Contemporary Mathematics

Construction and investigation of lattices with matrix groups

Gabriele Nebe

1. Finite matrix groups and lattices

Let L be a lattice in a positive definite symmetric rational bilinear space $(\mathbb{Q}^d, F)$ of dimension d. Then the orthogonal group of L is

$$O(L,F) := \{g \in GL_d(\mathbb{Q}) \mid Lg \subseteq L,\ gFg^{tr} = F\}$$

a finite subgroup of $GL_d(\mathbb{Q})$. Writing $O(L,F)$ with respect to some $\mathbb{Z}$-basis of L one obtains a finite subgroup of $GL_d(\mathbb{Z})$. So orthogonal groups of lattices are distinguished finite integral matrix groups the so called *Bravais groups*.

On the other hand, if one starts with a finite subgroup G of $GL_d(\mathbb{Q})$, an easy summation argument shows that one always finds a G-invariant lattice, i.e. the set

$$\mathcal{Z}(G) := \{L \leq \mathbb{Q}^d \mid L \text{ is a full } \mathbb{Z}\text{-lattice in } \mathbb{Q}^d \text{ and } Lg = L \text{ for all } g \in G\}$$

of G-invariant lattices is not empty. Also the form $F_0 := \sum_{g\in G} gFg^{tr}$ is a G-invariant positive definite bilinear form on V, i.e. $G \leq O(V, F_0)$. This shows that the vector space

$$\mathcal{F}(G) := \{F \in \mathbb{Q}^{d\times d} \mid F = F^{tr}, gFg^{tr} = F \text{ for all } g \in G\}$$

contains a positive definite bilinear form. This means that every finite matrix group embeds into a Bravais group.

One may use the invariant positive definite lattices to say something about the Bravais groups and, more important for this paper, one may use the finite matrix groups to construct nice lattices and to deduce properties of the invariant lattices. The rational normalizer $N_{\mathbb{Q}} := N_{GL_d(\mathbb{Q})}(G)$ of a finite subgroup G of $GL_d(\mathbb{Q})$ plays an important role in the investigation of G-invariant lattices, since $N_{\mathbb{Q}}$ acts on $\mathcal{Z}(G)$ and on $\mathcal{F}(G)$. In particular if G is *uniform*, which means that $\mathcal{F}(G) = \mathbb{Q}F$ has dimension 1, the elements in $N_{\mathbb{Q}}$ induce similarities of F. Such similarities can be used to construct overlattices of tensor products as defined in section 2.

Fixing an invariant lattice L of a non uniform group G one may regard the metric properties of L with respect to all G-invariant positive definite quadratic forms. In section 3, examples of 2- and 3-dimensional spaces of invariant quadratic forms are investigated.

The last section gives a method to compute the minimum of certain lattices using their automorphism group. With this method one proves the extremality

1991 *Mathematics Subject Classification.* 11H50, 11H56.

(in the sense of [**Que 95**]) of a certain even unimodular and an even 3-modular 64-dimensional lattice.

2. A tensor product that preserves modularity.

This section presents a quite important construction in the classification of maximal finite subgroups of $GL_d(\mathbb{Q})$ (cf. [**PlN 95**, Proposition (II.4)]) reformulated in the language of lattices.

Let L_1 resp. L_2 be a lattice in the rational bilinear space $(\mathbb{Q}^{d_1}, F_1)$ resp. $(\mathbb{Q}^{d_2}, F_2)$. Let $r \in \mathbb{N}$ be a square free natural number and α_i be a similarity of F_i of rate r, i.e.

$$\alpha_i \in GL_{d_i}(\mathbb{Q}) \text{ with } \alpha_i F_i \alpha_i^{tr} = rF_i (i = 1, 2).$$

Assume that $M_i := L_i\alpha_i \subseteq L_i$ and $L_i\alpha_i^2 = rL_i$ $(i = 1, 2)$. The orthogonal mapping $\frac{1}{r}\alpha_1 \otimes \alpha_2$ interchanges the two lattices $L_1 \otimes L_2$ and $\frac{1}{r}M_1 \otimes M_2$ and therefore induces an isometry between them.

DEFINITION 2.1. The lattice

$$L_1 \overset{(r)}{\otimes} L_2 := L_1 \otimes L_2 + \frac{1}{r} M_1 \otimes M_2$$

is called the *r-normalized tensor product* (with respect to α_1 and α_2) of L_1 and L_2.

REMARK 2.2. Since $\alpha_i \in GL_{d_i}(\mathbb{Q})$ is a similarity of rate r, its determinant is $r^{\frac{d_i}{2}}$. Hence d_1 and d_2 are even, if $r > 1$.
$L_1 \overset{(r)}{\otimes} L_2$ is invariant under $\frac{1}{r}\alpha_1 \otimes \alpha_2$ and contains $L_1 \otimes L_2$ of index $r^{\frac{d_1 d_2}{4}}$.

PROOF. The first statement is clear. $\frac{1}{r}\alpha_1 \otimes \alpha_2$ interchanges the two lattices $L_1 \otimes L_2$ and $\frac{1}{r}M_1 \otimes M_2$ and therefore preserves the lattice $L_1 \overset{(r)}{\otimes} L_2$ generated by them. Let $B_i := A_i \cup A_i'$ be a $\mathbb{Z}$-basis of L_i such that $rA_i \cup A_i'$ is a $\mathbb{Z}$-basis of M_i $(i = 1, 2)$. Then $|A_i'| = \frac{d_i}{2}$ and $\{\frac{1}{r}b_1 \otimes b_2 \mid b_1 \in A_1', b_2 \in A_2'\}$ is a basis of the free $\mathbb{Z}/r\mathbb{Z}$-module $L_1 \overset{(r)}{\otimes} L_2 / L_1 \otimes L_2$. □

A lattice (L, F) is called *r-modular*, if there is a similarity $\alpha \in GL_d(\mathbb{Q})$ with $\alpha F \alpha^{tr} = rF$ mapping the *dual lattice* $L^{\#} := \{v \in \mathbb{Q}^d \mid lFv^{tr} \in \mathbb{Z} \text{ for all } l \in L\}$ onto L (cf. [**Que 95**]). Such a similarity is also called a *modularity* of L. The determinant $det(L, F)$ of an integral lattice is $det(L, F) = |L^{\#}/L|$.

THEOREM 2.3. *Let L_1 and L_2 be r-modular lattices. Let $\alpha_i : L_i^{\#} \to L_i$ $(i = 1, 2)$ be corresponding modularities. Then $L_1 \overset{(r)}{\otimes} L_2$ is r-modular and $\alpha_1 \otimes 1 : (L_1 \overset{(r)}{\otimes} L_2)^{\#} \to L_1 \overset{(r)}{\otimes} L_2$ is a modularity.*

PROOF. By Remark 2.2, the determinant of $L_1 \overset{(r)}{\otimes} L_2$ is

$$det(L_1 \overset{(r)}{\otimes} L_2, F_1 \otimes F_2) = r^{d_1 d_2/2 + d_1 d_2/2 - d_1 d_2/2} = r^{d_1 d_2/2}.$$

Clearly $(\alpha_1 \otimes 1)(F_1 \otimes F_2)(\alpha_1 \otimes 1)^{tr} = rF_1 \otimes F_2$, so $\alpha_1 \otimes 1$ is a similarity of rate r of $F_1 \otimes F_2$. Therefore

$$(\alpha_1^{-1} \otimes 1)(L_1 \overset{(r)}{\otimes} L_2) = L_1^{\#} \otimes L_2 + L_1 \otimes L_2^{\#} \subseteq (L_1 \overset{(r)}{\otimes} L_2)^{\#}$$

implies $(\alpha_1^{-1} \otimes 1)(L_1 \overset{(r)}{\otimes} L_2) = (L_1 \overset{(r)}{\otimes} L_2)^{\#}$. □

Generalizing the notion of modular lattices, Quebbemann [**Que 97**] defined *strongly modular lattices.* For an integral lattice (L, F) let

$$\pi(L) := \{L \subseteq M \subseteq L^{\#} \mid gcd(|M : L|, |L^{\#} : M|) = 1\}.$$

Then L is called *strongly modular*, if L is similar to M for all $M \in \pi(L)$.

