



Circulant graphs and GCD and LCM of subsets



Joachim von zur Gathen^a, Igor E. Shparlinski^{b,*}

^a B-IT, Universität Bonn, 53113 Bonn, Germany

^b Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia

ARTICLE INFO

Article history:

Received 21 February 2014

Received in revised form 14 June 2014

Accepted 25 July 2014

Available online 8 August 2014

Communicated by Ł. Kowalik

Keywords:

Analysis of algorithms

Computational complexity

Graph algorithms

Circulant graphs

Minimum cover

ABSTRACT

Given two sets A and B of integers, we consider the problem of finding a set $S \subseteq A$ of the smallest possible cardinality such the greatest common divisor of the elements of $S \cup B$ equals that of those of $A \cup B$. The particular cases of $B = \emptyset$ and $\#B = 1$ are of special interest and have some links with graph theory. We also consider the corresponding question for the least common multiple of the elements. We establish NP -completeness and approximation results for these problems by relating them to the Set Cover Problem.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

1.1. Description of the problem and motivation

For a nonempty set A of integers, $\gcd(A)$ and $\text{lcm}(A)$ denote the greatest common divisor and the least common multiple of the elements of A , respectively. We consider some questions of how \gcd and lcm behave on various subsets S of the original set A .

We are interested in both designing algorithms to construct such sets S with prescribed properties of $\gcd(S)$ and $\text{lcm}(S)$ and also in upper and lower bounds on what one can possibly achieve.

We consider the question of finding a subset $S \subseteq A$ of the smallest possible cardinality with minimal \gcd , namely, $\gcd(S) = \gcd(A)$, or with maximal lcm , namely, $\text{lcm}(S) = \text{lcm}(A)$. We also consider a modification of this question where we impose that a specific set B of integers be

contained in S . This B may contain elements of A . This question arises in the theory of *circulant graphs* and is a special case of *graph editing problems*, see Damaschke & Molokov [4], Golovachy [6], Mathieson [8], and Mathieson & Szeider [9] for the background and further references.

To explain this connection we recall that an (undirected) *circulant graph* $G(A, m)$ on m nodes, labelled $0, 1, \dots, m-1$, is defined by a set A of integers called *links*, where the nodes i and j are connected if and only if $|i - j| \equiv a \pmod{m}$ for some $a \in A$. Clearly, $G(A, m)$ is connected if and only if $\gcd(A \cup \{m\}) = 1$. Thus it is natural to ask how many links can at most be removed from A so that the new circulant graph is still connected. This leads to the above question with $B = \{m\}$.

The above can be generalized as follows:

Question 1. Given two sets A and B of positive integers, find a subset $S \subseteq A$ of the smallest possible size with $\gcd(S \cup B) = \gcd(A \cup B)$.

Similarly, we also ask:

* Corresponding author.

E-mail addresses: gathen@bit.uni-bonn.de (J. von zur Gathen), igor.shparlinski@unsw.edu.au (I.E. Shparlinski).

Question 2. Given two sets A and B of positive integers, find a subset $S \subseteq A$ of the smallest possible size with $\text{lcm}(S \cup B) = \text{lcm}(A \cup B)$.

We first formalize these questions as decision problems.

Problem 3. *Minimum subset with minimal gcd*, MINGCD

Input Sets A and B of positive integers, positive integer k .

Question Does A contain a subset S with $\#S \leq k$ and $\text{gcd}(S \cup B) = \text{gcd}(A \cup B)$?

Problem 4. *Minimum subset with maximal lcm*, MAXLCM

Input Sets A and B of positive integers, positive integer k .

Question Does A contain a subset S with $\#S \leq k$ and $\text{lcm}(S \cup B) = \text{lcm}(A \cup B)$?

Throughout the paper, we assume that $A \subseteq \mathbb{Z}$ is nonempty when we write $\text{gcd}(A)$ or $\text{lcm}(A)$.

The input size of an instance (A, B) for both MINGCD and MAXLCM is naturally defined as

$$\text{size}(A, B) = \sum_{a \in A \cup B} \lceil \log(a + 1) \rceil$$

where $\log z$ denotes the binary logarithm of $z \geq 1$.

