p) = 1\}$

(ii) $dB^{(i)} = b^{(i)} = \frac{1}{(q_1-1)\cdots(q_r-1)} \prod_{p \leq q_r} (1 - \frac{1}{p})$.

Proof: Since A is left compressed and $P(A)$ is written in lexicographical order q is of the described form and (i) holds.

To verify (ii) just observe that from (1.6)

$$\begin{aligned} dB^{(i)} &= \sum_{\alpha_j \geq 1} \frac{1}{q_1^{\alpha_1} \cdots q_r^{\alpha_r}} \prod_{q \leq q_r} (1 - \frac{1}{p}) \\ &= \prod_{p \leq q_r} (1 - \frac{1}{p}) \sum_{\alpha_1 = 1}^{\infty} \frac{1}{q_1^{\alpha_1}} \sum_{\alpha_2 = 1}^{\infty} \frac{1}{q_2^{\alpha_2}} \cdots \sum_{\alpha_r = 1}^{\infty} \frac{1}{q_r^{\alpha_r}} \\ &= \prod_{p \leq q_r} (1 - \frac{1}{p}) \frac{1}{(q_1 - 1) \cdots (q_r - 1)}. \end{aligned}$$

We are now ready to prove Theorem 1A.

Suppose to the contrary that there exists an $A \in \mathcal{S}(\infty, k)$ with

$$\underline{d}A > 1 - \prod_{j=1}^{k} (1 - \frac{1}{p_j}).$$

We know already that we can assume $A \in \mathcal{C}(\infty, k)$, $P(A) \subset \mathbb{N}^*$, $M(P(A)) = A$ and that $P(A) = \{a_1, a_2, \dots\}$ is in lexicographical order.
By

$$\sum_{i=1}^{\infty} b^{(i)} > 1 - \prod_{j=1}^{k} (1 - \frac{1}{p_j}) \tag{4.3}$$

and hence for a suitable $m(A)$ also

$$\sum_{i=1}^{m} b^{(i)} > 1 - \prod_{j=1}^{k} (1 - \frac{1}{p_j}) \quad \text{for} \quad m \geq m(A).$$

We can consider therefore $A' = M(\{a_1, \dots, a_m\})$, because $A' \in \mathcal{S}(\infty, k)$ and still

$$\underline{d}A' = dA' = \sum_{i=1}^{m} b^{(i)} > 1 - \prod_{j=1}^{k} (1 - \frac{1}{p_j}). \tag{4.5}$$

Write $P(A') = \{a_1, \dots, a_m\}$ in the form

$$P(A') = R_1 \dot{\cup} R_2 \dot{\cup} \cdots \dot{\cup} R_t, \tag{4.6}$$

where R_s is the set of all a_j's with greatest prime factor $p^+(a_j) = p_s$. Notice that in case $t > k$ we have by left compressedness that necessarily $p_t \notin A'$ and also $p_t \notin R_t$, because otherwise $A' \notin \mathcal{S}(\infty, k)$. Hence

$$dM\ (P(A')) = \sum_{i=1}^{m} b^{(i)} = \sum_{s=1}^{t} \tau(R_s),$$

where

$$(4.7) \qquad \tau(R_s) = \sum_{\substack{a=q_1\cdots q_r p_s\in R_s\\ q_1<\cdots<q_r<p_s}} \frac{1}{(q_1-1)\cdots(q_r-1)(p_s-1)} \prod_{i=1}^{s} (1-\frac{1}{p_i}).$$

We consider now $R_t = \{a_\ell, a_{\ell+1}, \cdots, a_m\}$ for some $\ell \le m$.
We have

$$(4.8) \qquad \tau(R_t) = \sum_{i=\ell}^{m} b^{(i)}.$$

By the pigeon–hole principle there exists a subset $R_t' = \{a_{i_1}, \dots, a_{i_1}\} \subset R_t$ such that

$$(4.9) \qquad \sum_{j=1}^{r} b^{(i_j)} \ge \frac{\tau(R_t)}{t-1} \text{ and } (\frac{a_{i_1}}{p_t}, \dots, \frac{a_{i_r}}{p_t}) > 1.$$

Now we replace the set A' by the set $A'' = M(R_1 \cup \cdots \cup R_{t-1} \cup R_t'')$, where

$$R_t'' = \Big\{\frac{a_{i_j}}{p_t} : a_{i_j} \in R_j'\Big\}.$$

One readily verifies that $A'' \in \mathcal{C}(\infty, k)$.

We estimate now dA'' from below. The contribution of every element $\frac{a_{i_j}}{p_t} \in R_t''$ to $M(R_1 \cup \cdots \cup R_{t-1} \cup R_t'') \setminus M(R_1 \cup \cdots \cup R_{t-1})$ are the elements in the form $u = q_1^{\beta_1} \cdots q_r^{\beta_r} \cdot q$, where $a_{i_j} = q_1 \cdots q_r \ p_t, \beta_j \ge 1$, and $(q, \prod_{i=1}^{t} p_i) = 1$.

The density of this set of integers equals

$$b^{''(i_j)} = \frac{1}{(q_1-1)\dots(q_r-1)} \prod_{i=1}^{t} (1-\frac{1}{p_i})$$

and hence

$$b^{''(i_j)} = (p_t - 1)\ b^{(i_j)}.$$

Therefore, using (4.9) we have

$$dA'' \ge \sum_{s=1}^{t-1} \tau(R_s) + (p_t - 1)\ \frac{\tau(R_t)}{t-1} > \sum_{s=1}^{t} \tau(R_s) = dA', \quad \text{because } \ p_t > t.$$