One even has that the construction $\overset{(r)}{\otimes}$ preserves strong modularity. Let $r \in \mathbb{N}$ be square free, L an r-modular lattice and p a divisor of r. Then $L^{\#(p)} := \frac{1}{p}L \cap L^{\#} \in \pi(L)$ is the p-partial dual of L. Note that, since r is square free, $L^{\#(p)} \cap L^{\#(r/p)} = L$ and $L^{\#(p)} + L^{\#(r/p)} = L^{\#}$. Moreover $\pi(L) = \{L^{\#(p)} \mid p|r\}$.

THEOREM 2.4. *Let L_1 and L_2 be r-modular lattices with corresponding similarities $\alpha_i : L_i^{\#} \to L_i$ $(i = 1, 2)$. Let $M := L_1 \overset{(r)}{\otimes} L_2$. Let p be a divisor of r such that $\beta : L_1^{\#(p)} \to L_1$ is a similarity (of rate p). Then $\beta \otimes 1 : M^{\#(p)} \to M$ is a similarity. In particular, if L_1 is strongly modular and L_2 is r-modular, then $L_1 \overset{(r)}{\otimes} L_2$ is strongly modular.*

PROOF. Clearly $\beta \otimes 1$ is a similarity of rate p. Let $\beta' := \alpha_1 \beta^{-1}$. Then $\beta' \otimes 1 \in End(L_1 \overset{(r)}{\otimes} L_2)$ maps M into itself. Therefore $(\beta^{-1} \otimes 1)(M) = (\alpha_1^{-1} \otimes 1)(\beta' \otimes 1)(M) \subseteq M^{\#}$. Since $\beta \otimes 1$ has determinant $p^{d_1 d_2/2}$ one gets $(\beta^{-1} \otimes 1)(M) = M^{\#(p)}$. □

EXAMPLE 2.5. For the hexagonal lattice A_2 one has

$$A_2 \overset{(3)}{\otimes} A_2 \cong A_2 \perp A_2.$$

From the root lattice D_4 one obtains the 16-dimensional Barnes-Wall lattice

$$D_4 \overset{(2)}{\otimes} D_4 \cong BW_{16}.$$

This construction can not only be applied to modular lattices. Let $L_1 := \mathbb{Z}^2$ be the 2-dimensional unimodular lattice. With respect to an orthonormal basis of L_1, a similarity α_1 of rate 2 has the matrix $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

For L_2 one chooses either the root lattice A_6 or the Craig lattice $A_6^{(2)}$ which may be constructed as a sublattice of index 7 of A_6. From the construction of A_6 as lattice in the ring of integers $\mathbb{Z}[\zeta_7]$ of the 7-th cyclotomic number field, one sees that A_6 and $A_6^{(2)}$ have a structure over $\mathbb{Z}[\alpha_2]$ where $\alpha_2 := \frac{1+\sqrt{-7}}{2}$ is an element of norm 2 in an imaginary quadratic number field. One easily sees that α_2 induces a similarity of rate 2.

The lattices $L_1 \overset{(2)}{\otimes} L_2$ have determinants $2^{-6}7^2$ resp. $2^{-6}7^6$ and minimum 2 resp. 4. Their automorphism groups are maximal finite subgroups of $GL_{12}(\mathbb{Q})$ (cf. [**PlN 95**, p. 36]).

If one chooses L_1 to be D_4 and $\alpha_1 : D_4^{\#} \to D_4$ then one obtains 24-dimensional lattices of determinant 7^4 resp. 7^{12} and minimum 4 resp. 8 (cf. [**Neb 95a**], [**Neb 96a**]).

2.1. Testing strong modularity. Let G be a finite subgroup of $GL_d(\mathbb{Q})$ and

$$N_{\mathbb{Q}} := N_{GL_d(\mathbb{Q})}(G) := \{x \in GL_d(\mathbb{Q}) \mid xgx^{-1} \in G \text{ for all } g \in G\}$$

be its rational normalizer. Then $N_{\mathbb{Q}}$ acts on the set $\mathcal{Z}(G)$ of G-invariant lattices and also on the vector space $\mathcal{F}(G)$ of G-invariant quadratic forms. Recall that G

is called *uniform*, if $dim_{\mathbb{Q}}(\mathcal{F}(G)) = 1$, i.e. there is a unique (up to scalar multiples) G-invariant quadratic form.

REMARK 2.6. Let G be a uniform subgroup of $GL_d(\mathbb{Q})$ and F a positive definite G-invariant form. Then $N_{GL_d(\mathbb{Q})}(G)$ consists of similarities in the sense that for all $n \in N_{GL_d(\mathbb{Q})}(G)$ there is an $a \in \mathbb{Q}_{>0}$ such that $nFn^{tr} = aF$.

On the other hand it is shown in [**Neb 97**, Proposition 3] that for $L' \in \pi(L)$ the similarity $\alpha : L' \to L$ normalizes the orthogonal group $O(L,F)$. Therefore one gets

THEOREM 2.7. *Let $G := O(L,F)$ be a uniform subgroup of $GL_d(\mathbb{Q})$. Then L is strongly modular, if and only if $N_{\mathbb{Q}} := N_{GL_d(\mathbb{Q})}(G)$ permutes the elements of $\pi(L)$ transitively.*

This observation can be used to prove strong modularity of many lattices invariant under uniform (maximal) finite rational matrix groups (cf. [**Neb 97**]).

Also the similarities needed to construct a normalized tensor product of two not necessarily modular lattices L_1 and L_2 with uniform automorphism groups $G_1 = O(L_1, F_1)$ and $G_2 = O(L_2, F_2)$ may be constructed using the rational normalizers of G_1 and G_2.

EXAMPLE 2.8. Let L_1 be again $\mathbb{Z}^2$ and α_1 be as above. Let L_2 be the 18-dimensional lattice invariant under the group $Sp_4(4) =: G$ of determinant 2^8 described in [**PlN 95**, p. 44]. There is $\alpha_2 \in N_{GL_{18}(\mathbb{Q})}(G)$, a similarity of rate 2, mapping the dual $L_2^{\#}$ to the even sublattice L_2^{ev} of L_2. Then $L_1 \overset{(2)}{\otimes} L_2$ has minimum 3 and is not integral but the dual of the even sublattice of three (odd) unimodular lattices. One of these three lattices has minimum 4, which answers an existence question of [**CoS 98**].

2.2. The semiring of isometry classes of r-modular lattices.

REMARK 2.9. (i) The r-normalized tensor product $L_1 \overset{(r)}{\otimes} L_2$ only depends on $L_1\alpha_1$ and $L_2\alpha_2$ and not on the particular choice of α_1 and α_2.
(ii) $L_1 \overset{(r)}{\otimes} L_2$ is isometric to $L_2 \overset{(r)}{\otimes} L_1$.

Assume for the rest of this section that the lattices L_i are r-modular.

REMARK 2.10. The r-normalized tensor product with respect to modularities $L_1 \overset{(r)}{\otimes} L_2 := L_1 \otimes L_2 + r L_1^{\#} \otimes L_2^{\#}$ is a canonical construction. One calculates the dual lattice as

$$(L_1 \overset{(r)}{\otimes} L_2)^{\#} = L_1^{\#} \otimes L_2 + L_1 \otimes L_2^{\#}.$$

One may view the r-normalized tensor product as a product on the set of isometry classes of r-modular lattices. The associativity follows from the next lemma.

LEMMA 2.11. *Let L_1, L_2, and L_3 be r-modular lattices. Then*

$$(L_1 \overset{(r)}{\otimes} L_2) \overset{(r)}{\otimes} L_3 = L_1 \overset{(r)}{\otimes} (L_2 \overset{(r)}{\otimes} L_3)$$

and

$$(L_1 \oplus L_2) \overset{(r)}{\otimes} L_3 = L_1 \overset{(r)}{\otimes} L_3 \oplus L_2 \overset{(r)}{\otimes} L_3$$

PROOF. $(L_1 \overset{(r)}{\otimes} L_2) \overset{(r)}{\otimes} L_3 = (L_1 \otimes L_2) \otimes L_3 + r(L_1^{\#} \otimes L_2^{\#}) \otimes L_3 + r(L_1^{\#} \otimes L_2) \otimes L_3^{\#} + r(L_1 \otimes L_2^{\#}) \otimes L_3^{\#}$. Since the tensor product is associative, the right hand side is symmetric in L_1, L_2, and L_3 and therefore equals $L_1 \overset{(r)}{\otimes} (L_2 \overset{(r)}{\otimes} L_3)$. The distributivity is clear. □

From this, one gets the following Theorem.