We also write

$$\text{size}(A) = \text{size}(A, \emptyset).$$

For each of these (and other similar) problems X , we denote as $\text{OPT-}X$ the corresponding optimization problem, where one has to find subsets as described with minimal k .

1.2. Main results

We can now formulate our main results.

Theorem 5. MINGCD and MAXLCM are NP-complete.

Furthermore, a combination of the classical greedy approximation algorithm of Theorem 4 of Johnson [7] and known inapproximability results, see, for example, Theorem 7 of Alon, Moshkovit & Safra [1], yield the following.

Theorem 6. OPT-MINGCD and OPT-MAXLCM can be approximated in polynomial time within a factor $O(\log \text{size}(A, B))$, but not within a factor $o(\log \text{size}(A, B))$ if $P \neq NP$.

2. Various reductions

In this section, we produce reductions between various problems that conserve optimality solutions. This allows us to transfer (in)approximability results between these problems, and also provides standard polynomial-time Cook-reductions as used in the theory of NP-completeness.

2.1. Reduction to $B = \emptyset$

We start by constructing from $A, B \subseteq \mathbb{Z}$ a set $A_B \subseteq \mathbb{Z}$ so that

$$\text{OPT-MINGCD}(A, B) = \text{OPT-MINGCD}(A_B, \emptyset).$$

Lemma 7. For any sets $A, B \subseteq \mathbb{Z}$ one can construct, in polynomial time, a set $A_B \subseteq \mathbb{Z}$ such that $\text{size}(A_B) \leq \text{size}(A, B)$ and

$$\text{gcd}(A \cup B) = \text{gcd}(A_B),$$

and for subset $S \subseteq A$ and $T \subseteq A_B$ of the smallest possible sizes with $\text{gcd}(S \cup B) = \text{gcd}(A \cup B)$ and $\text{gcd}(T) = \text{gcd}(A_B)$, respectively, we have

$$\#S = \#T.$$

Proof. For any integer a , we define the nonnegative integer

$$a_B = \text{gcd}(\{a\} \cup B),$$

and apply this element-wise to any $S \subseteq \mathbb{Z}$:

$$S_B = \{a_B : a \in S\}.$$

We claim that for any $S \subseteq A$ we have

$$\text{gcd}(S \cup B) = \text{gcd}(S_B). \tag{1}$$

For any $c \in \mathbb{Z}$, we have

$$\begin{aligned} c \mid \text{gcd}(S \cup B) &\iff \forall a \in S \forall b \in B \quad c \mid a \quad \text{and} \quad c \mid b \\ &\iff (\forall a \in S \quad c \mid a) \quad \text{and} \quad c \mid \text{gcd}(B) \\ &\iff \forall a \in S \quad c \mid a_B \\ &\iff c \mid \text{gcd}(S_B). \end{aligned}$$

In particular, we have $\text{gcd}(A \cup B) = \text{gcd}(A_B)$.

Distinct $a \in A$ may yield the same a_B . However, if $S \subseteq A$ has minimal size with $\text{gcd}(S \cup B) = \text{gcd}(A \cup B)$, then $a \mapsto a_B$ is injective on S , and $\#S = \#S_B$. Thus

$$\text{OPT-MINGCD}(A, B) \geq \text{OPT-MINGCD}(A_B, \emptyset).$$

For the reverse direction, we take an “inverse” map $\sigma: A_B \rightarrow A$ of $a \mapsto a_B$ on A , namely $\sigma(b) = \min\{a \in A : a_B = b\}$. That is, for every $b \in A_B$, the image $\sigma(b)$ is an element $a \in A$ with $a_B = \text{gcd}(\{a\} \cup B) = b$. For $T \subseteq A_B$ we also define

$$\sigma(T) = \bigcup_{b \in T} \sigma(b).$$

Then $(\sigma(T))_B = T$, since $(\sigma(T))_B \subseteq T$ and for $b \in T$ and $a = \sigma(b)$ we have $b = a_B \in (\sigma(T))_B$. Thus σ is a bijection between T and $\sigma(T)$. For any $T \subseteq A_B$ of minimal size with $\text{gcd}(T) = \text{gcd}(A_B)$, we claim that

$$\text{gcd}(\sigma(T) \cup B) = \text{gcd}(A \cup B).$$

This follows from (1), since $(\sigma(T))_B = T$ and

$$\text{gcd}(A \cup B) = \text{gcd}(A_B) = \text{gcd}(T) = \text{gcd}(\sigma(T) \cup B).$$

