Integer factorization implemented in time polynomial

Yuly Shipilevsky

Toronto, Ontario, Canada
E-mail address: yulysh2000@yahoo.ca

Abstract

A polynomial-time algorithm for integer factorization, wherein integer factorization reduced to a polynomial-time integer minimization problem over the integer points in a two-dimensional polyhedron.

Keywords: integer factorization, integer programming, polynomial-time, NP-hard.

1. Introduction

Cryptography, elliptic curves, algebraic number theory have been brought to bear on integer factorization problem.

Until now, no algorithm has been published that can factor in deterministic polynomial time. For an ordinary computer the best published asymptotic running time is for the general number field sieve (GNFS) algorithm [10,12].

The purpose of this paper is to develop a polynomial-time integer factorization algorithm, factoring in deterministic polynomial time.

The plan of this paper is as follows. In Section 2 we reduce integer factorization problem to some 2-dimensional integer minimization problem and show that if there exists a nontrivial divisor of N, those divisor is a minimizer of those 2-dimensional integer minimization problem, and any minimizer of those integer minimization problem is a nontrivial divisor of N.

In Section 3 we introduce and investigate a notion of U-equivalent conversion of minimization problems for changing properties of the objective functions and preserving the set of minimizers of the original problem.

In Section 4 we reduce integer factorization problem to the polynomial-time integer minimization problem over the integer points in a 2-dimensional polyhedron, solvable in time polynomial in log(N).

Finally, we conclude that since we found a polynomial-time algorithm to solve an NP-hard problem, it would mean that P is equal to NP.

2. Reduction to the Integer Programming problem

Let us reduce integer factorization problem to some integer minimization problem, so that any minimizer that is found solves integer factorization problem.

The key idea is to construct the objective function and constraints so that any minimizer satisfies the equation: $xy = N$, and, therefore, is a solution of the integer factorization problem.

Let us consider the following integer minimization problem:

$$\begin{aligned} &\text{minimize} \quad xy \\ &\text{subject to} \quad xy \geq N, \qquad (1) \\ &\qquad 2 \leq x \leq N - 1, \\ &\qquad N/(N-1) \leq y \leq N/2, \\ &\qquad x \in \mathbf{N},\ y \in \mathbf{N},\ N \in \mathbf{N}. \end{aligned}$$

Let $\Omega := \{ (x, y) \in \mathbf{R}^2 \mid xy \geq N,\ 2 \leq x \leq N - 1, N/(N-1) \leq y \leq N/2, x \in \mathbf{R},\ y \in \mathbf{R} \}$ for a given $N \in \mathbf{N}$.

Hence, $\Omega^I = \Omega \cap \mathbf{Z}^2$ is a feasible set of the problem (1).

It is clear that if there exists a nontrivial solution of integer factorization problem $xy = N$, the objective function: $f(x, y) = xy$ reaches minimum at the integer point of the border $xy = N$ of the region Ω and if there exists a nontrivial solution of integer factorization problem, any minimizer of the problem (1) provides a (nontrivial) solution of integer factorization problem.

Thus, in this case, any minimizer of the problem (1) guarantees solution of integer factorization problem and there exists at least one such minimizer.

Theorem 1. *If there exists a nontrivial solution of integer factorization problem, that solution is a minimizer of problem* (1) *and if there exists a nontrivial solution of integer factorization problem, any minimizer of the problem* (1) *is a nontrivial solution of integer factorization problem.*

As a result, we obtain the following Integer Factorization Algorithm.

Algorithm 1(Integer Factorization Algorithm).

```
Input:    A positive integer number N.
Output:   A nontrivial divisor of N(if it exists).
          Solve the problem (1):
          Based on the input data compute a minimizer ( $x_{min}$, $y_{min}$ )
          of the problem (1).
          if ($x_{min} y_{min} = N$)
          then
              Return a nontrivial divisor $x_{min}$ of N
          else
              Return "N is a prime"
```

Let us determine the complexity of the problem (1).

