A Note on Integer Factorization Using Lattices

Antonio Vera

A NOTE ON INTEGER FACTORIZATION USING LATTICES

ANTONIO VERA

CNRS/INRIA/NANCY-UNIVERSITÉ

Abstract. We revisit Schnorr's lattice-based integer factorization algorithm, now with an effective point of view. We present effective versions of Theorem 2 of [11], as well as new properties of the Prime Number Lattice bases of Schnorr and Adleman.

Contents

1. Introduction

Let $N \geq 1$ be a composite integer that we want to factor. The *congruence of squares method* consists of finding $x, y \in \mathbb{Z}$ such that

$$x^2 \equiv y^2 \mod N \tag{1}$$

with $x \not\equiv \pm y \mod N$, and factor N by computing $\gcd(x+y, N)$. Although this is a heuristic method, it works pretty well in practice and one can show under reasonable hypotheses (see [3, page 268, remark (5)]) that for random x, y satisfying (1), one has $x \not\equiv \pm y \mod N$ with probability $\geq 1/2$. This report considers an algorithm based on this philosophy, namely Schnorr's algorithm [11], whose outline is given in figure 1.

Call B-smooth an integer free of prime factors $> B$, and let p_i be the i-th prime number. Fix some $d \geq 1$ and suppose that N is free of prime factors $\leq p_d$. The core computational task of the algorithm consists in finding $d+2$ integer quartets (u, v, k, γ), with u, v p_d-smooth, k coprime with N, and $\gamma \in \mathbb{N} \setminus \{0\}$, solutions of the Diophantine equation

$$u = v + kN^\gamma. \tag{2}$$

(1) Receive input number N to be factored.
(2) Set the dimension d and the constant C of the lattice $\mathcal{S}_p(d, C)$, and form the extended prime number list $\mathcal{P} = \{p_0, p_1, \ldots, p_d\}$ where $p_0 = -1$ and the rest is the usual sequence of the first d prime numbers. Perform trial division of N by the primes of $\mathcal{P}$. If N is factored, return the factor.
(3) Using the lattice described in section 2, construct a list of at least $d + 2$ pairs $(u_i, k_i) \in \mathbb{N} \times \mathbb{Z}$ such that u_i is p_d-smooth with
$$u_i = \prod_{i=0}^{d} p_i^{a_{i,j}}, \quad a_{i,0} = 0,$$
and
$$|u_i - k_i N| \leq p_d.$$
(4) Factorize $u_i - k_i N$, for $i \in [\![1, d + 2]\!]$ over $\mathcal{P}$ to obtain
$$u_i - k_i N = \prod_{i=0}^{d} p_i^{b_{i,j}}.$$
(5) Put $\mathbf{a}_i = (a_{i,0}, \ldots, a_{i,d})$ and $\mathbf{b}_i = (b_{i,0}, \ldots, b_{i,d})$.
(6) For every nonzero $\mathbf{c} = (c_1, \ldots, c_{d+1}) \in \{0, 1\}^{d+1}$ solution of
$$\sum_{j=0}^{d+1} c_i(\mathbf{a}_i + \mathbf{b}_i) = \mathbf{0} \mod 2$$
do
 (a) Put
$$x = \prod_{j=1}^{d+2} p_j^{\sum_{i=1}^{d+2} c_i(a_{i,j}+b_{i,j})/2} \mod N,$$
 and
$$y = \prod_{j=1}^{d+2} p_j^{\sum_{i=1}^{d+2} c_i a_{i,j}} \mod N.$$
 (b) If $x \neq \pm y \mod N$ then return $\gcd(x + y, N)$ and stop.

FIGURE 1. Outline of Schnorr's algorithm

By design, Schnorr's algorithm is only able to find solutions where k is p_d-smooth and $\gamma = 1$ (Adleman's variant can yield, in principle, solutions with $\gamma > 1$). We look for pairs (u, k) of p_d-smooth numbers satisfying the inequality

$$|u - kN| \leq p_d, \tag{3}$$

and we build solutions out of these pairs by setting $v = u - kN$: the inequality guarantees the p_d-smoothness of v. This search is lattice-based, and it involves lattice reduction and lattice enumeration algorithms.

Although in 1987 de Weger [4] had already applied lattice reduction to the effective resolution of Diophantine equations of the form (2), it was Schnorr who first applied it to factorization, in 1993 [11]. In 1995, Adleman [1] used Schnorr's approach to propose a reduction (not completely proved) from integer factorization to the search of a shortest nonzero vector in a lattice. Schnorr's algorithm was successfully implemented by Ritter and Rössner in 1997 [10].

