Reduction and Minkowskian sublattices

Jacques Martinet

Université de Bordeaux, IMB

Caen, June 4th, 2010

Colloquium for Brigitte Vallée's birthday

This talk relies on recent joint work with
Achill SCHÜRMANN and Wolfgang KELLER (Delft, Magdeburg)

An example

Consider first $\mathbb{Z}^n$, viewed as a Euclidean lattice, equipped with its canonical (orthonormal) basis $(\varepsilon_1, \ldots, \varepsilon_n)$, next the *centred cubic lattice*

$$C_n = \mathbb{Z}^n \cup \frac{\varepsilon_1 + \cdots + \varepsilon_n}{2},$$

for some large value of n, for instance, $n = 100$.
To construct a basis for C_{100}, we *may* take 99 very short vectors, of norm $x \cdot x$ $(= \|x\|^2$, the squared length) equal to 1, and at least one vector of norm $N \geq 100$.

An example

Consider first $\mathbb{Z}^n$, viewed as a Euclidean lattice, equipped with its canonical (orthonormal) basis $(\varepsilon_1, \ldots, \varepsilon_n)$, next the *centred cubic lattice*

$$C_n = \mathbb{Z}^n \cup \frac{\varepsilon_1 + \cdots + \varepsilon_n}{2},$$

for some large value of n, for instance, $n = 100$.
To construct a basis for C_{100}, we *may* take 99 very short vectors,
of norm $x \cdot x$ $(= \|x\|^2$, the squared length) equal to 1,
and at least one vector of norm $N \geq 100$.

Thus when working with vectors up to the minimal norm which allows us to construct a basis, we meet a huge number of useless vectors of norm $2, 3, \ldots, 99$.

Better consider C_{100} as a lattice containing to index 2 the "easy" lattice $\mathbb{Z}^n$!

An example

Consider first $\mathbb{Z}^n$, viewed as a Euclidean lattice, equipped with its canonical (orthonormal) basis $(\varepsilon_1, \ldots, \varepsilon_n)$, next the *centred cubic lattice*

$$C_n = \mathbb{Z}^n \cup \frac{\varepsilon_1 + \cdots + \varepsilon_n}{2},$$

for some large value of n, for instance, $n = 100$.
To construct a basis for C_{100}, we *may* take 99 very short vectors, of norm $x \cdot x$ $(= \|x\|^2$, the squared length) equal to 1, and at least one vector of norm $N \geq 100$.

Thus when working with vectors up to the minimal norm which allows us to construct a basis, we meet a huge number of useless vectors of norm $2, 3, \ldots, 99$.

Better consider C_{100} as a lattice containing to index 2 the "easy" lattice $\mathbb{Z}^n$!

The remaining of the talk is devoted to *Watson's index theory*. I shall explain the relations which exist between the point of views of bases (HERMITE) and of successive minima (MINKOWSKI).

This talk owes much to recent joint work with Achill SCHÜRMANN (Magdeburg, now in Delft).

References (General results)

[Wat] G.L. Watson, *On the minimum points of a positive quadratic form*, Mathematika **18** (1971), 60–70.

[Ryš] Ryshkov, S. S., *On the problem of the determination of quadratic forms in many variables*, Proc. Steklov Inst. Math. **142** (1979), 233–259 ; Russian original: 1976.

[Za] N.V. Zahareva, *Centerings of* 8*-dimensional lattices that preserve a frame of successive minima*, Proc. Steklov Inst. Math. **152** (1982), 107–134 ; Russian original: 1980.

References (General results)

[Wat] G.L. Watson, *On the minimum points of a positive quadratic form*, Mathematika **18** (1971), 60–70.

[Ryš] Ryshkov, S. S., *On the problem of the determination of quadratic forms in many variables*, Proc. Steklov Inst. Math. **142** (1979), 233–259 ; Russian original: 1976.

[Za] N.V. Zahareva, *Centerings of 8-dimensional lattices that preserve a frame of successive minima*, Proc. Steklov Inst. Math. **152** (1982), 107–134 ; Russian original: 1980.

Complete results in dimension 8 ([Mar1]) and 9 ([K-M-S])

[Mar1] J. Martinet, *Sur l'indice d'un sous-réseau* (with an appendix by C. Batut), in Réseaux euclidiens, designs sphériques et formes modulaires, L'Ens. Math., Monographie **37**, Genève (2001), 163–211.

[K-M-S] W. Keller, J. Martinet, A. Schürmann, *On classifying Minkowskian sublattices*, arXiv:0904.3110v1; see also my homepage.

References (Applications)

On Louis Michel's problem

[Mar2] J. Martinet, *Bases of minimal vectors in Euclidean lattices, I* Archiv Math. **89** (2007), 404–410.

[M-S] J. Martinet, A. Schürmann, *Bases of minimal vectors in Euclidean lattices, III*, in preparation.