THEOREM 2.12. *Let $r \in \mathbb{N}$ be square free. With respect to orthogonal sums and r-normalized tensor products, the set of isometry classes of r-modular lattices forms a commutative semiring (without a unit element for $r > 1$).*

3. Changing the invariant quadratic form.

In this section we look at lattices from the view of geometry of numbers. For this purpose it is better to work with quadratic forms. So let $d \in \mathbb{N}$ be fixed and let $\mathcal{F}_{\mathbb{R}}$ be the space of all real symmetric $d \times d$-matrices. It contains an open cone $\mathcal{F}_{\mathbb{R}}^{>0}$ of positive definite symmetric matrices. For $F \in \mathcal{F}_{\mathbb{R}}^{>0}$ the minimum $min(F)$ is defined as the minimum of a $\mathbb{Z}$-lattice with Gram matrix F

$$min(F) := min\{vFv^{tr} \mid 0 \neq v \in \mathbb{Z}^d\}.$$

The set of *minimal vectors* of F is denoted by

$$Min(F) := \{v \in \mathbb{Z}^d \mid vFv^{tr} = min(F)\}.$$

The *Hermite function* $\gamma : \mathcal{F}_{\mathbb{R}}^{>0} \to \mathbb{R}$ is defined via $\gamma(F) := min(F)det(F)^{-1/n}$ for all $F \in \mathcal{F}_{\mathbb{R}}^{>0}$. The function γ is continuous and, considered as a function on similarity classes of lattices, it has only finitely many local maxima, called *extreme* forms. The extreme forms are similar to integral forms. Restricting γ to intersections of $\mathcal{F}_{\mathbb{R}}^{>0}$ with subspaces of $\mathcal{F}_{\mathbb{R}}$ such as

$$\mathcal{F}_{\mathbb{R}}^{>0} \cap \mathbb{R} \otimes_{\mathbb{Q}} \mathcal{F}(G) =: \mathcal{F}_{\mathbb{R}}^{>0}(G)$$

for a finite subgroup G of $GL_d(\mathbb{Q})$, one gets a notion of relative extremeness (cf. [**Mar 96**], [**Opg 96**]). As in the classical case, the relative extreme forms in $\mathcal{F}_{\mathbb{R}}^{>0}(G)$ are the ones that are eutactic and *G-perfect*, where $F \in \mathcal{F}_{\mathbb{R}}^{>0}(G)$ is called G-perfect, if the matrices $p_G(x) := \sum_{g\in G} g^{tr} x^{tr} x g$ with $x \in Min(F)$ span $\mathcal{F}(G^{tr})$. Not only the extreme lattices are interesting, but one finds in their neighborhood many good lattices of which the density approaches the density of the extreme lattice. In particular if the space of invariant quadratic forms of some finite matrix group G is of dimension 2 and can be identified with a real quadratic number field the investigation of a sequence of integral forms approaching a relatively extreme form, becomes easy.

There is a close connection between $\mathcal{F}(G)$ and the commuting algebra

$$C_{\mathbb{Q}^{d\times d}}(G) := \{x \in \mathbb{Q}^{d\times d} \mid xg = gx \text{ for all } g \in G\}.$$

Namely let $F_0 \in \mathcal{F}(G)$ be positive definite. Then, for $F \in \mathcal{F}(G)$, the matrix FF_0^{-1} commutes with all elements of G. F_0 induces an involution $^- : C_{\mathbb{Q}^{d\times d}}(G) \to C_{\mathbb{Q}^{d\times d}}(G)$ defined by $\bar{c} := F_0 c^{tr} F_0^{-1}$ for all $c \in C_{\mathbb{Q}^{d\times d}}(G)$. Note that this involution may depend on the choice of F_0, if the fixed space $Fix(^-) =: C^+$ is not contained in the center of $C_{\mathbb{Q}^{d\times d}}(G)$. On the other hand for $c \in C_{\mathbb{Q}^{d\times d}}(G)$ the matrix cF_0 clearly also fulfills $g(cF_0)g^{tr} = cF_0$ for all $g \in G$. The matrix cF_0 is symmetric, if $cF_0 = F_0 c^{tr}$, i.e. $\bar{c} = c$, hence the vectorspaces $\mathcal{F}(G)$ and C^+ can be identified.

In the situations considered in this section, G is an irreducible subgroup of $GL_d(\mathbb{Q})$ and $a := dim(C^+) = dim(\mathcal{F}(G)) \leq 3$. In this case one has:

LIST 3.1. $a = 1$: Then $C_{\mathbb{Q}^{d\times d}}(G)$ is either $\mathbb{Q}$, an imaginary quadratic number field or a definite quaternion algebra with center $\mathbb{Q}$ and $C^+ = \mathbb{Q}$.
$a = 2$: Then $C_{\mathbb{Q}^{d\times d}}(G)$ is either a real quadratic field K, a totally complex extension of K, or a totally definite quaternion algebra over K and $C^+ = K$.
$a = 3$: Then $C_{\mathbb{Q}^{d\times d}}(G)$ is an indefinite quaternion division algebra over $\mathbb{Q}$, i.e. a quaternion division algebra over $\mathbb{Q}$ ramified only at finite places and C^+ is a 3-dimensional subspace of $C_{\mathbb{Q}^{d\times d}}(G)$, or $C_{\mathbb{Q}^{d\times d}}(G)$ is isomorphic to a real cubic field K, a totally complex extension of K, or a totally definite quaternion algebra over K, and $C^+ = K$.

Note that in the case $a = 1$ and $a = 2$ the subspace C^+ is contained in the center of $C_{\mathbb{Q}^{d\times d}}(G)$.

So let G be a finite subgroup of $GL_d(\mathbb{Q})$ such that the fixed space C^+ of the involution on the commuting algebra $C_{\mathbb{Q}^{d\times d}}(G)$ is isomorphic to $\mathbb{Q}[\sqrt{p}]$ for some square free natural number $p > 1$ (case $a = 2$ in List 3.1). Let $F_0 \in \mathcal{F}(G)$ be positive definite. Then the positive definite G-invariant rational quadratic forms are precisely the forms cF_0 for $c \in C^+$ totally positive. Since we fix a G-invariant lattice L, we consider G as a finite subgroup of $GL_d(\mathbb{Z})$ by writing the matrices with respect to a $\mathbb{Z}$-basis of L. Assume that $G = O(L, F')$ is a Bravais group and let

$$N_{\mathbb{Z}} := N_{GL_d(\mathbb{Z})}(G) := \{x \in GL_d(\mathbb{Z}) \mid xgx^{-1} \in G \text{ for all } g \in G\}$$

be the normalizer of G in $GL_d(\mathbb{Z})$. Assume that $N_{\mathbb{Z}}/G$ is isomorphic to an infinite dihedral group. Let $t, x \in N_{\mathbb{Z}}$ such that tG generates the translation subgroup of $N_{\mathbb{Z}}/G$ and xG has order 2 in $N_{\mathbb{Z}}/G$. Then the finite subgroups of $N_{\mathbb{Z}}$ that contain G are conjugate to $G_1 := \langle G, x\rangle$ resp. $G_2 := \langle G, tx\rangle$. The element x fixes a one dimensional subspace of $\mathcal{F}(G)$ with positive definite generator F. Then $F_0 := F + tFt^{tr}$ is a positive definite generator of $\mathcal{F}(G_2)$.

