

Maximal sets of numbers not containing $k + 1$ pairwise coprimes and having divisors from a specified set of primes

Rudolf Ahlswede and Vladimir Blinovsky

1 Introduction and Main Results

Let $\mathbb{P} = \{p_1 < p_2 < \dots\}$ be the set of primes and \mathbb{N} be the set of natural numbers. Denote $\mathbb{N}(n) = \{1, \dots, n\}$, $\mathbb{P}(n) = \mathbb{P} \cap \mathbb{N}(n)$. For $a, b \in \mathbb{N}$ denote the maximal common divisor of a and b by (a, b) . Let also $S(n, k)$ be the family of sets $A \subset \mathbb{N}(n)$ of positive integers not containing $k + 1$ coprimes. Define

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

In the paper [?] the following result was proved.

Theorem 1 *For all sufficiently large n*

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

where

$$\mathbb{E}(n, k) = \{a \in \mathbb{N}(n) : a = up_i, \text{ for some } i = 1, \dots, k\}. \quad (1)$$

Let now $\mathbb{Q} = \{q_1 < q_2 < \dots < q_r\} \subset \mathbb{P}$ be a finite set of primes and $R(n, \mathbb{Q}) \subset S(n, 1)$ be such a family of sets of positive integers that for arbitrary $a \in A \in R(n, \mathbb{Q})$, $(a, \prod_{j=1}^r q_j) > 1$. In [?] the following result was proved.

Theorem 2 *Let $n \geq \prod_{j=1}^r q_j$, then*

$$f(n, \mathbb{Q}) \stackrel{\Delta}{=} \max_{A \in R(n, \mathbb{Q})} |A| = \max_{1 \leq t \leq r} |M(2q_1, \dots, 2q_t, q_1 \dots q_t) \cap \mathbb{N}(n)|, \quad (2)$$

where $M(B)$ is the set of multiples of the set of integers B .

In [?] was also stated the problem of finding a maximal set of positive integers from $\mathbb{N}(n)$ which satisfies the conditions of Theorems ?? and ?? simultaneously, i.e. to find a set A without $k + 1$ coprimes and such that each element of this set has a divisor from \mathbb{Q} . This paper is devoted to the solution of this problem. In our work we use the methods from paper [?].

Denote by $R(n, k, \mathbb{Q}) \subset S(n, k)$ the family of sets of positive integers with the property that an arbitrary $a \in A \in R(n, k, \mathbb{Q})$ has a divisor from \mathbb{Q} . For given s and $\mathbb{T} = \{r_1 < r_2 < \dots\} = \mathbb{P} - \mathbb{Q}$ let $F(n, k, s, \mathbb{Q}) \subset R(n, k, \mathbb{Q})$ be the family of sets of squarefree positive numbers such that for arbitrary $a \in A \in F(n, k, s, \mathbb{Q})$ we have $(r_i, a) = 1, i > s$. For given s, r the cardinality of the family $F(n, k, s, \mathbb{Q})$ and the cardinalities of $A \in F(n, k, s, \mathbb{Q})$ are bounded from above as $n \rightarrow \infty$.

Next we formulate our main result, which extends both, Theorem ?? and Theorem ??.

Theorem 3 *For sufficiently large n the following relation is valid*

$$\varphi(n, k, \mathbb{Q}) \triangleq \max_{A \in R(n, k, \mathbb{Q})} |A| = \max_{F \in F(n, k, s-1, \mathbb{Q})} |M(F) \cap \mathbb{N}(n)|, \quad (3)$$

where s is the minimal integer which satisfies the inequality $r_s > r$.

We have the following important

Corollary 1 *If $r = k + 1$, then*

$$\varphi(n, k, \mathbb{Q}) = |M(q_1, \dots, q_k) \cap \mathbb{N}(n)|. \quad (4)$$

This corollary gives the solution of obtaining an explicit formula for $\varphi(n, k, \mathbb{Q})$ in the first nontrivial case (since if $r \leq k$, then trivially $M(q_1, \dots, q_r) \cap \mathbb{N}(n)$ is a maximal set).