We notice that $P(A'') \subseteq R_1 \cup \cdots \cup R_{t-1} \cup R_t''$ and hence

$$\max_{a \in P(A'')} p^+(a) \le p_{t-1}.$$

Continuing this procedure we arrive after finitely many steps at the set $M(\{p_1, \dots, p_k\})$ and by (4.5) to the statement that its density $1 - \prod_{i=1}^{k} (1 - \frac{1}{p_i})$ must be bigger than itself.
This proves that

$$\max_{B \in \mathcal{S}(\infty,k)} \underline{d}B = d\mathbb{E}(\infty, k).$$

5. A finite version of Lemma 3

We work now in $\mathbb{N}(n)$ and need sharper estimates on cardinalities than just bounds on densities. It suffices to consider $A \in \mathcal{C}(n,k) \cap \mathcal{O}(n,k)$. We know that $P(A) = \{a_1 < a_2 < \ldots < a_m\} \subset \mathbb{N}^*$ and that $A = M(P(A)) \cap \mathbb{N}(n)$. Define $B^{(i)}(n) = \{u \in \mathbb{N}(n) : a_i | u$ and $a_j \nmid u$ for $j = 1, \ldots, i-1\}$ and write

$$A = \bigcup_{i=1}^{m} B^{(i)}(n). \tag{5.1}$$

Lemma 4. *Let* $a_i = q_1, \ldots, q_r,\ q_1 < q_2 < \ldots < q_r$ *with* $q_j \in \mathbb{P}$.
Then

(i) $B^{(i)}(n) = \Big\{u \in \mathbb{N}(n) : u = q_1^{\alpha_1} \ldots q_r^{\alpha_r} \cdot T,\ \alpha_i \geq 1$ *and* $(T, \prod\limits_{p \leq q_r} p) = 1\Big\}$.

(ii) $\lim\limits_{n \to \infty} \frac{|B^{(i)}(n)|}{n} = \frac{1}{(q_1-1)\ldots(q_r-1)} \cdot \prod\limits_{p \leq q_r} (1 - \frac{1}{p})$.

(iii) For every $\epsilon > 0$, *every* $h \in \mathbb{N}$ *and every* $a_i = q_1 \ldots q_r,\ q_1 < q_2 < \ldots < q_r \leq p_h$ *there exists an* $n(h,\epsilon)$ *such that for* $n > n(h,\epsilon)$ *we have*

$$(1-\epsilon)\ n \cdot \frac{1}{(q_1-1)\ldots(q_r-1)} \prod_{p \leq q_r} (1 - \frac{1}{p}) < |B^{(i)}(n)|$$
$$< (1+\epsilon) n \cdot \frac{1}{(q_1-1)\ldots(q_r-1)} \cdot \prod_{p \leq q_r} (1 - \frac{1}{p}).$$

Proof: (i) immediately follows from the facts that A is compressed, "upset" and "downset".

(ii) We know that for $m \in \mathbb{N}$

$$d\ \mathbb{N}_m = \prod_{p \leq p_m} (1 - \frac{1}{p})$$

and hence

$$\lim_{n \to \infty} \frac{|B^{(i)}(n)|}{n} = \sum_{\alpha_i \geq 1} \frac{1}{q_1^{\alpha_1} \ldots q_r^{\alpha_r}} \cdot \prod_{p \leq q_r} (1 - \frac{1}{p}) = \frac{1}{(q_1-1)\ldots(q_r-1)} \cdot \prod_{p \leq q_r} (1 - \frac{1}{p}).$$

(iii) follows from (ii), because the constant number of sequences converges uniformly.

6. Combinatorial result for shadows and a proof of Theorem 2

For $\mathcal{A} \subset \binom{[m]}{\ell}$ and $\mathcal{B} \subset \binom{[m]}{\ell-1}$ the lower shadow $\Delta\, \mathcal{A}$ and the upper shadow $\delta\, \mathcal{B}$ were defined in Section 2.

We begin with a special case of Theorem 2.

Lemma 5. *Let* $\mathcal{A} \subset \binom{[m]}{\ell}$ *have the property that no* $k+1$ *of its members are pairwise disjoint, then*

$$|\Delta\ \mathcal{A}| \geq \frac{1}{k}\ |\mathcal{A}|.$$

Proof: The standard left pushing operation preserves the "no $k+1$ disjoint"–property and only can decrease the shadow. We can assume therefore that $\mathcal{A}$ is left–compressed.

We distinguish two cases.

Case $\mathbf{m \leq (k+1)\ell - 1}$

Counting pairs $(A;B)$ with $B \subset A$ in two ways we get

$$|\Delta\ \mathcal{A}|\ \geq\ \frac{\ell}{m-\ell+1}\ |\mathcal{A}|\ \geq\ \frac{\ell}{(k+1)\ell-1-\ell+1}\ |\mathcal{A}|\ =\ \frac{1}{k}\ |\mathcal{A}|.$$

Case $\mathbf{m \geq (k+1)\ell}$

We consider the following partition of $< 1,m >$:

$$\begin{aligned}&I_1 =< 1,k >,\ I_2 =< k+1, 2k+1 >, \dots ,\ I_j =< (j-1)(k+1),\ j(k+1)-1 >, \dots ,\\ &I_\ell =< (\ell-1)(k+1),\ \ell(k+1)-1 >,\ I_{\ell+1}, =< \ell(k+1), m > .\end{aligned}$$

At first we show that for every $A \in \mathcal{A}$ there exists an index $j, 1 \leq j \leq \ell$, for which

$$|A \cap (I_1 \cup I_2 \cup \ldots \cup I_j)| = j. \tag{6.1}$$

To see this, let us assume to the opposite that it does not hold for some $A \in \mathcal{A}$. Then necessarily $|A \cap I_{\ell+1}| \geq 1$, because otherwise $|A \cap (I_1 \cup \ldots \cap I_\ell| = \ell$ since $|A| = \ell$. Therefore we must have $|A \cap (I_1 \cup \ldots \cup I_\ell| \leq \ell - 1$ and a fortiori $|A \cap (I_1 \cup \ldots \cup I_{\ell-1})| \leq \ell - 2,\ |A \cap (I_1 \cup \ldots \cup I_{\ell-2}| \leq \ell - 3, \dots , |A \cap (I_1 \cup I_2)| \leq 1,\ |A \cap I_1| = 0$.

However, since $\mathcal{A}$ is also left compressed, we can choose then $k+1$ elements from $\mathcal{A}$ (including A), which are pairwise disjoint. This contradicts our assumption on $\mathcal{A}$.

