JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

FRANÇOIS SIGRIST

# Cyclotomic quadratic forms

*Journal de Théorie des Nombres de Bordeaux*, tome 12, n° 2 (2000), p. 519-530

<http://www.numdam.org/item?id=JTNB_2000__12_2_519_0>

© Université Bordeaux 1, 2000, tous droits réservés.

L'accès aux archives de la revue « Journal de Théorie des Nombres de Bordeaux » (http://jtnb.cedram.org/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

*Article numérisé dans le cadre du programme*
*Numérisation de documents anciens mathématiques*
http://www.numdam.org/

*Journal de Théorie des Nombres*
*de Bordeaux* **12** (2000), 519–530

# Cyclotomic quadratic forms

par François SIGRIST

RÉSUMÉ. L'algorithme de Voronoï est un procédé permettant d'obtenir la liste complète des formes quadratiques positives parfaites à $n$ variables. Sa généralisation aux $G$-formes permet de classer les formes $G$-parfaites, avec l'avantage de se dérouler dans un espace de dimension plus petite ($G$ est un sous-groupe fini de $GL(n, \mathbb{Z})$). On étudie ici la représentation standard du groupe cyclique $G = C_m$ en dimension $\phi(m)$, de polynôme caractéristique $\Phi_m(x)$ (polynôme cyclotomique). Une forme $G$-invariante est dite forme cyclotomique. Toute les formes $G$-parfaites sont données pour $\phi(m) < 16$, de même que pour $m = 17$, où la forme cyclotomique la plus dense est entièrement nouvelle. On obtient ainsi une constante d'Hermite cyclotomique, qui s'avère être souvent meilleure que la constante d'Hermite habituelle. C'est le cas pour $m = 5, 7, 11, 13, 16, 17, 36$, et vraisemblablement 32 (les calculs pour $m = 32$ sont en cours, et ont déjà fourni 4600 formes $C_{32}$-parfaites). Les résultats complets sont disponibles à `http://www.unine.ch/math`.

ABSTRACT. Voronoï 's algorithm is a method for obtaining the complete list of perfect n-dimensional quadratic forms. Its generalization to $G$-forms has the advantage of running in a lower-dimensional space, and furnishes a finite, and complete, classification of $G$-perfect forms ($G$ is a finite subgroup of $GL(n, \mathbb{Z})$). We study the standard, $\phi(m)$-dimensional irreducible representation of the cyclic group $C_m$ of order m, and give the, often new, densest $G$-forms. Perfect cyclotomic forms are completely classified for $\phi(m) < 16$ and for $m = 17$. As a consequence, we obtain precise upper bounds for the Hermite invariant of cyclotomic forms in this range. These bounds are often better than the known or conjectural values of the Hermite constant for the corresponding dimensions; this is indeed the case for $m = 5, 7, 11, 13, 16, 17, 36$. The complete results can be taken from `http://www.unine.ch/math`.

Manuscrit reçu le 29 février 2000.
Supported by FNSRS grant 056816.99.

## 1. Introduction

Denote by $\Phi_m(x) = 1 + c_1 x + \ldots + c_{n-1}x^{n-1} + x^n$ the $m$-th cyclotomic polynomial, of degree $n = \phi(m)$. Let $G \in GL(n, \mathbb{Z})$ be the matrix

$$\begin{pmatrix} 0 & 0 & \cdot & \cdot & \cdot & 0 & -1 \\ 1 & 0 & \cdot & \cdot & \cdot & 0 & -c_1 \\ 0 & 1 & \cdot & \cdot & \cdot & 0 & -c_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & 1 & -c_{n-1} \end{pmatrix}$$

generating the standard $n$-dimensional representation of the cyclic group $C_m$. A *cyclotomic form* is a real quadratic form $q(x) = \sum a_{ij}x_i x_j$ in $n$ variables, invariant under this action of $C_m$: the symmetric matrix $A = (a_{ij})$ satisfies $G^t A G = A$.

An easy computation shows that the matrix $A$ has then constant diagonals ($a_{i+k,j+k} = a_{i,j}$), and is completely known from the first half of its first row: the space of cyclotomic forms is a linear subspace of $Sym_n(\mathbb{R})$ of dimension $n/2$. Nevertheless, for convenience, we always shall give a cyclotomic matrix by its full first row.

A positive definite real quadratic form has

- a *minimum* $\underline{m} = \min(x^t A x | x \in \mathbb{Z}^n - \{0\})$.
- a set $S = \{\pm v_1, \pm v_2, \ldots, \pm v_s\}$of pairs of *minimal vectors* in $\mathbb{Z}^n$, satisfying $v_i^t A v_i = \underline{m}$. $2s$ is called the *kissing number* of the form.
- a *Hermite invariant* $\gamma_n(A) = \underline{m} \cdot (\det A)^{-1/n}$.

