Polynomial-time Integer Factorization Algorithms

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 rational polyhedron with conclusion that P = NP and a polynomial-time algorithm for integer factorization using enumeration of vertices of integer hull of those two-dimensional rational polyhedron

Keywords: integer factorization, integer programming, polynomial-time, NP-hard, rational polyhedron, integer hull

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(see, e.g., A. K. Lenstra and H. W. Jr. Lenstra [10], P. Stevenhagen [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 two-dimensional integer minimization problem and show that if there exists a nontrivial divisor of N, those divisor is a mi-

nimizer of those two-dimensional integer minimization problem, and any minimizer of those integer minimization problem is a nontrivial divisor of N.

We show that those two-dimensional integer minimization problem is NP-hard problem.

In Section 3 we construct a special two-dimensional rational polyhedron and reduce those NP-hard integer minimization problem to the integer minimization problem over the integer points in those rational polyhedron, solvable in time polynomial together with the original integer factorization problem.

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.

We develop a polynomial-time algorithm for integer factorization by enumeration of vertices of integer hull of those two-dimensional rational polyhedron.

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:

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

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 target 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, $f_i : \mathbf{R}^n \to \mathbf{R}$,

$f_i(x)$, $i = 0, \ldots, k$ are polynomials of degree at most $p \geq 2$, 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]). 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. [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 $2 \leq x \leq N - 1$, $N/(N-1) \leq y \leq N/2$, the problem (1) and the respective Algorithm 1 are computable(see, e.g., Hemmecke et al. [7]), but still are NP-hard, since the problem (1) is a quadratically constrained integer minimization problem(see, e.g., Del Pia and Weismantel [4], Del Pia et al. [5]).

Note that NP-hardness of (1) is clearly confirmed, e.g. in Del Pia et al. [5] : "... Using the same reduction as Lemma 1.2, it is possible to show that problem (1) is NP-hard even when $n = d = 2$, P is a bounded, rational polyhedron, and we add a single quadratic inequality constraint (see [18]) ...".

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

It was shown in Del Pia and Weismantel [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 cubic and homogeneous polynomials in Del Pia et al. [5].

Del Pia and Weismantel [4] consider the following problem:

$\min\{ f^k(z) : z \in P \cap \mathbf{Z}^n \}$, 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 and Weismantel [4], this problem can be solved in time polynomial for $n = k = 2$.

Theorem 2(Theorem 1.1 in Del Pia and Weismantel [4]). *If $n = k = 2$, problem $\min\{ f^k(z) : z \in P \cap \mathbf{Z}^n \}$ can be solved in polynomial time.*

Recall that Theorem 2 is given(Theorem 1.1) in generalized form in aforementioned Del Pia et al. [5] as well as the following standard definitions are clearly mentioned there.

For a rational polyhedron $P := \{\mathbf{x} \in \mathbf{R}^n : A\mathbf{x} \leq \mathbf{b}\}$, with $A \in \mathbf{Z}^{mxn}$, $\mathbf{b} \in \mathbf{Z}^m$ the following is defined in Del Pia et al. [5]: "...We use the words size and binary encoding length synonymously. The size of P is the sum of the sizes of A and **b**. We say that problem can be solved in polynomial time if in time bounded by a polynomial in the size of A,**b** and M we can either determine that the problem is infeasible, find a feasible minimizer...". (M = 1 in our case). We use here exactly the same definitions. These definitions and Theorem 2 are extremely and critically important for understanding the results, obtaned in the paper. We emphasize, that according to Theorem 2, for general rational polyhedron the only conditions for the polynomial-time minimization are the following conditions: "n" and "k" must be fixed and n = k = 2: the number of linear inequalities - "m" is not supposed to be fixed to provide the fact of polynomiality in time and "m" does not belong to the binary encoded input: it is unary encoded.

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 2(Theorem 1.1 in Del Pia and Weismantel [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 $x = i$, $2 \leq i \leq N - 2$, 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 region 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: $x + a_i y \leq b_i$, wherein $a_i = -(i + 1)i$, $b_i = i(1 - N) - N$, $2 \leq i \leq N - 2$, and wherein $(x, y) \in \mathbf{R}^2$, plus inequalities for edges M_2A and $M_{N-1}A$.

Theorem 3. $\Omega \cap \boldsymbol{Z}^2 = G \cap \boldsymbol{Z}^2$.

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

Theorem 4. *Problem (1) is equivalent to the problem:*

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

Proof. It follows from Theorem 3 and problems (1) and (2). □

Theorem 5(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 4. □

Note that rational polyhedron G can be constructed e.g. so that it contains edge M_2M_{N-1} instead of edges M_2A and $M_{N-1}A$.

Recall that the fact of polynomiality in Theorem 2 does not require that "m"(the number of inequalities) must be fixed: just "n" and "k" must be fixed in Theorem 2, wherein "m", "n" and "k" are unary encoded.

