Least Common Multiplier and P vs. NP problem

Yuly Shipilevsky

Toronto, Ontario, Canada

ABSTRACT We reduce finding of Least Common Multiplier of two integer numbers to polynomial-time integer optimization problem and to NP-hard integer optimization problem that would imply P = NP.

1. Introduction.

In arithmetic and number theory, the least common multiple, lowest common multiple, or smallest common multiple of two integers n and m, usually denoted by lcm(n, m), is the smallest positive integer that is divisible by both n and m (see e.g. [6]). Let us reduce the problem of finding of the Least Common Multiplier of two integer numbers to the following two integer minimization problems.

2. Reducing to the polynomial-time linear programming two-dimensional problem.

The problem of finding of Least Common Multiplier of two integer numbers: n and m can be reduced to the following linear minimization problem:

$$\mathrm{lcm}(n, m) = \{ \min \; nx, \quad \text{subject to} \quad nx - my = 0, \quad x, y, n, m \in N \}. \tag{1}$$

Due to Lenstra [11], minimizing a linear function over the integer points in a polyhedron is solvable in polynomial time provided that the number of integer variables is a constant.

So, problem (1) can be solved in time polynomial.

3. Reducing to the NP-hard non-linear two-dimensional minimization problem.

On the other hand, the problem of finding of Least Common Multiplier of two integer numbers: n and m can be reduced to the following non-linear integer mnimization problem:

$$\mathrm{lcm}(n, m) = \{ \min \ (nx - my)^{2k} + nx, \quad \text{subject to} \quad x, y, n, m, k \in N \}. \tag{2}$$

Despite in general, integer programming is NP-hard or even incomputable (see, e.g., Hemmecke et al. [8]), for some subclasses of target functions and constraints it can be computed in time polynomial.

Note that the dimension of the problem (2) is fixed and is equal to 2.

A fixed-dimensional polynomial minimization in integer variables, where the objective function is a convex polynomial and the convex feasible set is described by arbitrary polynomials can be solved in time polynomial(see, e.g ., Khachiyan and Porkolab [9]).

A fixed-dimensional polynomial minimization over the integer variables, where the objective function $f_0(x)$ is a quasiconvex polynomial with integer coefficients and where the constraints are inequalities $f_i(x) \le 0$, $i = 1, \ldots, k$ with quasiconvex polynomials $f_i(x)$ with integer coefficients, $f_i : \mathbf{R}^n \to \mathbf{R}$, $f_i(x)$, $i = 0, \ldots, k$ are polynomials of degree at most $p \ge 2$, can be solved in time polynomial in the degrees and the binary encoding of the coefficients(s-ee, e.g., Heinz [7], Hemmecke et al. [8], Lee [10]). Note that the degrees are unary encoded here as well as the number of the constraints.

A mixed-integer minimization of a convex function in a convex, bounded feasible set can be done in time polynomial, according to Baes et al. [1], Oertel et al. [12].

As a result, we can expect that there exists such number k, that problem (2) is NP-hard and therefore, since we reduced the same problem to polynomial-time problem (1) and to NP-hard problem (2), it would imply that P = NP.

REFERENCES

[1] M. Baes, T. Oertel, C. Wagner, R. Weismantel, Mirror-Descent Methods in Mixed-Integer Convex Optimization, in: M. Jünger, G. Reinelt (Eds.), Facets of combinatorial optimization, Springer, Berlin, New York, 2013, pp. 101–131. http://arxiv.org/pdf/1209.0686.pdf

[2] S. Boyd and L. Vandenberghe. Convex Optimization. Cambridge University Press, 2004. https://web.stanford.edu/~boyd/cvxbook/bv_cvxbook.pdf

[3] T. Cormen, C. Leiserson, R. Rivest, C. Stein, Introduction To Algorithms, third ed, The MIT Press, Cambridge, 2009.

[4] A. Del Pia, R. Weismantel, Integer quadratic programming in the plane, Proceedings of SODA, 2014, pp. 840-846. https://sites.google.com/site/albertodelpia/home/publications

[5] A. Del Pia, R. Hildebrand, R. Weismantel, K. Zemmer, Minimizing Cubic and Homogeneous Polynomials over Integers in the Plane,To appear in Mathematics of Operations Research (2015). https://arxiv.org/pdf/1408.4711.pdf

[6] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers (Fifth edition), Oxford University Press, 1979.

[7] S. Heinz, Complexity of integer quasiconvex polynomial optimization, J. Complexity 21(4) (2005) 543–556.

[8] R. Hemmecke, M. Köppe, J. Lee, R. Weismantel, Nonlinear Integer Programming, in: M. Jünger, T. Liebling, D. Naddef, W. Pulleyblank, G. Reinelt, G. Rinaldi, L.Wolsey (Eds.), 50 Years of Integer Programming 1958–2008: The Early Years and State-of-the-Art Surveys, Springer-Verlag, Berlin, 2010, pp. 561–618. http://arxiv.org/pdf/0906.5171.pdf

[9] L. G. Khachiyan, L. Porkolab, Integer optimization on convex semialgebraic sets, Discrete and Computational Geometry 23(2) (2000) 207–224.

[10] J. Lee, On the boundary of tractability for nonlinear discrete optimization, in: Cologne Twente Workshop 2009, 8th Cologne Twente Workshop on Graphs and Combinatorial Optimization, Ecole Polytechnique, Paris, 2009, pp. 374–383. http://www.lix.polytechnique.fr/ctw09/ctw09-proceedings.pdf#page=385

[11] A. K. Lenstra, H. W. Jr. Lenstra, (Eds.), The development of the numb-

er field sieve, Springer-Verlag, Berlin, 1993.
[12] T. Oertel, C. Wagner, R. Weismantel, Convex integer minimization in fixed dimension, CoRR 1203–4175(2012). http://arxiv.org/pdf/1203.4175.pdf