There is a familiar dictionary linking positive definite forms and Euclidean lattices, via the Gram matrix. A Euclidean lattice has an associated sphere packing, and the packing density $\delta$ is related to the Hermite invariant by the relation $\delta = \mathrm{Const}(n) \cdot \gamma_n(A)^{n/2}$ : a dense form means a high Hermite invariant.

A quadratic form is *perfect* if it is the unique quadratic form having minimum $\underline{m}$ and set $S$ of minimal vectors. Similarly, a cyclotomic form is said to be *$C_m$-perfect* if it is the unique *cyclotomic form* with $\underline{m}$ and $S$ as before. A quadratic form is *extreme* if its density is locally maximal in the space of quadratic forms. A cyclotomic form is *$C_m$-extreme* if its density is locally maximal in the space of *cyclotomic forms.*

An extreme form is always perfect. For the converse, a theorem of Voronoï requires a condition called eutaxy (cf [Mar]). These properties carry over verbatim to the case of $C_m$-forms [B-M]. A $C_m$-perfect form is proportional to an integral form, as are the usual perfect forms.

There is a second useful dictionary linking rational cyclotomic forms to the cyclotomic field $\mathbb{Q}(\zeta_m)$. If $A$ is (the matrix of) a cyclotomic form, there is a unique real element $\alpha \in \mathbb{Q}(\zeta_m)$ such that $x^t A x = \mathrm{Trace}(\alpha x \overline{x})$. The practical computation runs as follows: write $\vec{a}$ for the first column of the matrix $A$, and associate to $\alpha = \alpha_0 + \alpha_1\zeta_m + \ldots + \alpha_{n-1}\zeta_m^{n-1}$ the column $\vec{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})^t$. Then $\vec{a} = D\vec{\alpha}$ with matrix $D = (d_{ij}) = \mathrm{Trace}(\zeta_m^{i-j})$. The determinant of $D$ is the discriminant of the field $\mathbb{Q}(\zeta_m)$, and is therefore nonzero: $A$ and $\alpha$ determine each other. If a cyclotomic form is positive definite, the element $\alpha$ is totally positive ($\alpha \gg 0$): all its conjugates are positive. Further, if $u$ is a unit, the cyclotomic form corresponding to $u \cdot \bar{u} \cdot \alpha$ is clearly $C_m$-equivalent to the original form. This method is extremely useful for finding, or checking, $G$-equivalences.

Taking determinants in $x^t A x = \mathrm{Trace}(\alpha x \overline{x})$, one gets (using the fact that $\alpha$ is real):
$\det(A) = \det(D) \cdot \mathrm{Norm}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha) = \mathrm{Disc}(\mathbb{Q}(\zeta_m)) \cdot (\mathrm{Norm}_{\mathbb{Q}(\zeta_m+\zeta_m^{-1})/\mathbb{Q}}(\alpha))^2$. It follows that the determinant of an integral cyclotomic form is equal to $k(m)d^2$, where $k(m)$ is the square-free part of the discriminant of the cyclotomic field $\mathbb{Q}(\zeta_m)$. Further, using the detailed study of decomposition of primes in cyclotomic fields, E. Bayer-Fluckiger and J. Martinet obtained the following useful

**Proposition** ([Bay-M]). *If $q$ is a prime power dividing $d$, and prime to $m$, then $q \equiv \pm 1$ (mod $m$).*

Up to equivalence, there are only finitely many perfect quadratic forms. Voronoï 's algorithm, deviced in 1908 [Vor], constitutes a method of explicit complete classification. The densest quadratic form(s) in each dimension can be found with an entirely mechanical computation, the only problem being the gigantic computational complexity.

For cyclotomic forms, it was shown in [B-M-S] that the orthogonal projection of Voronoï 's algorithm onto the (dual) space of cyclotomic forms provides an exhaustive classification. Later, it was proved [JCb] that the number of $C_m$-inequivalent $C_m$-perfect forms is finite. The practical advantage lies in the dimension of the space of forms ($n/2$ instead of $n(n+1)/2$), bringing the computing time to almost nothing for $n \leq 12$, and to"tolerable" values for the groups $C_{17}$ and $C_{32}$ ($n = 16$). There are 1344 $C_{17}$-perfect forms, and at least 4600 $C_{32}$-perfect forms. Both densest forms are completely new.

As is customary in algebraic number theory, we take $m$ to be either odd or divisible by 4.

For many values of $m$, the conjectured (or proved) densest form ($D_4$, $E_6$, $E_8$, $K_{12}$, $\Lambda_{16}$) appears as a $C_m$-form. This gives new matrix representations of these well-known forms, and is particularly suitable for further computation of their algebraic invariants.

Even with a long reference list, I cannot do justice to those who helped me during the preparation of this article. However, I wish to thank my

Bordeaux colleagues Anne-Marie Bergé and Jacques Martinet, for their help with many crucial points.