In this report, we improve a result of [11] by recycling a result of Micciancio [9, Prop. 5.10]. This result may be useful (cf. remark 4) to show the existence of solutions to (2). In addition, we provide explicit computations of the volumes and

the Gram-Schmidt Orthogonalizations of the involved lattices and lattice bases, respectively.

The road map is the following. First, in section 2, we introduce the lattice framework of Adleman, and we explain how can we solve the Diophantine equation (2) by searching short vectors in Adleman's lattice. Later in the same section, we explain the original approach of Schnorr, by particularizing Adleman's approach. Afterwards, in section 3 we give some properties of the Prime Number Lattices of Schnorr and Adleman. Finally, in section 4, we provide our conclusions and perspectives.

2. Detecting solutions

In this section we present the approaches of Adleman and Schnorr to solving (2) using lattices. We start by the approach of Adleman, which considers a search for short vectors. We show a sufficient condition to solving inequality (3). Then we present the approach of Schnorr, which considers a search for close vectors, and which can be seen as a particular case of Adleman's. We show a corresponding sufficient condition to solving (3).

2.1. Coding a candidate solution.

Let $\mathbf{z} \in \mathbb{Z}^{d+1}$ be a vector with negative last coordinate. To this vector we associate a candidate solution to (2) in the following way

$$u = \prod_{z_i>0, i\leq d}^{d} p_i^{z_i}, \quad k = \prod_{z_i<0, i\leq d} p_i^{-z_i} \quad \text{and} \quad \gamma = |z_{d+1}|. \tag{4}$$

Note that u and k are coprime. We would like to have candidate solutions providing an actual solution with high probability, that is, we want $v = u - kN^{\gamma}$ to be probably p_d-smooth. Now we will describe a way to find such candidate solutions.

2.2. Making smoothness probable : the Prime Number Lattice of Adleman.

Define Adleman's p-norm Prime Number Lattice $\mathcal{A}_p$ by the columns of the basis matrix

$$\mathbf{A}_p = \begin{bmatrix} \sqrt[p]{\ln p_1} & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & \sqrt[p]{\ln p_d} & 0 \\ C\ln p_1 & \cdots & C\ln p_d & C\ln N \end{bmatrix},$$

where $C > 0$ is an arbitrary constant, which can depend on N. The vector $\mathbf{z} \in \mathbb{Z}^{d+1}$ satisfies

$$\mathbf{A}_p\mathbf{z} = \begin{bmatrix} z_1\sqrt[p]{\ln p_1} \\ \vdots \\ z_d\sqrt[p]{\ln p_d} \\ C\left(\sum_{i=1}^{d} z_i \ln p_i + z_{d+1}\ln N\right) \end{bmatrix}$$

and

$$||\mathbf{A}_p\mathbf{z}||_p^p = \sum_{i=1}^{d} |z_i|^p \sqrt[p]{\ln p_i}^p + C^p \left|\sum_{i=1}^{d} z_i \ln p_i - |z_{d+1}| \ln N\right|^p,$$

and considering that this vector codes a candidate solution, we have

$$||\mathbf{A}_p\mathbf{z}||_p^p = \sum_{i=1}^{d} |z_i|^p \ln p_i + C^p |\ln u - \ln(kN^{\gamma})|^p$$

and hence

$$||\mathbf{A}_1\mathbf{z}||_1 = \ln u + \ln k + C|\ln u - \ln(kN^{\gamma})|.$$

We have the following theorem in the case of the 1-norm.

Theorem 1. *Let $C > 1$ and $\mathbf{z} \in \mathbb{Z}^{d+1}$, with $\gamma = |z_{d+1}|$ and $z_{d+1} < 0$. Then, whenever*

$$||\mathbf{A}_1\mathbf{z}||_1 \leq 2\ln C + 2\sigma \ln p_d - \gamma \cdot \ln N, \tag{5}$$

we have

$$|u - kN^\gamma| \leq p_d^\sigma.$$

Proof. Just use lemma 1 (in the appendix) with $\varepsilon = 2\ln C + 2\sigma \ln p_d - \gamma \cdot \ln N$. □

Remark 1. The requirement $z_{d+1} < 0$ is just needed to obtain a valid candidate solution. It does not reduce the space of solutions in any way, since a lattice is an additive group: for each vector of nonzero last coordinate, either itself or its opposite will have a strictly negative last coordinate.

Remark 2. When $\sigma = 1$ and $\mathbf{z}$ satisfies (5), we necessarily have a solution to the original equation (2). In addition, when $\sigma > 1$ is not too big, we can be quite optimistic about the p_d-smoothness of $v = u - kN^\gamma$, and hence on obtaining a solution too.

