Contemporary Mathematics

Sampling cubic rings

Fabian Gundlach

Abstract. We explain how to construct a uniformly random cubic integral domain S of given signature with $|\mathrm{disc}(S)| \leq T$ in expected time $\widetilde{\mathcal{O}}(\log T)$.

1. Introduction

In the past decades, there has been an increasing amount of interest in the statistical properties of arithmetic objects such as number fields or orders in number fields.

In [**2**], Belabas gave an algorithm that computes a list of all cubic number fields K with $|\mathrm{disc}(K)| \leq T$ in time $\widetilde{\mathcal{O}}(T)$. One can similarly enumerate all cubic integral domains S (i.e., orders in cubic number fields) with $|\mathrm{disc}(S)| \leq T$ in time $\widetilde{\mathcal{O}}(T)$. The running time is essentially optimal since the number of such fields (or rings) is $\asymp T$ as was shown by Davenport and Heilbronn in [**9**].

In this paper, we give an algorithm that constructs a uniformly random cubic integral domain S of given signature with $|\mathrm{disc}(S)| \leq T$ in expected time $\widetilde{\mathcal{O}}(\log T)$. More precisely:

Theorem 1.1 (cf. Corollary 3.9)**.** *There is an algorithm which for given numbers $r \in \{1, 3\}$ and*

$$T \geq \begin{cases} 49, & r = 3, \\ 23, & r = 1 \end{cases}$$

computes in expected time $\widetilde{\mathcal{O}}(\log T)$ a cubic integral domain S of signature r with $|\mathrm{disc}(S)| \leq T$ and such that all such rings occur with the same probability.

Like [**2**] and [**9**], we use Levi's parametrization of cubic rings by $\mathrm{GL}_2(\mathbb{Z})$-orbits of integral binary cubic forms. (See [**11**].)

The running time $\widetilde{\mathcal{O}}(\log T)$ of the algorithm referred to in Theorem 1.1 is essentially optimal since the input has $\log T$ bits. (Moreover, the smallest possible total number of bits in the coefficients of a cubic form corresponding to such a random ring S is on average $\asymp \log T$.)

The lower bound on T in Theorem 1.1 ensures that there is at least one cubic integral domain S of signature r with $|\mathrm{disc}(S)| \leq T$.

2020 *Mathematics Subject Classification.* 11Y40, 11R16.

This work was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) — Project-ID 491392403 — TRR 358, project A4.

The most straightforward idea (used in [**2**] and [**9**]) for enumerating or counting the orbits with bounded discriminant is to construct a fundamental domain for the action of $\mathrm{GL}_2(\mathbb{Z})$ on the space of binary cubic forms and to then enumerate or count the lattice points in this domain.

The unboundedness of the fundamental domain, i.e., the presence of (long and narrow) cusps presents an inconvenience when enumerating or counting the lattice points. To deal with this issue, Bhargava introduced an elegant approach, which he calls "averaging over fundamental domains" or "thickening and cutting off the cusps". Very roughly speaking, he showed that it suffices to be able to estimate the number of points in linear transforms of a fixed region U of our choice! But it is relatively easy to count lattice points in a linear transform of a fixed (large) ball, at least as long as the linear transformation does not deform the ball too much. His method was for example used to obtain more precise counting results in [**7**].

In this paper, we adapt his method to the problem of selecting orbits uniformly at random. Very roughly speaking, it suffices to be able to pick uniformly random lattice points from linear transforms of a fixed region U of our choice and to have a good "uniform" upper bound on the number of lattice points in this transform. We use rejection sampling to ensure that all orbits occur with exactly the same probability. The quality of the uniform upper bound on the number of lattice points is important for estimating the running time of the algorithm.

Instead of using Bhargava's method, one could try to use rejection sampling to directly pick a point uniformly at random from the fundamental domain described in [**2**]. This seems possible, but not easier than the approach described in this article.

Being able to choose cubic orders of large discriminant uniformly at random could be advantageous for statistical experiments compared to completely enumerating all cubic orders of bounded discriminant when faced with error terms that decay slowly compared to the main term. For example, in [**13**, section 5], Malle experimentally studied the 2-ranks of class groups of cubic number fields. To this end, he used the algorithm of Belabas [**2**] to enumerate all number fields of small discriminant and computed the class groups of a small sample of these number fields. As Malle pointed out, his data is not entirely clear since he could (with Belabas' algorithm) only consider a relatively small range of discriminants.

An implementation of the algorithm as a standalone program is provided. (See section 4.)

Our approach can be adapted to other arithmetic objects parameterized by prehomogeneous vector spaces such as the famous parameterization of ideal classes of quadratic rings by orbits of binary quadratic forms or the parameterizations given in [**3**], [**5**]. (See section 5.)

Acknowledgements. The author is grateful for helpful conversations with Noam Elkies, Jürgen Klüners, and Anne-Edgar Wilke. Moreover, the author would like to thank the anonymous referees for their careful reading and helpful suggestions.

2. Preparations

It is easy to select an integer lattice point in an axis-parallel box with integer side lengths uniformly at random. This remains true if we apply a triangular linear transformation to the box:

Lemma 2.1. *Consider an axis-parallel box $I = I_1 \times \cdots \times I_n \subset \mathbb{R}^n$, where $I_1, \ldots, I_n$ are half-open intervals, say $I_i = [a_i, a_i + l_i)$, of integer lengths $l_1, \ldots, l_n \in \mathbb{Z}$. Let $M = (m_{ij})_{i,j}$ be a lower-triangular unipotent matrix with inverse $M^{-1} = (m'_{ij})_{i,j}$. Then, the set $\mathbb{Z}^n \cap MI$ has size $l_1 \cdots l_n$ and the following algorithm selects an element $v = (v_1, \ldots, v_n)$ of $\mathbb{Z}^n \cap MI$ uniformly at random.*

Algorithm 2.1 Finding a random lattice point in a transformed box

1: **for** $i \leftarrow 1, \ldots, n$ **do**
2: Pick an element δ_i of $\{0, \ldots, l_i - 1\}$ uniformly at random.
3: $v_i \leftarrow \left\lceil a_i - \sum_{j<i} m'_{ij} v_j \right\rceil + \delta_i$
4: **end for**

Proof. By definition, for any $v \in \mathbb{R}^n$, we have $v \in MI$ if and only if

$$\sum_j m'_{ij} v_j \in [a_i, a_i + l_i) \qquad \text{for all } i.$$

The inverse matrix M^{-1} is also lower-triangular and unipotent, so the sum on the left-hand side is $v_i + \sum_{j<i} m'_{ij} v_j$.

Hence, $v \in MI$ if and only if

$$a_i - \sum_{j<i} m'_{ij} v_j \le v_i < a_i - \sum_{j<i} m'_{ij} v_j + l_i \qquad \text{for all } i.$$

The integer solutions v_i to these inequalities are

$$v_i = \left\lceil a_i - \sum_{j<i} m'_{ij} v_j \right\rceil + \delta_i \qquad \text{for } \delta_i \in \{0, \ldots, l_i - 1\}. \qquad \square$$

Our algorithm will work with approximations of random real numbers and we will show that a given precision suffices with large probability to decide whether a particular polynomial inequality $f(x) > 0$ holds. The following lemma will help with this analysis. (Here, ε will be the precision to which we have computed $f(x)$.)