Despite in general integer programming is NP-hard or even incomputable, see, e.g., Hemmecke et al. [7], for some subclasses of the objective functions and constraints it can be computed in time polynomial.

Note that the dimension of the problem (1) 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 [8].

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 $f_i(x) \le 0$, $i = 1, \dots, k$ with quasiconvex polynomials $f_i(x)$ with integer coefficients, $f_i : \mathbf{R}^n \to \mathbf{R}$, $f_i(x)$, $i = 0, \dots, k$ 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, - see, e.g., Heinz [6], Hemmecke et al. [7], Lee [9].

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. [2], Oertel et al. [11].

Since the objective function $f(x, y) = xy$ of the problem (1) is a quasiconcave function in the feasible set Ω of the problem (1), we cannot use the results described in Baes et al. [2], Heinz [6], Hemmecke et al. [7], Khachiyan and Porkolab [8], Oertel et al. [11] in order to solve the problem (1) in time polynomial in log(N). Note that Ω^I is described by quasiconvex polynomials, since $(-xy + N)$ is a quasiconvex function for $x > 0$, $y > 0$.

In general, since variables $x \in \mathbf{N}$, $y \in \mathbf{N}$ are bounded by the finite bounds $2 \le x \le N - 1$, $N/(N-1) \le y \le N/2$, the problem (1) and the respective Algorithm 1 are computable [7], but still are NP-hard, since the problem (1) is a quadratically constrained integer programming problem [4].

3. U-equivalent minimization

The following results give us a possibility to change the properties of the objective function with preservation of the set of minimizers of the original problem.

Theorem 2. *Let* O *be the minimization problem:*

$$O = \{\textit{minimize } g(x) \textit{ subject to } x \in G\},\ g\colon X \to \mathbf{R},\ G \subseteq X.$$

Let E *be the minimization problem:*

$$E = \{\textit{minimize } U(g(x)) \textit{ subject to } x \in G\},\ G \subseteq X,$$

where U: $\mathbf{R} \to \mathbf{R}$, $U = U(u)$ *is any increasing function.*

Let M_O *be a set of minimizers of problem* O *and*

let M_E *be a set of minimizers of problem* E. *Then:*

$$M_O = M_E.$$

Proof. If $x_0 \in M_O$ then $g(x_0) \le g(x)$ for any $x \in G$. Hence, $U(g(x_0)) \le U(g(x))$ for any $x \in G$, since function U is the increasing function and therefore $x_0 \in M_E$ and $M_O \subseteq M_E$. If $x_0 \in M_E$ then we have: $U(g(x_0)) \le U(g(x))$ for any $x \in G$ and therefore $g(x_0) \le g(x)$ for any $x \in G$, as otherwise there exists $y_0 \in G$ such that $g(x_0) > g(y_0)$ and since function U is the increasing function it would mean that $U(g(x_0)) > U(g(y_0))$ in contradiction to the original supposition that $U(g(x_0)) \le U(g(x))$ for any $x \in G$. So, since $g(x_0) \le g(x)$ for any $x \in G$ then $x_0 \in M_O$ and $M_E \subseteq M_O$ and finally: $M_O = M_E$. □

Definition 1. *We say that the minimization problem:*

$$E = \{\textit{minimize}\ \ U(g(x))\ \ \textit{subject to}\ \ x \in G\},$$

is U*–equivalent to the minimization problem:*

$$O = \{\textit{minimize}\ \ g(x)\ \ \textit{subject to}\ \ x \in G\},\ g\colon X \to \mathbf{R},\ G \subseteq X,$$

where $U\colon \mathbf{R} \to \mathbf{R}$, $U = U(u)$ *is some increasing function.*

Corollary 1. *If* E *is* U*-equivalent to* O *then* E *and* O *have the same set of minimizers.*

Proof. It follows from Theorem 2 and Definition 1. □

Thus, using U-equivalence we can convert original minimization problem into minimization problem that has objective function with desired properties, so that both problems, - the original one, and U-equivalent have the same set of minimizers and share the same feasible set.

