Computations of Cyclotomic Lattices

Christian Batut, Heinz-Georg Quebbemann and Rudolf Scharlau

CONTENTS

1. Introduction
2. Unimodular Cyclotomic Lattices over Imaginary-Quadratic Fields
3. Computational Results
Acknowledgements
References

We study even modular lattices having level l and dimension $2(p-1)$, for p prime, and arising from the ideal class group of the p-th cyclotomic extension of $\mathbb{Q}(\sqrt{-l})$. After giving the basic theory we concentrate on Galois-invariant ideals, obtain computational results on minimal vectors and isometries, and identify several old or new extremal lattices.

1. INTRODUCTION

In this paper—a sequel to [Bachoc and Batut 1992; Quebbemann 1992; Quebbemann 1995]—we deal mainly with a family of lattices $B_{n,l}^{(m)}$ in euclidean spaces, related to Craig's lattices $A_{p-1}^{(m)}$. Each lattice $B_{n,l}^{(m)}$ has dimension $n = 2(p-1)$, contains the tensor product of $A_{p-1}^{(m)}$ with the ring of integers in $\mathbb{Q}(\sqrt{-l})$, and is hermitian-unimodular over this ring (therefore similar to its $\mathbb{Z}$-dual, with determinant l^{p-1}). Like $A_{p-1}^{(m)}$, each lattice $B_{2(p-1),l}^{(m)}$ admits a simple description as a cyclotomic ideal displaying the affine-linear group $\mathbb{F}_p^+ \rtimes \mathbb{F}_p^*$ as a group of automorphisms. Our family, however, includes more prominent individuals: there are $E_8 = B_{8,1}^{(1)}$, $K_{12} = B_{12,3}^{(1)}$, $\Lambda_{24} = B_{24,1}^{(2)}$, but also Plesken and Nebe's

$$[2.M_{12}.2]_{20} = B_{20,2}^{(2)} \quad \text{and} \quad [2.M_{22}.2]_{20} = B_{20,7}^{(2)}$$

(the latter appears to give the highest "isodual Hermite number" known for $n = 20$, and it is one of three "extremal" lattices of minimum 8 we know). On the other hand, our lattices are harder to analyze than Craig's: we cannot give a general lower bound on the minimum, nor theoretically decide eutaxy when $l > 3$. Information on these and related questions is obtained for $p \leq 29$ by machine computations using PARI [Batut et al. 1993].

Key words and phrases: lattice, integral quadratic form, Craig lattice, hermitian lattice, modular lattice, extremal lattice, isodual Hermite number, cyclotomic ideal.

1991 Mathematics Subject Classification: 11E12; 11H55, 11R18, 11-04.

2. UNIMODULAR CYCLOTOMIC LATTICES OVER IMAGINARY-QUADRATIC FIELDS

Let l be a square-free positive integer. Set $K = \mathbb{Q}(\sqrt{-l})$, and let $\mathcal{O}_K$ be the ring of integers in K. Given a positive definite hermitian space (V, h) of dimension k over K, we also consider it as an inner product space of dimension $n = 2k$ over $\mathbb{Q}$ for

$$x \cdot y = c \operatorname{Tr}_{K/\mathbb{Q}} h(x, y)$$

with

$$c = \begin{cases} 1 & \text{if } l \equiv 3 \bmod 4, \\ \frac{1}{2} & \text{otherwise.} \end{cases} \tag{2.1}$$

Then, if Λ is an $\mathcal{O}_K$-lattice on V, its hermitian dual lattice Λ_h^* is $\sqrt{-l}\,\Lambda^*$, where Λ^* is the euclidean dual. We shall deal with lattices satisfying

$$\Lambda = \Lambda_h^* \quad \text{and} \quad x \cdot x \in 2\mathbb{Z} \quad \text{for all} \quad x \in \Lambda. \tag{2.2}$$

(Of course, for $l \equiv 3 \bmod 4$ the first condition here implies the second.) As a euclidean lattice such a Λ is even and isometric to $\sqrt{l}\,\Lambda^*$, therefore of determinant l^k.