Remark 3. In order to factor N, one will typically search for (short) vectors $\mathbf{A}_1\mathbf{z}$ satisfying (5) for some σ not too big, and then reconstruct from $\mathbf{z}$ the candidate solution to (2), testing afterwards if it really constitutes a solution. In that case, the solution is stored, until we collect $d + 2$ of them.

Remark 4. Together with some extra knowledge on the properties of γ for $\mathbf{z}$ satisfying (5) (see remark 6), theorem 1 could be useful to prove the existence of solutions to inequality (3) and hence to equation (2), since we have explicit estimates on the length of a short nonzero vector of $\mathcal{A}_1$, thanks to Minkowski's theorem for the 1-norm. See Siegel [13, Theorem 14].

Remark 5. Obtaining an analog of theorem 1 for the Euclidean norm could be very useful, since this norm has better properties and it is the usual norm for lattice algorithms.

2.3. **A similar approach : the Prime Number Lattice of Schnorr.** The Prime Number Lattice of Schnorr $\mathcal{S}_p$ is generated by the columns of the basis matrix

$$\mathbf{S}_p = \begin{bmatrix} \sqrt[p]{\ln p_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \sqrt[p]{\ln p_d} \\ C\ln p_1 & \cdots & C\ln p_d \end{bmatrix}. \tag{6}$$

The vector

$$\mathbf{t} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ C\ln N \end{bmatrix} \tag{7}$$

is the target vector of a close vector search in $\mathcal{S}_p$, which replaces the short vector search of Adleman's approach. Schnorr's algorithm considers vectors $\mathbf{z} \in \mathbb{Z}^d$, to which it associates the candidate solution (u, k, γ) to (3) with u and k defined

exactly as in (4), and $\gamma = 1$. We have

$$\mathbf{S}_p\mathbf{z} - \mathbf{t} = \begin{bmatrix} z_1 \sqrt[p]{\ln p_1} \\ \vdots \\ z_d \sqrt[p]{\ln p_d} \\ C(\sum_{i=1}^{d} z_i \sqrt[p]{\ln p_i} \ln N) \end{bmatrix},$$

and hence

$$||\mathbf{S}_p\mathbf{z} - \mathbf{t}||_p^p = \sum_{i=1}^{d} |z_i|^p \ln p_i + C^p \left| \sum_{i=1}^{d} z_i \ln p_i - \ln N \right|^p.$$

The following theorem is the analog of theorem 1.

Theorem 2. *Let $C > 1$ and $\mathbf{z} \in \mathbb{Z}^d$. Hence, if*

$$||\mathbf{S}_1\mathbf{z} - \mathbf{t}||_1 \leq 2\ln C + 2\sigma \ln p_d - \ln N, \tag{8}$$

then

$$|u - kN| \leq p_d^{\sigma}.$$

Proof. Just use lemma 2 with $\varepsilon = 2\ln C + 2\sigma \ln p_d - \ln N$. □

Remark 6. In order to factor N, we should look for vectors of $\mathcal{S}_1$ close to $\mathbf{t}$. The main idea is that vectors satisfying (8) for some $\sigma \geq 1$ not too big are more likely to provide candidate solutions which in turn will provide solutions to (2). Adleman's approach has the apparent advantage of having a larger search space, hence having a greater potential for finding solutions. In practice, this seems to be a disadvantage, since the solutions to (2) seem to be exactly those coming from Schnorr's approach too. Hence, in Adleman's approach one seems to search for many candidates that do not provide solutions. This could be related to the fact that the target vector $\mathbf{t}$ does not belong to the real span of $\mathcal{S}_1$: if the component of $\mathbf{t}$ in the orthogonal complement of the span of $\mathcal{S}_1$ is sufficiently big, any short vector in Adleman's lattice $\mathcal{A}_1$ having nonzero last coordinate must have a last coordinate of absolute value equal to 1, hence leading to the same solutions as Schnorr's lattice (see [9, Chapter 4, Lemma 4.1] for a related discussion).

Remark 7. A great algorithmic advantage of the approach of Schnorr over that of Adleman is that the choice of the basis can be *essentially independent of the number N*. For example, this will be the case if C depends only on the size of N. This has the very important implication of allowing a precomputation on the basis (for example an HKZ reduction) valid for all numbers of some fixed size.

Remark 8. Proving the existence of solutions to (8) seems harder in this case, since one needs a bound on the covering radius, which is less well understood than the first minimum.

Remark 9. Just as in the case of Adleman, obtaining an analog of theorem 2 for the Euclidean norm could be very useful. First attempts at finding this analog were stopped by involved computations.

3. Some properties of the Prime Number Lattices

We present some useful computations which extend those given by Micciancio and Goldwasser [9, Chapter 5, section 2.3].