Now, for every $A \in \mathcal{A}$ define $j_A,\ 1 \leq j_A \leq \ell$, as the largest index j for which (6.1) holds. This can be used to partition $\mathcal{A}$ into disjoint subsets:

$$\mathcal{A} = \dot{\bigcup_{i=1}^{\ell}} \mathcal{A}_i, \quad \text{where} \quad \mathcal{A}_i = \{A \in \mathcal{A} : j_A = i\}. \tag{6.2}$$

Some of the subsets may be empty. Consider now the shadows $\Delta\ \mathcal{A}_i \quad (1 \leq i \leq \ell)$ and its sub–shadows $\Delta^* \mathcal{A}_i = \{B \in \Delta\ \mathcal{A}_i : |B \cap (I_1 \cup \ldots \cup I_i)| = i-1\}$.

It follows immediately from the definition of the $\mathcal{A}_i$ that

$$\Delta^*\ \mathcal{A}_{i_1} \cap \Delta^* \mathcal{A}_{i_2} = \emptyset \ \text{ for all } \ i_1 \neq i_2. \tag{6.3}$$

Moreover, using left compressedness of $\mathcal{A}$ it can be shown easily that

$$\Delta\ \mathcal{A} = \bigcup_{i=1}^{\ell} \Delta^* \mathcal{A}_i. \tag{6.4}$$

In the light of (6.2), (6.3), and (6.4) it suffices to show that

$$|\Delta^* \mathcal{A}_i| \geq \frac{1}{k}|\mathcal{A}_i| \ \text{ for } \ i = 1, 2, \dots, \ell. \tag{6.5}$$

We look therefore for fixed i at the intersections

$$\mathcal{U}_i = \{A \cap (I_1 \cup \ldots \cup I_i) : A \in \mathcal{A}_i\}$$

and partition $\mathcal{A}_i$ as follows:

$$\mathcal{A}_i = \dot{\bigcup_{U \in \mathcal{U}_i}} \mathcal{A}_i^U, \ \mathcal{A}_i^U = \{A \in \mathcal{A}_i : A \cap (I_1 \cap \ldots \cap I_i) = U\}. \tag{6.6}$$

Also, we introduce the intersections

$$\mathcal{V}_i = \{B \cap (I_1 \cup \ldots \cup I_i) = B \in \Delta^* \mathcal{A}_i\}$$

and partition $\Delta^* \mathcal{A}_i$ as follows:

$$\Delta^* \mathcal{A}_i = \dot{\bigcup_{V \in \mathcal{V}_i}} (\Delta^* \mathcal{A}_i)^V, \ (\Delta^* \mathcal{A}_i)^V = \{B \in \Delta^* \mathcal{A}_i : B \cap (I_1 \cup \ldots \cup I_i) = V\}. \tag{6.7}$$

Now counting for the Δ^* –operation pairs again in two ways we get the inequality

$$i \cdot \sum_{U \in \mathcal{U}_i} |\mathcal{A}_i^U| \leq \sum_{V \in \mathcal{V}_i} (i(k+1) - 1 - (i-1))| \ (\Delta^* \mathcal{A}_i)^V| \ \leq \ ik \sum_{V \in \mathcal{V}_i} |(\Delta^* \mathcal{A}_i)^V|.$$

Together with (6.6) and (6.7) it implies (6.5).

The next result is for a more general structure. It enables us to get immediately Theorem 2 from Lemma 5. Let $G = (V, W, E)$ be a bipartite graph. With $\sigma(S)$ for the set of vertices adjacent to vertex s and $\sigma(s)$ for the set of vertices adjacent to vertices in S. We assume that

$$\sigma(V) = W.$$

Lemma 6. *Suppose that for some* $\alpha \in \mathbb{R}^+$ *we have for every* $S \subset V$

$$|S| \leq \ \alpha|\sigma(s)|, \tag{6.8}$$

then for every function $g : V \to \mathbb{R}^+$ *and associated function* $h : W \to \mathbb{R}^+$ *, where* $h(b) = \max\limits_{a \in \sigma(b)} g(a)$ *for all* $b \in W$ *,*

$$\sum_{a \in V} g(a) \leq \ \alpha \sum_{b \in W} \ h(b) \tag{6.9}$$

holds.

Proof: Let $\{\gamma_1 < \gamma_2 < \ldots < \gamma_r\}$ be the range of g. Then we have the partition $V = V_1 \dot{\cup} \ldots \dot{\cup} V_r$, where

$$V_i = \{v \in V : g(v) = \gamma_i\}, \ 1 \leq i \leq r.$$

Clearly

$$\sum_{a\in V} g(a) = \sum_{i=1}^{r} \gamma_i \ |V_i|. \tag{6.10}$$

By the definition of h obviously

$$h(b) = \gamma_r \ \text{ for all } \ b \in \sigma(V_r). \tag{6.11}$$

We proceed now by induction on r .

$r = 1$ **:** Here $h(b) = \gamma_1$ for all $b \in W$ and hence by (6.8)

$$\sum_{a\in V} g(a) = \gamma_1 \cdot |V| \le \gamma_1 \cdot \alpha \cdot |W| = \alpha \cdot \sum_{b\in W} h(b).$$

$r-1 \to r$ **:** We assume that (6.9) holds for every function $g' : V \to \mathbb{R}^+$ with $r-1$ different values.

With our g under consideration we associate the function $g^* : V \to \mathbb{R}^+$ defined by

$$g^*(a) = \begin{cases} \gamma_i & \text{for } \ a \in V_i, \ i \le r-1 \\ \gamma_{r-1} & \text{for } \ a \in V_r. \end{cases}$$

Denote by $h^* : W \to \mathbb{R}^+$ the usual function corresponding to g^* . We verify that

$$\sum_{a\in V} g(a) = \sum_{a\in V} g^*(a) + (\gamma_r - \gamma_{r-1})|V_r|, \tag{6.12}$$

$$\sum_{b\in W} h(b) = \sum_{b\in W} h^*(b) + (\gamma_r - \gamma_{r-1})|\sigma(V_r)|. \tag{6.13}$$

From the condition (6.8) and the induction hypothesis applying to g^* we know that

$$|V_r| \le \alpha|\sigma(V_r)| \ \text{ and } \ \sum_{a\in V} g^*(a) \le \alpha \sum_{b\in W} h^*(b).$$

These inequalities and (6.12), (6.13) give (6.9).