Let p be an odd prime not dividing l, and ζ a nontrivial p-th root of unity over K. We put $F = K(\zeta)$ and remark that $[F : K] = p - 1$. Consequently, if p divides the order of the isometry group $\operatorname{Aut}_h \Lambda$ for a lattice Λ as above, part of V must be a nonzero F-vector space, and therefore $p - 1$ is at most equal to k. We shall deal with the case $k = p - 1$, and then can assume [Feit 1974, § 9] that

$$V = F, \quad h(x, y) = \operatorname{Tr}_{F/K}(\delta x \bar{y}), \quad \Lambda = \mathcal{I}, \tag{2.3}$$

where the bar indicates complex conjugation, δ is a totally positive element in $F^+ = F \cap \mathbb{R}$, and $\mathcal{I}$ is a fractional ideal of F. Note that $\Lambda_h^* = (\delta \bar{\mathcal{I}} \mathcal{D}_{F/K})^{-1}$, where $\mathcal{D}_{F/K} = (1 - \zeta)^{p-2}$ is the different. To satisfy (2.2) we therefore require that

$$p \delta \mathcal{I} \bar{\mathcal{I}} = (1 - \zeta). \tag{2.4}$$

Actually, (2.4) is equivalent to (2.2) because the absence of dyadic ramification in F/F^+ guarantees Λ is even [Bayer-Fluckiger and Martinet 1994, § 3].

Proposition 2.1. *Condition* (2.4) *can be satisfied* (*with some $\delta \in F^+$ totally positive*) *if and only if*

$$\left(\frac{-l}{p}\right) = 1.$$

Proof. The extension F/F^+ is unramified at all finite primes, so class field theory tells us that the left-hand side of (2.4) is in the kernel of the Artin map. In other words, for (2.4) to hold $(1 - \zeta)$ must be decomposed in F, and so p decomposed in K. Conversely, if this is satisfied, we can write

$$(1 - \zeta) = \mathcal{P} \bar{\mathcal{P}}, \tag{2.5}$$

where $\mathcal{P}$ is a prime ideal in $\mathcal{O}_F$, and then (2.4) holds with $\delta = 1/p$ and $\mathcal{I} = \mathcal{P}$. □

From now on we assume $\left(\frac{-l}{p}\right) = 1$, and fix $\mathcal{P}$ as in (2.5). In order to satisfy (2.4) with $\delta = 1/p$, we may also put $\mathcal{I} = \mathcal{J} \bar{\mathcal{J}}^{-1} \mathcal{P}$, where $\mathcal{J}$ is any nonzero fractional ideal of F. This will turn out to be already the most general case. Namely, let $\operatorname{cl}(\mathcal{J})$ denote the ideal class of $\mathcal{J}$, and $\operatorname{Cl}(F)$ the class group; put $G = \operatorname{Gal}(F/K)$. Denote the K-isometry class of the lattice Λ by $[\Lambda]$.

Theorem 2.2. *If* (V, h, Λ) *is given by* (2.3) *and* (2.4) *is satisfied*, *then* $\delta = 1/p$ *up to isometry. Furthermore*, *with this choice of* δ, *the mapping*

$$\operatorname{cl}(\mathcal{J}) \mapsto [\Lambda], \quad \textit{where } \Lambda = \mathcal{J} \bar{\mathcal{J}}^{-1} \mathcal{P},$$

gives a bijection between $G \setminus (\operatorname{Cl}(F)/\operatorname{im} \operatorname{Cl}(F^+))$ *and the set of all K-isometry classes of lattices Λ as before.*

Proof. Exactly the same as for the case $l = 1$ treated in [Quebbemann 1992, Theorem 3]. □

To produce an explicit family of lattices we shall make use of G-invariant ideal classes.