3.1. **Volumes of the Prime Number Lattices.** Here we provide closed forms for the volumes of the p-norm Schnorr and Adleman lattices. This generalizes Proposition 5.9 of [9], which considers only $p = 2$.

Remark 10. Recall that the volume of the lattice generated by the columns of a (not necessarily full rank) basis matrix $\mathbf{B}$ is

$$\mathrm{vol}(\mathcal{L}(\mathbf{B})) = \sqrt{|\det(\mathbf{B}^T \cdot \mathbf{B})|},$$

which is exactly $\det(\mathbf{B})$ when $\mathbf{B}$ has full rank.

Theorem 3. *The volume of the p-norm Adleman lattice $\mathcal{A}_p$, whose basis is*

$$\mathbf{A}_p = \begin{bmatrix} \sqrt[p]{\ln p_1} & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & \sqrt[p]{\ln p_d} & 0 \\ C \ln p_1 & \cdots & C \ln p_d & C \ln N \end{bmatrix}$$

is given by

$$\mathrm{vol}(\mathcal{A}_p) = C \ln N \cdot \prod_{i=1}^{d} \sqrt[p]{\ln p_i}.$$

Furthermore, the volume of the p-norm Schnorr lattice $\mathcal{S}_p$, whose basis is

$$\mathbf{S}_p = \begin{bmatrix} \sqrt[p]{\ln p_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \sqrt[p]{\ln p_d} \\ C \ln p_1 & \cdots & C \ln p_d \end{bmatrix},$$

is given by

$$\mathrm{vol}(\mathcal{S}_p) = \sqrt{1 + C^2 \sum_{i=1}^{d} (\ln p_i)^{2-2/p}} \cdot \prod_{i=1}^{d} \sqrt[p]{\ln p_i}.$$

Proof. The case of $\mathcal{A}_p$ is trivial, as the basis matrix is lower triangular. Let us consider the case of $\mathcal{S}_p$. It is easy to see that the volume of $\mathcal{S}_p$ is a multilinear function of the columns of $\mathbf{S}_p$. Hence, factoring out $\sqrt[p]{\ln p_i}$, $i \in [\![1, d]\!]$ from the i-th column, we obtain

$$\mathrm{vol}(\mathcal{S}_p) = \sqrt{|\det(\mathbf{S}_p^T \mathbf{S}_p)|} = \sqrt{|\det(\hat{\mathbf{S}}_p^T \hat{\mathbf{S}}_p)|} \cdot \prod_{i=1}^{d} \sqrt[p]{\ln p_i},$$

where $\hat{\mathbf{S}}_p$ is of the form (11) (see lemma 3 in the appendix) with

$$x_i = C \cdot (\ln p_i)^{1-1/p}.$$

Lemma 3 implies that

$$\sqrt{|\det(\hat{\mathbf{S}}_p^T \hat{\mathbf{S}}_p)|} = \sqrt{1 + \sum_{i=1}^{d} (C(\ln p_i)^{1-1/p})^2} = \sqrt{1 + C^2 \sum_{i=1}^{d} (\ln p_i)^{2-2/p}},$$

which concludes the proof. □

3.2. **Explicit Gram-Schmidt Orthogonalization.** Here we give explicit expressions for the coefficients of the Gram-Schmidt Orthogonalization (GSO) of the set $\{\mathbf{b}_1, \ldots, \mathbf{b}_d, \mathbf{t}\}$ of columns of $\mathbf{S}_p$, augmented by the target vector $\mathbf{t}$ (or, equivalently, of the set of columns of $\mathbf{A}_p$).

Theorem 4. *Consider the columns $\{\mathbf{b}_i\}_{i=1}^d$ of Schnorr's Prime Number Lattice basis (6), as well as the target vector $\mathbf{t}$ defined in (7). The Gram-Schmidt Orthogonalization of $\{\mathbf{b}_1, \ldots, \mathbf{b}_d, \mathbf{t}\}$ involves the quantities*

$$D_j = 1 + C^2 \sum_{i=1}^{j} (\ln p_i)^{2-2/p} \quad 1 \leq j \leq d$$

and is given by

$$(\mathbf{b}_k^\star)_i = \begin{cases} -\frac{C^2 \ln p_k (\ln p_i)^{1-1/p}}{D_{k-1}} & i < k \\ (\ln p_k)^{1/p} & i = k \\ 0 & k < i < d+1 \\ \frac{C \ln p_k}{D_{k-1}} & i = d+1 \end{cases}$$

and

$$(\mathbf{t}^\star)_i = \begin{cases} -\frac{C^2 (\ln N)(\ln p_i)^{1-1/p}}{D_d} & i < d+1 \\ \frac{C(\ln N)}{D_d} & i = d+1 \end{cases}.$$

