INTEGER OPTIMIZATION AND P vs NP PROBLEM

YULY SHIPILEVSKY

Toronto, Ontario, Canada

ABSTRACT. We give a polynomial-time solution for the "modulo $\mathcal{NP}$-complete problem" on the base of integer optimization algorithms.

1. **Introduction.** Despite in general, Integer Programming is $\mathcal{NP}$-hard or even incomputable (see, e.g., Hemmecke et al. [10]), for some subclasses of target functions and constraints it can be computed in time polynomial.

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 [11]), see Lenstra [13] as well.

A fixed-dimensional polynomial minimization over the integer variables, where the objective function is a quasiconvex polynomial with integer coefficients and where the constraints are inequalities with quasiconvex polynomials of degree at most ≥ 2 with integer coefficients can be solved in time polynomial in the degrees and the binary encoding of the coefficients(see, e.g., Heinz [8], Hemmecke et al. [10], Lee [12]).

Minimizing a convex function over the integer points of a bounded convex set is polynomial in fixed dimension, according to Oertel et al. [15].

Del Pia and Weismantel [4] showed that Integer Quadratic Programming can be solved in polynomial time in the plane.

It was further generalized for cubic and homogeneous polynomials in Del Pia et al. [5].

We are going to transform well-known $\mathcal{NP}$-complete problem to the polynomial-time integer minimization algorithm. It would mean, that $\mathcal{P} = \mathcal{NP}$, since if there is a polynomial-time algorithm for any $\mathcal{NP}$-hard problem, then there are polynomial-time algorithms for all problems in $\mathcal{NP}$ (see Garey and Johnson [7], Manders and Adleman [14], Cormen et al. [2]).

2020 *Mathematics Subject Classification*. Primary: 90C11; Secondary: 90C48, 68Q25.
Key words and phrases. Integer optimization, $\mathcal{NP}$-complete, polynomial-time.

Fortnow in [6] stated: "We call the very hardest $\mathcal{NP}$ problems (which include Partition Into Triangles, Clique, Hamiltonian Cycle and 3-Coloring) "$\mathcal{NP}$-complete", i.e. given an efficient algorithm for one of them, we can find efficient algorithm for all of them and in fact any problem in $\mathcal{NP}$".

2. **Polynomial-time Algorithm. Sliding Tangent.**

Lemma 1 (De Loera et al. [3], Hemmecke et al. [10], Del Pia et al. [5]).
The problem of minimizing a degree-4 polynomial over the lattice points of a convex polygon is $\mathcal{NP}$-hard.

Proof. They use the $\mathcal{NP}$-complete problem AN1 on page 249 of Garey and Johnson [7]. This problem states it is $\mathcal{NP}$-complete to decide whether, given three positive integers a, b, c, there exists a positive integer $x < c$ such that x^2 is congruent with "a" modulo "b". This problem is clearly equivalent to asking whether the minimum of the quartic polynomial function $(x^2 - a - by)^2$ over the lattice points of the rectangle:

$\{ (x,y) \mid 1 \le x \le c-1,\ 1-a \le by \le (c-1)^2 - a \}$ is zero or not. □

According to Del Pia and Weismantel [4], minimization problem, given in the above proof of Lemma 1 is equivalent to the following problem:

$$\min \{ (x^2 - a - by) \text{ subject to } x^2 - a - by \ge 0,\ 1 \le x \le c-1,\ 1-a \le by \le (c-1)^2 - a,\ x, y \in \mathbf{Z} \}. \tag{1}$$

If $L := \{ (x, y) \in \mathbf{R}^2 \mid x^2 - a - by \ge 0,\ x \ge 0 \}$,
$G := \{ (x, y) \in \mathbf{R}^2 \mid 1 \le x \le c-1,\ 1-a \le by \le (c-1)^2 - a \}$,

problem (1) can be rewritten as follows:

$$\mu := \min \{ (x^2 - a - by) \mid (x, y) \in (L \cap G) \cap \mathbf{Z}^2 \}. \tag{2}$$

If $by_{min} = 1 - a$, $by_{max} = (c-1)^2 - a$, then the above defined rectangle:

$G = \{ (x, y) \in \mathbf{R}^2 \mid 1 \le x \le c - 1, \ y_{min} \le y \le y_{max} \}$.