For general results on quadratic forms and lattices, we refer to the books by Conway-Sloane [C-S], and Martinet [Mar].

## 2. The Voronoï algorithm

Start with a quadratic form $q(x) = x^t Ax$, with minimum $\underline{m}$, and minimal vectors $\{\pm v_i\}, (1 \leq i \leq s)$. Endow the space $Sym_n(\mathbb{R})$ of symmetric matrices with the Euclidean structure given by $A \cdot B = \mathrm{Trace}(AB)$. Consider the $s$ matrices $V_i = v_i v_i^t$ as elements of the dual space $Sym_n(\mathbb{R})^*$.

The simple observation: $\underline{m} = v_i^t A v_i = \mathrm{Trace}(v_i^t A v_i) = A \cdot V_i$ exhibits the matrix coefficients $a_{ij}$ as a solution of the system of linear equations $A \cdot V_i = \underline{m}$.

The *Voronoï domain* of the matrix $A$, denoted by $\mathcal{D}(A)$, is the convex hull, in $Sym_n(\mathbb{R})^*$, of the rays $\lambda V_i, \lambda \geq 0$; it is a convex polyhedral cone. Its dimension in $Sym_n(\mathbb{R})^*$ is called the *perfection rank* of $A$, its codimension the *default of perfection* of $A$. A perfect form has default zero by definition: the system of equations $X \cdot V_i = \underline{m}$ has $X = A$ as its unique solution. The dual of the Voronoï domain is, by construction, the subset $\{X | X \cdot V_i = v_i^t X v_i \geq 0\}$ of $Sym_n(\mathbb{R})$.

Suppose first that $A$ is not perfect. Then there is a matrix $F \neq 0$ vanishing on all $v_i$. If $|\theta|$ is small enough, all forms $A(\theta) = A + \theta F$ have same minimum $\underline{m}$ and same set of minimal vectors. There are two values $\rho_1, \rho_2 > 0$ (possibly infinite, but not both) such that $A(-\rho_1)$ and $A(\rho_2)$ still have minimum $\underline{m}$, but a strictly larger set of minimal vectors. Consequently, after a finite number of steps, one reaches a perfect form.

If $A$ is perfect, the domain $\mathcal{D}(A)$ is of maximal dimension, and is bounded by faces which are hyperplanes in $Sym_n(\mathbb{R})^*$. Given such a face $\mathcal{F}$, we denote by $F$ the (uniquely defined, up to a positive scalar factor) matrix which is the inner normal to $\mathcal{F}$.

It is convenient, at this stage, to give the practical method for finding all faces of $\mathcal{D}(A)$. A face matrix $F$ has the following algorithmic description: If $S = \{\pm v_i\}$ is the set of minimal vectors of $A$, there is a non-trivial partition $S = S_1 \cup S_2$ satisfying:

- $v_i^t F v_i = 0$ for all $v_i \in S_1$ (the $V_i$ lie in the face $\mathcal{F}$).
- $v_i^t F v_i > 0$ for all $v_i \in S_2$.
- $F$ is unique, up to a positive scalar factor.

The important fact here is that this computation runs entirely in $Sym_n(\mathbb{R})$, though, clearly, the geometric description in $Sym_n(\mathbb{R})^*$ is more convenient for understanding the process.

Take now a perfect form $A$, $F$ one of its face matrices, and consider the form $A(\theta) = A + \theta F$, with $\theta \geq 0$. If $\theta > 0$ is small enough, $A(\theta)$ still has minimum $\underline{m}$, but has default of perfection 1, because, by construction above, its set of minimal vectors is $S_1$. Define $\rho = \sup\ (\theta \mid A(\theta)$ has minimum $\underline{m})$. If $\rho$ is infinite, the matrix $F$ is semi-positive definite, and the face $\mathcal{F}$ is said to be a "cul-de-sac". As was observed in [JCa] , and implicitely used in [Vor], this does not happen in the $Sym_n(\mathbb{R})$ - case, but should be kept in mind in generalizing this process. If $\rho$ is finite, $A(\rho)$ is again a perfect form: the *neighbouring form of* $A$ *along* $\mathcal{F}$.

The neighbouring relation gives the set of perfect forms the structure of a graph, and Voronoï's fundamental result [Vor] asserts that this graph is *connected*. Moreover, the $GL(n,\mathbb{Z})$-equivalence of forms preserves the neighbouring relation, so a quotient graph can be defined. By standard arguments (e.g. Hermite reduction), the quotient graph is *finite*: this is Voronoï 's algorithm.

Besides the finding of all faces of a domain, a time-consuming task, there are three other practical steps needed. We list them for completeness (More on this in [Vor], [JCa], [Mar]):

- Find all minimal vectors.
- Given a face, find the neighbouring form (i.e. find $\rho$).
- Decide $GL(n,\mathbb{Z})$-equivalence between two perfect forms.