Proposition 2.3. *The group* $\operatorname{Cl}(F)^G$ *is generated by* $\operatorname{im} \operatorname{Cl}(K)$ *and* $\operatorname{cl}(\mathcal{P})$. *Its order is* $r = h_K(p-1)/u_K$, *where* $h_K = \# \operatorname{Cl}(K)$ *and* $u_K = \# \mathcal{O}_K^*$.

Proof. Let σ be a generator of G. If $\operatorname{cl}(\mathcal{J})$ is G-invariant, then $\mathcal{J} = \alpha \mathcal{J}^\sigma$ for some $\alpha \in F$ satisfying $N_{F/K}(\alpha) \in \mathcal{O}_K^*$. The local norm at the ramified prime $\mathcal{P}$ is the $(p-1)$-st power (i.e., trivial) on $\mathbb{F}_p$. This shows that $\mathrm{Norm}_{F/K}(\alpha) = 1$. Then $\alpha = \beta/\beta^\sigma$ for some $\beta \in F^*$ by Hilbert's Theorem 90, and J may be changed to become a G-invariant ideal. Since only $\mathcal{P}$ and $\bar{\mathcal{P}}$ are ramified in F/K, then $\mathcal{J}$ is equivalent to a power of $\mathcal{P}$ times an ideal coming from K. The value of r is given by the formula of Takagi and Chevalley in [Lang 1990, Ch. 13, § 4]. □

Definition 2.4. For $m = 1, \dots, r$, let $B_{n,l}^{(m)}$ denote the unimodular $\mathcal{O}_K$-lattice given as above by (the class of) $\mathcal{J} = \mathcal{P}^{m-1}$. Explicitly,

$$B_{n,l}^{(m)} = \mathcal{P}^m \bar{\mathcal{P}}^{1-m}, \quad h(x,y) = \frac{1}{p}\,\mathrm{Tr}_{F/K}\, x\bar{y}.$$

The relation $\mathrm{cl}(\mathcal{P})^r = 1$ implies that $B_{n,l}^{(r+1-m)}$ must be isometric to the complex conjugate of $B_{n,l}^{(m)}$. Therefore, being interested in $B_{n,l}^{(m)}$ as a euclidean lattice, we can restrict ourselves to the range

$$1 \le m \le \lfloor \tfrac{1}{2}(r+1) \rfloor.$$

We note that $\mathcal{P}^m \bar{\mathcal{P}}^{1-m}$ contains the ideal $(1-\zeta)^m$, and the latter is just the lattice $A_{p-1}^{(m)}$ of Craig [Conway and Sloane 1988, Ch. 8], tensored with $\mathcal{O}_K$.

Theorem 2.5. *Considered as a euclidean lattice in dimension $n = 2(p-1)$, the lattice $B_{n,l}^{(m)}$ is even, of determinant l^{p-1}, and isometric to $\sqrt{l}\,(B_{n,l}^{(m)})^*$. Moreover we have $\min B_{n,l}^{(m)} \le 2c \min A_{p-1}^{(m)}$, where c is as in* (2.1). *If $l \in \{1, 2, 3, 5, 7, 11, 23\}$ (that is, if $24/(1+l)$ is integral), we also have*

$$\min B_{n,l}^{(m)} \le 2\,\lfloor n(1+l)/48 \rfloor + 2. \tag{2.6}$$

Proof. Only the last statement is not yet obvious. It uses Fricke modular forms and is a general bound based on [Quebbemann 1995, Theorem 7]. For $l = 1$ and 3 see [Conway and Sloane 1988, Ch. 7]. □

One has $\min A_{p-1}^{(m)} \ge 2m$, with conjectural equality when $m \le \frac{1}{4}(p+1)$ [Bachoc and Batut 1992, § 3]. However, only in some special cases does $B_{n,l}^{(m)}$ attain the minimum value of $4mc$ and the bound in (2.6). The computations reported on in the next section will exemplify this. We are particularly interested in examples that attain the bound (2.6). Such lattices are called *extremal* (after Sloane), and their theta-series are uniquely determined by the theory of modular forms [Quebbemann 1995].