Since $\#\sigma(T) = \#T$, we have

$$\text{OPT-MINGCD}(A, B) \leq \text{OPT-MINGCD}(A_B, \emptyset).$$

Overall, it follows that the minimal solution sizes for (A, B) and A_B are equal, and that the solution sets are related by the above correspondence. Clearly the set A_B can be constructed in time polynomial in $\text{size}(A, B)$. \square

An almost identical argument implies an analog of [Lemma 7](#) for $\text{lcm}(A, B)$.

Lemma 8. For any sets $A, B \subseteq \mathbb{Z}$ one can construct in polynomial time a set $A_B \subseteq \mathbb{Z}$ such that $\text{size}(A_B) \leq \text{size}(A, B)$ and

$$\text{lcm}(A \cup B) = \text{lcm}(A_B),$$

and for subset $S \subseteq A$ and $T \subseteq A_B$ of the smallest possible sizes with $\text{lcm}(S \cup B) = \text{lcm}(A \cup B)$ and $\text{lcm}(T) = \text{lcm}(A_B)$, respectively, we have

$$\#S = \#T.$$

Thus both the decision and the optimization versions of the general and the special cases are polynomial-time equivalent.

[Lemmas 7 and 8](#) reduce the general case to the special situation where $B = \emptyset$. Moreover, given a minimum solution set S for one of the two problems, one can easily find a solution for the other one.

So from now on we assume that the input consists of one set A and use $\text{MINGCD}(A)$ and $\text{MAXLCM}(A)$.

2.2. Equivalence of MAXLCM and MINGCD

Here we show that both the decision and the approximation versions of MAXLCM and MINGCD are equivalent. We start with a reduction from MAXLCM to MINGCD .

Lemma 9. For a set $A = \{a_1, \dots, a_n\}$ of positive integers and $L = \text{lcm}(A)$, we define the set

$$B = \{L/a_j : j = 1 \leq j \leq n\}.$$

Then for any set $J \subseteq \{1, \dots, n\}$ we have

$$\text{lcm}(\{a_i : i \in J\}) = L \iff \text{gcd}(\{b_i : i \in J\}) = 1.$$

Proof. For a prime p and $1 \leq j \leq n$ let α_j and β_j be the p -adic orders of a_j and b_j , respectively. Then

$$\alpha = \max_{1 \leq j \leq n} \alpha_j$$

is the p -adic order of L , and $\beta_j = \alpha - \alpha_j$ for all j . For any $J \subseteq \{1, \dots, n\}$ we have

$$\max_{j \in J} \alpha_j = \alpha \iff \max_{j \in J} \{\alpha_j - \alpha\} = 0$$

$$\iff \min_{j \in J} \{\alpha - \alpha_j\} = 0$$

$$\iff \min_{j \in J} \beta_j = 0.$$

Denoting the dependence on p by a superscript, we have

$$\begin{aligned} \text{lcm}(\{a_i : i \in J\}) = \text{lcm}(A) &\iff \forall p \quad \max_{j \in J} \alpha_j^{(p)} = \alpha^{(p)} \\ &\iff \forall p \quad \min_{j \in J} \beta_j^{(p)} = 0 \\ &\iff \text{gcd}(\{b_i : i \in J\}) = 1, \end{aligned}$$

which concludes the proof. \square

The reverse reduction from MINGCD to MAXLCM goes as follows.

Lemma 10. For a set $A = \{a_1, \dots, a_n\}$ of positive integers and $d = \text{gcd}(A)$, we define the set

$$B = \{\text{lcm}(A)/a_j : j = 1 \leq j \leq n\}.$$

Then for any set $J \subseteq \{1, \dots, n\}$ we have

$$\text{gcd}(\{a_i : i \in J\}) = d \iff \text{lcm}(\{b_i : i \in J\}) = \text{lcm}(A)/d.$$

Proof. Without loss of generality we may assume that $d = 1$. Then $\text{lcm}(B) = \text{lcm}(A)$.