If $G$ is a finite subgroup of $GL(n,\mathbb{Z}))$, it is possible to run Voronoï 's algorithm in the linear subspace $\mathcal{T}$ of $G$-invariant forms in $Sym_n(\mathbb{R})$. If $A$ is a $G$-form, its relative Voronoï domain $\mathcal{D}_G(A)$ is then the *orthogonal projection* of $\mathcal{D}(A)$ onto the dual subspace $\mathcal{T}^*$ of $Sym_n(\mathbb{R})^*$. It is proved in [B-M-S] that the resulting neighbourhood graph is *connected*. The finiteness of the quotient graph is more delicate to obtain ($G$-equivalences have to be taken in the subgroup of $GL(n,\mathbb{Z})$ preserving $\mathcal{T}$), and has been proved for $G$-forms in [JCb]. "Culs-de-sac" can appear (see [B-M-S]), and it also happens that the complete graph is already finite. However, for cyclotomic forms, one has the

**Proposition.** *If $G$ is a $\mathbb{Q}$-irreducible subgroup of $GL(n,\mathbb{Z}))$, there are no "culs-de-sac" in running $G$-Voronoï 's algorithm.*

*Proof.* Irreducibility implies that the orbit of any minimal vector spans the whole space. A positive semi-definite form vanishing on a minimal vector must consequently be the zero form. □

## 3. Raw data

We shall separate the lists of cyclotomic forms into three families. In family A, the critical form ($D_4$, $E_6$, $E_8$, $K_{12}$, $\Lambda_{16}$) is cyclotomic. Family B describes $C_p$-perfect forms, with $p$ a prime. The remaining cases are listed in family C.

For each family, the first table gives successively $m$, $\phi(m)$, GP = number of $C_m$-perfect forms, P = number of $C_m$-perfect forms which are also perfect in the ordinary sense, H=Hermite invariant of the densest form, with its Name, if known. The second table gives first $m$, $\phi(m)$, First row, then min, det = minimum, resp. determinant of the densest form, in its smallest integral representative, E, F = number of edges, resp. faces, of its Voronoï domain.

**Theorem A.** *The data for family A are*

| $m$ | $\phi(m)$ | GP | P | H | Name |
|---|---|---|---|---|---|
| 8 | 4 | 1 | 1 | 1.414 | $D_4$ |
| 12 | 4 | 1 | 1 | 1.414 | $D_4$ |
| 9 | 6 | 2 | 2 | 1.665 | $E_6$ |
| 15 | 8 | 1 | 1 | 2.000 | $E_8$ |
| 20 | 8 | 1 | 1 | 2.000 | $E_8$ |
| 24 | 8 | 1 | 1 | 2.000 | $E_8$ |
| 21 | 12 | 8 | 8 | 2.309 | $K_{12}$ |
| 28 | 12 | 13 | 7 | 2.309 | $K_{12}$ |
| 40 | 16 | ? | ? | 2.828 | $\Lambda_{16}$ |
| 60 | 16 | ? | ? | 2.828 | $\Lambda_{16}$ |

| $m$ | $\phi(m)$ | First row | min | det | E | F | Name |
|---|---|---|---|---|---|---|---|
| 8 | 4 | $(2,-1,0,1)$ | 2 | 4 | 3 | 2 | $D_4$ |
| 12 | 4 | $(2,-1,1,0)$ | 2 | 4 | 2 | 2 | $D_4$ |
| 9 | 6 | $(2,1,0,-1,-1,-1)$ | 2 | 3 | 4 | 3 | $E_6$ |
| 15 | 8 | $(2,0,0,0,1,-1,-1,0)$ | 2 | 1 | 8 | 10 | $E_8$ |
| 20 | 8 | $(2,0,0,1,-1,0,1,-1)$ | 2 | 1 | 10 | 10 | $E_8$ |
| 24 | 8 | $(2,1,0,0,1,1,0,-1)$ | 2 | 1 | 9 | 8 | $E_8$ |
| 21 | 12 | $(4,1,-1,-2,1,2,1,-2,-2,-1,1,1)$ | 4 | 729 | 15 | 36 | $K_{12}$ |
| 28 | 12 | $(4,2,1,0,0,0,1,0,-1,0,0,0)$ | 4 | 729 | 21 | 76 | $K_{12}$ |
| 40 | 16 | $((4,-1,0,-1,0,2,-2,1,-2,$ $1,0,-1,2,-1,2,-2)$ | 4 | 256 | 74 | ? | $\Lambda_{16}$ |
| 60 | 16 | $(4,-1,0,2,-1,2,0,0,2,$ $-1,2,1,-2,2,-1,0)$ | 4 | 256 | 52 | ? | $\Lambda_{16}$ |

**Comment.** In the cases with $\Lambda_{16}$, the number of edges of the domain makes the finding of the faces practically impossible.