Note that parabola: $by = bf(x) = x^2 - a, \ x \ge 0$ is a part of the border of set L (the top) and we have:

$bf(1) = 1 - a = by_{min}$, $bf(c-1) = (c-1)^2 - a = by_{max}$.
Thus: $f(1) = y_{min}$, $f(c-1) = y_{max}$.

Set L is not convex, as well as the set $L \cap G$ (see Boyd and Vandenberghe [1], Osborne [16]).
The equation of the tangent to the parabola: $by = bf(x) = x^2 - a$, at the point i: $1 \le i \le c - 1$, $i \in \mathbf{Z}$, $x \in \mathbf{R}$ is given by:

$$by_i(x) = 2i(x - i) + i^2 - a. \qquad (3)$$

The segment of this tangent (hypotenuse), which is inside G and having one end $D_i = (d_{1i}, d_{2i})$ on the horizontal line $by = 1 - a$, and another end $H_i = (h_{1i}, h_{2i})$ on the vertical line $x = c - 1$, together with two other segments: on the horizontal line $by = 1 - a$ and on the vertical line $x = c - 1$, both segments intersect at the point $E = (e_1, e_2)$: $e_1 = c - 1$, $be_2 = 1 - a$ (cathetuses), form some right triangle D_iH_iE:

$$D_iH_iE := S_i := \{ (x, y) \in G \mid y \le y_i(x) \}, \ 1 \le i \le c - 1, i \in \mathbf{Z}.$$

Proposition 1. *$2id_{1i} = i^2 + 1$, $bd_{2i} = 1 - a$,
$h_{1i} = c - 1$, $bh_{2i} = 2i(c - 1) - i^2 - a$,
$1 \le i \le c - 1$, $i \in \mathbf{Z}$.*

Proof. It follows from the definition of points D_i, H_i and (3): considering points D_i and H_i as intersections of the tangent (3) and the corresponding horizontal and vertical lines, described above, we have for the points D_i:
$y_i(d_{1i}) = d_{2i} = y_{min}$, and for the points H_i: $h_{2i} = y_i(h_{1i}) = y_i(c - 1)$. □

Corollary 1. *$d_{11} = 1$, $2(c - 1)\, d_{1\,c-1} = 1 + (c - 1)^2$,
$d_{11} < d_{1i} < d_{1\,c-1}$, $i = 2, \ldots, c - 2$,
$d_{1i} < d_{1i+1}$, $i = 1, \ldots, c - 2$.*

Proof. Function $d(t)$: $2d(t) = t + t^{-1}$ is a strictly increasing function over the interval $1 \leq t \leq c - 1$, since its derivative $d'(t)$: $2d'(t) = 1 - t^{-2}$ is positive for $t > 1$ and equal to zero at the point $t = 1$, $t \in \mathbf{R}$. □

Corollary 2. $bh_{21} = 2c - 3 - a$, $bh_{2\,c-1} = (c - 1)^2 - a$,
$h_{21} < h_{2i} < h_{2\,c-1}$, $i = 2, \ldots, c - 2$,
$h_{2i} < h_{2i+1}$, $i = 1, \ldots, c - 2$.

Proof. Function $h(t)$: $bh(t) = 2t(c - 1) - t^2 - a$ is a strictly increasing function over the interval $1 \leq t \leq c - 1$, since its derivative $h'(t)$: $bh'(t) = 2(c - 1) - 2t$ is positive on the interval $1 \leq t < c - 1$ and equal to zero at the point $t = c - 1$, $t \in \mathbf{R}$. □

Lemma 2. $(L \cap G) \cap \mathbf{Z}^2 = \cup (S_i \cap \mathbf{Z}^2)$, $1 \leq i \leq c - 1$, $i \in \mathbf{Z}$.