References (Applications)

On Louis Michel's problem

[Mar2] J. Martinet, *Bases of minimal vectors in Euclidean lattices, I* Archiv Math. **89** (2007), 404–410.

[M-S] J. Martinet, A. Schürmann, *Bases of minimal vectors in Euclidean lattices, III*, in preparation.

On a problem of van der Waerden

[vdW] B. L. van der Waerden, *Die Reduktionstheorie der positiven quadratischen Formen*, Acta Math. **96** (1956), 265–309.

[Mar3] J. Martinet, *Hermite versus Minkowski*, preprint, November 2007.

Bases (Hermite)

For any basis $\mathcal{B} = (e_1, \ldots, e_n)$ of Λ, let

$$H_{\mathcal{B}}(\Lambda) = \left(\frac{N(e_1) \ldots N(e_n)}{\det(\Lambda)} \right)^{1/n} \quad \text{and} \quad H(\Lambda) = \min_{\mathcal{B}} H_{\mathcal{B}}(\Lambda);$$

$H(\Lambda)$ only depends on the similarity class of Λ.

Bases (Hermite)

For any basis $\mathcal{B} = (e_1, \ldots, e_n)$ of Λ, let

$$H_{\mathcal{B}}(\Lambda) = \left(\frac{N(e_1) \ldots N(e_n)}{\det(\Lambda)} \right)^{1/n} \quad \text{and} \quad H(\Lambda) = \min_{\mathcal{B}} H_{\mathcal{B}}(\Lambda);$$

$H(\Lambda)$ only depends on the similarity class of Λ.

Theorem

(HERMITE, # 1850) *We have* $H(\Lambda) \leq \left(\frac{4}{3}\right)^{(n-1)/2}$.

Bases (Hermite)

For any basis $\mathcal{B} = (e_1, \ldots, e_n)$ of Λ, let

$$H_{\mathcal{B}}(\Lambda) = \left(\frac{N(e_1) \ldots N(e_n)}{\det(\Lambda)} \right)^{1/n} \quad \text{and} \quad H(\Lambda) = \min_{\mathcal{B}} H_{\mathcal{B}}(\Lambda) ;$$

$H(\Lambda)$ only depends on the similarity class of Λ.

Theorem

(HERMITE, # 1850) *We have* $H(\Lambda) \leq \left(\frac{4}{3}\right)^{(n-1)/2}$.

We may now define the *Hermite invariant* and the *Hermite constant* by

$$\gamma(\Lambda) = \frac{\min \Lambda}{\det(\Lambda)^{1/n}} \quad \text{and} \quad \gamma_n = \sup_{\dim \Lambda = n} \gamma(\Lambda) .$$

Corollary

(HERMITE, August 6th, 1845) *We have the* (exponential) *bound* $\gamma_n \leq \left(\frac{4}{3}\right)^{(n-1)/2}$.

Successive minima (Minkowski)

MINKOWSKI proved two fundamental results concerning the questions above; they can be read in his 1896 book *Geometrie der Zahlen*.

For any system $\mathcal{B}$ of *independent* vectors $f_1, \ldots, f_n$ of Λ, let

$$M_{\mathcal{B}}(\Lambda) = \left(\frac{N(f_1) \ldots N(f_n)}{\det(\Lambda)} \right)^{1/n} \quad \text{and} \quad M(\Lambda) = \min_{\mathcal{B}} M_{\mathcal{B}}(\Lambda) \, ;$$

thus we consider vectors of Λ which constitute a basis for E, but not necessarily for Λ.

Successive minima (Minkowski)

MINKOWSKI proved two fundamental results concerning the questions above; they can be read in his 1896 book *Geometrie der Zahlen*.

For any system $\mathcal{B}$ of *independent* vectors $f_1, \ldots, f_n$ of Λ, let

$$M_{\mathcal{B}}(\Lambda) = \left(\frac{N(f_1) \ldots N(f_n)}{\det(\Lambda)} \right)^{1/n} \quad \text{and} \quad M(\Lambda) = \min_{\mathcal{B}} M_{\mathcal{B}}(\Lambda) ;$$

thus we consider vectors of Λ which constitute a basis for E, but not necessarily for Λ.

Theorem

$M(\Lambda) \leq \gamma_n$.

Theorem

There exist linear bounds for γ_n *(a* universal bound *is* $\gamma_n \leq 1 + \frac{n}{4}$*).*

This last statement was obtained by a *density argument*, which applies to all sphere packings.

Our knowledge on the Hermite constants

Known exact values were obtained by the following authors.
- $n = 2$: Lagrange; $n = 3$: Gauss;
- $n = 4, 5$: Korkine & Zolotareff (1877);
- $n = 6, 7, 8$: Blichfeldt (1935);
- $n = 24$: Cohn & Kumar (2007); Ann. of Math (2010).