Before giving the data on family B, let's briefly discuss the Craig lattices $A_n^{(r)}$. These famous lattices are thoroughly investigated in [C-S] and [Mar]. Their direct construction as difference lattices gives them matrices (cf.[C-S] p. 433) which are invariant under the $n$-dimensional representation of $C_{n+1}$

having characteristic polynomial $1+x+\ldots+x^{n-1}+x^n$. The diagonals are constant, and the first row is filled from left and from right with binomial coefficients:

$$\left(\binom{2r}{r} \quad -\binom{2r}{r+1} \quad \binom{2r}{r+2} \quad \cdots \quad \binom{2r}{r+4} \quad -\binom{2r}{r+3} \quad \binom{2r}{r+2}\right)$$

This description is very convenient, but does not show the value of the minimum, whose determination is a difficult combinatorial problem (cf. [Mar] p. 139).

When $n+1$ is a prime $p$, the Craig lattices $A_{p-1}^{(r)}$ are *cyclotomic.* In our range of investigation, their minimum is $2r$, by [Ba-Ba], and their density is pretty high. We shall evidently meet these forms below. In high dimensions, Craig lattices are sometimes the densest known (e.g. p=151, cf [C-S] p. 43), although it is generally accepted that the $C_p$-Hermite constant is lower than the absolute constant. Theorem B below shows that, up to a single, and surprising exception, the densest cyclotomic form is a Craig form.

**Theorem B**. *The data for family B are*

| $m$ | $\phi(m)$ | GP | P | H | $\gamma_n$ | Name |
|---|---|---|---|---|---|---|
| 5 | 4 | 1 | 1 | 1.337 | 1.414 | $A_4^{(1)}$ |
| 7 | 6 | 2 | 2 | 1.511 | 1.665 | $A_6^{(2)}$ |
| 11 | 10 | 5 | 5 | 1.948 | 2.058 | $A_{10}^{(2)}$ |
| 13 | 12 | 25 | 23 | 2.106 | 2.309 | $A_{12}^{(2)}$ |
| 17 | 16 | 1344 | 1333 | 2.513 | 2.828 | New |

| $m$ | $\phi(m)$ | First row | min | det | E | F | Name |
|---|---|---|---|---|---|---|---|
| 5 | 4 | $(2,-1,0,0)$ | 2 | 5 | 2 | 2 | $A_4^{(1)}$ |
| 7 | 6 | $(4,-2,1,-1,-1,1)$ | 4 | $7^3$ | 3 | 3 | $A_6^{(2)}$ |
| 11 | 10 | $(4,-2,0,0,1,-1,-1,1,0,0)$ | 4 | $11^3$ | 10 | 20 | $A_{10}^{(2)}$ |
| 13 | 12 | $(4,-2,0,0,0,1,-1,-1,1,0,0,0)$ | 4 | $13^3$ | 15 | 84 | $A_{12}^{(2)}$ |
| 17 | 16 | $(6,-3,2,-1,-2,2,-3,2,0,$ $0,2,-3,2,-2,-1,2)$ | 6 | $17\cdot 2^{16}$ | 28 | 402 | New |

**Comment**. The Craig form $A_{16}^{(3)}$ is the densest Craig form, with minimum 6 and determinant $17^5$. Our new form is denser, because $2^4 < 17$. The proportion of perfect forms is high, and will be explained below.

For the last family of forms, with the exceptions of $D_8$ (for $C_{16}$) and $D_{16}$ (for $C_{32}$), there are no otherwise known $C_m$-perfect forms. The computation for $C_{32}$ is still under way, but the available data suggest that the densest form has already been found (dense forms tend to have high kissing numbers, and consequently to appear early in the search).

**Theorem C.** *The data for family C are*

| $m$ | $\phi(m)$ | GP | P | H | $\gamma_n$ |
|---|---|---|---|---|---|
| 16 | 8 | 3 | 1 | 1.707 | 2.000 |
| 36 | 12 | 23 | 8 | 2.106 | 2.309 |
| 32 | 16 | $> 4500$ | ? | 2.446 | 2.828 |

| $m$ | $\phi(m)$ | First row | min | det | E | F |
|---|---|---|---|---|---|---|
| 16 | 8 | $(8, 2, -4, -3, 0, 3, 4, -2)$ | 8 | $2^2 \cdot 241^2$ | 5 | 4 |
| 36 | 12 | $(36, 18, 8, -1, -6, 0, 18, 18, 14, 0, -14, -18)$ | 36 | $4463^2 \cdot 5581^2$ | 6 | 6 |
| 32 | 16 | $(12, 5, 0, 3, 4, 3, 0, -4, 0, 4, 0, -3, -4, -3, 0, -5)$ | 12 | $2^2 \cdot 31^2 \cdot 5407^2$ | 21 | 190 |