PROPOSITION 3.2. *With the notation above let L be the natural G-lattice and R the ring of integers in C^+. Assume that $RL = L$. Let $s = a + b\sqrt{p}$ with $a, b \in \frac{1}{2}\mathbb{N}$ be a fundamental unit, i.e. a generator of the torsion free part of the unit group of R. Then $\langle sG\rangle \leq \langle tG\rangle$.*
If the norm $N(s) = a^2 - b^2p$ of s is -1 then $\langle sG\rangle = \langle tG\rangle$ and $det(F_0) = det(F)(4pb^2)^{d/2}$ (case -1).
If $N(s) = 1$ then $\langle sG\rangle$ is of index at most 2 in $\langle tG\rangle$ and $det(F_0) = det(F)(2+2a)^{d/2}$ if this index is two (case $+2$) and $det(F_0) = det(F)(4a^2)^{d/2}$ if $\langle sG\rangle = \langle tG\rangle$ (case $+1$).

PROOF. Since sG generates an abelian normal subgroup of $N_{\mathbb{Z}}/G$ one always has $sG \in \langle tG\rangle$. Therefore $sG = t^{\alpha}G$ for some $\alpha \in \mathbb{Z}$. Now $tFt^{tr} \in \mathcal{F}(G)$ is positive definite, so there is a totally positive unit $u \in R^*$ such that $tFt^{tr} = uF$.

Assume that $N(s)$ is negative. Then $u = s^{2\beta}$ is a square and $s^{\beta}F(s^{\beta})^{tr} = s^{2\beta}F = tFt^{tr}$. So F is a fixed point of $t^{\alpha\beta-1}$. Since $\langle tG\rangle$ acts fixed point free on $\mathcal{F}(G)$, one has $\alpha\beta = 1$ and $\langle sG\rangle = \langle tG\rangle$. So one may choose $s = t \in N_{\mathbb{Z}}$ and gets $F_0 = F + sFs^{tr} = (1+s^2)F$. Hence $det(F_0)det(F)^{-1} = det(1+s^2) = N(1+s^2)^{d/2} = N(1 + a^2 + 2ab\sqrt{p} + b^2p)^{d/2} = N(2pb^2 + 2ab\sqrt{p})^{d/2} = (4pb^2)^{d/2}$ where we identified C^+ with $\mathbb{Q}[\sqrt{p}]$ and used that $N(s) = a^2 - b^2p = -1$.

If $N(s) = 1$ one similarly finds that $u = s$ or $u = s^2$. In the first case t^2 acts like s on $\mathcal{F}(G)$ and therefore $\langle t^2 G\rangle = \langle sG\rangle$. In the second case one has as above $\langle tG\rangle = \langle sG\rangle$. One calculates $N(1+s) = 2+2a$ and $N(1+s^2) = 4a^2$ and gets the statement. □

The next proposition compares the minima of the invariant forms of the two subgroups G_1 and G_2 of $N_{\mathbb{Z}}$ that contain G properly.

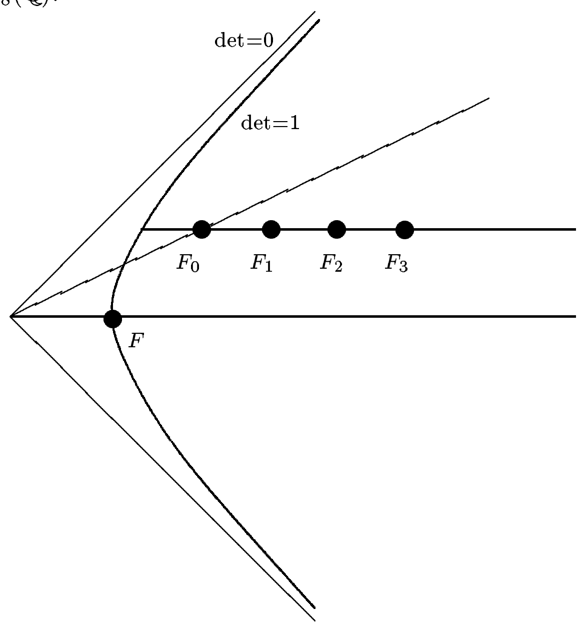
PROPOSITION 3.3. *With the notation above one has*

$$(\frac{det(F_0)}{det(F)})^{2/d}\frac{1}{2}min(F) \geq min(F_0) \geq 2min(F).$$

PROOF. Let $v \in L$ be a minimal vector of F_0. Then $vt \in L$ and both vFv^{tr} and $(vt)F(vt)^{tr}$ are $\geq min(F)$. Therefore one finds $min(F_0) = vF_0v^{tr} = vFv^{tr} + (vt)F(vt)^{tr} \geq 2min(F)$ and therefore the right inequality.

To get the left inequality, note that if $tFt^{tr} = uF$ for some totally positive unit $u \in C^+$ then $t^{-1}F(t^{-1})^{tr} = u^{-1}F$ and therefore $F_0 + t^{-1}F_0(t^{-1})^{tr} = 2F + t^{-1}F(t^{-1})^{tr} + tFt^{tr} = (1+u)(1+u^{-1})F = (\frac{det(F_0)}{det(F)})^{2/d}F$. As above one concludes $min((\frac{det(F_0)}{det(F)})^{2/d}F) \geq 2min(F_0)$ whence the left inequality. □

EXAMPLE 3.4. The space of invariant quadratic forms of $SL_2(5) \circ SL_2(5) : 2 \leq GL_8(\mathbb{Q})$.



$E_8 = (L,F)$ is the even unimodular lattice, $H_4 = L_0 = (L,F_0)$ is the extremal (in the sense of [**Que 95**]) 5-modular lattice. For $j \in \mathbb{Z}_{\geq 0}$ let $F_j := F_0 + jF$. Then the lattices $L_j := (L,F_j)$ are modular lattices of determinant $(j^2+5j+5)^4$ and minimum $2j+4$ in dimension 8. All these lattices are densest lattices in their genus since any even lattice of the same determinant with higher minimum has Hermite constant at least $\frac{2j+6}{\sqrt{j^2+5j+5}} > 2$. The inequality on the minima says $\frac{5}{2}\cdot 2 \geq min(H_4) = 4 \geq 2\cdot 2$.

We now look a little bit closer on the Hermite function on such 2-dimensional spaces of invariant quadratic forms as in the example above. Recall, that we are in the situation where G is a Bravais group and $N_{\mathbb{Z}}/G$ is isomorphic to an infinite dihedral group. Then $N_{\mathbb{Z}}/G$ is a reflection group and acts properly discontinuously on $\mathcal{F}_{\mathbb{R}}^{>0}(G)$ with open fundamental domain $C(F, F_0) := \{\lambda F + \lambda_0 F_0 \mid \lambda, \lambda_0 > 0\}$ the cone spanned by F and F_0. To determine γ on $\mathcal{F}_{\mathbb{R}}^{>0}$ it clearly suffices to calculate γ on representatives of the similarity classes of forms in $\overline{C(F, F_0)}$ such as $F_j := F_0 + jF$ $(0 \leq j \in \mathbb{R})$ and F. Using the notation of Proposition 3.2, the determinant of F_j can easily be calculated as
$det(F_j) = (j^2 + 4b^2p(1+j))^{d/2} det(F)$ in the case -1,
$det(F_j) = (j^2 + 4a^2(1+j))^{d/2} det(F)$ in the case $+1$, and
$det(F_j) = (j^2 + 2(1+a)(1+j))^{d/2} det(F)$ in the case $+2$.

REMARK 3.5. Assume that $Min(F) \cap Min(F_0) \neq \emptyset$. Let $m_0 := min(F_0)$ and $m := min(F)$. Then the forms F_j with $j > 0$ are not G-perfect, $min(F_j) = m_0 + jm$ and $Min(F_j) = Min(F_0) \cap Min(F)$. If $Min(F_0) \not\subseteq Min(F)$ then F_0 is G-perfect and if $Min(F) \not\subseteq Min(F_0)$ then F is G-perfect.

Note that the condition of Remark 3.5 is in particular fulfilled if $min(F_0) = 2min(F)$.