Lemma 2.2. *Let $n \ge 1$. For any monic polynomial $f \in \mathbb{R}[X]$ of degree n and any $\varepsilon > 0$, the set of $x \in \mathbb{R}$ with $|f(x)| \le \varepsilon$ has measure at most $2n\varepsilon^{1/n}$.*

Proof. Let $r_1, \ldots, r_n$ be the complex roots of f, so that $f(X) = (X - r_1) \cdots (X - r_n)$. Any $x \in \mathbb{R}$ with $|f(x)| \le \varepsilon$ must have distance at most $\varepsilon^{1/n}$ from one of the roots r_i. For any given root r_i, the set of $x \in \mathbb{R}$ with $|x - r_i| \le \varepsilon^{1/n}$ forms an interval of length at most $2\varepsilon^{1/n}$. The claim follows by summing over all roots. $\square$

3. Cubic rings

In this section, we describe an algorithm to construct random cubic rings.

We first remind the reader of some basic definitions. A *cubic ring* is a (commutative unitary) ring which is isomorphic to $\mathbb{Z}^3$ as a $\mathbb{Z}$-module. A *cubic integral domain* is a cubic ring which is an integral domain. They are exactly the orders in cubic number fields. The *signature* of a cubic integral domain is the number of real embeddings of its field of fractions.

13 Jun 2025 06:52:58 PDT
250131-Gundlach Version 2 - Submitted to LuCaNT

3.1. Levi's parameterization. In this subsection, we recall Levi's parameterization of cubic rings by binary cubic forms.

For any ring R, let $\mathcal{V}(R)$ denote the set of binary cubic forms $f = aX^3 + bX^2Y + cXY^2 + dY^3$ with $a, b, c, d \in R$. We can naturally identify $\mathcal{V}(R)$ with R^4 by identifying a cubic form f with its coefficient vector (a, b, c, d).

Define an action of $\mathrm{GL}_2(R)$ on $\mathcal{V}(R)$ by

$$(Mf)(v) = \det(M)^{-1} \cdot f(M^T v) \qquad \text{for } M \in \mathrm{GL}_2(R) \text{ and } f \in \mathcal{V}(R) \text{ and } v \in R^2.$$

The discriminant $\mathrm{disc}(f)$ is a homogeneous degree 4 polynomial in the coefficients a, b, c, d. It is invariant under the action of the group

$$\mathrm{SL}_2^{\pm}(R) = \{g \in \mathrm{GL}_2(R) : \det(g) = \pm 1\}.$$

In [**11**], Levi described a bijection

$$\mathrm{GL}_2(\mathbb{Z})\backslash\mathcal{V}(\mathbb{Z}) \longleftrightarrow \{\text{cubic rings}\}$$

with the following properties:

a) If an orbit $\mathrm{GL}_2(\mathbb{Z})f$ corresponds to the cubic ring S, then $\mathrm{disc}(f) = \mathrm{disc}(S)$ and there is a group isomorphism $\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(f) \cong \mathrm{Aut}(S)$, where we denote by $\mathrm{Aut}(S)$ the automorphism group of the ring S.

b) The *irreducible orbits* (orbits consisting of cubic forms f that are irreducible over $\mathbb{Q}$) correspond to the cubic integral domains. If an irreducible orbit $\mathrm{GL}_2(\mathbb{Z})f$ corresponds to the cubic integral domain S, then the signature of S is the number of roots of f in $\mathbb{P}^1(\mathbb{R})$.

c) Concretely, the cubic ring S corresponding to an orbit $\mathrm{GL}_2(\mathbb{Z})f$ with $f = aX^3 + bX^2Y + cXY^2 + dY^3$ has a $\mathbb{Z}$-basis of the form $(1, \omega_1, \omega_2)$ with

$$\begin{aligned}
\omega_1 \cdot \omega_2 &= -ad \cdot 1, \\
\omega_1 \cdot \omega_1 &= -ac \cdot 1 - b \cdot \omega_1 + a \cdot \omega_2, \\
\omega_2 \cdot \omega_2 &= -bd \cdot 1 - d \cdot \omega_1 + c \cdot \omega_2.
\end{aligned}$$

3.2. The Siegel set and Gauss' fundamental domain. We next describe Gauss' well-known fundamental domain for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $\mathrm{SL}_2^{\pm}(\mathbb{R})$.

Any element g of $\mathrm{SL}_2^{\pm}(\mathbb{R})$ can be written uniquely as a product nak with

$$n \in N(\mathbb{R}) = \left\{ \begin{pmatrix} 1 & \\ t & 1 \end{pmatrix} : t \in \mathbb{R} \right\}, \quad a \in A(\mathbb{R}) = \left\{ \begin{pmatrix} s^{-1} & \\ & s \end{pmatrix} : s \in \mathbb{R}^\times \right\}, \quad k \in O_2(\mathbb{R}).$$

In fact, the resulting bijection $N(\mathbb{R}) \times A(\mathbb{R}) \times O_2(\mathbb{R}) \leftrightarrow \mathrm{SL}_2^{\pm}(\mathbb{R})$ is a diffeomorphism. Let $\mathrm{d}t, \mathrm{d}^\times s, \mathrm{d}^\times k$ be Haar measures on the groups $N(\mathbb{R}) \cong \mathbb{R}$, $A(\mathbb{R}) \cong \mathbb{R}^\times$, and $O_2(\mathbb{R})$, respectively. Then, the pushforward of the measure $\mathrm{d}t \cdot s^{-2}\mathrm{d}^\times s \cdot \mathrm{d}^\times k$ is a Haar measure $\mathrm{d}^\times g$ on $\mathrm{SL}_2^{\pm}(\mathbb{R})$.

Matrices of the form

$$n(t) := \begin{pmatrix} 1 & \\ t & 1 \end{pmatrix} \qquad \text{or} \qquad a(s) := \begin{pmatrix} s^{-1} & \\ & s \end{pmatrix}$$

act on $\mathcal{V}(\mathbb{R}) \cong \mathbb{R}^4$ as

$$\begin{pmatrix} 1 & & & \\ 3t & 1 & & \\ 3t^2 & 2t & 1 & \\ t^3 & t^2 & t & 1 \end{pmatrix} \qquad \text{or} \qquad \begin{pmatrix} s^{-3} & & & \\ & s^{-1} & & \\ & & s & \\ & & & s^3 \end{pmatrix}.$$

13 Jun 2025 06:52:58 PDT
250131-Gundlach Version 2 - Submitted to LuCaNT

Let $s_{\min} := \sqrt{\sqrt{3}/2}$. The *Siegel set*

$$\mathcal{F} := \{n(t)a(s)k : |t| \le \tfrac{1}{2},\ s \ge s_{\min},\ k \in O_2(\mathbb{R})\} \subset \mathrm{SL}_2^{\pm}(\mathbb{R}) \tag{3.1}$$

contains the famous fundamental domain

$$\mathcal{F}' := \{n(t)a(s)k : |t| \le \tfrac{1}{2},\ s \ge \sqrt[4]{1-t^2},\ k \in O_2(\mathbb{R})\} \subset \mathrm{SL}_2^{\pm}(\mathbb{R}). \tag{3.2}$$