The corresponding Euclidean norms satisfy

$$||\mathbf{b}_k^\star||_2^2 = (\ln p_k)^{2/p} \frac{D_k}{D_{k-1}} \qquad ||\mathbf{t}^\star||_2^2 = \frac{(C \ln N)^2}{D_d}.$$

Furthermore, the projection $\mathbf{t}$ on the span of $\{\mathbf{b}_1, \ldots, \mathbf{b}_d\}$, which is the effective target vector for the close vector search of Schnorr's algorithm, is given by

$$(\mathbf{t} - \mathbf{t}^\star)_i = \begin{cases} \frac{C^2 (\ln N)(\ln p_i)^{1-1/p}}{D_d} & i < d+1 \\ \frac{C(\ln N)(D_d - 1)}{D_d} & i = d+1 \end{cases}.$$

Proof. The matrix having $\{\mathbf{b}_1, \ldots, \mathbf{b}_d, \mathbf{t}\}$ as columns is of the form (12) (see lemma 4 in the appendix) with

$$x_i = \sqrt[p]{\ln p_i}, \qquad y_i = C \cdot \ln p_i \quad 1 \leq i \leq d,$$

and

$$y_{d+1} = C \ln N.$$

Hence, using lemma 4, we directly obtain the theorem. □

Remark 11. The explicit value of $||\mathbf{t}^\star||_2$ can be used to better understand the search for close vectors of Schnorr's algorithm. This is a consequence of the fact that $\mathbf{t}$ does not belong to the span of $\{\mathbf{b}_1, \ldots, \mathbf{b}_d\}$.

4. Conclusions and perspectives

Using an idea of Micciancio, we presented partial but rigorous results advancing towards an *effective* reduction from factorization to the search of short or close lattice vectors in the Prime Number Lattice of Adleman or Schnorr, respectively. These results, valid only for the 1-norm, improve over those of Schnorr [11, Theorem 2] by getting rid of asymptotically vanishing terms. Proving similar results for the Euclidean norm may be very useful, since it has much better properties than the 1-norm and it is the natural choice for lattice algorithms[1].

[1]Although recently, in [12, Theorem 2], Schnorr restated [11, Theorem 2] in the context of the Euclidean norm, this is essentially a generic restatement valid for every p-norm, $p \geq 1$, which still involves asymptotic terms.

Furthermore, we provided new properties of the Prime Number Lattices and their usual bases (in p-norm, $p \geq 1$), extending those of Micciancio [9, Chapter 5, Section 2.3]. These properties could be useful to better understand the close vector search which takes place at the core of Schnorr's algorithm.

The next step of this work is to understand the distribution of lattice elements providing solutions to (3) or even (2), in order to choose on a well-grounded basis between enumeration algorithms ([7, 5]) and random sampling algorithms ([6], [8]), in the context of an effective implementation.

4.1. **Acknowledgements.** Thanks to Damien Stehlé for regular discussions and encouragement, as well as for many pointers to the relevant literature. Thanks to Guillaume Hanrot for useful discussions.

References

[1] Adleman, L. M. Factoring and lattice reduction. A draft on the reduction of Factoring to the Shortest Vector Problem, 1995.
[2] Brookes, M. The matrix reference manual. `http://www.ee.ic.ac.uk/hp/staff/dmb/matrix/proof003.html#DetSumI_AB_p`.
[3] Crandall, R., and Pomerance, C. *Prime Numbers: A Computational Perspective*, 2nd ed. Springer, 2005.
[4] De Weger, B. Solving exponential diophantine equations using lattice basis reduction algorithms. *Journal of Number Theory 26*, 325-367 (1987), 31.
[5] Fincke, U., and Pohst, M. A procedure for determining algebraic integers of given norm. In *EUROCAL* (1983), pp. 194–202.
[6] Gentry, C., Peikert, C., and Vaikuntanathan, V. Trapdoors for hard lattices and new cryptographic constructions. In *STOC* (2008), pp. 197–206.
[7] Kannan, R. Improved algorithms for integer programming and related lattice problems. In *STOC* (1983), pp. 193–206.
[8] Klein, P. N. Finding the closest lattice vector when it's unusually close. In *SODA* (2000), pp. 937–941.
[9] Micciancio, D., and Goldwasser, S. *Complexity of Lattice Problems: a cryptographic perspective*, vol. 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, Massachusetts, Mar. 2002.
[10] Ritter, H., and Rössner, C. Factoring via strong lattice reduction algorithms. Tech. rep., Goethe Universität Frankfurt, 1997.
[11] Schnorr, C. P. Factoring integers and computing discrete logarithms via diophantine approximation. In *Advances in Computational Complexity Theory*, J.-Y. Cai, Ed., vol. 13 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*. AMS, 1993, pp. 171–182.
[12] Schnorr, C. P. Average time fast SVP and CVP algorithms for low density lattices and the factorization of integers. Tech. rep., Goethe Universität Frankfurt, March 2010.
[13] Siegel, C. L. *Lectures on the Geometry of Numbers*. Springer-Verlag, 1989.