COROLLARY 3.6. *With the assumption of the Remark 3.5 one has*

$$\gamma(F_j) = \begin{cases} (m_0 + jm)/((j^2 + 4b^2p(1+j))D) & \textit{in case } -1 \\ (m_0 + jm)/((j^2 + 4a^2(1+j))D) & \textit{in case } +1 \\ (m_0 + jm)/((j^2 + 2(1+a)(1+j))D) & \textit{in case } +2 \end{cases}$$

where $D = det(F)^{2/d}$.

This corollary proves the calculation of the Hermite function in Example 3.4. Several other examples for $p = 2, 3, 5$ are given in Table 1 and 2 (cf. [**Neb 95a**, Chapter (VI)], [**Neb 98b**, Appendix]). These Tables are built up as follows. The first column contains the dimension d followed by p. The third column gives the Bravais group G in the notation e.g. introduced in [**PlN 95**], [**Neb 95a**], [**Neb 96a**]. The reader should be able to get some idea on the isomorphism type of G without further explanation. In the next columns the relevant data for the forms F_0 and F are given below each other. First the determinant, followed by the minimum and the number of minimal vectors decomposed in orbits under the automorphism group $O(L, F_0)$ resp. $O(L, F)$.

If $p = 2$ or is a prime $p \equiv 1 \pmod 4$ then the fundamental unit of $\mathbb{Q}[\sqrt{p}]$ has negative norm. It turns out that in the cases where $p = 3$, the fundamental unit $s \in C^+$ (in the notation above) only generates a subgroup $\langle sG \rangle$ of index 2 of the translation subgroup of $N_{GL_d(\mathbb{Z})}(G)$. Hence the scaling factor $(det(F_0)/det(F))^{2/d}$ is

p	2	3	5
$(det(F_0)/det(F))^{2/d}$	8	6	5

.

In all examples, $Min(F_0) \subset Min(F)$. Therefore F is up to the action of $\mathbb{R}^* N_{\mathbb{Z}}$ the unique G-perfect form.

Table 1: 2-dimensional spaces with one G-perfect form, $d \leq 24$

d	p	G	det	min	$\|Min\|$
4	5	$\pm D_{10}$	5^3 5	4 2	10 20
6	5	$\pm Alt_5$	$2^2 5^3$ 2^2	4 2	30 60
8	5	$(SL_2(5) \circ SL_2(5)) : 2$	5^4 1	4 2	120 240
12	5	$\pm 3.Alt_6.2$	$3^6 5^6$ 3^6	8 4	270 756
16	5	$\pm Alt_6.2$	$3^8 5^8$ 3^8	8 4	180 720
16	5	$SL_2(5) \otimes_{\infty,3} SL_2(9)$	$3^8 5^{16}$ $3^8 5^8$	20 10	720 1440
16	5	$SL_2(5) \otimes_{\infty,3} (SL_2(3) \overset{2}{\square} C_3)$	$2^8 3^8 5^8$ $2^8 3^8$	12 6	480 960
24	5	$2.J_2 \circ SL_2(5)$	5^{12} 1	8 4	37800 196560
24	5	$(SL_2(5) \circ SL_2(5)).2 \otimes_{\sqrt{5}} Alt_5$	$2^8 5^{12}$ 2^8	8 4	1800 $3600 + 8640$
24	5	$SL_2(5) \otimes_{\infty,3} (\pm 3_+^{1+2}).GL_2(3)$	$3^8 5^{12}$ 3^8	8 4	1080 2160
24	5	$3.Alt_6 \overset{2(2)}{\boxtimes}_{\sqrt{-3}} SL_2(3)$	$2^{12} 5^{12}$ 2^{12}	8 4	1080 3024
24	5	$Alt_5 \otimes_{\sqrt{5}} (C_3 \overset{2(2)}{\boxtimes} D_8)$	$2^{12} 3^{12} 5^{12}$ $2^{12} 3^{12}$	16 8	$360 + 2 \cdot 720$ $3024 + 7560$
24	5	$3.Alt_6 \overset{2(2)}{\boxtimes} D_8$	$2^{12} 3^{12} 5^{12}$ $2^{12} 3^{12}$	16 8	$1080 + 1080$ $3024 + 7560$
24	2	$6.Alt_7$	$2^{12} 4^{12}$ 1	8 4	3024 196560
24	2	$U_3(3) \otimes_{\infty,3} \tilde{S}_4$	$2^{12} 4^{12}$ 1	8 4	3024 196560
24	3	$6.L_3(4).2 \overset{2}{\boxtimes} C_4$	$2^{12} 3^{12}$ 1	8 4	$3024 + 7560$ 196560
24	3	$(\pm U_3(3).2) \circ SL_2(3)$	$2^{12} 3^{12}$ 1	8 4	$4536 + 6048$ 196560
24	3	$6.U_4(3).2 \overset{2}{\boxtimes} C_4$	$2^{12} 6^{12}$ 2^{12}	8 4	1512 3024

Table 2: 2-dimensional spaces with one G-perfect form, $d = 32$

d	p	G	det	min	$\|Min\|$
32	5	$SL_2(5) \underset{\infty,2}{\otimes} 2_-^{1+6}.O_6^-(2)$	5^{16}	8	21600
			1	4	146880
32	5	$\otimes^4 SL_2(5) : S_4$	5^{16}	8	21600
			1	4	$43200 + 103680$
32	5	$4.L_3(4).2$	5^{16}	8	$11520 + 10080$
			1	4	146880 (5 orbits)
32	5	$SL_2(5) \underset{\infty,3}{\otimes} (Sp_4(3) \overset{2}{\square} C_3)$	$3^{16}5^{16}$	12	4800
			3^{16}	6	9600

Assume now that $Min(F_0) \cap Min(F) = \emptyset$. Let

$$m_0 := min(F_0) \text{ and } \tilde{m}_0 := min\{vFv^{tr} \mid v \in Min(F_0)\}.$$

For $i = 0, 1, \ldots$ let

$$\tilde{m}_{i+1} := max\{vFv^{tr} \mid 0 \neq v \in \mathbb{Z}^d, vFv^{tr} < \tilde{m}_i\}.$$

Then $\tilde{m}_0 > \tilde{m}_1 > \ldots > \tilde{m}_s = m := min(F)$ for some $s \geq 1$. For $i = 0, \ldots, s$ let $m_i := min\{vF_0v^{tr} \mid v \in \mathbb{Z}^d,\ vFv^{tr} = \tilde{m}_i\}$. Then

$$min(F_j) = min\{m_i + j\tilde{m}_i \mid 0 \leq i \leq s\} =: M(j).$$

Let $\alpha(0) := 0$ and for $i = 0, 1, \ldots, t-1$ let $\alpha(i+1) := min\{a > \alpha(i) \mid \exists j > 0$ such that $m_a + j\tilde{m}_a = M(j)\}$ until $\alpha(t) = s$. We now define for $1 \leq i \leq t$

$$j_i := \frac{m_{\alpha(i)} - m_{\alpha(i-1)}}{\tilde{m}_{\alpha(i-1)} - \tilde{m}_{\alpha(i)}}.$$

PROPOSITION 3.7. *Assume that $Min(F_0) \cap Min(F) = \emptyset$. With the notation above one has $0 =: j_0 \leq j_1 \leq \ldots \leq j_t < \infty =: j_{t+1}$. The forms $F_{j_1}, \ldots, F_{j_t}$ and possibly F_0 and F (if there is $v \in Min(F_0)$, $vFv^{tr} > \tilde{m}_0$ resp. $v \in Min(F)$, $vF_0v^{tr} > m_{\alpha(t)}$) represent the orbits of G-perfect forms under the action of $\mathbb{R}^* N_{\mathbb{Z}}$. The Hermite function is given by $\gamma(F_j) = (m_{\alpha(i)} + j\tilde{m}_{\alpha(i)})/(det(F_j)^{2/d})$ if $j \in [j_i, j_{i+1}]$ for $0 \leq i \leq t$.*