This set $\mathcal{F}'$ (called the *Gauss set*) is a fundamental domain for the left action of $\mathrm{GL}_2(\mathbb{Z})$ on $\mathrm{SL}_2^{\pm}(\mathbb{R})$. More precisely, we have

$$\sum_{h \in \mathrm{GL}_2(\mathbb{Z})} \alpha(hg) = 4 \text{ for all } g \in \mathrm{SL}_2^{\pm}(\mathbb{R}),$$

where $\alpha(g) = \alpha(t,s)$ for $g = n(t)a(s)k$ with

$$\begin{array}{lll} \alpha(g) = 0 & \text{if } g \text{ lies outside } \mathcal{F}', & \text{i.e., } |t| > \dfrac{1}{2} \text{ or } s < \sqrt[4]{1-t^2}, \\ \alpha(g) = 1 & \text{if } g \text{ lies in the interior of } \mathcal{F}', & \text{i.e., } |t| < \dfrac{1}{2} \text{ and } s > \sqrt[4]{1-t^2}, \\ \alpha(g) \in [0,1] & \text{always.} & \end{array} \tag{3.3}$$

(For simplicity, we don't give the formulas for $\alpha(g)$ on the measure 0 boundary of $\mathcal{F}'$. The sum is 4 because for any matrix g in $\mathcal{F}'$, the matrices $\left(\begin{smallmatrix} \pm 1 & \\ & \pm 1 \end{smallmatrix}\right) g$ also lie in $\mathcal{F}'$.)

3.3. Bhargava's averaging trick. We now fix a signature $r \in \{1,3\}$ and let $\mathcal{V}^r(\mathbb{R}) \subset \mathcal{V}(\mathbb{R})$ be the set of squarefree cubic forms with exactly r real roots. Let $\mathcal{W}^r(\mathbb{R}) \subset \mathcal{V}^r(\mathbb{R})$ be the subset consisting of those cubic forms f with $|\mathrm{disc}(f)| = 1$. The group $\mathrm{SL}_2^{\pm}(\mathbb{R})$ acts transitively on $\mathcal{W}^r(\mathbb{R})$. The set $\mathcal{W}^r(\mathbb{R})$ is a 3-dimensional smooth submanifold of $\mathcal{V}(\mathbb{R})$. It follows that the pushforward of $\mathrm{d}^\times g$ along the map $\mathrm{SL}_2^{\pm}(\mathbb{R}) \to \mathcal{W}^r(\mathbb{R})$, $g \mapsto g^{-1} f_0$, is independent of the choice of $f_0 \in \mathcal{W}^r(\mathbb{R})$. Denote this pushforward by $\mathrm{d}f$. Bhargava's averaging over fundamental domains / thickening of cusps trick (see for example [**4**, section 2.2] or [**7**, section 5.3]) relies on the following lemma:

Lemma 3.1. *Fix an integrable subset $U \subseteq \mathcal{W}^r(\mathbb{R})$. We define the function η on $\mathcal{W}^r(\mathbb{R})$ to be the following average of the indicator functions of linear transforms of U by elements g of the fundamental domain $\mathcal{F}'$:*

$$\eta(f) \coloneqq \int_{\mathcal{F}'} \chi_{gU}(f) \mathrm{d}^\times g$$

and let

$$C \coloneqq \int_{\mathcal{W}^r(\mathbb{R})} \chi_U(f) \mathrm{d}f.$$

We then have for all $f \in \mathcal{W}^r(\mathbb{R})$:

$$\sum_{h \in \mathrm{GL}_2(\mathbb{Z})} \eta(hf) = 4C.$$

Proof. We have

$$\sum_{h \in \mathrm{GL}_2(\mathbb{Z})} \eta(hf) = \sum_{h \in \mathrm{GL}_2(\mathbb{Z})} \int_{\mathcal{F}'} \chi_{gU}(hf) \mathrm{d}^\times g$$

$$
\begin{aligned}
&= \sum_{h\in \mathrm{GL}_2(\mathbb{Z})} \int_{\mathrm{SL}_2^{\pm}(\mathbb{R})} \alpha(g)\chi_{gU}(hf)\mathrm{d}^{\times}g \\
&= \sum_{h\in \mathrm{GL}_2(\mathbb{Z})} \int_{\mathrm{SL}_2^{\pm}(\mathbb{R})} \alpha(g)\chi_{h^{-1}gU}(f)\mathrm{d}^{\times}g \\
&= \sum_{h\in \mathrm{GL}_2(\mathbb{Z})} \int_{\mathrm{SL}_2^{\pm}(\mathbb{R})} \alpha(hg)\chi_{gU}(f)\mathrm{d}^{\times}g \\
&= 4\int_{\mathrm{SL}_2^{\pm}(\mathbb{R})} \chi_{gU}(f)\mathrm{d}^{\times}g = 4\int_{\mathrm{SL}_2^{\pm}(\mathbb{R})} \chi_U(g^{-1}f)\mathrm{d}^{\times}g \\
&= 4\int_{\mathcal{W}^r(\mathbb{R})} \chi_U(f)\mathrm{d}f = 4C. \qquad \square
\end{aligned}
$$

3.4. A ball and its $\mathrm{GL}_2(\mathbb{R})$-transforms. Let $\|\cdot\|$ be the norm on $\mathcal{V}(\mathbb{R})$ associated to the following positive definite quadratic form q on $\mathcal{V}(\mathbb{R})$:

$$q(aX^3+bX^2Y+cXY^2+dY^3) = 5a^2+b^2+c^2+5d^2+2ac+2bd.$$

Lemma 3.2. *The quadratic form q is positive definite and invariant under the action of the orthogonal group $O_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{R})$.*

Proof. One can check that for any $f \in \mathcal{V}(\mathbb{R})$,

$$\int_{\{(x,y)\in\mathbb{R}^2 : x^2+y^2\le 1\}} f(x,y)^2 \mathrm{d}(x,y) = \frac{\pi}{64}\cdot q(f).$$

The left-hand side is clearly positive definite and $O_2(\mathbb{R})$-invariant. $\square$

Lemma 3.3. *Consider the closed unit ball of radius 1 in $\mathcal{V}(\mathbb{R})$. The maximum values of $|a|,|b|,|c|,|d|$ on this set are $\frac{1}{2}, \frac{\sqrt{5}}{2}, \frac{\sqrt{5}}{2}, \frac{1}{2}$, respectively.*

Proof. To achieve the maximum value of $|a|$, for instance, the derivatives of $q(f)$ with respect to b, c, d need to vanish. One easily checks that this occurs exactly at the two points $\pm\frac{1}{2}(X^3 - XY^2)$.

