ERRATA: *ALGORITHMIC ENUMERATION OF IDEAL CLASSES FOR QUATERNION ORDERS*

MARKUS KIRSCHMER AND JOHN VOIGHT

This note gives errata and addenda for the article *Algorithmic enumeration of ideal classes for quaternion orders* [1]. (See also the corrigendum [2].)

Errata

(1) There was a programming error in enumerating Eichler orders of class number two due to a problem with enumerating composite ideals in the base number field. The revised list has 172 equivalence classes of Eichler orders of class number two, according to the revised Table 8.3 below.

This bug did not affect the list of Eichler orders of class number one.

The lists of Eichler orders of class number one and two have been independently verified by Kirschmer–Lorch [3].

TABLE 8.3: Definite Eichler orders $\mathcal{O}$ with class number $h(\mathcal{O}) = 2$.

n	d_F	D	N	n	d_F	D	N	n	d_F	D	N	n	d_F	D	N
1	1	2	7	2	8	1	9	3	49	7	8	4	725	1	16
		2	15			1	17			7	13			1	25
		2	17			1	28			7	27			1	31
		2	23			1	31			8	7			1	41
		3	5			1	32			13	7			1	49
		3	7			1	47			13	13			1	79
		3	8			14	7			27	1			1	89
		3	11			34	1			41	1		1125	1	1
		5	3			62	1			71	1			1	5
		5	4			63	1			97	1			1	9
		7	2		12	1	1			113	1			1	29
		7	3			1	2			127	1			1	59
		11	1			1	3		81	3	17			80	1
		17	1			1	4			3	19		1600	1	1
		19	1			1	6			8	1		1957	1	7
		30	1			1	8			17	1			1	23
		42	1			1	11			19	3			21	1
		70	1			1	12			73	1		2000	20	1
		78	1			1	23		148	2	17		2048	1	1
2	5	1	31			6	1			2	23		2225	1	1
		1	36			6	11			5	4		2304	18	1
		1	41			26	1			17	1		2525	1	1
		1	45			39	1			25	1		2624	1	1
		1	49			50	1		169	5	5		2777	1	8
		1	55		13	1	4			8	1			1	11
		1	64			1	9		229	2	1		3981	1	1
		1	71			1	17			4	1			15	1
		1	79			1	23			7	1		4205	1	1
		1	80			9	1		257	3	1		4352	14	1
		1	81			12	3			5	1		4752	12	1
		1	89			39	1			7	1		6809	1	1
		1	95		17	1	4		316	2	1	5	14641	11	1
		1	99			1	8			2	4			23	1
		20	9			4	1		321	3	1		24217	17	1
		36	1			18	1			3	3		36497	3	1
		45	1			26	1			7	1		38569	7	1
		55	1		21	1	1		361	7	1			13	1
		95	1			1	3		404	2	1	6	300125	1	1
		99	1			1	5		469	4	1		371293	1	1
		124	1			12	1		568	2	1		434581	1	1
		155	1			20	1						485125	1	1
		164	1		24	6	1						592661	1	1
						15	1								
					28	6	1								
					29	1	1								
					33	6	1								
					37	1	1								
					41	1	1								

Addenda

One can solve Problem 2.4 (IsPrincipal) in the definite case without rescaling the ideals as explained in Section 6 of [1]. In particular, Algorithm 6.3 can be slightly simplified. The idea is based on the fact that given any totally positive element $\alpha \in \mathbb{F}^*$ the rational quadratic form

$$\begin{aligned} \varphi_\alpha \colon B &\to \mathbb{Q} \\ x &\mapsto \operatorname{Tr}_{F/\mathbb{Q}}(\alpha \operatorname{nrd} x) \end{aligned}$$

is positive definite. We restate the improved version of the algorithm and its proof.

Algorithm 6.3. *Let $I \subset \mathcal{O}$ be a right fractional $\mathcal{O}$-ideal and let $c \in \mathbb{Z}_F$ such that $\operatorname{nrd} I = c\mathbb{Z}_F$. This algorithm solves Problem* 2.4 (IsPrincipal).

(1) Determine if there exists a unit $u \in \mathbb{Z}_F^*$ such that $c_v u_v > 0$ for all real places v; if not, then return false.
(2) For each totally positive unit $z \in \mathbb{Z}_{F,+}^*/\mathbb{Z}_F^{*2}$:
   a. Let ξ be a shortest vector of the $\mathbb{Z}$-lattice I with respect to the rational quadratic form $\varphi_{(ucz)^{-1}}$.
   b. If $\varphi_{(ucz)^{-1}}(\xi) = [F : \mathbb{Q}]$ then return true and the element ξ.
(3) Return false.

Remark 6.4. Note that if $F = \mathbb{Q}$ then in Step 2 we have $z = u = 1$. Hence the algorithm simply amounts to find a shortest vector in the $\mathbb{Z}$-lattice I (with respect to the reduced norm form).

Proof of correctness. If I is principal, then $\operatorname{nrd} I$ is generated by a totally positive element uc where $u \in \mathbb{Z}_F^*$. Then Lemma 4.8 implies that $\xi \in I$ generates I if and only if $\operatorname{nrd} \xi = ucz$ for some $z \in \mathbb{Z}_{F,+}^*$. To find such an element ξ, we only need to search for elements of norm ucz where z runs through some arbitrary transversal of $\mathbb{Z}_{F,+}^*/\mathbb{Z}_F^{*2}$.

Let $n = [F : \mathbb{Q}]$, $z \in \mathbb{Z}_{F,+}^*$, and $\xi \in I$. Then $\operatorname{nrd} \xi \in \operatorname{nrd} I = (ucz)\mathbb{Z}_F$, so $\alpha = (\operatorname{nrd} y)/(ucz) \in \mathbb{Z}_F$. The arithmetic-geometric mean inequality implies

$$n \leq n(\operatorname{N} \alpha)^{1/n} \leq \operatorname{Tr} \alpha = \varphi_{(ucz)^{-1}}(\xi).$$

Moreover, equality holds if and only if $1 = \operatorname{N} \alpha$ and α_v is independent of the real place v of F, so equality holds if and only if $\alpha = 1$. Hence $\operatorname{nrd}(\xi) = ucz$ if and only if $\xi \in I$ satisfies $\varphi_{(ucz)^{-1}}(y) = n$ and is a shortest vector. □

References

[1] Markus Kirschmer and John Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput. **39** (2010), no. 5, 1714–1747.

[2] Markus Kirschmer and John Voight, *Corrigendum: Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput. **41** (2012), no. 3, 714.

[3] Markus Kirschmer and David Lorch, *Ternary quadratic forms over number fields with small class number*, submitted.

Lehrstuhl D für Mathematik, RWTH Aachen University, Templergraben 64, 52062 Aachen, Germany

E-mail address: Markus.Kirschmer@math.rwth-aachen.de

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA

E-mail address: jvoight@gmail.com