We close this chapter with a few general facts, gathered from our present sample of ca. 6000 $C_m$-perfect cyclotomic forms. First, in all cases, there is a spanning orbit of minimal vectors, bringing the minimum of the form on the diagonal of the matrix. This seems to be a general fact, but the low dimension, and the triviality of the ideal class group, could contribute to this. Nevertheless, let's formulate this for perfect cyclotomic lattices:

**Conjecture 1.** *Any perfect cyclotomic lattice has a spanning orbit of minimal vectors.*

Being more pessimistic leads to:

**Conjecture 2.** *Any perfect cyclotomic lattice is generated by its minimal vectors.*

Another intriguing fact in our sample is

**Observation 1.** *All perfect cyclotomic forms are even.*

**Comment.** In the case the prime 2 is unramified in the cyclotomic field, then *any* cyclotomic form, perfect or not, is even[1]. In the ramified case, one has to assume $C_m$-perfection, but the fact is unexplained.

[1]This result is due to J. Martinet. The representative element $\alpha$, being real, has an even trace. When 2 is unramified, this property implies that the corresponding lattice is even.

## 4. Two detailed samples

We begin with $C_{28}$, a case appearing in Theorem A. Notations "H", "E", "F", "min", "det" are as above. "No" is the numbering used by the Voronoï algorithm, and is simply used here to locate neighbours. "s" is the half kissing number, and "i" the default of perfection. Nbr gives the list of neighbours. These 13 forms are listed by decreasing H, beginning with $K_{12}$.

**Theorem A28.** *The $C_{28}$-perfect forms are*

| No | H | $s$ | $i$ | E | F | Nbr | min | det |
|---|---|---|---|---|---|---|---|---|
| 5 | 2.309 | 378 | 0 | 21 | 76 | $1^6, 2^3, 4^3, 5^{13}, 6^6, 7^9, 8^6,$ $9^6, 10^6, 11^6, 12^9, 13^3$ | 4 | $3^6$ |
| 7 | 2.091 | 126 | 1 | 8 | 9 | $1^2, 5^3, 8, 9, 12^2$ | 12 | $29^2 \cdot 1231^2$ |
| 1 | 2.073 | 154 | 0 | 9 | 10 | $2, 3^2, 4, 5^2, 6, 7^2, 8$ | 6 | $587^2$ |
| 12 | 2.054 | 112 | 1 | 7 | 8 | $5^3, 6, 7^2, 9, 10$ | 12 | $39703^2$ |
| 4 | 2.045 | 168 | 0 | 9 | 12 | $1^6, 5^6$ | 4 | $2^{6.2}$ |
| 10 | 2.007 | 112 | 1 | 7 | 8 | $2, 3, 5^2, 9^2, 11, 12$ | 8 | $2^{1}2 \cdot 4003^2$ |
| 9 | 2.005 | 112 | 1 | 7 | 8 | $2, 5^2, 7, 10^2, 11, 12$ | 8 | $29^2 \cdot 139^2$ |
| 8 | 1.978 | 84 | 0 | 6 | 6 | $1, 5^2, 7, 11, 13$ | 10 | $3^6 \cdot 617^2$ |
| 3 | 1.978 | 98 | 0 | 6 | 6 | $1^2, 2, 6, 10, 11$ | 10 | $7^2 \cdot 2381^2$ |
| 11 | 1.974 | 84 | 1 | 6 | 6 | $3, 5^2, 8, 9, 10$ | 16 | $3^6 \cdot 10501^2$ |
| 6 | 1.973 | 98 | 0 | 6 | 6 | $1, 2, 3, 5^2, 12$ | 6 | $7^2 \cdot 113^2$ |
| 13 | 1.928 | 84 | 7 | 6 | 6 | $5^3, 8^3$ | 8 | $3^{12} \cdot 7^2$ |
| 2 | 1.915 | 98 | 0 | 6 | 6 | $1, 3, 5, 6, 9, 10$ | 4 | $83^2$ |

The next example is $C_{13}$, contained in Theorem B. The Craig forms appear, and one can observe, contrary to the preceeding case, the high proportion of perfect forms.