The maximum for $|b|$ occurs at $\pm\frac{\sqrt{5}}{2}(X^2Y - \frac{1}{5}Y^3)$. The maxima for $|c|$ and $|d|$ follow by symmetry. $\square$

Consider the open unit ball in $\mathcal{V}(\mathbb{R})$:

$$B = \{f \in \mathcal{V}(\mathbb{R}) : \|f\| < 1\}$$

By Lemma 3.3, B is contained in the box $I := I_1 \times \cdots \times I_4$ given by

$$
\begin{aligned}
I_1 &:= \{a \in \mathbb{R} : |a| \le \tfrac{1}{2}\}, & I_2 &:= \{b \in \mathbb{R} : |b| \le \tfrac{\sqrt{5}}{2}\}, \\
I_3 &:= \{c \in \mathbb{R} : |c| \le \tfrac{\sqrt{5}}{2}\}, & I_4 &:= \{d \in \mathbb{R} : |d| \le \tfrac{1}{2}\}.
\end{aligned}
$$

Hence, for any $\lambda, s > 0$, the set $\lambda \cdot a(s)B$ is contained in the box $\lambda \cdot a(s)I$ with side lengths

$$
\begin{aligned}
l_1(\lambda,s) &:= \lambda s^{-3}, & l_2(\lambda,s) &:= \sqrt{5}\lambda s^{-1}, \\
l_3(\lambda,s) &:= \sqrt{5}\lambda s, & l_4(\lambda,s) &:= \lambda s^3.
\end{aligned}
$$

The box $\lambda \cdot a(s)I$ is in turn contained in the box $I'(\lambda,s) = I_1'(\lambda,s) \times \cdots \times I_4'(\lambda,s)$ with integer side lengths $l_i'(\lambda,s)$, where

$$I_i'(\lambda,s) := \left[-\tfrac{1}{2}l_i'(\lambda,s), \tfrac{1}{2}l_i'(\lambda,s)\right) \text{ with } l_i'(\lambda,s) := \lfloor 1 + l_i(\lambda,s)\rfloor \in \mathbb{Z} \text{ for } i = 1,\dots,4.$$

13 Jun 2025 06:52:58 PDT
250131-Gundlach Version 2 - Submitted to LuCaNT

Let $s_{\max} = \sqrt[3]{\lambda/2}$. For $s_{\min} \le s \le s_{\max}$, we can bound the side lengths $l'_i(\lambda, s)$ from above as follows:

$$\begin{aligned} l'_1(\lambda,s) &\le L'_1(\lambda)\cdot s^{-3}, \quad l'_2(\lambda,s) \le L'_2(\lambda)\cdot s^{-1}, \\ l'_3(\lambda,s) &\le L'_3(\lambda)\cdot s, \qquad l'_4(\lambda,s) \le L'_4(\lambda)\cdot s^{3}, \end{aligned} \tag{3.4}$$

where

$$\begin{aligned} L'_1(\lambda) &:= s_{\max}^3 + \lambda, & L'_2(\lambda) &:= s_{\max} + \sqrt{5}\lambda, \\ L'_3(\lambda) &:= s_{\min}^{-1} + \sqrt{5}\lambda, & L'_4(\lambda) &:= s_{\min}^{-3} + \lambda. \end{aligned}$$

3.5. The high-level algorithm. Fix a radius $R > 0$ large enough so that $R \cdot B \cap \mathcal{W}^r(\mathbb{R}) \neq \emptyset$. (For example, you can take $R = 7/4$ for $r = 1$ and $R = 5/4$ for $r = 3$.)

We now give an algorithm for computing random irreducible $\mathrm{GL}_2(\mathbb{Z})$-orbits. This first algorithm uses real arithmetic and we later explain how to deal with precision issues.

Theorem 3.4. *Let $T \ge 1$ and $\lambda = RT^{1/4}$. Let $s_{\min} = \sqrt{\sqrt{3}/2}$ and $s_{\max} = \sqrt[3]{\lambda/2}$.*

a) The following algorithm either fails or produces an element f of an irreducible $\mathrm{GL}_2(\mathbb{Z})$-orbit in $\mathcal{V}^r(\mathbb{Z})$ with $0 < |\mathrm{disc}(f)| \le T$.

b) The probability of returning an element of any given such orbit $\mathrm{GL}_2(\mathbb{Z})f$ is (for fixed r and T) proportional to $1/\#\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(f)$.

c) The probability of success is $> p_0$ for a constant p_0 (depending only on r and R, but not on T) if there is at least one such orbit $\mathrm{GL}_2(\mathbb{Z})f$.

Algorithm 3.1 Finding a random orbit of cubic forms

1: Pick an element t of $(-\frac{1}{2}, \frac{1}{2})$ uniformly at random.
2: Pick an element s of $(s_{\min}, \infty)$ at random with probability measure proportional to $s^{-2}\mathrm{d}^\times s$.
3: **return** FAIL **unless** $\sqrt[4]{1-t^2} < s < s_{\max}$.
4: **return** FAIL **with probability** $1 - \frac{l'_1(\lambda,s)\cdots l'_4(\lambda,s)}{L'_1(\lambda)\cdots L'_4(\lambda)}$.
5: Pick a point $f \in \mathcal{V}(\mathbb{Z}) \cap n(t)I'(\lambda, s)$ uniformly at random using Algorithm 2.1.
6: **return** FAIL **unless** $f \in \mathcal{V}^r(\mathbb{R})$ and $0 < |\mathrm{disc}(f)| \le T$ and f is irreducible over $\mathbb{Q}$ and $f \in R|\mathrm{disc}(f)|^{1/4} \cdot n(t)a(s)B$.
7: **return** f.

Remark 3.5. Repeat the algorithm until it succeeds. According to c), if there is such an orbit, it will succeed after at most $1/p_0$ attempts on average.

Remark 3.6. The smallest absolute discriminant of an irreducible orbit with signature $r = 3$ is 49. The smallest absolute discriminant of an irreducible orbit with signature $r = 1$ is 23. (See for example tables of number fields of degree 3 and small discriminant, such as the one available at [**12**].)

Remark 3.7. The following algorithm satisfies a) and c), but every orbit has the same probability of being returned: Compute a random orbit $\mathrm{GL}_2(\mathbb{Z})f$ using Algorithm 3.1. Return this orbit $\mathrm{GL}_2(\mathbb{Z})f$ with probability $\#\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(f)/3$ and return FAIL otherwise. (If f corresponds to the cubic integral domain S with field of fractions K, the group $\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(f) \cong \mathrm{Aut}(S) \subseteq \mathrm{Aut}(K)$ is either trivial or cyclic of order 3.)

13 Jun 2025 06:52:58 PDT
250131-Gundlach Version 2 - Submitted to LuCaNT

Proof of Theorem 3.4. For $s_{\min} \le s \le s_{\max}$, we have

$$0 \le \frac{l_1'(\lambda,s)\cdots l_4'(\lambda,s)}{L_1'(\lambda)\cdots L_4'(\lambda)} \le 1,$$

according to (3.4), so line 4 of the algorithm makes sense. Claim a) is clear.

Now, consider any irreducible cubic form $f \in \mathcal{V}^r(\mathbb{Z})$ with $0 < |\mathrm{disc}(f)| \le T$.