PROOF. Let $0 < j < j' \in \mathbb{R}$ and $0 \leq a, b \leq s$ be such that $m_a + j\tilde{m}_a = min_{0\leq l \leq s}(m_l + j\tilde{m}_l)$ and $m_b + j'\tilde{m}_b = min_{0 \leq l \leq s}(m_l + j'\tilde{m}_l)$. Then $m_b - m_a + j(\tilde{m}_b - \tilde{m}_a) \geq 0$ and $m_a - m_b + j'(\tilde{m}_a - \tilde{m}_b) \geq 0$ and hence the sum $(j' - j)(\tilde{m}_a - \tilde{m}_b) \geq 0$. Since $j' > j$ this implies $\tilde{m}_a \geq \tilde{m}_b$ or equally $a \leq b$. For $1 \leq i \leq t$ let j_i be minimal such that $m_{\alpha(i)} + j_i\tilde{m}_{\alpha(i)} = M(j_i)$. Then for $j_{i-1} \leq j < j_i$ the minimum $M(j)$ is $m_{\alpha(i-1)} + j\tilde{m}_{\alpha(i-1)} = M(j)$. Since the Hermite function γ and the determinant both are continuous on $\mathcal{F}_{\mathbb{R}}^{>0}(G)$, one gets $M(j_i) = m_{\alpha(i-1)} + j_i\tilde{m}_{\alpha(i-1)}$. Hence the j_i are given by the formula above. For $j_{i-1} < j < j_i$ one has $Min(F_j) = \{v \in \mathbb{Z}^d \mid vF_0v^{tr} = m_{\alpha(i-1)}\} \cap \{v \in \mathbb{Z}^d \mid vFv^{tr} = \tilde{m}_{\alpha(i-1)}\} =: V(i-1)$. But $Min(F_{j_i}) = V(i-1) \cup V(i)$. To show that F_{j_i} is G-perfect we note that the bilinear pairing $\mathcal{F}(G) \times \mathcal{F}(G^{tr}) \to \mathbb{Q}, (A, A') \mapsto trace(AA')$ is nondegenerate. For $v \in V(i)$ one gets $trace(p_G(v)F) = \sum_{g\in G}(trace(vgFg^{tr}v^{tr})) = |G|\tilde{m}_{\alpha(i)}$ and for $w \in V(i-1)$ similarly $trace(p_G(w)F) = |G|\tilde{m}_{\alpha(i-1)}$. Analogously one calculates $trace(p_G(v)F_0) = |G|m_{\alpha(i)}$ and $trace(p_G(w)F_0) = |G|m_{\alpha(i-1)}$. By definition $0 < \tilde{m}_{\alpha(i)} < \tilde{m}_{\alpha(i-1)}$ and $0 < m_{\alpha(i-1)} < m_{\alpha(i)}$ because $j_i > 0$. Therefore $p_G(v)$ and

$p_G(w)$ span the 2-dimensional space $\mathcal{F}(G^{tr})$ which means that F_{j_i} is G-perfect. The rest is clear now. □

Examples for such situations are given in Table 3, which is built up as Table 1 and 2.

Table 3: 2-dimensional spaces with two G-perfect forms

d	p	G	det	min	$\|Min\|$
14	13	$\pm L_2(13)$	$13^7 2^2$ 2^2	8 2	182 364
24	13	$SL_2(13) \circ SL_2(3)$	13^{12} 1	12 4	$2 \cdot 2184 + 8736$ 196560
32	17	$SL_2(17) \circ \tilde{S}_3$	$2^{32} 17^{16}$ 1	24 4	1632 $3 \cdot 4896 + 4 \cdot 14688$

In the examples one finds $t = 1$. For $p = 13$ one gets $m_1 = m_0 + 2$, $\tilde{m}_0 = m + 2$ and therefore $j_1 = 1$ and the form $\frac{1}{3}F_1$ is a G-perfect form of determinant $3^{d/2} det(F)$ and minimum $(m_0 + m + 2)/3$. For $p = 17$ one has $m_1 = m_0 + 48$, $\tilde{m}_0 = m + 8$ and therefore $j_1 = 6$ and the form $\frac{1}{16}F_6$ is a G-perfect form of determinant $2^{d/2} det(F)$ and minimum $(m_0 + 6m + 48)/16$.

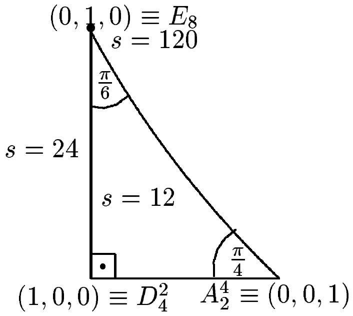


Fig. 1

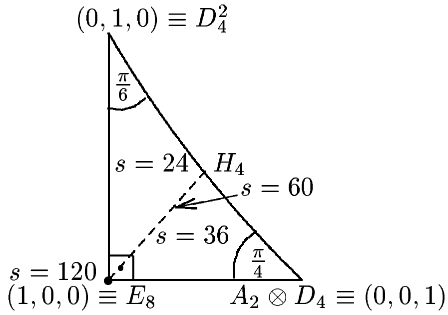


Fig. 2

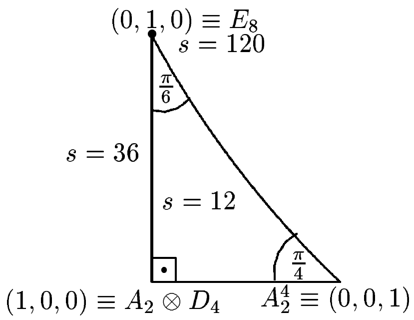


Fig. 3

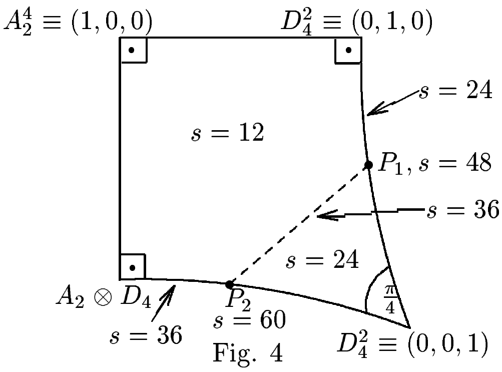
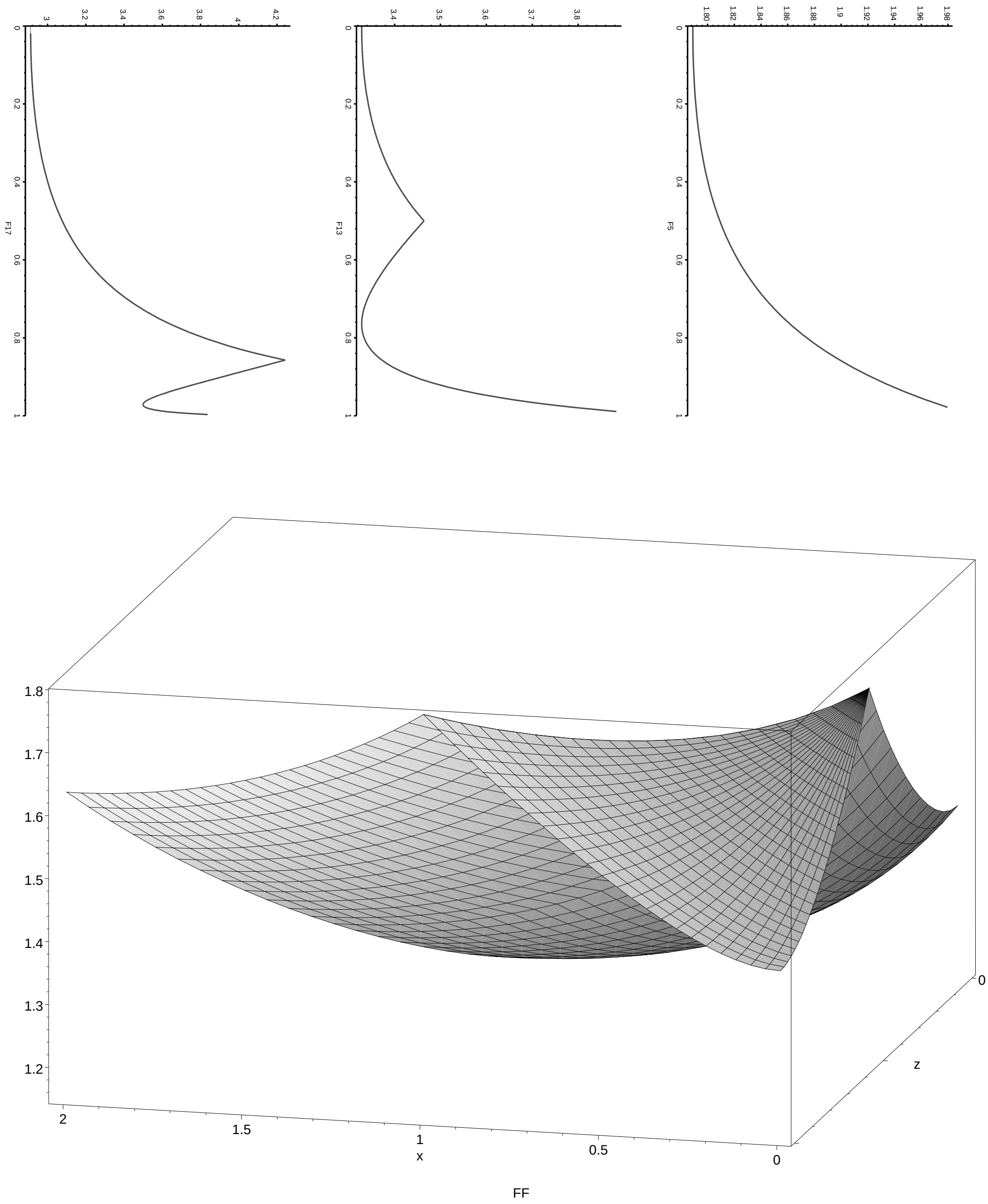


