Diophantine Approximation via the ILLL Algorithm

Joseph Ingenito

The College of New Jersey
Mathematics and Statistics

Abstract

We are studying the Iterated LLL algorithm (or ILLL algorithm) due to W. Bosma and I. Smeets. For a given list of irrational numbers, the ILLL algorithm returns a series of efficient rational approximations to the numbers. The central aim of our on-going project is to develop a new version of ILLL that will incorporate the continued fraction algorithm for storing real numbers for preprocessing. Since the continued fraction algorithm is optimal, we expect that our planned implementation will give us new insight into the overall performance of the ILLL algorithm.

Introduction

A very efficient solution to the problem of approximating a single real number by rationals is **the continued fraction algorithm**; see, e.g., [8, Chapter 1, Section 5]. The problem of **simultaneous Diophantine approximation** [5] is about approximating two or more real numbers by rational numbers having the same denominator. The problem for a single real number is solved by the continued fraction algorithm [8]. For simultaneous Diophantine approximation, however, the problem is much harder.

While many algorithms have been proposed for simultaneous Diophantine approximation, there still does not exist one that is a perfect analogue of the continued fraction algorithm; see, e.g., [4] for a description of such algorithms. Our project studies the LLL and ILLL algorithm for simultaneous Diophantine approximation, which is a fast and reasonably efficient solution.

The **ILLL algorithm** [2] builds on a well-known lattice basis reduction algorithm due to A. K. Lenstra, H. W. Lenstra and L. Lovàsz, referred to here as the (classical) **LLL algorithm**, which was shown to be applicable to the problem of simultaneous Diophantine approximation [7]. The advantage of the ILLL algorithm over the classical version is that it finds several increasingly accurate approximations per application, and with prescribed quality. Following the implementations of LLL in [3, 6], we aim to develop a version of ILLL which incorporates the continued fraction algorithm for preprocessing.

References

[1] W. Bosma, Optimal continued fractions, *Nederl. Akad. Wetensch. Indag. Math.* **49** (1987), 353--379.

[2] W. Bosma and I. Smeets, Finding simultaneous Diophantine approximations with prescribed quality, *The Open Book Series* **1** (2013), 167--185.

[3] M. R. Bremner, *Lattice Basis Reduction: An Introduction to the LLL Algorithm and its Applications*, Taylor & Francis, Boca Raton, 2011.

[4] A. J. Brentjes, *Multidimensional Continued Fraction Algorithms*, Vol. 145 of *Mathematical Centre Tracts.*, Mathematisch Centrum, Amsterdam, 1981.

[5] J. C. Lagarias, Best simultaneous Diophantine approximations. I. Growth rates of best approximation denominators, *Trans. Amer. Math. Soc.* **272** (1982), 545--554.

[6] M. L. Lapidus, M. van Frankenhuijse and E. K. Voskanian, Quasiperiodic patterns of the complex dimensions of nonlattice self-similar strings, via the LLL algorithm, e-print, arXiv:2009.03493v2, 2020

[7] A. K. Lenstra, H. W. Lenstra and L. Lovász, Factoring polynomials with rational coefficients, *Mat. Annal.* **261** (1982), 515--534.

[8] W. M. Schmidt, *Diophantine Approximation*, Springer, New York, 1980.

Materials and Methods

Dirichlet's Approximation Theorem [8, Theorem 1A, p. 27]: If $\alpha_1, \ldots, \alpha_n$ are n real numbers and at least one of them is irrational, then there are infinitely many n-tuples $\frac{p_1}{q}, \ldots, \frac{p_n}{q}$ with

$$\left|\alpha_j - \frac{p_j}{q}\right| < \frac{1}{q^{1+1/n}}.$$

For the case $n = 1$, the rational numbers generated via the continued fraction algorithm, which are called convergents, are the best solutions of Dirichlet's Approximation Theorem [8, Lemma 4D, pp. 14 -- 15]; see also, e.g., the **optimal continued fraction algorithm** [1]. The following theorem gives a solution for the case $n > 1$ that is based on the LLL algorithm.

Theorem 1 [7, Proposition 1.39, p. 525]: Given rational numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$ and ε satisfying $0 < \varepsilon < 1$, there exists a polynomial-time algorithm which finds integers $q \in \mathbb{N}$ and $p_1, \ldots, p_n \in \mathbb{Z}$ such that

$$\left|x_j - \frac{p_j}{q}\right| \leq \frac{\varepsilon}{q}, \quad \text{and} \quad 1 \leq q \leq 2^{\frac{n(n+1)}{4}} \varepsilon^{-n}$$

for $j = 1, \ldots, n$.