Since $|t| \le \frac{1}{2}$, we have $s_{\min} = \sqrt{\sqrt{3}/2} \le \sqrt[4]{1-t^2}$. The algorithm returns the cubic form f with probability

$$P(f) := \frac{\int_{-1/2}^{1/2}\int_{\sqrt[4]{1-t^2}}^{s_{\max}} p(f,t,s)\cdot s^{-2}\mathrm{d}^\times s\,\mathrm{d}t}{\int_{-1/2}^{1/2}\int_{s_{\min}}^{\infty} s^{-2}\mathrm{d}^\times s\,\mathrm{d}t},$$

where

$$p(f,t,s) := \frac{l_1'(\lambda,s)\cdots l_4'(\lambda,s)}{L_1'(\lambda)\cdots L_4'(\lambda)} \cdot \frac{\chi_{n(t)I'(\lambda,s)}(f)}{\#(\mathcal{V}(\mathbb{Z})\cap n(t)I'(\lambda,s))} \cdot \chi_{R|\mathrm{disc}(f)|^{1/4}\cdot n(t)a(s)B}(f).$$

We have $\#(\mathcal{V}(\mathbb{Z})\cap n(t)I'(\lambda,s)) = l_1'(\lambda,s)\cdots l_4'(\lambda,s)$ by Lemma 2.1.

Since $0 < |\mathrm{disc}(f)| \le T$ and $\lambda = RT^{1/4}$, we moreover have

$$R|\mathrm{disc}(f)|^{1/4}\cdot n(t)a(s)B \subseteq \lambda\cdot n(t)a(s)B \subseteq \lambda\cdot n(t)a(s)I \subseteq n(t)I'(\lambda,s). \tag{3.5}$$

Hence,

$$p(f,t,s) = \frac{\chi_{R|\mathrm{disc}(f)|^{1/4}\cdot n(t)a(s)B}(f)}{L_1'(\lambda)\cdots L_4'(\lambda)}.$$

Moreover, since $f = aX^3+\cdots+dY^3$ is irreducible, we have $a \neq 0$, so $|a| \ge 1$. On the other hand, if $p(f,t,s) \neq 0$, then by (3.5), we have $f \in \lambda\cdot n(t)a(s)I$, which implies $|a| \le \frac{1}{2}\lambda s^{-3}$. Therefore, if $p(f,t,s) \neq 0$, then $1 \le \frac{1}{2}\lambda s^{-3}$, so $s \le \sqrt[3]{\lambda/2} = s_{\max}$. (Bhargava calls this inequality "cutting off the cusp".) Hence, the upper bound on s in the integral in the numerator of $P(f)$ can be omitted without changing the value of the integral:

$$P(f) = \frac{\int_{-1/2}^{1/2}\int_{\sqrt[4]{1-t^2}}^{\infty} p(f,t,s)\cdot s^{-2}\mathrm{d}^\times s\,\mathrm{d}t}{\int_{-1/2}^{1/2}\int_{s_{\min}}^{\infty} s^{-2}\mathrm{d}^\times s\,\mathrm{d}t}.$$

We now multiply both the numerator and the denominator by the finite number $\int_{O_2(\mathbb{R})}\mathrm{d}^\times k$. Since B is $O_2(\mathbb{R})$-invariant and since the measure $\mathrm{d}t\cdot s^{-2}\mathrm{d}^\times s\cdot\mathrm{d}^\times k$ on $N(\mathbb{R})\times A(\mathbb{R})\times O_2(\mathbb{R})$ corresponds to the Haar measure $\mathrm{d}^\times g$ on $\mathrm{SL}_2^{\pm}(\mathbb{R})$, it follows together with the definitions of $\mathcal{F}$ and $\mathcal{F}'$ in (3.1) and (3.2) that

$$P(f) = \frac{\int_{\mathcal{F}'} p(f,g)\mathrm{d}^\times g}{\int_{\mathcal{F}}\mathrm{d}^\times g}$$

with

$$p(f,g) := \frac{\chi_{R|\mathrm{disc}(f)|^{1/4}\cdot gB}(f)}{L_1'(\lambda)\cdots L_4'(\lambda)}.$$

Note that $|\mathrm{disc}(|\mathrm{disc}(f)|^{-1/4}\cdot f)| = 1$ and therefore $|\mathrm{disc}(f)|^{-1/4}\cdot f \in \mathcal{W}^r(\mathbb{R})$ because $\mathrm{disc}(f)$ is a homogeneous polynomial of degree 4 in the coefficients of f. Setting $U := R\cdot B\cap\mathcal{W}^r(\mathbb{R})$, we can therefore rewrite $p(f,g)$ as

$$p(f,g) := \frac{\chi_{gU}(|\mathrm{disc}(f)|^{-1/4}\cdot f)}{L_1'(\lambda)\cdots L_4'(\lambda)},$$

so

$$P(f) = \frac{\int_{\mathcal{F}'} \chi_{gU}(|\mathrm{disc}(f)|^{-1/4} \cdot f) \cdot \mathrm{d}^\times g}{L_1'(\lambda) \cdots L_4'(\lambda) \cdot \int_{\mathcal{F}} \mathrm{d}^\times g}$$

By Lemma 3.1 applied to the element $|\mathrm{disc}(f)|^{-1/4} \cdot f$ of $\mathcal{W}^r(\mathbb{R})$, we obtain

$$\sum_{h \in \mathrm{GL}_2(\mathbb{Z})} P(hf) = D(\lambda) := \frac{C}{L_1'(\lambda) \cdots L_4'(\lambda)},$$

with

$$C = \frac{4 \cdot \int_{\mathcal{W}^r(\mathbb{R})} \chi_U(f') \mathrm{d}f'}{\int_{\mathcal{F}} \mathrm{d}^\times g}.$$

The constant C is positive because U is a nonempty open subset of $\mathcal{W}^r(\mathbb{R})$ and $\int_{\mathcal{F}} \mathrm{d}^\times g < \infty$.

On the other hand,

$$\sum_{h \in \mathrm{GL}_2(\mathbb{Z})} P(hf) = \#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(f) \cdot \sum_{f' \in \mathrm{GL}_2(\mathbb{Z})f} P(f').$$

We conclude that for any irreducible cubic form $f \in \mathcal{V}^r(\mathbb{Z})$ with $0 < |\mathrm{disc}(f)| \le T$, we have the following probability of returning an element of its $\mathrm{GL}_2(\mathbb{Z})$-orbit:

$$\sum_{f' \in \mathrm{GL}_2(\mathbb{Z})f} P(f') = \frac{D(\lambda)}{\#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(f)}.$$

Since $D(\lambda)$ is independent of f, this proves b).

For c), we sum over all $\mathrm{GL}_2(\mathbb{Z})$-orbits of irreducible cubic forms $f \in \mathcal{V}^r(\mathbb{Z})$ with $0 < |\mathrm{disc}(f)| \le T$. The number of such orbits is $\asymp T$ for $T \to \infty$. (See [**9**].) In particular, it is $\gg T$ as long as there is at least one such orbit. Since $\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(f)$ has size at most 3 by Remark 3.7, the sum of $1/\#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(f)$ over all orbits is also $\gg T$.

By definition, $L_i'(\lambda) \ll \lambda$ for all i, so $D(\lambda) \gg \lambda^{-4} \gg T^{-1}$.