Fig. 4

FIGURE 5: The Hermite function on the fundamental domains $F5$ ($G = SL_2(5) \circ SL_2(5) : 2$), $F13$ ($G = SL_2(13) \circ SL_2(3)$), $F17$ ($G = SL_2(17) \circ \tilde{S}_3$), (all identified with $[0,1]$) and FF ($G = B_{20}$) (cut in the layer $\lambda_1 + \lambda_2 + \lambda_3 = 1$, $\lambda_1 = x, \lambda_3 = z$) of $N_{\mathbb{Z}}\mathbb{R}_{>0}$ on $\mathcal{F}_{\mathbb{R}}^{>0}(G)$:



There are 4 irreducible Bravais groups in dimension 8 that have a 3-dimensional space of invariant quadratic forms called $B_{19}, \ldots, B_{22}$ in [**Sou 94**]. One has that $B_{22} \cong Q_8 \otimes_{\sqrt{-1}} \tilde{S}_3$ is conjugate in $GL_8(\mathbb{Q})$ to a subgroup of $B_{21} \cong SL_2(3) \otimes_{\sqrt{-1}} \tilde{S}_3$ and B_{19} and B_{20} are conjugate in $GL_8(\mathbb{Q})$. In all cases one computes that $N_{\mathbb{Z}}/G$ is a hyperbolic reflection group. Therefore $N_{\mathbb{Z}}$ has a canonical fundamental domain $\mathbf{F}$ on $\mathcal{F}_{\mathbb{R}}^{>0}(G)$. Figure 1 ($G = B_{22}$), figure 2 ($G = B_{21}$), figure 3 ($G = B_{19}$), and figure 4 ($G = B_{20}$) above show the fundamental domains $\mathbf{F}$ of the action of $N_{\mathbb{Z}}$ on $\mathcal{F}_{\mathbb{R}}^{>0}(G)/\mathbb{R}_{>0}$ (cf. also [**Ple 96**]). For the forms F in $\bar{\mathbf{F}}$, the number $s = \frac{1}{2}|Min(F)|$ is given. Thick lines indicate that this number is bigger on the boundary than inside $\mathbf{F}$. The arrows point to the whole line segment. The G-perfect forms (E_8, P_1, and P_2) are marked by points. The determinant of the minimal integral representative of P_1 is $2^2 6^2 12^2$ and its minimum is 6. P_2 is represented by the extremal 5-modular lattice of dimension 8.

In the first 3 examples one may identify the fundamental domain with $\mathbb{R}^3_{>0}$ using the basis as given in the picture. In the last example one may identify it with $\{(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{R}^3 \mid \lambda_1 > 0, \lambda_3 > 0, \lambda_1 + \lambda_2 > 0, \lambda_2 + 2\lambda_3 > 0\}$. The Hermite function γ_i ($i = 1, \ldots, 4$) in this parametrization is given by

$$\gamma_1(\lambda_1, \lambda_2, \lambda_3) = 2(\lambda_1 + \lambda_2 + \lambda_3)(2\lambda_1^2 + \lambda_2^2 + 3\lambda_3^2 + 4\lambda_1\lambda_2 + 6\lambda_2\lambda_3 + 6\lambda_1\lambda_3)^{-1/2}$$

$$\gamma_2(\lambda_1, \lambda_2, \lambda_3) = \begin{cases} (2\lambda_1 + 2\lambda_2 + 6\lambda_3)/d(\lambda_1, \lambda_2, \lambda_3) & \text{if } \lambda_3 \leq \lambda_2 \\ (2\lambda_1 + 4\lambda_2 + 4\lambda_3)/d(\lambda_1, \lambda_2, \lambda_3) & \text{if } \lambda_3 \geq \lambda_2 \end{cases}$$

where $d(\lambda_1, \lambda_2, \lambda_3) = (\lambda_1^2 + 2\lambda_2^2 + 6\lambda_3^2 + 4\lambda_1\lambda_2 + 12\lambda_2\lambda_3 + 6\lambda_1\lambda_3)^{1/2}$.

$$\gamma_3(\lambda_1, \lambda_2, \lambda_3) = (4\lambda_1 + 2\lambda_2 + 2\lambda_3)(6\lambda_1^2 + \lambda_2^2 + 3\lambda_3^2 + 6\lambda_1\lambda_2 + 6\lambda_2\lambda_3 + 12\lambda_1\lambda_3)^{-1/2}$$

$$\gamma_4(\lambda_1, \lambda_2, \lambda_3) = \begin{cases} (2\lambda_1 + 2\lambda_2 + 4\lambda_3)/d(\lambda_1, \lambda_2, \lambda_3) & \text{if } 2\lambda_1 + \lambda_2 - \lambda_3 \geq 0 \\ (6\lambda_1 + 4\lambda_2 + 2\lambda_3)/d(\lambda_1, \lambda_2, \lambda_3) & \text{if } 2\lambda_1 + \lambda_2 - \lambda_3 \leq 0 \end{cases}$$

where $d(\lambda_1, \lambda_2, \lambda_3) = (3\lambda_1^2 + 2\lambda_2^2 + 2\lambda_3^2 + 6\lambda_1\lambda_2 + 8\lambda_2\lambda_3 + 12\lambda_1\lambda_3)^{1/2}$ (see Figure 5).

4. A method to compute the minimum of certain lattices.

In this section we derive a method to compute the minimum of lattices that are contained in an orthogonally decomposable overlattice of small index. This is applied to prove extremality (in the sense of [**Que 95**]) of a 64-dimensional even unimodular lattice and of a 64-dimensional even 3-modular lattice.

REMARK 4.1. Let (L, F) be an integral lattice that is contained in an orthogonally decomposable lattice $M_1 \perp M_2$ of finite index. Let $K_i := L \cap M_i$ ($i = 1, 2$) and assume that M_i is the projection of L into $\mathbb{Q}K_i$ ($i = 1, 2$). Define $\alpha : M_1/K_1 \to M_2/K_2$ by $\alpha(x + K_1) = y + K_2$ if $x + y \in L$.

Then the minimum of L is $\geq m$, if the minimum of K_1 and K_2 is $\geq m$ and for all $x \in M_1$ of square length $s := (x, x) < m$ the minimum of the subset of M_2 that is the full preimage of $\alpha(x)$ is $\geq m - s$.

We now apply this trivial remark to show that the minimum of the unimodular lattice of dimension 64 described on [**Neb 98a**, p. 496] is 6.