In the notation of the proof of [Lemma 9](#), we have $\beta_j = \alpha - \alpha_j$ for $1 \leq j \leq n$. Then,

$$\text{gcd}(\{a_i : i \in J\}) = 1$$

$$\iff \forall p \quad \min_{j \in J} \alpha_j^{(p)} = 0$$

$$\iff \forall p \quad \max_{j \in J} \{\alpha^{(p)} - \alpha_j^{(p)}\} = \alpha^{(p)}$$

$$\iff \forall p \quad \max_{j \in J} \beta_j^{(p)} = \alpha^{(p)}$$

$$\iff \text{lcm}(\{b_i : i \in J\}) = \text{lcm}(B) = \text{lcm}(A),$$

which concludes the proof. \square

Since $\#A = \#B$ in [Lemmas 9 and 10](#), it is enough to prove [Theorems 5 and 6](#) only for MAXLCM and OPT-MAXLCM , respectively.

2.3. The set cover problem

We present polynomial time reductions between MINGCD , MAXLCM and the following problem, SETCOVER , which is well studied in complexity theory.

Problem 11. SETCOVER

Input List \mathcal{C} of subsets of a finite set X , positive integer k .

Question Does \mathcal{C} contain a cover for X of size k or less, that is, a subset $\mathcal{D} \subseteq \mathcal{C}$ with $\#\mathcal{D} \leq k$ such that every element of X belongs to at least one member of \mathcal{D} ?

Let n be the input size, which is in $O(\#\mathcal{C} \cdot \#X \cdot \log t)$ if X consists of positive integers less than t . Furthermore OPT-SETCOVER takes just (\mathcal{C}, X) as input and returns the smallest possible value of k . This task can be approximated in polynomial time within a factor of $O(\log n)$, but no smaller factor (unless $P = NP$), see Alon, Moshkovitz & Safra [1].

It is well known that SETCOVER is NP-complete, see, for example, Problem SP5 in Section A.3.1 of Garey & Johnson [5]. In the next subsections, we present various reductions between SETCOVER and MAXLCM. The latter is trivially in NP, and its reduction to SETCOVER transfers approximation algorithms for the latter to approximation algorithms for MAXLCM. On the other hand, the reduction from SETCOVER to MAXLCM shows that the latter cannot be approximated too well.

2.4. Coprime bases

The basic tool in this reduction is to compute a *coprime basis* (B, e) of some $A \subseteq \mathbb{Z}$, where $B \subseteq \mathbb{Z}$ is a set of pairwise coprime integers $b \geq 2$ and $e: A \times B \rightarrow \mathbb{N}$ is such that $a = \prod_{b \in B} b^{e(a,b)}$ for all $a \in A$. By dropping the unneeded elements b where $e(a, b) = 0$ for all $a \in A$ from B , we may assume that

$$\forall b \in B \exists a \in A: e(a, b) \geq 1. \quad (2)$$

Bach & Shallit [2] discuss in their Section 4.8 coprime bases (under the designation of *gcd-free basis*).

2.5. Reduction from MAXLCM to SETCOVER

- Input* instance $A \subseteq \mathbb{Z}$ of OPT-MAXLCM.
Output instance (C, B) of OPT-SETCOVER.
1. Compute a coprime basis (B, e) of A satisfying (2).
 2. For $b \in B$, let $d(b) = \max\{e(a, b): a \in A\}$.
 3. For $a \in A$, let

$$C_a = \{b \in B: e(a, b) = d(b)\} \subseteq B.$$
 4. For $a \in A$, let

$$a^* = \min\{c \in A: C_a = C_c\} \in A.$$
 5. Set $A^* = \{a^*: a \in A\} \subseteq A$ and $C = \{C_c: c \in A^*\}$.
 6. Return (C, B) .