It follows that the probability of success is

$$\begin{aligned}\sum_{\substack{f \in \mathcal{V}^r(\mathbb{Z}) \\ \text{irreducible} \\ 0<|\mathrm{disc}(f)|\le T}} P(f) &= \sum_{\substack{[f] \in \mathrm{GL}_2(\mathbb{Z})\backslash\mathcal{V}^r(\mathbb{Z}) \\ \text{irreducible} \\ 0<|\mathrm{disc}(f)|\le T}} \sum_{f' \in \mathrm{GL}_2(\mathbb{Z})f} P(f') \\ &= \sum_{\substack{[f] \in \mathrm{GL}_2(\mathbb{Z})\backslash\mathcal{V}^r(\mathbb{Z}) \\ \text{irreducible} \\ 0<|\mathrm{disc}(f)|\le T}} \frac{D(\lambda)}{\#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(f)} \gg T \cdot T^{-1} = 1.\end{aligned}$$

This proves c). □

3.6. Finite precision real arithmetic. The above algorithm uses real arithmetic. In practice, we need to work with approximations of those real numbers to finite precision. Note that we need to be able to decide the inequalities appearing in the algorithm and to compute $\lfloor x \rfloor$ or $\lceil x \rceil$ for various real numbers x appearing in the algorithm. By analyzing the probability with which a given precision suffices to decide the inequalities and to compute the floor and ceiling values, we show:

Theorem 3.8. *Algorithm 3.1 can be implemented on a random access machine (with a random bit generator) with expected running time $\widetilde{\mathcal{O}}(\log T)$.*

13 Jun 2025 06:52:58 PDT
250131-Gundlach Version 2 - Submitted to LuCaNT

Proof. We use the well-known method of doubling the precision until it suffices. See Algorithm 3.2 below for the concrete implementation.

We leave it to the reader to verify that Algorithm 3.2 is functionally equivalent to Algorithm 3.1. (Line 5 of Algorithm 3.2 corresponds to line 3 of Algorithm 3.1. Lines 10 and 12–14 correspond to line 5.)

We show that the probability that the algorithm doesn't finish within the first i-th iterations (due to insufficient precision) is $\mathcal{O}(T^v\varepsilon^u) = \mathcal{O}(T^v 2^{-u2^i})$ for constants $u, v > 0$ and that the running time of the i-th iteration is $\widetilde{\mathcal{O}}(\log T + p) = \widetilde{\mathcal{O}}(\log T + 2^i)$, where $p \coloneqq 2^i$ and $\varepsilon \coloneqq 2^{-i}$. The expected total running time is then

$$\begin{aligned}
&\ll \sum_{i\geq 1} \min(1, T^v 2^{-u2^i}) \cdot \widetilde{\mathcal{O}}(\log T + 2^i) \\
&\ll \sum_{1\leq i\leq \lfloor \log_2(\frac{v}{u}\log_2 T)\rfloor} \widetilde{\mathcal{O}}(\log T + 2^i) + \sum_{i>\lfloor \log_2(\frac{v}{u}\log_2 T)\rfloor} T^v 2^{-u2^i} \cdot \widetilde{\mathcal{O}}(\log T + 2^i) \\
&\ll \widetilde{\mathcal{O}}(\log T) + \sum_{j\geq \lfloor \frac{v}{u}\log_2 T\rfloor} T^v 2^{-uj} \cdot \widetilde{\mathcal{O}}(\log T + j) \\
&\overset{(*)}{\ll} \widetilde{\mathcal{O}}(\log T) + \sum_{j'\geq 0} 2^{-uj'} \cdot \widetilde{\mathcal{O}}(\log T + j') \\
&\ll \widetilde{\mathcal{O}}(\log T)
\end{aligned}$$

as claimed, where the step marked by $(*)$ uses the substitution $j' \coloneqq j - \lfloor \frac{v}{u}\log_2 T\rfloor$, noting that $2^{-uj'} \asymp T^v 2^{-uj}$ and $\lfloor \frac{v}{u}\log_2 T\rfloor \ll \log T$.

All real numbers computed in the algorithm are $\ll T^{\mathcal{O}(1)}$. It follows that the real numbers in the i-th iteration can be computed to absolute precision $\mathcal{O}(T^{\mathcal{O}(1)}\varepsilon)$ in time $\widetilde{\mathcal{O}}(\log T + p)$.

Now, we explain the failure probabilities and running times of the individual steps of the algorithm:

Line 5: The probability that the inequalities in line 5 cannot be decided from the given approximation is $\mathcal{O}(T^{\mathcal{O}(1)}\varepsilon)$ since both sides of the inequalities are known to an absolute precision of $\mathcal{O}(T^{\mathcal{O}(1)}\varepsilon)$ and the probability that the values are within this distance is $\mathcal{O}(T^{\mathcal{O}(1)}\varepsilon)$ as σ is uniformly distributed on $(0, 1)$.

Line 8: This works similarly.

Line 7: Being able to compute $l_i'(\lambda, s) = \lfloor 1 + l_i(\lambda, s)\rfloor$ from the approximation of $1+l_i(\lambda, s)$ is equivalent to $l_i(\lambda, s)$ not lying within a distance of $\mathcal{O}(T^{\mathcal{O}(1)}\varepsilon)$ from any integer $k > 0$. The closest integer to $l_i(\lambda, s)$ is $\ll T$, so we only need to consider $\ll T$ such integers k. We first bound the probability that $|l_4(\lambda, s)-k| = |\lambda s^3-k| \ll T^{\mathcal{O}(1)}\varepsilon$. As $\lambda \asymp T^{\mathcal{O}(1)}$, this is equivalent to $|s^3-\lambda^{-1}k| \ll T^{\mathcal{O}(1)}\varepsilon$. By Lemma 2.2, the set of such values $s \in \mathbb{R}$ has Lebesgue measure $\mathcal{O}(T^{\mathcal{O}(1)}\varepsilon^{1/3})$. As s is bounded from below (by $\sqrt{\sqrt{3}/2}$), the probability measure (proportional to $s^{-2}\mathrm{d}^\times s$) of this set of values s is also $\mathcal{O}(T^{\mathcal{O}(1)}\varepsilon^{1/3})$. Summing over the $\ll T$ values k, we see that the probability that the approximation is insufficient for computing $l_4(\lambda, s)$ is $\mathcal{O}(T^{\mathcal{O}(1)}\varepsilon^{1/3})$. A similar argument works for $l_3(\lambda, s)$. For $l_1(\lambda, s)$, we instead use that the inequality $|l_1(\lambda, s) - k| = |\lambda s^{-3} - k| \ll T^{\mathcal{O}(1)}\varepsilon$ is

equivalent to $|s^3 - \lambda k^{-1}| \ll T^{\mathcal{O}(1)}\varepsilon$ since $1 \le k \ll T$ and $1 \ll s \ll T^{\mathcal{O}(1)}$. We then proceed as before. The same argument works for $l_2(\lambda, s)$.

Line 9: Since $l_i'(\lambda, s) \ll T^{\mathcal{O}(1)}$ and Δ_i is chosen uniformly at random from $(0, 1)$, the probability that $\Delta_i \cdot l_i'(\lambda, s)$ lies within a distance $\mathcal{O}(T^{\mathcal{O}(1)}\varepsilon)$ from an integer is at most $\mathcal{O}(T^{\mathcal{O}(1)}\varepsilon)$.