Proof of Theorem 2: Consider $G = (V, W, E) = (\mathcal{A}, \Delta\mathcal{A}, E)$, where $(A; B) \in E$ iff $A \supset B$, and $\mathcal{A}$ satisfies the hypothesis of Theorem 2 and hence also of Lemma 5. Since every subfamily $\mathcal{A}' \subset \mathcal{A}$ also satisfies this hypothesis, we know that

$$|\Delta\mathcal{A}'| \ge \frac{1}{k} \ |\mathcal{A}'|. \tag{6.14}$$

Since $\Delta\mathcal{A}' = \sigma(\mathcal{A}')$ (6.14) guarantees (6.8) for $\alpha = k$.

The conclusion (6.9) says now

$$\sum_{A\in\mathcal{A}} g(A) \le k \sum_{A\in\Delta\mathcal{A}} h(A)$$

and Theorem 2 is established.

Remark 2: One might consider instead of the (maximal) associated function h an (average) associated function $\bar{h}:\Delta\mathcal{A}\to\mathbb{R}^+$, where $\bar{h}(B)=|\delta(B)\cap\mathcal{A}|^{-1}\sum\limits_{A\in\delta(B)\cap\mathcal{A}} g(A)$.

Obviously $h(B)\ge\bar{h}(B)$ for all $B\in\Delta\mathcal{A}$.

While for the case $m\le(k+1)\ell-1$ one can replace h by $\bar{h}$ in Theorem 2. This is not possible in general.

Example 1: (h cannot be replaced by $\bar{h}$ in Theorem 2)

Choose $m=6,\ \ell=3$, and $k=1$ and define

$$\begin{aligned}\mathcal{A}=\{&\{1,2,3\},\ \{1,2,4\},\ \{1,2,5\},\ \{1,2,6\}\}\cup\{\{1,3,4\},\ \{1,3,5\},\ \{1,3,6\}\}\\ &\cup\{\{2,3,,4\},\ \{2,3,5\},\ \{2,3,6\}\}.\end{aligned}$$

No two sets in $\mathcal{A}$ are disjoint and $\mathcal{A}$ is left compressed. Choose

$$g(A)=\begin{cases}1 & \text{for } A=\{1,2,3\}\\ 0 & \text{otherwise}\end{cases}$$

and use the notation $f(\mathcal{C})=\sum\limits_{c\in\mathcal{C}} f(C)$.

Then $\frac{1}{k}\,g(\mathcal{A})=g(\mathcal{A})>\bar{h}(\Delta\mathcal{A})$, because $|\delta(\{1,2\})\cap\mathcal{A}|=|\delta(\{1,3\})\cap\mathcal{A}|=|\delta(\{2,3\})\cap\mathcal{A}|=4$, and thus

$$\bar{h}(\Delta\mathcal{A})=3\cdot\frac{1}{4}<g(\mathcal{A})=1.$$

7. A numbertheoretical consequence of Theorem 2

We present now a basic new auxiliary result for every $S\in\mathcal{C}(n,k)$ with properties (I) in Section 4. S need not be optimal, that is, it can be in $\mathcal{C}(n,k)\setminus\mathcal{O}(n,k)$. Define

(7.1) $$S_i=\{d\in S: p_i|d,\quad\text{but}\quad (p_1\dots p_{i-1},d)=1\}.$$

Clearly,

(7.2) $$S_i\cap S_i=\phi(i\ne j)\quad\text{and}\quad S=\dot{\bigcup_{i\ge1}}\,S_i.$$

Lemma 7. *For every* $k, n \in \mathbb{N}$ *and every* $S \in \mathcal{C}(n,k)$ *with properties (I) we have*

(i) $|S_r| \geq \frac{1}{k} \sum\limits_{i \geq r+1} |S_i)|$ *for every* $r \in \mathbb{N}$

(ii) For every $\alpha \in \mathbb{R}^+$ *and for* $k(\alpha) \geq k \cdot \alpha$ *(independent of* n *!)*

$$\sum_{i=1}^{k(\alpha)} |S_{k+i}| \geq \alpha \sum_{j \geq k+k(\alpha)+1} |S_j|.$$

Proof: (ii) follows from (i), so we have to prove (i).

We consider the set $\underset{i \geq r+1}{\cup} S_i$ and let for every $\ell \in \mathbb{N}$

(7.3) $T_\ell = \{d \in \underset{i \geq r+1}{\cup} S_i : d$ has exactly ℓ different primes in its factorization $\}$.

Obviously

(7.4) $$\underset{i \geq r+1}{\dot{\cup}} S_i = \underset{\ell \geq 1}{\dot{\cup}} T_\ell$$

and for $d \in T_\ell$

(7.5) $$d = q_1^{\beta_1} \dots q_\ell^{\beta_\ell}, \; p_r < q_1 < \dots < q_\ell; \; \beta_i \geq 1.$$

Since $S \in \mathcal{C}(n,k)$, we have

(7.6) $$d_i = p_r^{\beta_i} \; q_1^{\beta_1} \dots q_{i-1}^{\beta_{i-1}} \; q_{i+1}^{\beta_{i+1}} \dots q_\ell^{\beta_\ell} \in S_r \text{ for } i = 1, 2, \dots, \ell.$$

Define

(7.7) $$\sigma(d) = \{d_1, \dots, d_\ell\} \text{ and } \sigma(T_\ell) = \underset{d \in T_\ell}{\cup} \sigma(d).$$

Since $\sigma(T_\ell) \subset S_r$ and $\sigma(T_\ell) \cap \sigma(T_{\ell'}) = \phi (\ell \neq \ell')$, sufficient for proving (i) is to show that

(7.8) $$|\sigma(T_\ell)| \geq \frac{1}{k} \, |T_\ell| \text{ for all } \ell \in \mathbb{N}.$$

Let $T_\ell^* = T_\ell \cap \mathbb{N}^*$ be the squarefree integers in T_ℓ . Then $\sigma(T_\ell^*) = \underset{d \in T_\ell^*}{\cup} \sigma(d)$ is the set of all squarefree integers of $\sigma(T_\ell)$.