2 Proofs

Let's remind the definition of the left pushing which the reader can find in [?]. For arbitrary

$$a = up_j^\alpha, p_i < p_j, (p_i p_j, u) = 1, \alpha > 0 \text{ and } p_j \notin \mathbb{Q} \text{ or } p_i, p_j \in \mathbb{Q} \quad (5)$$

define

$$L_{i,j}(a, \mathbb{Q}) = p_i^\alpha u.$$

If a is not of the form (??), we set $L_{i,j}(a, \mathbb{Q}) = a$. For $A \subset \mathbb{N}$ denote

$$L_{i,j}(a, A, \mathbb{Q}) = \begin{cases} L_{i,j}(a, \mathbb{Q}), & L_{i,j}(a, \mathbb{Q}) \notin A, \\ a, & L_{i,j}(a, \mathbb{Q}) \in A. \end{cases}$$

At last set

$$L_{i,j}(A, \mathbb{Q}) = \{L_{i,j}(a, A, \mathbb{Q}); a \in A\}.$$

We say that A is left compressed if for arbitrary $i < j$

$$L_{i,j}(A, \mathbb{Q}) = A.$$

It can be easily seen that every finite $A \subset \mathbb{N}$, after finite number of left pushing operations, can be made left compressed,

$$|L_{i,j}(A, \mathbb{Q})| > |A|$$

and if $A \in R(n, k, \mathbb{Q})$, then $L_{i,j}(A, \mathbb{Q}) \in R(n, k, \mathbb{Q})$.

If we denote by $O(n, k, \mathbb{Q}) \subset R(n, k, \mathbb{Q})$ the family of sets achieving the maximum in (??) and if $C(n, k, \mathbb{Q}) \subset R(n, k, \mathbb{Q})$ is the family of left compressed sets from $R(n, k, \mathbb{Q})$, then it follows that $O(n, k, \mathbb{Q}) \cap C(n, k, \mathbb{Q}) \neq \emptyset$. Next we assume that $A \in C(n, k, \mathbb{Q}) \cap O(n, k, \mathbb{Q})$.

For arbitrary $a \in A$ we have the decomposition $a = a^1 a^2$, where $a^1 = r_{i_1}^{\alpha_1} \dots r_{i_f}^{\alpha_f}$, $r_i < r_j$, $i < j$, $a^2 = q_{j_1}^{\beta_1} \dots q_{j_\ell}^{\beta_\ell}$; $q_{j_m} < q_{j_s}$, m, s , $\alpha_j, \beta_j > 0$. If $a = r_{i_1}^{\alpha_1} \dots r_{i_f}^{\alpha_f} q_{j_1}^{\beta_1} \dots q_{j_\ell}^{\beta_\ell} \in A$, $\alpha_j, \beta_j > 0$, then $\bar{a} = r_{i_1} \dots r_{i_f} q_{j_1} \dots q_{j_\ell} \in A$ as well and also $\hat{a} = ua \in A$ for all $u \in \mathbb{N}$: $ua \leq n$. Consider all squarefree numbers $A^* \subset A$ and for given a^2 the set of all a^1 such that $a^1 a^2 \in A^*$. This set is the ideal generated by division. The set of minimal elements from this ideal we denote by $P(a^2, A^*)$. It follows that $(A \in O(n, k, \mathbb{N}))$,

$$A = M(\{a^1 a^2; a^1 \in P(a^2, A^*)\}) \cap \mathbb{N}(n),$$

For each a^2 we order $\{a_1^1 < a_2^1 < \dots\} = P(a^2, A^*)$ colexicographically according to their decompositions $a_i^1 = r_{i_1} \dots r_{i_f}$. Let ρ be the maximal over the choices of a^2 positive integers such that r_ρ divides some a_i^1 for which $a_i^1 a^2 \in A^*$. From the left compressedness of the set A it follows that $a' = a_j^1 a^2$, $j < i$ also belongs to A . Then the set B of elements $b = b^1 b^2 \leq n$, $(b^1, \prod_{j=1}^r q_j) = 1$ such that $b^2 = q_{j_1}^{\beta_1} \dots q_{j_\ell}^{\beta_\ell}$, $\beta_j > 0$ and $a_i^1 | b^1$, $a_j^1 \nmid b^1$, $j < i$ is exactly the set

$$B(a) = \left\{ u \leq n : u = r_{i_1}^{\alpha_1} \dots r_{i_f}^{\alpha_f} r_{i_\rho}^{\alpha_\rho} q_{j_1}^{\beta_1} \dots q_{j_\ell}^{\beta_\ell} F; \alpha_i, \beta_i > 0, \left(F, \prod_{j=1}^{\rho} r_j \prod_{j=1}^r q_j \right) = 1 \right\}.$$