Line 10: The number $\lceil -\frac{1}{2} l_1'(\lambda, s) \rceil$ can be computed with integer arithmetic since $l_1'(\lambda, s) \in \mathbb{Z}$.

Lines 12–14: We compute $\lceil x \rceil$ for various numbers x. Note that in each line, x is a polynomial in t of degree at most 3 whose leading coefficient has absolute value ≥ 1. By the same argument as for line 7, the probability that any of these values cannot be computed is $\mathcal{O}(T^{\mathcal{O}(1)}\varepsilon^{1/3})$.

Line 16: This involves only integer arithmetic.

Line 17: It suffices to check that $\mathrm{disc}(f) > 0$ if $r = 3$ and $\mathrm{disc}(f) < 0$ if $r = 1$.

Line 18: If

$$q(a(s)^{-1} n(-t) f) - R^2 |\mathrm{disc}(f)|^{1/2} \ll T^{\mathcal{O}(1)}\varepsilon,$$

then

$$s^6 \cdot (q(a(s)^{-1} n(-t) f) - R^2 |\mathrm{disc}(f)|^{1/2}) \ll T^{\mathcal{O}(1)}\varepsilon.$$

The left-hand side is a polynomial in s of degree 12 with leading coefficient $5a^2 \ge 5$. By Lemma 2.2, the Lebesgue measure of the set of values s satisfying the inequality is therefore $\mathcal{O}(T^{\mathcal{O}(1)}\varepsilon^{1/12})$. As $1 \ll s \ll T^{\mathcal{O}(1)}$, the probability measure of the corresponding set of values s is also $\mathcal{O}(T^{\mathcal{O}(1)}\varepsilon^{1/12})$.

Line 19: Note that a cubic form $f \in \mathcal{V}(\mathbb{Z})$ is reducible over $\mathbb{Q}$ if and only if it has a rational root. For $a \ne 0$, this is equivalent to the polynomial $f(X, 1) \in \mathbb{Z}[X]$ of degree 3 having a rational root. The denominator of such a root must divide $a \ll T$. Hence, it suffices to check whether $f(X, 1)$ has a root in $\frac{1}{a}\mathbb{Z}$. The real roots of $f(X, 1)$ can be approximated with accuracy $\frac{1}{a}$ for example using a binary search and Sturm sequences in time $\tilde{\mathcal{O}}(\log T)$. □

Algorithm 3.2 Finding a random orbit of cubic forms (using bit operations)

1: **for** $i \leftarrow 1, 2, \ldots$ **do**
2: Let $p = 2^i$ and $\varepsilon = 2^{-p}$. In this iteration, we will compute all occurring real numbers to absolute precision $\mathcal{O}(T^{\mathcal{O}(1)}\varepsilon)$. If the computed precision is insufficient to decide an occurring inequality or to compute an occurring floor or ceiling value, we immediately go to the next iteration, starting over with the next value of i.
3: Pick uniformly random elements $\tau, \sigma, \pi, \Delta_1, \ldots, \Delta_4$ of $(0, 1)$ to absolute precision ε by picking the first p binary digits of each of the numbers, keeping any digits that were already picked in the previous iteration.
4: Compute $t = \tau - \frac{1}{2}$.
5: **return** FAIL **unless** $\frac{s_{\min}^2}{s_{\max}^2} < \sigma < \frac{s_{\min}^2}{\sqrt{1-t^2}}$.
6: Compute $s = \frac{s_{\min}}{\sqrt{\sigma}}$.
7: Compute $l_i'(\lambda, s) = \lfloor 1 + l_i(\lambda, s) \rfloor$ for $i = 1, \ldots, 4$.
8: **return** FAIL **if** $\pi > \frac{l_1'(\lambda,s) \cdots l_4'(\lambda,s)}{L_1'(\lambda) \cdots L_4'(\lambda)}$.
9: Compute $\delta_i = \lfloor \Delta_i \cdot l_i'(\lambda, s) \rfloor$ for $i = 1, \ldots, 4$.

Compute $a = \lceil -\frac{1}{2} l_1'(\lambda, s) \rceil + \delta_1$.
return FAIL **unless** $a \neq 0$.
Compute $b = \lceil -\frac{1}{2} l_2'(\lambda, s) + 3ta \rceil + \delta_2$.
Compute $c = \lceil -\frac{1}{2} l_3'(\lambda, s) - 3t^2 a + 2tb \rceil + \delta_3$.
Compute $d = \lceil -\frac{1}{2} l_4'(\lambda, s) + t^3 a - t^2 b + tc \rceil + \delta_4$.
Let $f = aX^3 + bX^2Y + cXY^2 + dY^3$.
return FAIL **unless** $0 < |\mathrm{disc}(f)| \leq T$.
return FAIL **unless** $f \in \mathcal{V}^r(\mathbb{R})$.
return FAIL **unless** $q(a(s)^{-1} n(-t) f) < R^2 |\mathrm{disc}(f)|^{1/2}$.
return FAIL **unless** f is irreducible over $\mathbb{Q}$.
return f.
end for

Corollary 3.9 (cf. Theorem 1.1)**.** *There are algorithms which for a given number $r \in \{1, 3\}$ and T with*

$$T \geq \begin{cases} 49, & r = 3, \\ 23, & r = 1 \end{cases}$$

compute in expected time $\widetilde{\mathcal{O}}(\log T)$ a cubic integral domain S of signature r with $|\mathrm{disc}(S)| \leq T$ and such that

a) the probability of returning any given such ring S is for fixed T proportional to $1/\#\operatorname{Aut}(S)$ or
b) all such rings occur with the same probability.

(Here, cubic rings are represented by a corresponding binary cubic form.)

Proof. Claim a) follows immediately from Theorems 3.4 and 3.8 and Remarks 3.5 and 3.6. For b), we also use Remark 3.7. □

Remark 3.10. To compute a random cubic number field K with signature r and $|\mathrm{disc}(K)| \leq T$ (either uniformly or with probability proportional to $1/\#\operatorname{Aut}(K)$), one can compute cubic integral domains S until finding one which is the ring of integers of its field of fractions K. There are well-known algorithms for testing whether S is the ring of integers of its field of fractions, whose running time is dominated by the factorization of the integer $\mathrm{disc}(S)$. (See for example [**8**, section 6.1].)

In [**1**], Bach gave an algorithm that generates a uniformly random integer $1 \leq x \leq N$ together with its factorization. The expected running time of his algorithm is that required for $\mathcal{O}(\log N)$ primality tests of numbers $1 \leq p \leq N$. It could be an interesting problem to efficiently find a uniform random cubic integral domain together with the factorization of its discriminant.