Hence, as a result of the U-equivalent conversion the original feasible set and the original set of minimizers remain unchanged, whereas the objective function is being changed to obtain desired properties (e.g., faster minimization), which can consider it(U-equivalence) as a flexible and effective tool.

U-equivalent conversion can be considered as unary operation defined on the set of minimization problems, having the same feasible set.

Example 1. Suppose, the problem (1) is the original minimization problem. Let q be e^u-equivalent to the problem (1). The objective function of the problem (1) is xy, whereas the objective function of q is $f(x, y) = e^{xy}$.
Both problems, due to the Theorem 2 have the same set of minimizers (and each such minimizer is a solution of the integer factorization problem, according to the Theorem 1). Note that if N is not a prime, minimum $q = e^N$.

However, no U-equivalent conversion applied to the original problem (1) in order to get a quasiconvex objective function exists, since if a function g is quasiconcave and a function U is increasing, then a function f, defined as $f(x, y) = U(g(x, y))$ is still quasiconcave.

4. Linearization. Polynomial-time integer factorization. Minimum Principle.

It was shown in Del Pia et al. [4] that problem of minimizing a quadratic polynomial with integer coefficients over the integer points in a general two-dimensional rational polyhedron is solvable in time bounded by a polynomial in the input size and it was further extended to all homogeneous polynomials in Del Pia et al. [5].

Del Pia et al. [4] consider the following problem:

min{ f^k (z) : z ∊ P ∩ $\mathbf{Z}^n$ }, where f^k is a polynomial function of degree at most k with integer coefficients, and P is a rational polyhedron in $\mathbf{R}^n$. We recall that a rational polyhedron is the set of points that satisfy a system of linear inequalities with rational data. According to Del Pia et al. [4], this problem can be solved in time polynomial for n = k = 2.

Theorem 3(Theorem 1.1 in Del Pia et al. [4]). *If n = k = 2, problem min{ f^k (z) : z ∊ P ∩ $\boldsymbol{Z}^n$ } can be solved in polynomial time.*

We are going now to reformulate the original problem (1) by replacing it with the equivalent problem, having the same target function, but feasible set as the integer points in some two-dimensional rational polyhedron(polygon), which therefore can be solved in polynomial time according to Theorem 3(Theorem 1.1 in Del Pia et al. [4]).

Let us construct the corresponding polyhedron G, as having the edges M_iM_{i+1}, where the vertex M_i is a point on the portion xy = N of the boundary of region Ω of (1), the point, corresponding to x = i, 2 ≤ i ≤ N – 2, so M_i = (i, N/i), plus edges M_2A and $M_{N-1}A$, along two other portions(parallel to the x axis and y axis correspondingly) of three portions of the boundary of regi-Ω, where the vertex A := (N – 1, N/2). Polyhedron G can be described as a set of points that satisfy the corresponding system of linear inequalities with rational data, each inequality corresponds to one edge of G and can be described in the form: ax + by ≤ c, wherein a,b and c are rational and depend on N, and wherein (x, y) ∈ $\mathbf{R}^2$.

Theorem 4. $\Omega \cap \boldsymbol{Z}^2 = G \cap \boldsymbol{Z}^2$.

Proof. It follows from definitions of Ω and G and their convexity and convexity of G follows from the convexity of Ω. □

Theorem 5. *Problem (1) is equivalent to the problem:*

$$min\{\, xy : \ (x,y) \ \in \ G \cap \boldsymbol{Z}^2 \ \} \tag{2}$$

Proof. It follows from Theorem 4 and problem (1). □

Theorem 6(Minimum Principle). *If* N *is not a prime, any minimizer of (2) is a solution of integer factorization problem for* N *and any solution of integer factorization problem for* N *is a minimizer of (2).*

Proof. It follows from Theorem 1 and Theorem 5. □

Problem (2) completely satisfies Del Pia et al. [4] and therefore (2) and integer factorization problem can be solved in time polynomial in log(N).