Denote

$$P^\rho(a^2, A^*) = \{a \in P(a^2, A^*) : (a, r_\rho) = r_\rho\},$$

$$P_s^\rho(A^*) = \left\{ a \in P^\rho(a^2, A^*) \text{ for some } a^2, \text{ such that } (a^2, q_s) = q_s, \left(a^2, \prod_{j=1}^{s-1} q_j \right) = 1 \right\}$$

and

$$L^\rho(a^2) = \bigcup_{a \in P^\rho(a^2, A^*)} B(a).$$

Then the set $\bigcup_{s=1}^r P_s^\rho(A^*)$ is exactly the set $\bigcup_{a^2} P^\rho(a^2, A^*)$ of numbers which are divisible by r_ρ . Since each $a \in P(a^2, A^*)$ for all a^2 has divisor from \mathbb{Q} , it follows that for some $1 \leq s \leq r$

$$\left| \bigcup_{a \in P_s^\rho(A^*)} B(a) \right| \geq \frac{1}{r} \left| \bigcup_{a^2} L^\rho(a^2) \right|. \quad (6)$$

Next for this s we define the transformation

$$\bar{P}(a^2, A^*) = (P(a^2, A^*) - P^\rho(a^2, A^*)) \bigcup R_s^\rho(a^2, A^*),$$

where

$$\begin{aligned} R_s^\rho(a^2, A^*) &= \{v \in \mathbb{N}; vr_\rho \in P_s^\rho(a^2, A)\}, \\ P_s^\rho(a^2, A^*) &= \{a = a^1 a^2 \in P_s^\rho(A^*)\}. \end{aligned}$$

It is easy to see that

$$\bigcup_{a^2} \bar{P}(a^2, A^*) \subset S(n, k, \mathbb{Q}).$$

Next we prove that if $r_\rho > r$, then

$$\left| M \left(\bigcup_{a^2} \bar{P}(a^2, A^*) \right) \cap \mathbb{N}(n) \right| > |A| \quad (7)$$

which is a contradiction to the maximality of A .

For $a \in R_s^\rho(a^2, A^*)$, $a = r_{i_1} \dots r_{i_f} q_{j_1} \dots q_{j_\ell}$, $r_{i_1} < \dots < r_{i_f} < r_\rho$, $q_{j_1} \dots q_{j_\ell} = a^2$ denote

$$D(a) = \left\{ v \in \mathbb{N}(n) : v = r_{i_1}^{\alpha_1} \dots r_{i_f}^{\alpha_f} q_{j_1}^{\beta_1} \dots q_{j_\ell}^{\beta_\ell} T, \alpha_j, \beta_j \geq 1, \left(T, \prod_{j=1}^{\rho-1} r_j \prod_{j=1}^r q_j \right) = 1 \right\}.$$

It can be easily seen that

$$D(a) \cap D(a') = \emptyset, a \neq a'$$

and

$$M \left(\bigcup_{a^2} (P(a^2, A^*) - P^\rho(a^2, A^*)) \right) \cap D(a) = \emptyset.$$

Thus to prove (??) it is sufficient to show that for large $n > n_0$

$$|D(a)| > r |B(ar_\rho)|. \quad (8)$$

To prove (??) we consider three cases.

First case: $n/(ar_\rho) \geq 2$ and $\rho > \rho_0$.