Proof. It follows from the above given definitions and properties of sets

L, G, S_i, ($1 \leq i \leq c - 1$, $i \in \mathbf{Z}$) and due to continuity, differentiability, convexity and monotonicity of function $f(x)$, ($x \geq 0$).

In particular, it is well-known that a differentiable function of one variable is convex on an interval Ω if and only if its graph lies above all of its tangents: $f(x) \geq f(y) + f'(y)(x - y)$, $x, y \in \Omega$ (see, e.g., Boyd and Vandenberghe [1, section 3.1.3]). □

Thus, instead of non-convex set $L \cap G$, we can consider a collection of right triangles: $\{ S_i \}$, so that search space of the problem (2): $(L \cap G) \cap \mathbf{Z}^2$ is identical to the union: $\cup (S_i \cap \mathbf{Z}^2)$, $1 \leq i \leq c - 1$, $i \in \mathbf{Z}$.

Let us denote:

$$\mu_i := \min \{ (x^2 - a - by) \mid (x, y) \in S_i \cap \mathbf{Z}^2 \}, \quad 1 \leq i \leq c - 1, \ i \in \mathbf{Z}. \tag{4}$$

Theorem 1. $\mu = \min \{ \mu_i \mid 1 \leq i \leq c - 1, i \in \mathbf{Z} \}$.

Proof. It follows from the above given definitions of μ, μ_i and Lemma 2.

Each problem (4) is Integer Quadratic Programming problem in the plane. According to Del Pia and Weismantel [4], Theorem 1.1, they can be solved in polynomial time.

Recall that polynomial-time algorithms are closed under union, composition, concatenation, intersection, complementation and some other operations: see, e.g., Hopcroft et al. [9], pp. 425−426, Cormen et al. [2], p. 1055.

The class of languages decidable in polynomial time, class $\mathcal{P}$, is closed under union, concatenation and the other above mentioned operations. This means that if you have two languages in $\mathcal{P}$, their union, concatenation, etc., is also in $\mathcal{P}$. Using mathematical induction, it can be trivially extended to any finite number of languages and combinations of the above given operations.

That is why, due to Theorem 1, our original $\mathcal{NP}$-complete problem (2) can be solved in polynomial time as well.

As a result, since due to the above algorithm, $\mathcal{NP}$-complete problem can be solved in polynomial time, we can conclude that $\mathcal{P} = \mathcal{NP}$, since as we mentioned above, if there is a polynomial-time algorithm for any $\mathcal{NP}$-hard problem, then there are polynomial-time algorithms for all problems in $\mathcal{NP}$.

Since the original $\mathcal{NP}$-complete problem is asking whether the corresponding minimum is zero or not, we can, finally, give the following algorithm (polynomial-time) for its solution:

Input: positive integers a, b, c.
Output: Zero_Or_Not.

Set Zero_Or_Not = "Not_Zero" .

for i = 1, ... , c − 1 **do**
  if $\min \{ (x^2 - a - by) \mid (x, y) \in S_i \cap \mathbf{Z}^2 \} = 0$
  then Set Zero_Or_Not = "Zero"
  break
  end
end
return Zero_Or_Not

3. **Conclusion.** We reduced $\mathcal{NP}$-complete problem to the polynomial-time algorithm, Thus, we can conclude that $\mathcal{P} = \mathcal{NP}$, since if there is a polynomial-time algorithm for any $\mathcal{NP}$-hard problem then there are polynomial-time algorithms for all problems in $\mathcal{NP}$.

REFERENCES

[1] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.

[2] T. Cormen, C. Leiserson, R. Rivest and C. Stein, *Introduction To Algorithms*, fourth ed., The MIT Press, Cambridge, 2022.