Appendix A. Underlying lemmas

A.1. **Lemmas used in section 2.** The following two lemmas are elementary generalizations of a result of Micciancio [9, Prop. 5.10].

Lemma 1. *Let $C > 1$ and let $\mathbf{z} \in \mathbb{Z}^{d+1}$ have negative last coordinate of module $\gamma = |z_{d+1}| \geq 1$, satisfying*

$$||\mathbf{A}_1\mathbf{z}||_1 \leq \varepsilon.$$

Hence, we have

$$|u - kN^\gamma| \leq \frac{N^{\frac{\gamma}{2}}}{C} \cdot \exp\left(\frac{\varepsilon}{2}\right).$$

Proof. The proof is essentially the same of Proposition 5.10 of [9]. We maximize $|u - kN^\gamma|$ subject to the constraint

$$||\mathbf{A}_1\mathbf{z}||_1 \leq \varepsilon. \tag{9}$$

Since

$$||\mathbf{A}_1\mathbf{z}||_1 = \ln u + \ln k + C|\ln u - \ln(kN^\gamma)|,$$

the constraint (9) is symmetric in u and kN^γ, and we can suppose without loss of generality that $u \geq kN^\gamma$. Now, the constraint (9) can be rewritten as

$$(C+1)\cdot \ln u - (C-1)\cdot \ln k \leq \varepsilon + C\gamma \cdot \ln N,$$

which implies

$$u \leq k^{\frac{C-1}{C+1}} \cdot N^{\frac{C\gamma}{C+1}} \cdot \exp\left(\frac{\varepsilon}{C+1}\right).$$

Replacing this maximal value for u in the objective function we get

$$k^{\frac{C-1}{C+1}} \cdot N^{\frac{C\gamma}{C+1}} \cdot \exp\left(\frac{\varepsilon}{C+1}\right) - kN^\gamma. \tag{10}$$

Now, we optimize this last expression as a function of k. Differentiating (10) with respect to k we obtain

$$\left(\frac{C-1}{C+1}\right) \cdot k^{-\frac{2}{C+1}} \cdot N^{\frac{C\gamma}{C+1}} \cdot \exp\left(\frac{\varepsilon}{C+1}\right) - N^\gamma$$

and hence the maximum is reached in the point

$$k = \left(\frac{C-1}{C+1}\right)^{\frac{C+1}{2}} \cdot N^{-\frac{\gamma}{2}} \exp\left(\frac{\varepsilon}{2}\right).$$

The maximum of the original function is hence

$$\left(\frac{C-1}{C+1}\right)^{\frac{C-1}{2}} \cdot N^{\frac{\gamma}{2}} \cdot \exp\left(\frac{\varepsilon}{2}\right) \cdot \left(\frac{2}{C+1}\right)$$

and as[2]

$$\left(\frac{C-1}{C+1}\right)^{\frac{C-1}{2}} \cdot \left(\frac{2}{C+1}\right) \leq \frac{1}{C}$$

for $C > 1$, we conclude that

$$|u - kN^\gamma| \leq \frac{N^{\frac{\gamma}{2}}}{C} \cdot \exp\left(\frac{\varepsilon}{2}\right),$$

as wished. □

Lemma 2. *Let $C > 1$ and let $\mathbf{z} \in \mathbb{Z}^d$ satisfying*

$$||\mathbf{S}_1\mathbf{z} - \mathbf{t}||_1 \leq \varepsilon.$$

Hence,

$$|u - kN| \leq \frac{\sqrt{N}}{C} \cdot \exp\left(\frac{\varepsilon}{2}\right).$$

Proof. Just take $\gamma = 1$ in the proof of lemma 1. □

[2]When $x > 1$, the function $f(x) = \left(\frac{x-1}{x+1}\right)^{\frac{x-1}{2}} \left(\frac{2x}{x+1}\right)$ is monotonically decreasing, with $f(0^+) = 1$.

A.2. **Lemmas used in section 3.** The following are general lemmas, maybe of independent interest. Lemma 4 could find an application in the context of knapsack lattice bases.