The ILLL Algorithm:

A higher-dimensional version of the algorithm provided by Theorem 1 is presented in [2]. It works by computing a series of increasingly good approximations with prescribed quality by iterating LLL, and is appropriately called the iterated LLL algorithm.

Our project focuses on the application of ILLL to the case $n = 1$ from [2, Section 5]. Specifically, we study the comparisons of the distributions of Dirichlet coefficients (defined below) compared with those from the optimal continued fraction algorithm.

Definition 1: The Dirichlet coefficient of each approximation in Theorem 1 is

$$q^{1/n}\|q\alpha_1 + \cdots + q\alpha_n\|,$$

where $\|x\|$ denotes the distance from x to the nearest integer.

Main Work

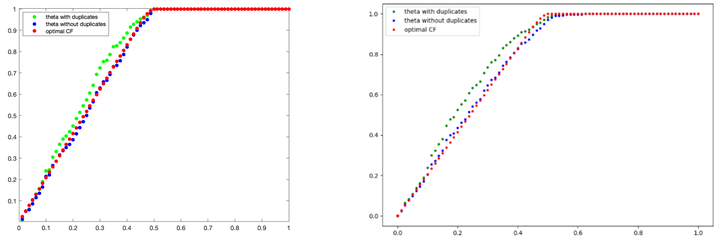

Figure: 1 Distributions for (left) $N = 100$ trials and (right) $N = 200$ trials.

Figure 1 above shows two plots of distributions of the Dirichlet coefficients up to each value on the horizontal axis for large numbers of approximations. It's possible that when running ILLL on some value, there could be duplicate approximations. When the duplicate approximations are filtered out of the data set, the distribution of Dirichlet coefficients is almost exactly that of the optimal continued fraction algorithm.

Main Work (cont.)

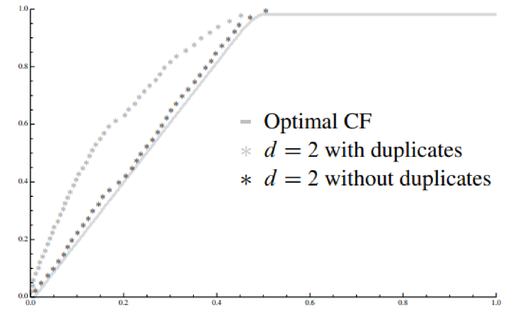

Figure: 2

Figure 2 above shows the same distributions as Figure 1 obtained by [2]. Note that the parameter d refers to a parameter of ILLL, which can be interpreted as the rate in which the precision increases during the *iteration* of LLL on each of the N trials.

Figure 2 implies that when including duplicate approximations, ILLL yields an approximation with Dirichlet coefficient up to any number on the horizontal axis more often than the optimal continued fraction algorithm. This is due to the increased amount of Dirichlet coefficients being considered, however many repeated. This would suggest that with larger numbers of trials, the plots in Figure 1 should look more similar to the results obtained by [2] shown in Figure 2. Our results shown in Figure 1 would certainly reflect this hypothesis, since the plot on the right in Figure 1 shows distributions closer to Figure 2 than the one on the left.

Future Plans

We have put together a software library which includes, but is not limited to, the original continued fraction algorithm, the original LLL algorithm and the ILLL algorithm. Since the software is ultimately run on a machine that will *chop* decimal digits just as when writing a number down on paper, there are different perspectives to consider for precision. For instance, when attempting to approximate the number $\sqrt{2}$ on a machine using the ILLL algorithm, the machine first has to approximate $\sqrt{2}$, ultimately affecting the accuracy before the algorithm even begins. The results obtained in Figures 1 and 2 were initially approximated using dyadic rationals[a].

Our current goal is to add to our software library, an implementation of the ILLL algorithm where the initial approximation is obtained using convergents of the original continued fraction algorithm. With the new implementation of ILLL, we can generate similar distributions to Figures 1 and 2 and compare results. Through comparison of results we hope to gain more insight in the overall performance and accuracy of ILLL.

The implementation of LLL in [6], which was for studying roots of nonlattice Dirichlet polynomials, is similar to ILLL in that it finds a sequence of approximations, except that it makes use of convergents as with the implementation from [3, Chapter 9, Example 9.5]. Hopefully the approximations found by our future implementation will be comparable to those found in [3, 6].

[a] A dyadic rational number is a rational number with denominator 2^M for some $M \in \mathbb{N}$.