For an $a \in T_\ell^*, \; a = x_1 \dots x_\ell, \; x_1 < \dots < x_\ell, \; x_i \in \mathbb{P}$ we consider

(7.9) $$T(a) = \{d \in S : d = x_1^{\beta_1} \dots x_\ell^{\beta_\ell}; \; \beta_i \geq 1\}$$

and for a $b \in \sigma(T_\ell^*), \; b = p_r \cdot y_1 \dots y_{\ell-1}$; $p_r < y_1 < \dots < y_{\ell-1}, \; y_i \in \mathbb{P}$, we consider

(7.10) $$U(b) = \{d \in S_r : d = p_r^{\gamma_\ell} \; y_1^{\gamma_1} \dots y_{\ell-1}^{\gamma_{\ell-1}}; \; \gamma_i \geq 1; \; y_1^{\gamma_1} \dots y_{\ell-1}^{\gamma_{\ell-1}} \cdot x^{\gamma_\ell} \in T_\ell \text{ for some } x \in \mathbb{P}\}.$$

It is clear that

$$T_\ell = \dot{\bigcup_{a \in T_\ell^*}} T(a) \ \text{ and } \ \sigma(T_\ell) = \dot{\bigcup_{b \in \sigma(T_\ell^*)}} U(b). \tag{7.11}$$

Next we observe that for any $b \in \sigma(T_\ell^*)$

$$|U(b)| = \max_{\frac{b}{p_r} \cdot x \in T_\ell^*} |T(\frac{b}{p_r} x)| \tag{7.12}$$

and this has brought us into the position to apply Theorem 2 to the sets $\mathcal{A} \sim T_\ell^*$ and $\Delta\ \mathcal{A} \sim \sigma(T_\ell^*)$, where " $\sim$ " is the canonical correspondence between squarefree numbers and subsets. We indicate the correspondence by using small and capital letters such as $a \sim A$.

We define $g : \mathcal{A} \to \mathbb{R}^+$ by

$$g(A) = |T(a)|. \tag{7.13}$$

The associated function $h : \Delta\ \mathcal{A} \to \mathbb{R}^+$ is defined by

$$h(B) = |U(b)|.$$

We see from (7.12) that this definition is appropriate.

Theorem 2 therefore yields (7.8) and thus (i).

8. Further auxiliary results

We state first the only auxiliary result, which is not derived in this paper and is not trivial.

It is the weaker version of De Bruijn's strengthening [3] of Buchstab's result [2], that can be found in [12].

Theorem. *For the function*

$$\phi(x,y) = |\{a \leq x : (a, \prod_{p<y} p) = 1\}| \tag{8.1}$$

there exist positive absolute constants c_1, c_2 *such that*

$$c_1\ x \prod_{p<y} (1 - \frac{1}{p}) \leq \phi(x,y) \leq c_2 \cdot x \prod_{p<y} (1 - \frac{1}{p}) \tag{8.2}$$

for all x, y *satisfying* $x \geq 2y \geq 4$ *.*

Furthermore, the right side inequality in (8.2) remains valid also for $x < 2y$ *.*

We need also

Lemma 8. *For positive constants* c_1, c_2, κ *there exists a* $t(c_1, c_2, \kappa)$ *such that for* $t > t(c_1, c_2, \kappa)$

$$\frac{c_1}{c_2} \cdot p_t \cdot \prod_{p \geq p_t} (1 - \frac{1}{p}) > \kappa.$$

Proof: Trivial.

Finally, we need a result on "bookkeeping".

We have two accounts at time 0 :

$x_0 = x$ and $y_0 = y$ where $x, y \in \mathbb{R}^+$.

In any step $i, i \geq 1$, we arbitrarily remove $a_i, b_i;\ 0 \leq a_i \leq x_{i-1},\ 0 \leq b_i \leq y_{i-1};$ and add $a_i^* \geq 0,\ b_i^* \geq 0$, where

$$a_i^* + b_i^* > \beta(a_i + b_i),\ \beta > 1.$$

The new accounts are

$$x_i = x_{i-1} - a_i + a_i^*,\ y_i = y_{i-1} - b_i + b_i^*.$$

Lemma 9. *If for some* $\ell \in \mathbb{N}$ *the account* $y_\ell = 0$ *(resp.* $x_\ell = 0$ *) occurs, then we have* $x_\ell > x + \beta y$ *(resp.* $y_\ell > y + \beta x$ *).*

Proof: Beginning with accounts x and y at the end the amount y has been removed and transferred to the first account with an increasing factor β .

9. Proof of Theorem 1

We can assume that — as in Section 7 — $S \in \mathcal{C}(n,k)$ satisfies (I) and additionally is also optimal, that is, $S \in \mathcal{O}(n,k)$. Define S_i as in (7.1) and recall (7.2). Notice also that $P(S) = P(S \cap \mathbb{N}^*)$. Equivalent to Theorem 1 is the statement that for big n always

(9.1) $$\bigcup_{i \geq k+1} S_i = \phi.$$

Henceforth we assume to the opposite that

(II) $$\bigcup_{i \geq k+1} S_i \neq \phi \text{ for infinitely many } n.$$

Let $k_0 \in \mathbb{N},\ k_o > k$ be an integer to be specified later.