From (??) follows that

$$\begin{aligned}
|B(ar_\rho)| &\leq c_2 \sum_{\alpha_i, \alpha, \beta_i \geq 1} \frac{n}{r_{i_1}^{\alpha_1} \cdots r_{i_f}^{\alpha_f} r_\rho^\alpha q_{j_1}^{\beta_1} \cdots q_{j_\ell}^{\beta_\ell}} \prod_{j=1}^{\rho} \left(1 - \frac{1}{r_j}\right) \prod_{j=1}^r \left(1 - \frac{1}{q_j}\right) \\
&= c_2 \frac{n}{(r_{i_1} - 1) \cdots (r_{i_f} - 1)(r_\rho - 1)(q_{j_1} - 1) \cdots (q_{j_\ell} - 1)} \prod_{j=1}^{\rho} \left(1 - \frac{1}{r_j}\right) \prod_{j=1}^r \left(1 - \frac{1}{q_j}\right).
\end{aligned} \tag{9}$$

At the same time

$$\bar{D}(a) \triangleq \left\{ v \in \mathbb{N}(n); v = r_{i_1} \cdots r_{i_f} q_{j_1} \cdots q_{j_\ell} F_1, \left(F_1, \prod_{j=1}^{\rho-1} r_j \prod_{j=1}^r q_j \right) = 1 \right\} \subset D(a)$$

and using (??) we obtain the inequalities

$$|D(a)| \geq |\bar{D}(a)| \geq c_1 \frac{n}{r_{i_1} \cdots r_{i_f} q_{j_1} \cdots q_{j_\ell}} \prod_{j=1}^{\rho-1} \left(1 - \frac{1}{r_j}\right) \prod_{j=1}^r \left(1 - \frac{1}{q_j}\right). \tag{10}$$

Thus from (??), (??) it follows that

$$\begin{aligned}
\frac{|D(a)|}{|B(ar_\rho)|} &\geq \frac{c_1}{c_2} r_\rho \frac{(r_{i_1} - 1) \cdots (r_{i_f} - 1)}{r_{i_1} \cdots r_{i_f}} \prod_{j \in [r] - \{j_1, \dots, j_\ell\}} \left(1 - \frac{1}{q_j}\right) \\
&\geq \frac{c_1}{c_2} \prod_{j=1}^f \left(1 - \frac{1}{r_j}\right) r_\rho \prod_{j=1}^r \left(1 - \frac{1}{q_j}\right) > r.
\end{aligned}$$

The last inequality follows from (??).

Second case: $n/(ar_\rho) \geq 2$, $\rho < \rho_0$.

Then we apply relations (??) and obtain the inequalities

$$\begin{aligned}
|B(ar_\rho)| &< (1 + \epsilon) \frac{n}{(r_{i_1} - 1) \cdots (r_{i_f} - 1)(r_\rho - 1)(q_{j_1} - 1) \cdots (q_{j_\ell} - 1)} \prod_{j=1}^{\rho} \left(1 - \frac{1}{r_j}\right) \prod_{j=1}^r \left(1 - \frac{1}{q_j}\right), \\
|D(a)| &> (1 - \epsilon) \frac{n}{(r_{i_1} - 1) \cdots (r_{i_f} - 1)(q_{j_1} - 1) \cdots (q_{j_\ell} - 1)} \prod_{j=1}^{\rho-1} \left(1 - \frac{1}{r_j}\right) \prod_{j=1}^r \left(1 - \frac{1}{q_j}\right).
\end{aligned}$$

From these inequalities it follows that

$$\frac{|D(a)|}{|B(ar_\rho)|} > \frac{1 - \epsilon}{1 + \epsilon} r_\rho > r.$$

Here the last inequality is valid for sufficiently small ϵ , because $r_\rho > r$.

Last case: $1 \leq n/(ar_\rho) < 2$.

In this case $|B(ar_\rho)| = 1$. Let $r_{i_1} \dots r_{i_f} r_\rho q_{j_1} \dots q_{j_\ell} = B(ar_\rho)$. Then we choose $r_g > (q_{j_1})^r$ and $n > \prod_{j=1}^g r_j \prod_{j=1}^r q_j$. We have $r_\rho > r_g$. Indeed, otherwise

$$n > \prod_{j=1}^g r_j \prod_{j=1}^r q_j > 2 \prod_{j=1}^{\rho} \prod_{j=1}^r q_j > 2ar_\rho$$

which is a contradiction to our case.

Hence

$$\{r_{i_1} \dots r_{i_f} q_{j_1} \dots q_{j_\ell}, r_{i_1} \dots r_{i_f} q_{j_1}^2 \dots q_{j_\ell}, \dots, r_{i_1} \dots r_{i_f} q_{j_1}^r \dots q_{j_\ell}, r_{i_1} \dots r_{i_f} q_{j_1} \dots q_{j_\ell} r_\rho\} \subset D(a).$$

Thus in this case also $|D(a)| > r = r|B(ar_\rho)|$.

