Journal of Symbolic Computation 64 (2014) 3–15

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

On the probability of generating a lattice

Felix Fontein [a], Pawel Wocjan [b,1]

[a] Institute of Mathematics, University of Zurich, Winterthurerstrasse 190, 8057 Zurich, Switzerland
[b] Mathematics Department and Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA

ARTICLE INFO

Article history:
Received 27 November 2012
Accepted 19 September 2013
Available online 6 December 2013

Keywords:
Random generation of lattice
Riemann zeta function
Infrastructure
Analysis of quantum algorithm

ABSTRACT

We study the problem of determining the probability that m vectors selected uniformly at random from the intersection of the full-rank lattice Λ in $\mathbb{R}^n$ and the window $[0, B)^n$ generate Λ when B is chosen to be appropriately large. This problem plays an important role in the analysis of the success probability of quantum algorithms for solving the Discrete Logarithm Problem in infrastructures obtained from number fields and also for computing fundamental units of number fields.

We provide the first complete and rigorous proof that $2n + 1$ vectors suffice to generate Λ with constant probability (provided that B is chosen to be sufficiently large in terms of n and the covering radius of Λ and the last $n + 1$ vectors are sampled from a slightly larger window). Based on extensive computer simulations, we conjecture that only $n + 1$ vectors sampled from one window suffice to generate Λ with constant success probability. If this conjecture is true, then a significantly better success probability of the above quantum algorithms can be guaranteed.

1. Introduction

Let G be a finite group. Denote by $p_m(G)$ the probability that m elements drawn uniformly at random from G with replacement generate G. The problem of determining or bounding this probability is of fundamental interest in group theory and has been extensively studied for various families of groups (Acciaro, 1996; Pomerance, 2001).

E-mail addresses: felix.fontein@math.uzh.ch (F. Fontein), wocjan@eecs.ucf.edu (P. Wocjan).

[1] On sabbatical leave from Department of Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL 32816, USA.

http://dx.doi.org/10.1016/j.jsc.2013.12.002

The purpose of this paper is to study a very natural generalization of this problem from finite abelian groups to finitely generated abelian torsion-free groups. More precisely, we consider the case of lattices, i.e., discrete subgroups of $\mathbb{R}^n$. The problem is now to determine the probability that m vectors selected uniformly at random with replacement from the intersection of the full-rank lattice Λ in $\mathbb{R}^n$ and a window $X \subset \mathbb{R}^n$ generate Λ. We denote this probability by $p_m(\Lambda, X)$.

Our study of this problem was initially motivated by its relevance to quantum algorithms and quantum cryptanalysis, which we explain in more detail at the end of the paper. But we also believe that this problem is interesting on its own due to its appeal as a very natural and fundamental problem in lattice theory. In fact, it can be viewed as a generalization of the following elementary problem in number theory. For $\Lambda = \mathbb{Z}$ and $X = [1, B]$, the probability $p_m(\Lambda, X)$ corresponds to the probability that m integers chosen uniformly at random from the set $\{1, \dots, B\}$ with replacement are coprime. It is known that $\lim_{B \to \infty} p_m(\mathbb{Z}, B) = 1/\zeta(m)$ where ζ denotes the Riemann zeta function. For $\Lambda = \mathbb{Z}^n$ and X, the probability $p_m(\Lambda, X)$ is equal to the probability that the $m \times n$ matrix whose column vectors are selected uniformly at random from $\Lambda \cap X$ is unimodular. This problem was studied for special forms of X asymptotically. For $X = [-B, B]^n$, $B \to \infty$, it was studied by Maze et al. (2011), and for $X = v + [-B, B]^n$, $B \to \infty$, where the entries of the vector v are bounded polynomially in terms of B, by Elizalde and Woods (2007). In both cases, it was shown that the limit of the probability for $B \to \infty$ is $\prod_{j=m-n+1}^{m} \zeta(j)^{-1}$. Both works did not study the problem of bounding the probability in the non-asymptotic case, i.e., in the case where B is fixed.

In this paper, we consider the case where Λ is an arbitrary full-rank lattice and $X = [0, B)^n$ for a sufficiently large but fixed B. Ideally, we want to minimize m, while at the same time ensure that the probability $p_m(\Lambda, [0, B))^n$ is bounded from below by a nonzero constant. We use $\nu(\Lambda)$ to denote the covering radius of Λ, $\lambda_1(\Lambda)$ the length of a shortest (nonzero) vector of Λ, and $\det(\Lambda)$ the determinant of Λ.

Our two major contributions to the study of this problem are:

Theorem 1.1. *Let Λ be a lattice of full rank in $\mathbb{R}^n$, and assume that $B \geqslant 8n^{n/2} \cdot \nu(\Lambda)$ and $B_1 \geqslant 8n^2(n+1)B$. Assume that n vectors are selected uniformly at random from $\Lambda \cap [0, B)^n$ and $n+1$ vectors uniformly at random from $\Lambda \cap [0, B_1)^n$. If the vectors are sampled independently, then the probability that all these vectors generate Λ is at least*

$$\alpha_n := \left(\prod_{i=2}^{n+1} \zeta(i)^{-1} - \frac{1}{4} \right) \cdot \prod_{k=0}^{n-1} \left(1 - n^{k/2} \frac{(4n^{n/2}+1)^k}{(4n^{n/2}-1)^n} \right) \geqslant 0.092.$$

Unfortunately, our current approach requires $m = 2n+1$ samples and two windows of different sizes to be able to prove that the probability of generating the lattice Λ is bounded from below by a nonzero constant. However, based on extensive numerical evidence, we formulate the following conjecture, which states that only $m = n+1$ samples and only one window size suffice to attain a constant probability of generating the lattice.

Conjecture 1.2. *For every $n \in \mathbb{N}$, there exists a constant $0 < c_n < 1$ and a rational function $f_n \in \mathbb{R}(x, y)$ satisfying*

$$\forall x_0 > 0,\ \forall y_0 \in \left(0, x_0^{1/n}\right]: \quad \sup\left\{ f_n(x, y) \,\middle|\, 0 < x \leqslant x_0,\ y_0 \leqslant y \leqslant x^{1/n} \right\} < \infty$$

such that the following holds:

Let Λ be a lattice in $\mathbb{R}^n$ and let $B > f_n(\det \Lambda, \lambda_1(\Lambda))$. Then the probability that $n+1$ vectors chosen uniformly at random from $\Lambda \cap [0, B)^n$ generate the lattice Λ is at least c_n. Moreover, the constant c_n can be chosen close to $\prod_{k=2}^{n+1} \zeta(k)^{-1}$.

2. Solving the lattice generation problem

We break down the lattice generation problem into two subproblems. First, we consider the probability that n vectors sampled uniformly at random from Λ generate a sublattice Λ_1 of full rank, i.e.