By the disjointness property (7.1) we can write

(9.2) $$S^0 = S \setminus (\bigcup_{i \geq k_0+1} S_i) = (\bigcup_{i=1}^{k} S_i) \cup (\bigcup_{i=k+1}^{k_0} S_i).$$

From (i) in Lemma 7 we know that

$$\Big| \bigcup_{i=k+1}^{k_0} S_i \Big| \geq \frac{k_0 - k}{k} \Big|\bigcup_{i \geq k_o+1} S_i \Big|$$

and hence also that

$$|S| \leq |\bigcup_{i=1}^{k} S_i) + \gamma \cdot |\bigcup_{i=k+1}^{k_o} S_i|, \tag{9.3}$$

where $\gamma = 1 + \frac{k}{k_o - k}$.

Let $P(S^0)$ be the primitive subset of S^0 , which generates S^0 .

We notice that by the properties of S

$$P(S^0) \subset P(S), \tag{9.4}$$

because $d' \in P(S^0)$ and $d|d'$ for some $d \in S$ would by compressedness imply the existence of an $e' \in P(S^0)$ with $e'|d'$.

Let p_t be the largest prime occuring in any element of $P(S^0)$. In other words, $(p_t, d) = p_t$ for some $d \in P(S^0)$ and

$$(p_{t'}, d) = 1 \ \text{ for all } \ t' > t \ \text{ and all } \ d \in P(S^0). \tag{9.5}$$

By assumption (II) we have $p_t > p_k$.

We consider now

$$p^t(S^0) = \{a \in P(S^0) : (a, p_t) = p_t\}. \tag{9.6}$$

From Lemma 3 (i) we know that the contribution of every element $a \in P^t(S^0)$, $a = q_1 \dots q_r \cdot p_t$ and $q_1 < q_2 \dots < q_r < p_t$, to $M(P(S^0))$ is the set of integers

$$B(a) = \{u = q_1^{\alpha_1} \dots q_r^{\alpha_r} \cdot p_t^{\beta} \cdot Q : \alpha_i \geq 1, \ \beta \geq 1, \ (Q, \prod_{p \leq p_t} p)) = 1\}. \tag{9.7}$$

We use the abbreviation

$$L_t = \bigcup_{a \in p^t(S^0)} B(a). \tag{9.8}$$

We consider also the partition

$$P^t(S^0) = \dot{\bigcup_{1 \leq i \leq k_0}} P_i^t(S^0), \ P_i^t(S^0) = P^t(S^0) \cap S_i. \tag{9.9}$$

By the pigeon–hole principle for some $\ell, \ 1 \leq \ell \leq k_0$,

$$|\bigcup_{a \in P_\ell^t(S^0)} B(a)| \ \geq \ \frac{|L_t|}{k_0}, \ \text{ if } \ t > k_0 \tag{9.10}$$

and for some $\ell, \ 1 \leq \ell \leq t-1$,

$$|\bigcup_{a \in P_\ell^t(S^0)} B(a)| \ \leq \ \frac{|L_t|}{t-1}, \ \text{ if } \ k < t \leq k_0. \tag{9.11}$$

Basic transformation

We consider for this ℓ corresponding to t the set (of squarefree numbers)

$$\widetilde{P}(S^0) = (P(S^0) \setminus P^t(S^0)) \cup R_\ell^t(S^0), \tag{9.12}$$

where

$$R_\ell^t(S^0) = \{u \in \mathbb{N} : u \cdot p_t \in P_\ell^t(S^0)\}. \tag{9.13}$$

It can happen that $\widetilde{P}(S^0)$ is not primitive, however, always $\widetilde{P}(S^0) \subset \mathcal{S}(n,k)$!

We state the main result for $\widetilde{P}(S^0)$ as

Proposition. *For* $n > n(k)$ *suitable*

(9.14) $$|M(\widetilde{P}(S^0)) \cap \mathbb{N}(n)| > |S^0| + \gamma |L_t|.$$

Proof: For an $a \in R_\ell^t(S^0)$, $a = q_1 \dots q_r$, $q_1 < q_2 < \dots < q_r < p_t$ we consider the set

$$D(a) = \{v \in \mathbb{N}(n) : v = q_1^{\alpha_1} \dots a_r^{\alpha_r} \cdot T_1,\ (T_1, \prod_{p \le p_{t-1}} p) = 1).$$

Since p_t was the biggest prime, which occured in $P(S^0)$, we observe that

(9.15) $$M(P(S^0) \setminus P^t(S^0)) \cap D(a) = \emptyset \ \text{ for } \ a \in R_\ell^t(S^0).$$

Moreover,

$$D(a) \cap D(a') = \emptyset \ \text{ for } \ a, a' \in R_\ell^t(S^0),\ a \neq a'.$$

Hence, in the light of (9.10) and (9.11) sufficient for showing (9.14) is that for $n > n(k)$

$$B(a \cdot p_t) = \{u \in \mathbb{N}(n) : u = q^{\alpha_1} \dots q_r^{\alpha_r} \cdot p_t^\beta T,\ \alpha_i \ge 1,\ \beta \ge 1 \ \text{ and } \ (T, \prod_{p \le p_t} p) = 1\}$$

(9.16) $$|D(a)| > \begin{cases} \gamma \cdot k_0 \ |B(a \cdot p_t)|, & \text{if } \ t > k_0 \\ \gamma \cdot (t-1) \ |B(a \cdot p_t)|, & \text{if } \ t \le k_0. \end{cases}$$

Three cases in proving (9.16)

We have always $a = q_1 \dots q_r$, $q_1 < q_2 < \dots < q_r < p_t$.