From the above follows that for sufficiently large $n > n_0(\mathbb{Q})$ for all $a \in R_s^\rho(a^2, A^*)$ inequality (??) is valid and taking into account (??) we obtain (??). This is a contradiction to the maximality of A . Hence the maximal $r_i \in \mathbb{P} - \mathbb{Q}$ which appears as a divisor of some $a \in \bigcup_{a^2} P(a^2, A^*)$ such that $M(A^*) \cap \mathbb{N}(n) \in O(n, k, \mathbb{Q})$ satisfies the condition $r_\rho \leq r$. This inequality implies the statement of the theorem.

To prove the corollary note that for $\mathbb{Q} = \{q_1 < \dots < q_k < q_{k+1}\}$

$$M(q_1, q_2, \dots, q_k) \cap \mathbb{N}(n) \in R(n, k, \mathbb{Q}).$$

From the left compressedness of A it follows that if $q_i \in A$, then $q_j \in A$, $j \leq i$. Let $q_1, \dots, q_t \in A$, $q_{t+1} \notin A$. Then $q_i q_j$ belongs to A for all $t < i < j \leq k + 1$. Next we should maximize (over the choice of $a_{ij} \in \mathbb{N} - M(\mathbb{Q})$) the value

$$\left| M(q_i a_{ij}, i = t + 1, \dots, k + 1) \cap \mathbb{N}(n) \right|$$

such that

$$Z \triangleq \{q_i a_{ij}, i = t + 1, \dots, k + 1\} \subset S(n, k, \mathbb{Q}). \quad (11)$$

Completely repeating the proof of the theorem one can show that each a_{ij} can be chosen in such a way that for each i, j a_{ij} is the product of some primes $r_m \in \mathbb{P} - \mathbb{Q}$ such that $r_m \leq k - t + 1$. Then it can be easily seen that for arbitrary $t < k$

$$r_{k-t} > k - t + 1 \quad (12)$$

except the cases $r_2 = 3$ and/or $r_1 = 2$, when equality holds in (??).

Thus if (??) is valid, then we can only increase the volume of Z if we choose

$$Z = \{q_i r_j, i = t + 1, \dots, k + 1, j = 1, \dots, k - t - 1\}.$$

But in this case

$$Z \in S(n, k - t - 1, \mathbb{Q})$$

and we only increase Z by choosing

$$Z = \{q_{t+1}, q_i r_j, i = t + 2, \dots, k + 1, j = 1, \dots, k - t - 1\}.$$

Continuing this process we arrive at the following three cases:

$$A = \begin{cases} M(q_1, \dots, q_{k-2}, q_{k-1}q_k, q_{k-1}q_{k+1}, q_kq_{k+1}, \\ q_i r_j, i = k - 1, k, k + 1, j = 1, 2) \cap \mathbb{N}(n), & r_2 = 3 \\ M(q_1, \dots, q_{k-1}, q_kq_{k+1}, q_k r_1, q_{k+1}r_1) \cap \mathbb{N}(n), & r_1 = 2, r_2 > 3 \\ M(q_1, \dots, q_k) \cap \mathbb{N}(n), & \text{otherwise} \end{cases} \quad (13)$$

Now by comparing the densities (see (??)) of the sets in the right hand side of (??) we prove that indeed a maximum cardinality among these three possibilities for large n has the set $M(q_1, \dots, q_k) \cap \mathbb{N}(n)$.