Lemma 3. *The volume of the lattice $\mathcal{L}$ generated by the columns of the matrix*

$$\mathbf{B} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 1 \\ x_1 & x_2 & \cdots & x_d \end{bmatrix} \tag{11}$$

satisfies

$$\mathrm{vol}(\mathcal{L}) = \sqrt{\det(\mathbf{B}^T\mathbf{B})} = \sqrt{1 + \sum_{i=1}^{d} x_i^2}.$$

Proof. We use Sylvester's determinant theorem (see for example [2]), which states that for every $\mathbf{A} \in \mathbb{R}^{m\times n}$ and $\mathbf{B} \in \mathbb{R}^{n\times m}$,

$$\det(\mathbf{I}_m + \mathbf{AB}) = \det(\mathbf{I}_n + \mathbf{BA}),$$

where $\mathbf{I}_k$ is the $k \times k$ identity matrix. Writing the matrix $\mathbf{B}$ by blocks, and computing the associated Gram matrix, we obtain

$$\mathbf{B} = \begin{bmatrix} \mathbf{I}_d \\ \mathbf{x}^T \end{bmatrix} \qquad \mathbf{B}^T\mathbf{B} = \mathbf{I}_d + \mathbf{x}\cdot\mathbf{x}^T,$$

and hence, using Sylvester's theorem,

$$\mathrm{vol}(\mathcal{L})^2 = \det(\mathbf{B}^T\mathbf{B}) = \det(\mathbf{I}_d + \mathbf{x}\cdot\mathbf{x}^T) = \det(\mathbf{I}_1 + \mathbf{x}^T\cdot\mathbf{x}) = 1 + \sum_{i=1}^{d} x_i^2,$$

as wished. □

Lemma 4. *The Gram-Schmidt Orthogonalization of the columns $\{\mathbf{v}_1, \ldots, \mathbf{v}_{d+1}\}$ of a nonsingular square matrix*

$$\begin{bmatrix} x_1 & 0 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & 0 & x_d & 0 \\ y_1 & y_2 & \cdots & y_d & y_{d+1} \end{bmatrix} \tag{12}$$

can be specified in function of its entries and the quantities

$$K_j = 1 + \sum_{i=1}^{j} \left(\frac{y_i}{x_i}\right)^2 \qquad 1 \le j \le d, \quad K_0 = 1,$$

by

$$(\mathbf{v}_k^\star)_i = \begin{cases} -\left(\frac{y_k}{K_{k-1}}\right)\cdot\left(\frac{y_i}{x_i}\right) & i < k \\ x_k & i = k \\ 0 & k < i < d+1 \\ \frac{y_k}{K_{k-1}} & i = d+1 \end{cases} \tag{13}$$

for $k \le d$, and by the same expression considering only the $i < k$ and $i = d+1$ cases, when $k = d+1$. The Euclidean norms satisfy

$$||\mathbf{v}_k^\star||^2 = x_k^2\frac{K_k}{K_{k-1}}, \quad ||\mathbf{v}_{d+1}^\star||^2 = \frac{y_{d+1}^2}{K_d}, \tag{14}$$

and the Gram-Schmidt coefficients are

$$\mu_{k,j} = \frac{\mathbf{v}_k \cdot \mathbf{v}_j^\star}{\mathbf{v}_j^\star \cdot \mathbf{v}_j^\star} = \frac{y_k \cdot y_j}{x_j^2 K_j}, \quad 1 \leq j < k \leq d+1. \tag{15}$$

Proof. The proof of (13) is carried out by induction. The result is clearly true for $k = 1$. Suppose that it holds for $\mathbf{v}_1^\star, \ldots, \mathbf{v}_{k-1}^\star$ for some $k \in [\![2, d+1]\!]$. Let us show that it still holds for $\mathbf{v}_k^\star$. First, observe that for $1 \leq j < k \leq d+1$,

$$\mathbf{v}_k \cdot \mathbf{v}_j^\star = (\mathbf{v}_k)_{d+1} \cdot (\mathbf{v}_j^\star)_{d+1} = y_k \frac{y_j}{K_{j-1}}$$

and

$$\begin{aligned}
||\mathbf{v}_j^\star||_2^2 = \mathbf{v}_j^\star \cdot \mathbf{v}_j^\star &= \sum_{i=1}^{j-1} \left(\frac{y_i}{x_i}\right)^2 \cdot \left(\frac{y_j}{K_{j-1}}\right)^2 + x_j^2 + \left(\frac{y_j}{K_{j-1}}\right)^2 \\
&= \left(\frac{y_j}{K_{j-1}}\right)^2 \cdot \left(1 + \sum_{i=1}^{j-1} \left(\frac{y_i}{x_i}\right)^2\right) + x_j^2 \\
&= \frac{y_j^2}{K_{j-1}} + x_j^2 \\
&= x_j^2 \left(1 + \frac{(y_j/x_j)^2}{K_{j-1}}\right) \\
&= x_j^2 \left(\frac{K_{j-1} + (y_j/x_j)^2}{K_{j-1}}\right) \\
&= x_j^2 \frac{K_j}{K_{j-1}},
\end{aligned}$$

which entails

$$\mu_{k,j} = \frac{\mathbf{v}_k \cdot \mathbf{v}_j^\star}{\mathbf{v}_j^\star \cdot \mathbf{v}_j^\star} = \frac{y_k \cdot y_j}{x_j^2 K_j}. \tag{16}$$