Case: $\mathbf{\frac{n}{a \cdot p_t} \ge 2}$ **and** $\mathbf{t > t(c_1, c_2, k_0)}$

Using the right side of the Theorem in Section 8, which is valid without restrictions, we get

(9.17) $$\begin{aligned} |B(a \cdot p_t)| &\le \ c_2 \sum_{\alpha_i \ge 1, \beta \ge 1} \frac{n}{q_1^{\alpha_1} \cdots q_r^{\alpha_r} \ p_t^\beta} \prod_{p \le p_t} (1 - \frac{1}{p}) \\ &< c_2 \cdot n \cdot \frac{1}{(q_1 - 1) \cdots (q_r - 1)} \prod_{p \le p_t} (1 - \frac{1}{p}) \ \frac{1}{(p_t - 1)}. \end{aligned}$$

For $D(a)$ we have

$$D(a) \supset D'(a) = \{u \in \mathbb{N}(n) : u = q_1 \dots q_r \cdot T_1,\ (T_1, \prod_{p \le p_{t-1}} p) = 1\},$$

and since $\frac{n}{q_1 \cdots q_r} \ \ge \ 2p_t$, we can apply the left side of the Theorem and get

(9.18) $$\begin{aligned} |D(a)| > |D'(a)| &\ge c_1 \cdot n \ \frac{1}{q_1 \dots q_r} \prod_{p \le p_{t-1}} (1 - \frac{1}{p}) \\ &= c_1 n \ \frac{1}{q_1 \dots q_r} \ \frac{p_t}{p_t - 1} \prod_{p \le p_t} (1 - \frac{1}{p}). \end{aligned}$$

Comparing (9.17) and (9.18) we get

$$\begin{aligned} \frac{|D(a)|}{|B(a \cdot p_t)|} &> \ \frac{c_1}{c_2} \ p_t \ \frac{(q_1 - 1) \cdots (q_r - 1)}{q_1 \cdots q_r} \\ &\ge \ \frac{c_1}{c_2} \ p_t \prod_{p \le p_{t-1}} (1 - \frac{1}{p}) > \kappa = \gamma \cdot k_0, \end{aligned}$$

where in the last step we used Lemma 8. Thus we established (9.16) in this case.

Case: $\mathbf{\frac{n}{ap_t} \geq 2}$ **and** $\mathbf{t \leq t(c_1, c_2, k_0)}$

At first let us specify k_0 and hence γ . We choose k_0 so large that

$$p_{k+i} > \gamma(k+i-1) = (1 + \frac{k}{k_0 - k})(k+i-1) \quad \text{for all} \quad i \in \mathbb{N}. \tag{9.19}$$

This is of course possible. Next we choose $\epsilon > 0$ such that

$$p_{k+i} \cdot \frac{1-\epsilon}{1+\epsilon} > \gamma(k+i-1). \tag{9.20}$$

Let $n(\epsilon)$ be a positive integer so that for $n > n(\epsilon)$ we can apply Lemma 4 (iii). So we have

$$|B(a \cdot p_t)| < (1+\epsilon)n \frac{1}{(q_1-1)\cdots(q_r-1)(p_t-1)} \cdot \prod_{p \leq p_t} (1 - \frac{1}{p}),$$

$$|D(a)| > (1-\epsilon)n \frac{1}{(q_1-1)\cdots(q_r-1)} \prod_{p \leq p_{t-1}} (1 - \frac{1}{p})$$

$$= (1-\epsilon)n \frac{1}{(q_1-1)\cdots(q_r-1)} \frac{p_t}{p_t-1} \prod_{p \leq p_t} (1 - \frac{1}{p}),$$

and hence by (9.20)

$$\frac{|D(a)|}{|B(a \cdot p_t)|} > \frac{1-\epsilon}{1+\epsilon} p_t > \gamma(t-1).$$

This establishes (9.16) in this case.

Case: $\mathbf{1 \leq \frac{n}{ap_t} < 2}$

In this case $B(a \cdot p_t)$ consists only of one element, namely $q_1 \cdots q_r \cdot p_t$. Let now $t_1 \in \mathbb{N}$ satisfy

$$p_{t_1} > (p_{k_0})^{\gamma k_0} \tag{9.21}$$

and let

$$n > \prod_{p \leq p_{t_1}} p. \tag{9.22}$$

Notice that in our case necessarily $p_t \geq p_{t_1}$, because $a\, p_t < \prod_{p \leq p_t} p$ and $p_{t_1} > p_t$ would imply

$$2\ ap_t < 2 \prod_{p \leq p_t} p < \prod_{p \leq p_{t_1}} p < n \text{ (by (9.22))}$$

and this contradicts our case $2a\, p_t > n$.

Now by (9.21) $p_t \geq p_{t_1} > (p_{k_0})^{\gamma k_0}$ and since $q_1 \leq p_{k_0}$ we get finally

$$q_1^{\gamma k_0} < p_t.$$

Therefore

$$D(a) \supset \{q_1 \dots q_r,\ q_1^2 q_2 \dots q_r, \dots, q_1^{\gamma k_0} q_2 \dots q_r,\ q_1 q_2 \dots q_r \cdot p_t\},$$

$|D(a)| > \gamma \cdot k_0$, and again (9.16) holds. k_0, γ , and ϵ are already fixed and depend only on k . Then for

$$n(k) = \max \Big\{ \prod_{p \leq (p_{k_0})^{\gamma k_0}} p, n(\epsilon) \Big\} \tag{9.23}$$

and $n > n(k)$ (9.16) holds in all three cases and the proof of the Proposition is complete.

Final iterative procedure and its accounting

We have already noticed that $\widetilde{P}(S^0)$ may be not primitive. Moreover, $M(\widetilde{P}(S^0))$ may even not be left compressed.

Let now $S^1 \subset \mathbb{N}(n)$ be any set which is obtained from $M(\widetilde{P}(S^0))$ by left pushing and is left compressed. We know that

$$S^1 \in \mathcal{C}(n,k),\ |S^1| \geq |M(\widetilde{P}(S^0)) \cap \mathbb{N}(n)| \tag{9.24}$$

and therefore we know from the Proposition that

$$|S^1| > |S^0| + \gamma |L_t|. \tag{9.25}$$

We notice that $(a, \prod\limits_{p \leq p_{k_0}} p) > 1$ for every $a \in S^1$ and the last prime p_{t^1} , which occurs as a factor of any primitive element of $P(S^1)$ is less than p_t .

If $S^1 \not\subset \mathbb{E}(n,k)$, then we repeat the whole procedure and get an S^2 for which

$$|S^2| > |S^1| + \gamma |L_{t^1}|,$$

where L_{t^1} is defined analogously to L_t with respect to the largest prime p_{t^1} occuring in a member of $P(S^1)$.