Finally, we obtain the following algorithm.

Algorithm 2(Integer Factorization Algorithm).
Input: A positive integer number N.
Output: A nontrivial divisor of N(if it exists).

```
Solve the problem (2) using algorithms [4]:
Based on the input data compute
a minimizer ( $x_{min}$, $y_{min}$ )
of the problem (2).
if ($x_{min} y_{min} = N$)
then
    Return a nontrivial divisor $x_{1 min}$ of N
else
    Return "N is a prime"
```

So, Algorithm 2 runs in time polynomial in log(N).

Thus, factoring is in FP(the class FP is the set of function problems which can be solved by a deterministic Turing machine in polynomial time(see e.g. Cormen et al. [3]).

Theorem 7. *Integer factorization is in* FP.

Algorithm 2 can be modified to serve the decision problem version as well - given an integer N and an integer q with $1 \leq q \leq N$, does N have a factor d with $1 < d < q$?

Let $\Omega_q := \{ (x, y) \in \mathbf{R}^2 \mid xy \geq N, \ 2 \leq x \leq q-1, \ N/(q-1) \leq y \leq N/2, \ x \in \mathbf{R}, \ x \in \mathbf{R} \}$ for a given q, $3 \leq q \leq N$, $N \in \mathbf{N}$.

Let G_q the polyhedron, corresponding to Ω_q. Let $G_q^I = G_q \cap \mathbf{Z}^2$

Let us replace (2) by the problem over the feasible set G_q^I and denote the modified minimization problem (corresponding to the problem (2)) as (3).

Algorithm 3(Integer Factorization Algorithm).
Input: Positive integer numbers N, $q < N$.
Output: Existence of a factor d with $1 < d < q$.

```
Solve the problem (3) using algorithms [4]:
Based on the input data compute
a minimizer $(x_{min}, y_{min})$
of the problem (3)
if $(x_{min} y_{min} = N)$
then
    Return "The corresponding factor exists"
else
    Return "The corresponding factor does not exist"
```

Hence, Algorithm 3 runs in time polynomial in log(N) as well.

Thus, factoring is in P. The class P is the class of sets accepted by a deterministic polynomial-time Turing machines (see, e.g., Cormen et al. [3]).

Theorem 8. *Integer factorization is in* P.

Note that algorithms 2-3 can be considered as polynomial-time primality tests and the only provably polynomial-time primality test was developed by Agrawal et al. [1].

We developed polynomial-time Algorithms 2-3 in order to find minimizers of (2) which is equivalent (due to Theorem 5) to NP-hard problem (1). It is well known that if there is a polynomial-time algorithm for any NP-hard problem, then, there are polynomial-time algorithms for all problems in NP, and hence, we would conclude that P is equal to NP.

References

[1] M. Agrawal, N. Kayal, N. Saxena, PRIMES is in P, Annals of Mathematics 160(2) (2004) 781–793.

[2] 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, available electronically from http://arxiv.org/pdf/1209.0686.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, available electronically from 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), available electronically from https://arxiv.org/pdf/1408.4711.pdf

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

[7] 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, available electronically from http://arxiv.org/pdf/0906.5171.pdf

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

[9] 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, available electronically from http://www.lix.polytechnique.fr/ctw09/ctw09-proceedings.pdf#page=385

[10] A. K. Lenstra, H. W. Jr. Lenstra, (Eds.), The development of the number field sieve, Springer-Verlag, Berlin, 1993.

[11] T. Oertel, C. Wagner, R. Weismantel, Convex integer minimization in fixed dimension, CoRR 1203–4175(2012), available electronically from http://arxiv.org/pdf/1203.4175.pdf

[12] P. Stevenhagen, The number field sieve, Algorithmic Number Theory: Lattices, Number Fields, Curves, and Cryptography, Mathematical Sciences Research Institute Publications, Cambridge University Press, Cambridge, 2008.