Now, let $i \in [\![1, k-1]\!]$. By the definition of the Gram-Schmidt process, we have

$$\begin{aligned}
(\mathbf{v}_k^\star)_i &= (\mathbf{v}_k)_i - \sum_{j=1}^{k-1} \mu_{k,j} \cdot (\mathbf{v}_j^\star)_i \\
&= 0 - \sum_{j=i}^{k-1} \mu_{k,j} \cdot (\mathbf{v}_j^\star)_i \\
&= -\mu_{k,i} \cdot (\mathbf{v}_i^\star)_i - \sum_{j=i+1}^{k-1} \mu_{k,j} \cdot (\mathbf{v}_j^\star)_i \\
&= -\left(\frac{y_k y_i}{x_i^2 K_i}\right) \cdot x_i - \sum_{j=i+1}^{k-1} \left(\frac{y_k \cdot y_j}{x_j^2 \cdot K_j}\right) \cdot \left(-\frac{y_i y_j}{x_i K_{j-1}}\right) \\
&= -y_k \left(\frac{y_i}{x_i}\right) \left(\frac{1}{K_i} - \sum_{j=i+1}^{k-1} \left(\frac{y_j}{x_j}\right)^2 \frac{1}{K_{j-1} K_j}\right) \\
&= -y_k \left(\frac{y_i}{x_i}\right) \left(\frac{1}{K_i} - \sum_{j=i+1}^{k-1} \left(\frac{1}{K_{j-1}} - \frac{1}{K_j}\right)\right) \\
&= -\frac{y_k}{K_{k-1}} \left(\frac{y_i}{x_i}\right),
\end{aligned}$$

as we wanted. Now, when $i = k \leq d$,

$$\begin{aligned}(\mathbf{v}_k^\star)_k &= (\mathbf{v}_k)_k - \sum_{j=1}^{k-1} \mu_{k,j} \cdot (\mathbf{v}_j^\star)_k \\ &= x_k - \sum_{j=1}^{k-1} \mu_{k,j} \cdot 0 \\ &= x_k,\end{aligned}$$

as we wanted. When $k < i \leq d$, we have

$$\begin{aligned}(\mathbf{v}_k^\star)_i &= (\mathbf{v}_k)_i - \sum_{j=1}^{k-1} \mu_{k,j} \cdot (\mathbf{v}_j^\star)_i \\ &= 0 - \sum_{j=1}^{k-1} \mu_{k,j} \cdot 0 \\ &= 0\end{aligned}$$

as wished. Finally, when $i = d+1$ we obtain, for every $k \in [\![2, d+1]\!]$,

$$\begin{aligned}(\mathbf{v}_k^\star)_{d+1} &= (\mathbf{v}_k)_{d+1} - \sum_{j=1}^{k-1} \mu_{k,j} \cdot (\mathbf{v}_j^\star)_{d+1} \\ &= y_k - \sum_{j=1}^{k-1} \left(\frac{y_k y_j}{x_j^2 K_j}\right) \cdot \left(\frac{y_j}{K_{j-1}}\right) \\ &= y_k \left(1 - \sum_{j=1}^{k-1} \left(\frac{y_j}{x_j}\right)^2 \frac{1}{K_{j-1} K_j}\right) \\ &= y_k \left(1 - \sum_{j=1}^{k-1} \left(\frac{1}{K_{j-1}} - \frac{1}{K_j}\right)\right) \\ &= y_k \left(1 - \left(\frac{1}{K_0} - \frac{1}{K_{k-1}}\right)\right) \\ &= \frac{y_k}{K_{k-1}},\end{aligned}$$

since $K_0 = 1$. Hence, (13) is proved, both in the $1 \leq k \leq d$ and the $k = d+1$ cases, as specified in the statement of the lemma. As a consequence of the computations preceding (16), properties (14) and (15) are also proved, except for the Euclidean norm of $\mathbf{v}_{d+1}^\star$, which is given by

$$||\mathbf{v}_{d+1}^\star||_2^2 = \left(\frac{y_{d+1}}{K_d}\right)^2 \cdot \left(1 + \sum_{i=1}^{d} \left(\frac{y_i}{x_i}\right)^2\right) = \frac{y_{d+1}^2}{K_d}.$$

The proof of the lemma is now complete. □