3. COMPUTATIONAL RESULTS

Proposition 3.1. *Let $a \in \mathbb{Z}$ satisfy $a^2 \equiv -l \bmod p$, and put $\pi = a - \sqrt{-l}$. Then $\mathcal{P} = (1-\zeta,\, \pi)$ satisfies* (2.5), *and*

$$\mathcal{P}^m \bar{\mathcal{P}}^{1-m} = ((1-\zeta)^m,\, (1-\zeta)^{1-m}\pi) \tag{3.1}$$

for $1 \le m < \frac{1}{2}p$.

Proof. Clearly $\mathcal{P}\bar{\mathcal{P}} = (1-\zeta)$. Then

$$\mathcal{P}^m \bar{\mathcal{P}}^{1-m} = (1-\zeta)^{1-m} \mathcal{P}^{2m-1},$$

and it suffices to consider $\mathcal{P}^i$ for $1 \le i \le p-1$. Now $(\pi, \bar{\pi}) = (1)$, and multiplying by π we obtain $(\pi) = (\pi^2, \pi\bar{\pi}) \subset (\pi^2, (1-\zeta)^i)$. Then, by induction,

$$\mathcal{P}^i = ((1-\zeta)^{i-1}, \pi)(1-\zeta, \pi) = ((1-\zeta)^i, \pi). \quad \square$$

Using (3.1) we obtain $2n$ generators of $B_{n,l}^{(m)}$ over $\mathbb{Z}$ (in an obvious integral basis of $F/\mathbb{Q}$). After Hermite reduction of the $(n, 2n)$ coefficient matrix, we arrive at a Gram matrix for this lattice. In the following examples the level will be restricted to the values $l = 1, 2, 3, 5, 7$. We always assume $1 \le m \le \lfloor \frac{1}{2}(r+1) \rfloor$, with r as in Proposition 2.3.

Dimension 12 ($p = 7$). Here $l = 3$ or 5. For $l = 3$ we have $r = 1$ and obtain $B_{12,3}^{(1)} = K_{12}$ as in [Bayer-Fluckiger and Martinet 1994, § 4]. For $l = 5$ we have $r = 6$ and $m \le 3$. Actually $B_{12,5}^{(2)}$ and $B_{12,5}^{(3)}$ are extremal, with minimum 4, and nonisometric (over $\mathbb{Z}$), with automorphism groups of order $2^5 3^2 7$ and $2^5 3^2 5\, 7$, respectively. It was shown in [Scharlau and Hemkemeier 1994] that there are exactly two further lattices of minimum 4 in this genus. They are modular and have automorphism groups of order $2^6 3^4$ and $2^8 3^4 5$, respectively, neither of which is divisible by 7. This result has been obtained independently by G. Nebe at Aachen.

Dimension 20 ($p = 11$). Here $l = 2$ and 7. In both cases $r = 5$, so $m \leq 3$. For $l = 2$ again two nonisometric extremal lattices arise, of which $B^{(2)}_{20,2} = [2.M_{12}.2]_{20}$ has first occurred in [Plesken and Nebe 1995]; also $B^{(3)}_{20,2}$ occurs there, but was known before. (In this case the identifications via Gram matrices were done by Nebe.) For $l = 7$ we obtain one extremal lattice (minimum 8), namely for $m = 2$; $B^{(3)}_{20,7}$ has minimum 6. We have identified $B^{(2)}_{20,7}$ with $[2.M_{22}.2]_{20}$ of [Plesken and Nebe 1995], which was commented on in Section 1.

Dimension 24 ($p = 13$), $l = 1$ and 3. For $l = 1$ we have $r = 3$, so $m \leq 2$, and $B^{(2)}_{24,1} = \Lambda_{24}$ as in [Quebbemann 1992]. For $l = 3$, the value $r = 2$ excludes extremality.