Lemma 12. *The above reduction works in time polynomial in $\text{size}(A)$, and we have*

- $\text{OPT-MAXLCM}(A) = \text{OPT-SETCOVER}(C, B)$;
- for any $k \geq 1$, transforming (A, k) into (C, B, k) is a polynomial-time Cook-reduction from MAXLCM to SETCOVER.

Proof. In step 2, we have $d(b) \geq 1$ by (2), and

$$\begin{aligned} \text{lcm}(A) &= \text{lcm}\left(\prod_{b \in B} b^{e(a,b)}: a \in A\right) \\ &= \prod_{b \in B} \text{lcm}(b^{e(a,b)}: a \in A) = \prod_{b \in B} b^{d(b)}; \end{aligned}$$

see also Corollary 4.8.2 in Bach & Shallit [2] for a less explicit form of this fact. Since $A^* \subseteq A$, $\text{lcm}(A^*)$ divides $\text{lcm}(A)$. On the other hand, for any of the pairwise coprime factors $b^{d(b)}$ making up $\text{lcm}(A)$, b occurs in some

C_a with $a \in A$ and hence also in C_{a^*} , so that $b^{d(b)}$ divides a^* . It follows that $\text{lcm}(A^*) = \text{lcm}(A)$.

Now we consider the SETCOVER instance with $X = B$ and $C = \{C_a: a \in A^*\}$. For $S \subseteq A^*$, we consider $\mathcal{D} = \{C_a: a \in S\}$. Then $\#\mathcal{D} = \#S$, and

$$\begin{aligned} \text{lcm}(S) = \text{lcm}(A^*) &\iff \forall b \in B \quad b^{d(b)} \mid \text{lcm}(S) \\ &\iff \forall b \in B \exists a \in S \quad b^{d(b)} \mid a \\ &\iff \forall b \in B \exists a \in S \quad e(a, b) = d(b) \\ &\iff \forall b \in B = X \exists a \in S \quad b \in C_a \\ &\iff \mathcal{D} \text{ covers } X. \end{aligned}$$

Thus a solution S of MAXLCM with $\#S \leq k$ implies one of SETCOVER with $\#\mathcal{D} \leq k$.

Conversely, given a cover $\mathcal{D} = \{C_a: a \in S\}$ of X with $\#\mathcal{D} \leq k$ we conclude that $\#S \leq k$, since the sets C_a for $a \in A^*$ are pairwise distinct.

Thus the smallest size of a set $S \subseteq A$ with $\text{lcm}(S) = \text{lcm}(A)$ and the smallest size of a cover \mathcal{D} of X coincide. This shows that the input and output problems have the same optimal solution, and also establishes the claimed reduction between the decision problems. The claim of polynomial time in step 1 follows from Bach & Shallit [2] who show in their Section 4.8 that it can be computed with $O(\text{size}(A)^2)$ bit operations, where, as before, $\text{size}(A)$ is the input size. They use classical arithmetic. According to [3], fast arithmetic yields an algorithm using $\text{size}(A)(\log \text{size}(A))^{O(1)}$ operations. The other steps are simple sorting and selection procedures that can be done in polynomial time. \square

By the above, the size of B is polynomial in that of A . We note that the size of B can actually be much smaller than that of A : take the first m primes, all exponent vectors e in $\{1, 2\}^m$, and then all 2^m values $a_e = \prod_{1 \leq i \leq m} p_i^{e_i}$. Then the coprime basis B consists of just these m primes and $\text{size}(A)$ is only logarithmic in $\text{size}(B)$. That is no worry, since we only use this reduction to derive good approximations for SETCOVER (which do not exist by the hardness result mentioned above) from good approximations to our problems; hence the latter do not exist either.

2.6. Reduction from SETCOVER to MAXLCM

- Input* instance (C, X) of OPT-SETCOVER, with $X = \{1, \dots, m\}$ and $C = \{C_1, \dots, C_l\}$ with each $C_i \subseteq X$.
Output instance $A \subseteq \mathbb{Z}$ of OPT-MAXLCM.
- 1 Let $p_1 < p_2 < \dots < p_m$ be the first m prime numbers.
 - 2 Set $a = \prod_{j \in X} p_j$ and $a_i = \prod_{j \in C_i} p_j$ for $i \leq l$.
 - 3 Return $A = \{a_1, \dots, a_l\}$.