**Theorem B13.** *The $C_{13}$-perfect forms are*

| No | H | $s$ | $i$ | E | F | Nbr | min | det | Name |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 2.106 | 195 | 0 | 15 | 84 | $1^6, 3^6, 4^6, 5^6, 6^6,$ $7^6, 8^6, 9^6, 10^{12},$ $11^6, 12^{12}, 13^6$ | 4 | $13^3$ | $A_{12}^{(2)}$ |
| 16 | 2.060 | 156 | 0 | 10 | 18 | $5^6, 9^6, 14^6$ | 6 | $13^5$ | $A_{12}^{(3)}$ |
| 14 | 2.010 | 78 | 0 | 6 | 6 | $3, 4, 10, 11, 15, 16$ | 28 | $13 \cdot 5^4 \cdot 81043^2$ | |
| 4 | 2.005 | 78 | 0 | 6 | 6 | $2, 5, 6, 12^2, 14$ | 16 | $13 \cdot 71527^2$ | |
| 11 | 1.997 | 78 | 0 | 6 | 6 | $2, 3, 5, 12, 14, 15$ | 24 | $13 \cdot 103^2 \cdot 8111^2$ | |
| 5 | 1.996 | 78 | 0 | 6 | 6 | $2, 4, 9, 10, 11, 16$ | 32 | $13 \cdot 4698461^2$ | |
| 20 | 1.994 | 78 | **12** | 6 | 6 | $7, 9, 13, 18, 19, 23$ | **78** | $13 \cdot 53^2 \cdot 79^2$ $\cdot 236783^2$ | |
| 12 | 1.992 | 91 | 0 | 7 | 10 | $2^2, 4^2, 6, 10, 11,$ $17, 21, 25$ | 12 | $13 \cdot 13259^2$ | |

| No | H | $s$ | $i$ | E | F | Nbr | min | det | Name |
|---|---|---|---|---|---|---|---|---|---|
| 15 | 1.985 | 78 | 0 | 6 | 6 | $3,6,7,11,14,18$ | 18 | $13\cdot 154127^2$ | |
| 3 | 1.983 | 78 | 0 | 6 | 6 | $7,9,11,13,14,15$ | 20 | $13\cdot 103^2\cdot 2833^2$ | |
| 19 | 1.981 | 78 | 0 | 6 | 6 | $7,13,17,18^2,20$ | 24 | $13\cdot 877109^2$ | |
| 10 | 1.980 | 78 | 0 | 6 | 6 | $2^2,5,12,13,14$ | 24 | $13\cdot 879113^2$ | |
| 6 | 1.975 | 78 | 0 | 6 | 6 | $2,4,7,12,15,17$ | 24 | $13\cdot 891983^2$ | |
| 18 | 1.972 | 78 | 0 | 6 | 6 | $7,15,17,19^2,20$ | 16 | $13^5\cdot 467^2$ | |
| 13 | 1.964 | 78 | 0 | 6 | 6 | $2,3,10,19,20,22$ | 42 | $13\cdot 467^2\cdot 56731^2$ | |
| 7 | 1.963 | 78 | 0 | 6 | 6 | $2,6,15,18,19,20$ | 14 | $13\cdot 36451^2$ | |
| 23 | 1.949 | 78 | **12** | 6 | 6 | $8,20,21,22^2,24$ | **26** | $13\cdot 1093^2\cdot 1429^2$ | |
| 22 | 1.932 | 78 | 0 | 6 | 6 | $8,13,21,23^2,24$ | 18 | $13\cdot 181193^2$ | |
| 17 | 1.929 | 78 | 0 | 6 | 6 | $6,12,18,19,24,25$ | 12 | $13\cdot 16067^2$ | |
| 21 | 1.926 | 78 | 0 | 6 | 6 | $8,12,22,23,24^2$ | 24 | $13\cdot 443^2\cdot 2341^2$ | |
| 24 | 1.926 | 78 | 0 | 6 | 6 | $8,17,21^2,22,23$ | 16 | $13\cdot 91079^2$ | |
| 9 | 1.901 | 78 | 0 | 6 | 6 | $2,3,5,8,16,20$ | 12 | $13\cdot 17551^2$ | |
| 8 | 1.889 | 91 | 0 | 7 | 12 | $2^2,9^2,21^2,22^2,$ $23^2,24^2$ | 4 | $13\cdot 5^4$ | |
| 25 | 1.865 | 78 | 0 | 6 | 6 | $12^3,17^3$ | 4 | $13\cdot 3^6$ | |
| 1 | 1.615 | 78 | 0 | 6 | 6 | $2^6$ | 2 | 13 | $A_{12}^{(1)}$ |

**Comment.** There are two non-perfect forms in this list, both with a default of perfection of 12, and both with a minimum divisible by 13. Similarly, in the list of 1344 $C_{17}$-perfect forms, one finds 11 non-perfect forms, all with a default of perfection of 16, and a minimum divisible by 17. This suggests

**Observation 2.** *The default of perfection of a $C_p$-perfect form is divisible by $(p-1)$.*

**Observation 3.** *The minimum of an integral $C_p$-perfect, non-perfect $C_p$-form is divisible by $p$.*

Observation 2 was first proved by J. Martinet (unpublished). Here is a more general result (proof of my own) settling the claim:

**Lemma.** *Let $A$ be the matrix of a positive cyclotomic form. Call $\delta(A)$, resp. $\delta_p(A)$ its default of perfection, resp. default of $C_p$-perfection. Then $\delta(A)-\delta_p(A)$ is divisible by $(p-1)$.*

*Proof.* The group $C_p$ acts on $\mathcal{D}(A)$, fixing $\mathcal{D}_p(A)$. As any fixpoint-free rational representation of $C_p$ has dimension divisible by $(p-1)$, the codimension of $\mathcal{D}_p(A)$ in $\mathcal{D}(A)$ is divisible by $(p-1)$. Hence $(p(p-1)/2-\delta(A))-((p-1)/2-\delta_p(A))$ is divisible by $(p-1)$. The lemma follows. □

Observation 3 remains, at present, at the botanical stage. An argument in favour is the fact that the orthogonal projection of $\mathcal{D}(A)$ on $\mathcal{D}_p(A)$ is the average on orbits, i.e. division by $p$.