Dimension 32 ($p = 17$), $l = 1$ and 2. In the first case we have $r = 4$, so $m \leq 2$. Actually $B^{(2)}_{32,1}$ is extremal and not isometric to the ubiquitous BW_{32}. The latter, however, arises from a noninvariant ideal class [Quebbemann 1992]. In the case $l = 2$ we have $r = 8, m \leq 4$. No extremal lattice is obtained here (for $m = 2, 3, 4$ the minimum is 4 and the number of minimal vectors is $2^3 7 \cdot 17$, $2^3 3^2 17$, and $2^3 13 \cdot 17$, respectively).

Dimension 36 ($p = 19$), $l = 2$ and 3. For $l = 2$ (with $r = 9$ and $m \leq 5$) we obtain extremal lattices (minimum 6) when $m = 3, 4, 5$. For $l = 3$ (with $r = 3$ and $m \leq 2$) an extremal lattice would have minimum 8 and improve the sphere packing record. However, $B^{(2)}_{36,3}$ has only minimum 6. Now in this case $h_F = 9$ and $h_{F^+} = 1$, and we are very grateful to H. Cohen for computing $\mathrm{Cl}(F)$ for us. The group turned out to be cyclic and generated by $\mathrm{cl}(\mathcal{Q})$, with $\mathcal{Q}$ a prime ideal over 37; but also $\Lambda = \mathcal{Q}\bar{\mathcal{Q}}^{-1}\mathcal{P}$ had minimum 6. (The six ideal classes of order 9 make up two G-orbits, and the two lattices are complex conjugate; so all lattices from Theorem 2.2 have been considered now.)

Dimension 44 ($p = 23$), $l = 5$ and 7. For $l = 5$ we have $r = 22$, so $m \leq 11$, and extremality would mean that the minimum were 12. However, computation gives the mysterious sequence of minima shown in Table 1. The last row τ^* in this table shows the number of minimal vectors, divided by $22 \cdot 23$. For $l = 7$ extremality is impossible already by the fact that in this case the extremal modular form contains a negative Fourier coefficient.

m	1	2	3	4	5	6	7	8	9	10	11
min	2	4	6	8	8	8	8	8	10	8	4
τ^*	1	5	9	11	2	15	3	5	114	8	1

TABLE 1. Minimum of $B^{(m)}_{44,5}$.

Dimension 56 ($p = 29$), $l = 1$, 5, and 7. For $l = 1$ we have $r = 7$ and $m \leq 4$. For $m = 2$ and 3 the lattices have minimum 4, and the number of minimal vectors is $42 \cdot 28 \cdot 29$ and $5 \cdot 28 \cdot 29$, respectively. The lattice $B^{(4)}_{56,1}$ turns out to be extremal. An extremal unimodular lattice in dimension 56 had been obtained previously by combining a construction of Ozeki with the existence of a ternary $[56, 28, 15]$-code [Ozeki 1989, Example 5]. We did not try to identify $B^{(4)}_{56,1}$ with some lattice coming from this code construction. For $l = 5$, the largest minimum of a lattice $B^{(m)}_{56,5}$ is 10. So these lattices are far from being extremal (min = 16). For $l = 7$, the extremal modular form has a negative coefficient.

Finally, Table 2 summarizes all extremal $B^{(m)}_{n,l}$ for $n \leq 56$. Part of the data also follows from theoretical reasons. For example, the number τ of minimal vectors is predicted by the extremal modular form, and for $l = 1$ and 3 all $B^{(m)}_{n,l}$ (no matter if extremal or not) are eutactic because then $\mathcal{O}^*_K \times (\mathbb{F}^+_p \rtimes \mathbb{F}^*_p)$, and therefore $\mathrm{Aut}\, B^{(m)}_{n,l}$, acts $\mathbb{R}$-irreducibly.