It is enough to calculate the contribution of the last three primes q_{k-1}, q_k, q_{k+1} to the corresponding densities. These contributions to the three sets are respectively

$$\begin{aligned} d_1 &= \left(\frac{2}{3} \left(\frac{1}{q_{k-1}} + \frac{1}{q_k} + \frac{1}{q_{k+1}} \right) - \frac{1}{3} \left(\frac{1}{q_{k-1}q_k} + \frac{1}{q_{k-1}q_{k+1}} + \frac{1}{q_kq_{k+1}} \right) \right) \prod_{j=1}^{k-2} \left(1 - \frac{1}{q_j} \right) \\ d_2 &= \left(\frac{1}{2q_k} + \frac{1}{2q_{k+1}} \right) \prod_{j=1}^{k-2} \left(1 - \frac{1}{q_j} \right) \\ d_3 &= \left(\frac{1}{q_{k-1}} + \frac{1}{q_k} - \frac{1}{q_{k-1}q_k} \right) \prod_{j=1}^{k-2} \left(1 - \frac{1}{q_j} \right). \end{aligned}$$

It is an easy exercise to show that $d_3 > d_1, d_2$. Thus the third case gives us the maximal set (for sufficiently large n) and the corollary is proved.

Open problems. It would be interesting to know whether it is possible to find a bound on ρ which depends only on k but not on \mathbb{Q} ? As it can be seen from (??) and (??) this can be done in the case $\mathbb{Q} = \emptyset$ and $k = 1$.

Another question is whether in some cases the optimal F satisfying $M(F) \cap \mathbb{N}(n) \in O(n, k, \mathbb{Q})$ should contain an $a \in F$, whose decomposition into primes contains more than one element from $\mathbb{P} - \mathbb{Q}$?

Auxiliary facts.

Statement 1 *We have*

$$p_t \prod_{j=1}^t \left(1 - \frac{1}{p_j} \right) \xrightarrow{t \rightarrow \infty} \infty. \quad (14)$$

This statement is a simple consequence of the following property of primes (see for ex. [?], Theorem 13.13):

$$\prod_{p \in \mathbb{P}(t)} \left(1 - \frac{1}{p}\right) \underset{t \rightarrow \infty}{\sim} \frac{e^{-C}}{\log t},$$

where C is the Euler constant.

Statement 2 *If*

$$\phi(x, y) = \left| \left\{ a \leq x : \left(a, \prod_{p_j < y} p_j \right) = 1 \right\} \right|,$$

then for some constants c_1, c_2 and all $x, y; x \geq 2y \geq 4$,

$$c_1 x \prod_{p_j < y} \left(1 - \frac{1}{p_j}\right) \leq \phi(x, y) \leq c_2 x \prod_{p_j < y} \left(1 - \frac{1}{p_j}\right). \quad (15)$$

The proof of this statement one can find in [?].

Define the dB density of $B \subset \mathbb{N}$ as the limit (if it exists)

$$dB = \lim_{n \rightarrow \infty} \frac{|B \cap \mathbb{N}(n)|}{n}. \quad (16)$$

It can be easily seen that the density of the set

$$B = \left\{ b = p_{i_1}^{\alpha_1} \dots p_{i_m}^{\alpha_m} F, \alpha_i \geq 1, \left(F, \prod_{s=1}^f p_{j_s} \right) = 1 \right\} \quad (17)$$

is equal to

$$\sum_{\alpha_j \geq 1} \frac{1}{p_{i_1}^{\alpha_1} \dots p_{i_m}^{\alpha_m}} \prod_{s=1}^f \left(1 - \frac{1}{p_{j_s}}\right) = \frac{1}{(p_{i_1} - 1) \dots (p_{i_m} - 1)} \prod_{s=1}^f \left(1 - \frac{1}{p_{j_s}}\right)$$

and for a fixed number of $B_j, j = 1, \dots, c$ of the form (??) for sufficiently large $n > n(\epsilon)$ we have

$$|B_j \cap \mathbb{N}(n)| = (1 \pm \epsilon) \frac{n}{(p_{i_1} - 1) \dots (p_{i_m} - 1)} \prod_{s=1}^f \left(1 - \frac{1}{p_{j_s}}\right), \quad (18)$$

where p_{i_j}, p_{j_s}, m, f can be different for different j .

References

- [1] R. Ahlswede and L. Khachatryan, Maximal sets of numbers not containing $k+1$ pairwise coprime integers, Acta Arithm., LXXII.1, 77–100, 1995.

- [2] R. Ahlswede and L. Khachatrian, Sets of integers with pairwise common divisor and a factor from a specified set of primes, *Acta Arithm.*, LXXV.3, 259–276, 1996.
- [3] H. Halberstam and K. Roth, *Sequences*, Oxford University Press, 1966
- [4] T. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, N.Y., Berlin, 1976