Lemma 13. *The reduction of Section 2.6 works in time polynomial in $\text{size}(C, X)$, and we also have*

- $\text{OPT-SETCOVER}(C, X) = \text{OPT-MAXLCM}(A)$
- for any $k \geq 1$, transforming (C, B, k) into (A, k) is a polynomial-time Cook-reduction from SETCOVER to MAXLCM.

Proof. We may assume that $X = \bigcup_{1 \leq i \leq l} C_i$. Then $a = \text{lcm}(A)$.

Suppose that $I \subseteq \{1, \dots, m\}$ is such that $\text{lcm}(S) = \text{lcm}(A)$, where $S = \{a_i; i \in I\}$. Let

$$\mathcal{D} = \{C_i; i \in I\}.$$

Then for any $j \in X$, p_j divides $\text{lcm}(A) = \text{lcm}(S)$ and hence a_i for some $i \in I$. It follows that $j \in C_i \in \mathcal{D}$. Thus \mathcal{D} covers X .

On the other hand, suppose that $I \subseteq \{1, \dots, m\}$ is such that $\mathcal{D} = \{C_i; i \in I\}$ covers X . Then $S = \{a_i; i \in I\}$ satisfies $\text{lcm}(S) = a = \text{lcm}(A)$.

In both transformations above, the sizes of the sets are conserved.

Since $p_m = (1 + o(1))m \ln m$ as $m \rightarrow \infty$, the bit size of A is in $O(lm \log m)$. The set A can be computed in time polynomial in lm , using the sieve of Eratosthenes for generating the primes. \square

Thus both the decision and the optimization versions of MAXLCM are transformed to those of SETCOVER .

2.7. Concluding the proofs

We start with the upper bounds claimed in [Theorems 5 and 6](#). The fact that MAXLCM is in NP is trivial. Furthermore, [Lemmas 7, 8, 10, and 12](#) show that the known approximation algorithms for SETCOVER also yield ones for our problem.

Furthermore, our claimed lower bounds (NP -hardness and inapproximability) follow from [Lemmas 7, 8, 9, and 13](#),

together with the NP -hardness and inapproximability of SETCOVER , as cited above.

Acknowledgements

The authors are grateful to Fedor Fomin for some references on the approximability and inapproximability of the set cover problem.

The first author's work was supported by the B-IT Foundation and the Land Nordrhein-Westfalen. The second author's work was supported by the Australian Research Council grants DP110100628 and DP140100118.

References

- [1] Noga Alon, Dana Moshkovitz, Shmuel Safra, Algorithmic construction of sets for k -restrictions, *ACM Trans. Algorithms* 2 (2006) 153–177.
- [2] Eric Bach, Jeffrey Shallit, *Algorithmic Number Theory, vol. 1: Efficient Algorithms*, MIT, Cambridge-MA, 1996.
- [3] Daniel J. Bernstein, Factoring into coprimes in essentially linear time, *J. Algorithms* 54 (2005) 1–30.
- [4] Peter Damaschke, Leonid Molokov, Parameterized reductions and algorithms for a graph editing problem that generalizes vertex cover, *Theor. Comput. Sci.* 452 (2012) 39–46.
- [5] Michael R. Garey, David S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W.H. Freeman and Co., San Francisco CA, 1979.
- [6] Petr A. Golovachy, Editing to a connected graph of given degrees, preprint, available from <http://arxiv.org/abs/1308.1802>, 2013.
- [7] David S. Johnson, Approximation algorithms for combinatorial problems, *J. Comput. Syst. Sci.* 9 (1974) 256–278.
- [8] Luke Mathieson, The parameterized complexity of editing graphs for bounded degeneracy, *Theor. Comput. Sci.* 411 (2010) 34–36.
- [9] Luke Mathieson, Stefan Szeider, Editing graphs to satisfy degree constraints: a parameterized approach, *J. Comput. Syst. Sci.* 78 (2012) 179–191.