One might hope for the existence of extremal even unimodular lattices in dimensions $n = 72$ and $n = 80$. Actually $B^{(4)}_{80,1}$ and $B^{(5)}_{80,1}$ remain candidates after LLL reduction, but we are unable to verify that the minimum really is 8. All $B^{(m)}_{72,1}$ have minimum at most 6.

ACKNOWLEDGEMENTS

Part of this work was done during stays of the second author at the University of Bordeaux, to which he expresses his gratitude for its hospitality.

n	l	m	min	τ	P	E
4	2	1	2	24	yes	yes
4	5	1	2	6	no	no
4	11	1	4	12	no	no
4	23	2	6	12	no	no
8	1	1	2	240	yes	yes
12	3	1	4	756	yes	yes
12	5	2	4	126	no	no
12	5	3	4	126	no	no
20	2	2	4	3960	yes	yes
20	2	3	4	3960	yes	yes
20	7	2	8	6160	yes	yes
24	1	2	4	196560	yes	yes
32	1	2	4	146880	yes	yes
36	2	3	6	164160	yes	yes
36	2	4	6	164160	yes	yes
36	2	5	6	164160	yes	yes
56	1	4	6	15590400	yes	yes

TABLE 2. Extremal $B_{n,l}^{(m)}$ for $n \leq 56$. The last two columns indicate whether the lattice is perfect and eutactic.

REFERENCES

[Batut et al. 1993] C. Batut, D. Bernardi, H. Cohen and M. Olivier, *User's Guide to Pari-GP*. This manual is part of the program distribution, available by anonymous ftp from the host megrez.ceremab.u-bordeaux.fr.

[Bachoc and Batut 1992] C. Bachoc et C. Batut, "Étude algorithmique de réseaux construits avec la forme trace", *Exper. Math.* **1** (1992), 184–190.

[Bayer-Fluckiger and Martinet 1994] E. Bayer-Fluckiger and J. Martinet, "Formes quadratiques liées aux algèbres semi-simples", *J. reine angew. Math.* **451** (1994), 51–69.

[Conway and Sloane 1988] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer, New York, 1988.

[Feit 1974] W. Feit, "On integral representations of finite groups", *Proc. London Math. Soc.* **29** (1974), 633–683.

[Lang 1990] S. Lang, *Cyclotomic Fields* I *and* II, Springer, New York, 1990.

[Ozeki 1989] M. Ozeki, "Ternary code construction of even unimodular lattices", pp. 772–784 in *Théorie des nombres*, Univ. Laval 1987 (edited by J.-M. de Koninck and C. Levesque), de Gruyter, Berlin, 1989.

[Plesken and Nebe 1995] W. Plesken and G. Nebe, "Finite rational matrix groups", to appear in *Memoirs Amer. Math. Soc.* **116** (1995), 1–144.

[Quebbemann 1992] H.-G. Quebbemann, "Unimodular lattices with isometries of large prime order II", *Math. Nachr.* **156** (1992), 219–224.

[Quebbemann 1995] H.-G. Quebbemann, "Modular lattices in euclidean spaces", to appear in *J. Number Theory* **54** (1995)

[Scharlau and Hemkemeier 1994] R. Scharlau and B. Hemkemeier, "Classification of integral lattices with large class number", preprint 94-102, Universität Bielefeld, Germany.

Christian Batut, Laboratoire A2X, U.M.R. 9936 du C.N.R.S., Université Bordeaux I, 351, cours de la Libération, 33405 Talence Cedex, France (batut@ceremab.u-bordeaux.fr)

Heinz-Georg Quebbemann, FB 6 Mathematik, Universität Oldenburg, D-26111 Oldenburg, Germany (quebbemann@math.uni-oldenburg.de)

Rudolf Scharlau, FB Mathematik, Universität Dortmund, D-44221 Dortmund, Germany (Rudolf.Scharlau@mathematik.uni-dortmund.de)

Received March 3, 1995; accepted June 16, 1995