

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

Vladimir Blinovsky

► **To cite this version:**

Vladimir Blinovsky. Maximal sets of integers not containing $k + 1$ pairwise coprimes and having divisors from a specified set of primes. 2005 European Conference on Combinatorics, Graph Theory and Applications (EuroComb '05), 2005, Berlin, Germany. pp.335-340. hal-01184442

HAL Id: hal-01184442

<https://hal.inria.fr/hal-01184442>

Submitted on 17 Aug 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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

Vladimir Blinovsky

¹ Bielefeld University, Math. Dept., P.O.100131, D-33501, Bielefeld, Germany, vblinovs@math.uni-bielefeld.de

We find the formula for the cardinality of maximal set of integers from $[1, \dots, n]$ which does not contain $k + 1$ pairwise coprimes and has divisors from a specified set of primes. This formula is defined by the set of multiples of the generating set, which does not depend on n .

Keywords: greatest common divisor, coprimes, squarefree numbers

1 Formulation of the result

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

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

In the paper [1] the following was proved.

Theorem 1 For all sufficiently large

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

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 finite set of primes and $R(n, \mathbb{Q}) \subset S(n, 1)$ is such family of sets of positive integers that for the arbitrary $a \in A \in R(n, \mathbb{Q})$, $(a, \prod_{j=1}^r q_j) > 1$. In [2] was proved the following

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

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

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

In [2] the problem was stated of finding the maximal set of positive integers from $\mathbb{N}(n)$ which satisfies the conditions of Theorems 1 and 2 simultaneously i.e. which is 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 the paper [1].

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

Next we formulate our main result which extent the result of the Theorems 1, 2 and in some sense include both of them.

Theorem 3 *If $\mathbb{Q} \neq \emptyset$, then for sufficiently large n the following relation is valid*

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

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

2 Proof of the Theorem 3

Let's remind the definition of the left pushing which the reader can find in [2]. For the arbitrary

$$a = up_j^\alpha, p_i < p_j, (p_i p_j, u) = 1, \alpha > 0 \text{ and } p_j \notin \mathbb{Q} \text{ or } p_i, p_j \in \mathbb{Q} \tag{4}$$

define

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

For a not of the form (4) 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 the 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 $O(n, k, \mathbb{Q}) \subset R(n, k, \mathbb{Q})$ the families of sets on which achieved max in (3) and $C(n, k, \mathbb{Q}) \subset R(n, k, \mathbb{Q})$ 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 the 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 the division. The set of minimal elements from this ideal 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 $\{a_1^1 < a_2^1 < \dots\} = P(a^2, A^*)$ lexicographically according to their decomposition $a_i^1 = r_{i_1} \dots r_{i_f}$. Let ρ is the maximal over the choice of a^2 positive integer such that r_ρ divide 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

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

Denote

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

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

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 . Because each $a \in P(a^2, A^*)$ for all a^2 has divisor from \mathbb{Q} it follows that for some $1 \leq s \leq r$

$$\left| \bigcup_{a \in P_s^\rho(A^*)} B(a) \right| \geq \frac{1}{r} \left| \bigcup_{a^2} L^\rho(a^2) \right|. \tag{5}$$

Next for this s we define the transformation

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

where

$$R_s^\rho(a^2, A^*) = \{v \in \mathbb{N}; vr_\rho \in P_s^\rho(a^2, A)\},$$

$$P_s^\rho(a^2, A^*) = \{a = a^1 a^2 \in P_s^\rho(A^*)\}.$$

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

$$\left| M \left(\bigcup_{a^2} \bar{P}(a^2, A^*) \right) \cap \mathbb{N}(n) \right| > |A| \tag{6}$$

which gives the 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 (6) it is sufficient to show, that for large $n > n_0$

$$|D(a) > r|B(ar_\rho)|. \tag{7}$$

To prove (7) we consider three cases.

First case when $n/(ar_\rho) \geq 2$ and $\rho > \rho_0$. It follows that

$$\begin{aligned} |B(ar_\rho)| &\leq c_2 \sum_{\alpha_i, \alpha, \beta_i \geq 1} \frac{n}{r_{i_1}^{\alpha_1} \dots r_{i_f}^{\alpha_f} r_\rho^\alpha q_{j_1}^{\beta_1} \dots q_{j_\ell}^{\beta_\ell}} \prod_{j=1}^\rho \left(1 - \frac{1}{r_j}\right) \prod_{j=1}^r \left(1 - \frac{1}{q_j}\right) \\ &= c_2 \frac{n}{(r_{i_1} - 1) \dots (r_{i_f} - 1) (r_\rho - 1) (q_{j_1} - 1) \dots (q_{j_\ell} - 1)} \prod_{j=1}^\rho \left(1 - \frac{1}{r_j}\right) \prod_{j=1}^r \left(1 - \frac{1}{q_j}\right). \end{aligned} \tag{8}$$

At the same time

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

and we obtain the inequalities

$$|D(a)| \geq |\bar{D}(a)| \geq c_1 \frac{n}{r_{i_1} \dots r_{i_f} q_{j_1} \dots q_{j_\ell}} \prod_{j=1}^{\rho-1} \left(1 - \frac{1}{r_j}\right) \prod_{j=1}^r \left(1 - \frac{1}{q_j}\right). \tag{9}$$

Thus from (8), (9) it follows that

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

Now let's $n/(ar_\rho) \geq 2$, $\rho < \rho_0$. Then we obtain the inequalities

$$|B(ar_\rho)| < (1 + \epsilon) \frac{n}{(r_{i_1} - 1) \dots (r_{i_f} - 1)(r_\rho - 1)(q_{j_1} - 1) \dots (q_{j_\ell} - 1)} \prod_{j=1}^{\rho} \left(1 - \frac{1}{r_j}\right) \prod_{j=1}^r \left(1 - \frac{1}{q_j}\right),$$

$$|D(a)| > (1 - \epsilon) \frac{n}{(r_{i_1} - 1) \dots (r_{i_f} - 1)(q_{j_1} - 1) \dots (q_{j_\ell} - 1)} \prod_{j=1}^{\rho-1} \left(1 - \frac{1}{r_j}\right) \prod_{j=1}^r \left(1 - \frac{1}{q_j}\right).$$

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 $r_\rho > r$.

The last case is when $1 \leq n/(ar_\rho) < 2$. In this case $|B(ar_\rho)| = 1$. Let's $r_{i_1} \dots r_{i_f} r_\rho q_{j_1} \dots q_{j_\ell} = B(ar_\rho)$. 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 the 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 $a \in R_g^{\rho}(a^2, A^*)$ inequality (7) is valid and taking into account (5) we obtain (6). This gives the contradiction to the maximality of A . Hence the maximal $r_\rho \in \mathbb{P} - \mathbb{Q}$ which appear as the 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 gives the statement of Theorem.

This is joint work with R.Ahlswede.

References

- [1] R.Ahlswede and L.Khachatryan, Maximal sets of numbers not containing $k + 1$ pairwise coprime integers, Acta Arithm., LXXII.1, 1995, 77–100
- [2] R.Ahlswede and L.Khachatryan, Sets of integers with pairwise common divisor and a factor from a specified set of primes, Acta Arithm., LXXV.3, 1996, 259–276
- [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