PROPOSITION 4.2. *The unimodular lattice (L, F) of dimension 64 described in* [**Neb 98a**, Section 5] *invariant under $SL_2(17) \underset{\infty,3}{\otimes} SL_2(5)$ is an even extremal unimodular lattice.*

Proof. Let g be an element of order 3 in $SL_2(17) \leq O(L,F)$ and let K_1 be its fixed lattice $K_1 := \{l \in L \mid lg = l\}$. Then K_1 is isometric to ${}^{(3)}E_8^2$ a rescaling of an even unimodular lattice of dimension 16. Let $K_2 := K_1^\perp$ and $M_i = K_i^\#$ be the projection of L into $\mathbb{Q}K_i$ and $\alpha : M_1/K_1 \to M_2/K_2$ be defined as in the remark above. Then $K_1 \perp K_2$ is a sublattice of L of index 3^{16}. One computes that the minimum of both lattices K_i is 6 and that M_2 has minimum 10/3. Hence the minimum of L is ≥ 4 and the vectors of square length 4 in L (if any) are of the form $x + y$, where x is a vector of length 2/3 in M_1 and y a vector of length 10/3 in the full preimage of $\alpha(x)$ in M_2.

A subgroup $\cong SL_2(5) : 2$ of the centralizer of g in $O(L,F)$ has two orbits of length 240 on the minimal vectors of M_1 with representatives say x_1 and x_2. One computes that the minimum of the two sublattices of M_2 that are generated by the full preimages of $\alpha(x_1)$ and $\alpha(x_2)$ is $> 10/3$. Therefore the minimum of L is > 4 which implies the extremality of L. □

Analogously, however with some more effort, one shows that the minimum of the even 3-modular lattice (L, p_3F) of dimension 64 described on [**Neb 98a**, p. 496] is 12. Note that this lattice is the densest lattice presently known in this dimension. The theory of modular forms shows that its kissing number is 138,458,880, which is the largest known for lattice packings in dimension 64. (cf. [**SPLAG3**], [**NeSl**]).

Proposition 4.3. *The 3-modular lattice (L, p_3F) of dimension 64 described in* [**Neb 98a**, Section 5] *invariant under $SL_2(17) \otimes_{\infty,3} SL_2(5)$ is an even extremal 3-modular lattice.*

Proof. In [**Neb 98a**] it is shown that (L, p_3F) is isometric to $(L^\#, 3p_3F)$. So we only prove that the minimum of (L, p_3F) (resp. the one of $(L^\#, 3p_3F)$) is ≥ 12. That the minimum is ≥ 10 can be shown directly using the backtrack algorithm to calculate short vectors in a lattice (cf. [**PoZ 89**]) but this will not be used here.

Let g, K_1 and K_2 be as in the proof of Proposition 4.2. Then $K_1 \perp K_2$ is a sublattice of index 3^{16} of L. Hence the dual lattice $M_1 \perp M_2 := (K_1 \perp K_2)^\#$ (with respect to p_3F) contains $L^\#$ of index 3^{16}. Since (L, p_3F) is isometric to $(L^\#, 3p_3F)$ we will work with the latter. $L^\#$ is a subdirect product of M_1 and M_2. So let $N_1 := M_1 \cap L^\# = 3M_1$ resp. $N_2 := M_2 \cap L^\#$ be the kernels of the projections $L^\# \to M_2$ resp. $L^\# \to M_1$, and $\alpha : M_1/N_1 \to M_2/N_2$ be defined as in the remark above. The elementary divisors of the Gram matrices of these lattices are $(1/3)^8 1^8$, $(1/3)^8 1^{24} 3^{16}$ (for M_1 and M_2) and $3^8 9^8$, $1^{16} 3^{24} 9^8$ (for N_1 and N_2). One easily checks that the minimum of N_1 and N_2 is 12.

Let $G := SL_2(17) \otimes_{\infty,3} SL_2(5) \leq O(L, p_3F)$. Then the normalizer of $\langle g \rangle$ in G is $N := N_G(\langle g \rangle) = Q_{36} \otimes_{\infty,3} SL_2(5)$ and acts L, preserving M_1 and M_2. The lattice M_1 has 720 vectors of length 4/3 falling into 3 orbits under N, 13440 vectors of length 6/3 (34 N-orbits), 97200 vectors of length 8/3 (159 N-orbits) and 455040 vectors of length 10/3 (670 N-orbits). The lattice M_2 has minimum 12/3 and 2160 vectors of length 12/3 falling into 3 orbits under N, no vectors of length 14/3 or 16/3 and 290880 vectors of length 18/3 forming 214 orbits under N. As in the proof of Proposition 4.2 one checks that for each representative x of the N-orbits on the vectors of length $s \leq 10/3$ in M_1 the minimum of the lattice of dimension 48 generated by the full preimage of $\alpha(x)$ is $> 10 - s$ and that for each representative

y of the N orbits on the vectors of length $s \leq 18/3$ in M_2 the minimum of the 16-dimensional lattices generated by the full preimage of $\alpha^{-1}(y)$ is $> 10 - s$. Therefore the minimum of $(L^{\#}, 3p_3F) \cong (L, p_3F)$ is > 10. □

References

[BaN 98] C. Bachoc, G. Nebe, *Extremal lattices of minimum 8 related to the Mathieu group M_{22}.* J. reine angew. Math., **494**, 155-171, (1998)

[CoS 98] J. H. Conway, N. J. A. Sloane, *A Note on Optimal Unimodular Lattices.* J. Number Theory (to appear)

[SPLAG3] J.H. Conway and N.J.A. Sloane, *Sphere packings, lattices and groups* Third edition, Springer 1998

[Mar 96] J. Martinet, *Réseaux parfaits des espaces Euclidiens.* Masson 1996

[Neb 95a] G. Nebe, *Endliche rationale Matrixgruppen vom Grad 24.* Aachener Beiträge zur Mathematik, Band 12, Verlag der Augustinus Buchhandlung (1995)

[NeP 95b] G. Nebe, W. Plesken, *Finite rational matrix groups of degree 16.* part II of [PlN 95], AMS-Memoir No. 556, vol. 116 (1995)

[Neb 96a] G. Nebe, *Finite subgroups of $GL_{24}(\mathbb{Q})$.* Exp. Math. Vol. 5, Number 3, 163-195 (1996)

[Neb 96b] G. Nebe, *Finite subgroups of $GL_n(\mathbb{Q})$ for $25 \leq n \leq 31$.* Comm. Algebra **24** (7), 2341-2397 (1996)

[Neb 97] G. Nebe, *The normaliser action and strongly modular lattices.* L'Enseignement Mathématique t. 43, 67-76 (1997)

[Neb 98a] G. Nebe, *Some cyclo quaternionic lattices.* J. Algebra 199, 472-498 (1998)

[Neb 98b] G. Nebe, *Finite quaternionic matrix groups.* Represent. Theory 2, 106-223 (1998)

[NeSl] G. Nebe and N. J. A. Sloane, *A Catalogue of Lattices*, published electronically at http://www.research.att.com/~njas/lattices/.

[Opg 96] J. Opgenorth, *Dual cones and the Voronoi algorithm.* Preprint (1996)

[Ple 96] W. Plesken, *Kristallographische Gruppen.* 75-96 in *Group Theory, Algebra, Number Theory.* H. Zimmer (ed.), de Gruyter 1996.

[PlN 95] W. Plesken, G. Nebe, *Finite rational matrix groups.* AMS-Memoir No. 556, vol. 116 (1995).

[PoZ 89] M. Pohst, H. Zassenhaus, *Algorithmic algebraic number theory.* Cambridge University Press 1989.

[Que 95] H.-G. Quebbemann, *Modular Lattices in Euclidean Spaces.* J. Number Theory, Vol 54, No 2, 190-202 (1995).

[Que 97] H.-G. Quebbemann, *Atkin-Lehner eigenforms and strongly modular lattices.* L'Enseignement Mathématique t. 43, 55-65 (1997).

[Sou 94] B. Souvignier, *Irreducible finite integral matrix groups of degree 8 and 10.* Math. Comp. **63** (207), 335-350 (1994)

Lehrstuhl B für Mathematik, RWTH-Aachen, Templergraben 64, 52062 Aachen, Germany

E-mail address: `gabi@math.rwth-aachen.de`