[3] J. A. De Loera, R. Hemmecke, M. Köppe and R.Weismantel, Integer polynomial optimization in fixed dimension, *Mathematics of Operations Research*, **31** (2006), 147–153.

[4] A. Del Pia and R. Weismantel, Integer quadratic programming in the plane, *SODA (Chandra Chekuri, ed.), SIAM*, (2014), 840–846.

[5] A. Del Pia, R. Hildebrand, R. Weismantel and K. Zemmer, Minimizing Cubic and Homogeneous Polynomials over Integers in the Plane, *Mathematics of Operations Research*, **41** (2015a), 511–530.

[6] L. Fortnow, *The Status of the P versus NP Problem*, Northwestern University, 2009.

[7] M. R. Garey and D. S. Johnson, *Computers and intractability*, W. H. Freeman and Co., San Francisco, Calif., A guide to the theory of NP-completeness, A Series of Books in the Mathematical Sciences, 1979.

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

[9] J. E. Hopcroft, R. Motwani and J. D. Ullman, *Introduction to automata theory, languages and computation*, second ed., Addison-Wesley, Boston, 2001.

[10] R. Hemmecke, M. Köppe, J. Lee and 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), 561–618.

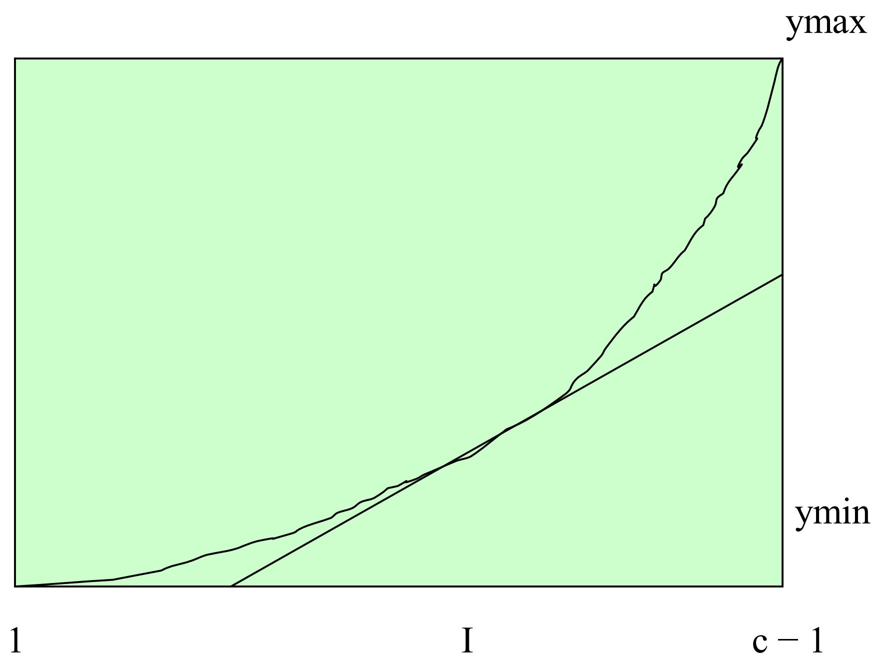
[11] L. G. Khachiyan and L. Porkolab, Integer optimization on convex semialgebraic sets, *Discrete and Computational Geometry*, **23** (2000), 207–224.

[12] 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), 374–383.

[13] H.W. Jr. Lenstra, Integer programming with a fixed number of variables, *Mathematics of Operations Research*, **8** (1983), 538–548.

[14] K. Manders and L. Adleman, NP-complete decision problems for binary quadratics, Journal of Computer and System Sciences, **16** (1978), 168–184.

[15] T. Oertel, C. Wagner and R. Weismantel, Convex integer minimization in fixed dimension, preprint, 2012, arXiv:1203.4175.
[16] M. J. Osborne, *Mathematical Methods for Economic Theory: a tutorial*, University of Toronto, 2007.



E-Mail: yulysh2000@yahoo.ca