By iteration we get an $S^i \in \mathcal{C}(n,k)$ with

$$|S^i| > |S^{i-1}| + \gamma |L_{t^{i-1}}| \tag{9.26}$$

and again in analogy to the first step we define now S^i_j and the partition

$$S^i = (\bigcup_{j=i}^{k} S^i_j) \cup (\bigcup_{j=k+1}^{k_0} S^i_j)$$

and also sets $R^{t^i}_\ell\ (S^i)$.

It is clear that the procedure is finite, i. e. there exists an $m \in \mathbb{N}$ for which

$$\bigcup_{j=k+1}^{k_0} S^m_j = \emptyset,\ S^m \subset \mathbb{E}(n,k). \tag{9.27}$$

Now we do the accounting via Lemma 9.

The integers x, y are here

$$x = x_0 = |\bigcup_{j=1}^{k} S_j|,\ y = y_0 = |\bigcup_{j=k+1}^{k_0} S_i|$$

and $\beta = \gamma > 1$. Furthermore
$x_i = |\overset{k}{\underset{j=1}{\cup}} S_j^i|,\ y_i = |\overset{k_0}{\underset{j=k+1}{\cup}} S_j^i|,\ a_i = |L_{t^{i-1}} \cap (\overset{k}{\underset{j=1}{\cup}} S_j^{i-1})|,\ b_i = |L_{t^{i-1}} \cap (\overset{k_0}{\underset{j=k+1}{\cup}} S_j^{i-1})|,$
and so

$$a_i + b_i = L_{t^{i-1}} \quad \text{and} \quad a^* + b^* = |\underset{a \in R_\ell^{t^{i-1}}}{\cup} D(a)|$$

count the new elements in the i–th step.

We know from the Proposition that

$$a^* + b^* > \gamma(a_i + b_i)$$

and from (9.27) that $y_m = 0$.
Hence, by Lemma 9

$$(9.28)\ \ |\mathbb{E}(n,k)| \geq x_m = |S^m| > x + \gamma y = |\overset{k}{\underset{j=0}{\cup}} S_j| + |\overset{k_0}{\underset{j=k+1}{\cup}} S_j| + (\gamma - 1)|\overset{k_0}{\underset{j=k+1}{\cup}} S_j| \geq |S|,$$

because $\gamma = 1 + \frac{k}{k_0 - k}$, $S = |\overset{k}{\underset{j=1}{\cup}} S_i| + |\overset{k_0}{\underset{j=k+1}{\cup}} S_i| + |\underset{j \geq k_0+1}{\cup} S_j|$, and

$$|\overset{k_0}{\underset{j=k+1}{\cup}} S_j| \geq \frac{k_0 - k}{k} \cdot |\underset{j \geq k_0+1}{\cup} S_j|.$$

However, (9.28) says that $\mathbb{E}(n,k) > |S|$, which contradicts the optimality of S . Therefore (II) must be false and Theorem 1 is proved.

Remark 3: For fixed k, s and **every** n let $H(n,k,s) \in \mathcal{S}(n,k,s)$ be a set with

$$|H(n,k,s)| = \max\{|B| : B \in \mathcal{S}(n,k,s),\ B \not\subset E(n,k,s)\}.$$

We know from the counterexample in [1] that $|\mathbb{E}(n,k,s)| - |H(n,k,s)| < 0$ is possible and that $|\mathbb{E}(n,k,s)| - |H(n,k,s)| > 0$ for all $n > n(k,s)$ (Uniqueness).
However, by the method of proof of Theorem 1 one can derive

$$\lim_{n \to \infty} (|\mathbb{E}(n,k,s)| - |H(n,k,s)|) = \infty$$

for all $k, s \in \mathbb{N}$.

References

[1] R. Ahlswede and L.H. Khachatrian, *On extremal sets without coprimes*, Acta Arithmetica 46.1, 89–99, 1994.

[2] A.A. Buchstab, *Asymptotische Abschätzungen einer allgemeinen zahlentheoretischen Funktion*, Mat.Sb. N.S. 44, 1239–1246, 1937.

[3] N.G. De Bruijn, *On the number of uncancelled elements in the sieve of Eratosthenes*, Indag.math. 12, 247–256, 1950.

[4] P. Erdös, *Remarks in number theory*, IV, Mat. Lapok 13, 228–255, 1962.

[5] P. Erdös, *Extremal problems in number theory*, Proc. Symp. in Pure Math. VIII, Theory of Numbers, Amer. Math. Soc., Providence, RI, 181–189, 1965.

[6] P. Erdös, *Problems and results on combinatorial number theory*, Chapt. 12 in: A Survey of Combinatorial Theory, J.N. Srivastava et al (eds.), North–Holland, 1973.

[7] P. Erdös, *A survey of problems in combinatorial number theory*, Ann. Discrete Math. 6, 89–115, 1980.

[8] P. Erdös and A. Sárközy, *On sets of coprime integers in intervals*, Hardy–Ramanujan J. 16, 1–20, 1993.

[9] P. Erdös, A. Sárközy and E. Szemerédi, *On some extremal properties of sequences of integers*, Ann. Univ. Sci. Budapest, Eötvös 12, 131–135, 1969.

[10] P. Erdös, A. Sárközy and E. Szemerédi, *On some extremal properties of sequences of integers, II*, Publ. Math. 27, 117–125, 1980.

[11] R. Freud, Paul Erdös, *80 — A Personal Account*, Periodica Math. Hungarica, Vol. 26, (2), 87–93, 1993.

[12] H. Halberstam and K.F. Roth, *Sequences*, Oxford University Press, 1966, Springer Verlag, 1983.

[13] R.R. Hall and G. Tenenbaum, *Divisors*, Cambridge Tracts in Mathematics 90, 1988.

[14] C. Szabó and G. Tóth, *Maximal sequences not containing 4 pairwise coprime integers*, Mat. Lapok 32, 253–257, 1985, (in Hungarian).

[15] P. Erdös, *On the density of some sequences of integers*, Bull. Am. Math. Soc. 54, 685–692, 1948.