Remark 3.11. One of the referees raised the question whether it would be possible to generate cubic rings in narrow discriminant bands. There is indeed an algorithm similar to the one described above (but slightly more complicated) to generate a uniformly random cubic integral domain S of signature r with discriminant in $[T, T + T^{5/6+\varepsilon}]$ in expected time $\widetilde{\mathcal{O}}_\varepsilon(\log T)$. We briefly comment on the main differences:

The ball B of radius 1 centered at the origin should be replaced by a ball B' centered at a (fixed) point on $W_r(\mathbb{R})$ of radius $T^{-1/6+\varepsilon}$. In addition to $n(t)$ and $a(s)$, we need to first apply a random element k of $O_2(\mathbb{R})$ to this ball B' (as, unlike B, the

ball B' is not $O_2(\mathbb{R})$-invariant). In Algorithm 3.1, we pick a random integral point in $n(t)I'(\lambda, s)$, where $I'(\lambda, s)$ is a box with integer side lengths containing $\lambda \cdot a(s)B$. We now need to instead pick a random integral point in $n(t)I''(\lambda, s, k)$, where $I''(\lambda, s, k)$ is a box with integer side lengths containing $[T^{1/4}, (T + T^{5/6+\varepsilon})^{1/4}] \cdot a(s)kB'$. The volume of this box is at most $C \cdot f(T, s)$ for some constant $C > 0$ and

$$f(T,s) := \begin{cases} T^{1/3+4\varepsilon} & \text{if } s^3 \le T^{1/12+\varepsilon}, \\ T^{1/4+3\varepsilon} s^3 & \text{if } T^{1/12+\varepsilon} \le s^3 \le s_{\max}^3. \end{cases}$$

To make up for the fact that the volume of this box now very much depends on s, one needs to actually choose s at random with probability measure proportional to $f(T, s)s^{-2}\mathrm{d}^\times s$, and then change line 4 of Algorithm 3.1 to make up for the difference between this upper bound on the volume of the box and its actual volume.

(Even for ε slightly smaller than 0, the resulting algorithm would be correct, but the probability of success would go to 0 as $T \to \infty$. The lower bound 5/6 for the exponent of the width of the interval $[T, T + T^{5/6+\varepsilon}]$ corresponds to the second order term in the count of cubic integral domains [**7**].)

4. Implementation

An implementation of the algorithm described above is available at `https://github.com/fagu/random-orbits`. It makes use of the FLINT library [**14**] for large integer and polynomial arithmetic, and in particular for arbitrary-precision interval arithmetic [**10**].

Figure 1 gives the approximate average time it takes to generate one random cubic integral domain S with signature r and $|\mathrm{disc}(S)| \le 2^t$, where the probability of obtaining a given ring S is proportional to $1/\#\operatorname{Aut}(S)$. For example, it takes roughly 10^{-3} seconds to generate a random ring with $r = 3$ and $|\mathrm{disc}(S)| \le 2^{200}$ and roughly one second to generate a random ring with $r = 3$ and $|\mathrm{disc}(S)| \le 2^{200\,000}$. (These computations were performed on an Intel Core i7-1355U processor.)

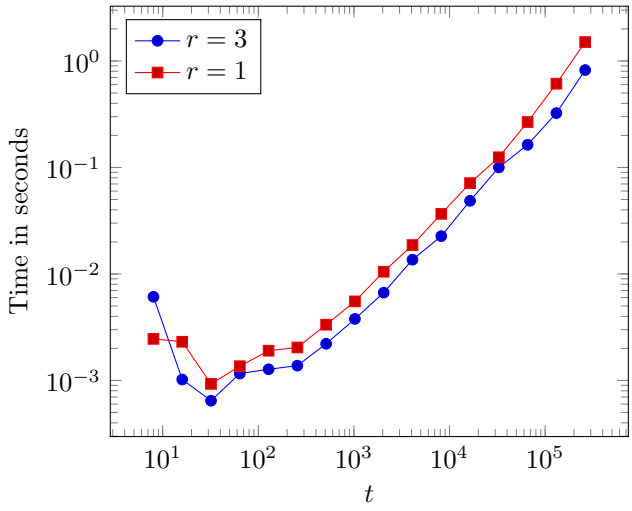

FIGURE 1. Average time to generate one random ring

5. Other parameterizations

The method described above can be adapted to other parameterizations by prehomogeneous vector spaces.

For example, it is well-known that there is a bijection between the set of $\mathrm{GL}_2(\mathbb{Z})$-orbits of primitive binary quadratic forms and the set of ideal classes of orders in quadratic number fields. One obtains an algorithm which constructs a random pair (S, I), where S is a quadratic integral domain with given signature and $|\mathrm{disc}(S)| \leq T$ and I is an invertible ideal class of S with expected running time $\widetilde{\mathcal{O}}(\log T)$. The probability the algorithm returns a given such pair (S, I) is proportional to $\frac{\mathrm{Reg}(S)}{\omega_S}$, where $\mathrm{Reg}(S)$ is the regulator of S and ω_S is the number of roots of unity in S.

The method can also be used to construct random quartic or quintic rings as in [**3**], [**5**] (with bounds derived as in [**4**] and [**6**]). Unfortunately, the constant factor in the running time crucially depends on the dimension of the prehomogeneous vector space. Quintic rings are parameterized by orbits in a 40-dimensional prehomogeneous vector space and the constant factor becomes impractically large.

References

1. Eric Bach, *How to generate factored random numbers*, vol. 17, 1988, Special issue on cryptography, pp. 179–193. MR 935336
2. K. Belabas, *A fast algorithm to compute cubic fields*, Math. Comp. **66** (1997), no. 219, 1213–1237. MR 1415795
3. Manjul Bhargava, *Higher composition laws. III. The parametrization of quartic rings*, Ann. of Math. (2) **159** (2004), no. 3, 1329–1360. MR 2113024
4. ———, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063. MR 2183288
5. ———, *Higher composition laws. IV. The parametrization of quintic rings*, Ann. of Math. (2) **167** (2008), no. 1, 53–94. MR 2373152
6. ———, *The density of discriminants of quintic rings and fields*, Ann. of Math. (2) **172** (2010), no. 3, 1559–1591. MR 2745272
7. Manjul Bhargava, Arul Shankar, and Jacob Tsimerman, *On the Davenport-Heilbronn theorems and second order terms*, Invent. Math. **193** (2013), no. 2, 439–499. MR 3090184
8. Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR 1228206
9. H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420. MR 491593
10. F. Johansson, *Arb: efficient arbitrary-precision midpoint-radius interval arithmetic*, IEEE Transactions on Computers **66** (2017), 1281–1292.
11. Friedrich Levi, *Kubische Zahlkörper und binäre kubische Formenklassen*, Berichte über die Verhandlungen der Königlich Sächsischen Gesellschaft der Wissenschaften zu Leipzig, Mathematisch-Physische Klasse **66** (1914), 26–37.
12. The LMFDB Collaboration, *The L-functions and modular forms database*, `https://www.lmfdb.org`, 2024, [Online; accessed 18 January 2024].
13. Gunter Malle, *Cohen-Lenstra heuristic and roots of unity*, J. Number Theory **128** (2008), no. 10, 2823–2835. MR 2441080
14. The FLINT team, *FLINT: Fast Library for Number Theory*, 2024, Version 3.1.3, `https://flintlib.org`.

Universität Paderborn, Fakultät EIM, Institut für Mathematik, Warburger Str. 100, 33098 Paderborn, Germany

Email address: `fabian.gundlach@uni-paderborn.de`