## 5. Final remarks

Our definition of cyclotomic forms is not as general as is used in algebraic number theory, where it means Trace($\alpha x\bar{x}$) on an ideal $\mathcal{I}$ of rank one in $\mathbb{Q}(\zeta_m)$. This general description is very convenient, as is illustrated with the Craig forms $A_{p-1}^{(r)}$, which are obtained with $\alpha = \frac{1}{p}$ and $\mathcal{I} = \mathcal{P}^r$ ($\mathcal{P} = (1-\zeta_p)$). Further, our densest $C_{17}$-form was identified by J. Martinet: $\alpha = \frac{1}{p}$ and $\mathcal{I} = \mathcal{P}^{-7}\mathcal{Q}$, where $\mathcal{Q}$ is an ideal such that $\mathcal{Q}\bar{\mathcal{Q}} = (2)$. It is denser than $A_{16}^{(3)}$ because $2^8 < 17^2$: this ultimately boils down to the fact that 17 is a Fermat prime ! Voronoï's algorithm does not fit well in this context, because it runs under a *fixed* representation of the group $C_m$. In presence of exotic cyclotomic representations, one has to rerun the algorithm entirely, only changing the matrix $G$ generating the representation at the beginning of the program. There is therefore a cyclotomic Hermite constant for each pair of conjugate ideals in the ideal class group of $\mathbb{Q}(\zeta_m)$. Twisting forms with an ideal can only increase the Hermite constant, and looking at the results of [Ba-Ba] on $C_{23}$, one deduces for example: for the standard cyclotomic representation, the presumably densest form is $A_{22}^{(4)}$ with a Hermite invariant of 2.94..; twisting with one of the exotic representations has the effect of doubling the minimum 2 of $A_{22}^{(1)}$ to 4, giving it an invariant of 3.46... As the presumed $\gamma_{22}$ is 3.57.., this shows that $C_p$-cyclotomic forms can become very dense. However, all cases treated in this paper have a trivial ideal class group, and the Hermite invariant of the densest $C_m$-form can safely be called the *cyclotomic Hermite constant.*

We did not include results on eutaxy in this paper. One reason is that eutaxy is an absolute notion (a cyclotomic form is $C_m$-eutactic iff it is eutactic). But in view of the very interesting recent results on the classification of eutactic forms (cf [Mar], chap. IX,4), there is no doubt that the study of cyclotomic eutactic forms will prove fruitful.

## References


[Ba-Ba] C. BACHOC, C. BATUT, *Etude algorithmique de réseaux construits avec la forme trace.* J. Exp. Math. **1** (1992), 183–190.

[Bay-M] E. BAYER-FLUCKIGER, J. MARTINET, *Formes quadratiques liées aux algèbres semi-simples.* J. reine angew. Math. **451** (1994), 51–69.

[B-M] A.-M. BERGÉ, J. MARTINET, *Réseaux extrêmes pour un groupe d'automorphismes.* Astérisque **198-200** (1992), 41–66.

[B-M-S] A.-M. BERGÉ, J. MARTINET, F. SIGRIST, *Une généralisation de l'algorithme de Voronoï pour les formes quadratiques.* Astérisque **209** (1992), 137–158.

[C-S] J.H. CONWAY, N.J.A. SLOANE, *Sphere Packings, Lattices, and Groups.* Springer-Verlag (1992).

[JCa] D.-O. JAQUET-CHIFFELLE, *Enumération complète des classes de formes parfaites en dimension* 7. Ann. Inst. Fourier **43** (1993), 21–55.

[JCb] D.-O. JAQUET-CHIFFELLE, *Trois théorèmes de finitude pour les G-formes.* J. Théor. Nombres Bordeaux **7** (1995), 165–176.

[Mar] J. MARTINET, *Les réseaux parfaits des espaces euclidiens.* Masson (1996).

[Vor] G. VORONOÏ, *Sur quelques propriétés des formes quadratiques positives parfaites.* J. reine angew. Math. **133** (1908), 97–178.

François SIGRIST
Institut de Mathématiques
Université de Neuchâtel
Rue Emile Argand 11
CH-2007 Neuchâtel
Switzerland
*E-mail* : francois.sigrist@maths.unine.ch