Problem (2) completely satisfies Theorem 2 (Theorem 1.1 in Del Pia and Weismantel [4]), because target function of (2) is a quadratic polynomial with integer coefficients, G is a two-dimentional rational polyhedron, and, therefore, (2), (1) and integer factorization problem can be solved in time polynomial, according to the Theorem 2 (Theorem 1.1 in Del Pia and Weismantel [4]). It means, according to aforementioned definitions that it can be solved in time, bounded by a polynomial in the size of A and **b**. In fact, as it was mentioned above, and it is extremely and critically important, that according to the clear definition given in Del Pia et al. [5]: "...We say that problem can be solved in polynomial time if in time bounded by a polynomial in the size of A,**b** we can either determine that the problem is infeasible, find a feasible minimizer...". Thus, the fact of polynomiality in time of problem (2) means that it can be solved in time bounded by a polynomial in the size of coefficients of the inequalities, describing our polyhedron G and according to the Theorem 2 (Theorem 1.1 in Del Pia and Weismantel [4], Theorem 1.1 in Del Pia et al. [5]) this is the case(it is polynomial in time). As a result, problems (2)

(1) and integer factorization can be solved in time bounded by a polynomial in log (N). Thus, polynomiality in time of (2) and (1) is guaranteed by Theorem 2(n = k =2 in our case), Theorem 4, aforementioned standard definitions and by the encoding unarity of the "m". It is important to note that since m = N – 3, those running time, bounded by a polynomial, comprises unary encoding, depended on N, parameter m = N – 3 and binary encoding length, depended on N as well. The following example demonstrates a fixed-dimensional algorithm, that can be done in time polynomial in unary variables, including "m", as well as in the binary encoding length. In fact, for aforementioned in section 2 quasiconvex polynomial integer minimization problem, similarly, it can be solved in time, polynomial in the degrees and the binary encoding of the coefficients, when the dimension is fixed, as well as in "m"(in the number of constraints), see, e,g., Theorem 1.5 in Lee [9], Heinz [6], section 3.1, Theorem 10 in Hemmecke et al. [7]. In another example, again, the corresponding algorithm is polynomial in "m" (in the number of constraints) and in the binary encoding of the coefficients, see, e.g., section 2.1, Theorem 5 in Hemmecke et al. [7]. In both examples, the degrees and the number of constraints are unary encoded and are not fixed.

Thus, 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_{min} **of N**
else
Return "N is a prime"

Now we are going to make final conclusions about the complexity of Algorithm 2.

Two fundamental facts, considered above in full details are crucial arguments for polinomiality in log(N) of the Algorithm 2.

First, as we mentioned above, according to the standard definition the fact of polynomiality in time of problem (2) means that it can be solved in time bounded by a polynomial in the size of coefficients of the inequalities, describing our polyhedron G and according to the Theorem 2 (Theorem 1.1 in Del Pia and Weismantel [4], Theorem 1.1 in Del Pia et al. [5]) this is the case: it is polynomial in time.

Second, two examples, described above in full details, demonstrate a role of unary encoded unfixed parameters, which provide, nevertheless, algorithms that are not exponential, they are polynomial.

That is why, 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 6. *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 $\Omega_q := \{ (x, y) \in \mathbf{R^2} \mid xy \geq N, \quad 2 \leq x \leq q-1, \; N/(q-1) \leq y \leq N/2, \; x \in \mathbf{R}, \; y \in \mathbf{R} \}$ for a given q, $3 \leq q \leq N$, $N \in \mathbf{N}$.

Let G_q rational 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 7. *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 4) 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.

Theorem 8. *P = NP*.

Let us develop a polynomial-time integer factorization algorithm that use aforementioned polyhedron G and does not use integer programming. Note that any solution of integer factorization problem for a non-prime N corresponds to the certain vertex M = (p, q) of G, where both p and q are integers.

(Here and further we use rational polyhedron G that contains edge M_2M_{N-1} instead of edges M_2A and $M_{N-1}A$).

Due to convexity of G its clear that all vertices of G corresponding to solutions of integer factorization problem for a non-prime N belong to the integer hull of G and according to the mentioned above section 2.1, Theorem 5 in Hemmecke et al. [7]: "... when the dimension is fixed there is only a polynomial number of vertices ... ". On the other hand, as its mentioned in those section 2.1 in Hemmecke et al. [7]: "... Moreover, Hartmann [64] gave an algorithm for enumerating all the vertices, which runs in polynomial time in fixed dimension...". That is why by applying aforementioned Hurtmann's algorithm for enumeration of integer hull of our polyhedron G we get a polynomial-time algorithm for integer factorization. (It is important to use aforementioned two fundamental facts).

Algorithm 4(Integer Factorization Algorithm).
Input: A positive integer number N.
Output: A nontrivial divisor of N(if it exists).

```
while(1)
{
Enumerate vertices of the corresponding
integer hull of polyhedron G by using
Hartmann's algorithm and when
vertex (p, q) is enumerated, issue verification:
if (pq  =  N)
    Return  a nontrivial divisor p of  N
}
    Return  "N is a prime"
```

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.