In each case, they are attained on exactly **one** lattice (up to similarity).

For $9 \leq n \leq 23$ and $25 \leq n \leq 36$, the best bounds are those of Cohn & Elkies, published in Ann. of Math (2003), improving on the 1957 Rogers' bounds. (Their bounds apply for arbitrary sphere packings and all $n \in [4, 36]$.)

For applications to index theory, we shall need bounds for $\gamma_n^{n/2}$ (proportional to the density of the associated sphere packing).

The index problem

Let Λ be an n-dimensional lattice. Denote by Λ' the sublattice of Λ generated by representatives $f_1, \ldots, f_n$ of the successive minima of Λ.

Question

(1) What is the maximal index $\imath(\Lambda) = \max[\Lambda : \Lambda']$ *? [As a function of* n*.]*

The index problem

Let Λ be an n-dimensional lattice. Denote by Λ' the sublattice of Λ generated by representatives $f_1, \ldots, f_n$ of the successive minima of Λ.

Question

(1) What is the maximal index $\imath(\Lambda) = \max[\Lambda : \Lambda']$? [As a function of n.]

Question

(2) What are the possible structures for Λ/Λ' ?

The index problem

Let Λ be an n-dimensional lattice. Denote by Λ' the sublattice of Λ generated by representatives $f_1, \ldots, f_n$ of the successive minima of Λ.

Question

(1) What is the maximal index $\imath(\Lambda) = \max[\Lambda : \Lambda']$ *? [As a function of n.]*

Question

(2) What are the possible structures for Λ/Λ' ?

Denote by d the *annihilator* of Λ/Λ'. Choose a basis $(e_1, \ldots, e_n)$ for Λ, and write

$$e_i = \frac{\sum_{j=1}^{n} a_j^{(i)} f_j}{d} .$$

The $(a_1^{(i)}, a_2^{(i)}, \ldots, a_n^{(i)})$ are codewords which generate a $\mathbb{Z}/d\mathbb{Z}$-code $\mathcal{C}$ of length n. Up to equivalence, $\mathcal{C}$ depends only on the pair (Λ, Λ').

Question

(3) What is the (finite) list of codes afforded by Λ/Λ' ?

A deformation argument

We say that a lattice L is well rounded if its minimal vectors span E.
It is proved in [Mar1] that any lattice Λ can be continuously transformed by elements of $\mathrm{GL}(E)$ into a well-rounded lattice $u(\Lambda)$, using transformations which preserve the set of quotients Λ/Λ'.
From now on, we assume that (Λ) *is well rounded*.
Scaling lattices to minimum 1, we have $\det(\Lambda) \leq 1$ (by Hadamard), $\det(\Lambda) \geq \gamma_n^n$ (by the definition of γ_n), and $\det(\Lambda') = [\Lambda : \Lambda']^2 \det(\Lambda)$, whence

Proposition

$$[\Lambda : \Lambda'] \leq \gamma_n^{n/2}$$

A deformation argument

We say that a lattice L is well rounded if its minimal vectors span E.
It is proved in [Mar1] that any lattice Λ can be continuously transformed by elements of $\mathrm{GL}(E)$ into a well-rounded lattice $u(\Lambda)$, using transformations which preserve the set of quotients Λ/Λ'.
From now on, we assume that (Λ) *is well rounded*.
Scaling lattices to minimum 1, we have $\det(\Lambda) \leq 1$ (by Hadamard), $\det(\Lambda) \geq \gamma_n^n$ (by the definition of γ_n), and $\det(\Lambda') = [\Lambda : \Lambda']^2 \det(\Lambda)$, whence

Proposition

$$[\Lambda : \Lambda'] \leq \gamma_n^{n/2}$$

A complete answer to the questions of the previous slide has been obtained (in [Mar1] and [M-S]) for all $n \leq 9$. A consequence is that equality holds for $n \leq 8$ (and for $n = 24$), but that the inequality is strict for $n = 9$.

Strict inequality is expected in dimension 10 (and . . .).

Numerical results ($n = 1$–$8, 24$)

n	≤ 3	4	5	6	7	8	24
$\gamma_n^{n/2}$	< 2	2	2.8...	4.6...	8	16	2^{24}
$\lfloor \gamma_n^{n/2} \rfloor$	1	2	2	4	8	16	2^{24}
$\imath_{\max}$	1	2	2	4	8	16	2^{24}
restricted *	1	1	2	3	4	8	$< 2^{24}$

$(^*)$: $\Lambda \neq \mathbb{D}_4, \mathbb{D}_6, \mathbb{E}_7, \mathbb{E}_8, \Lambda_{24}$

Definition

The *index system* $\mathcal{I}(\Lambda)$ of Λ is the set of quotients Λ/Λ' ; $\mathcal{I}_n = \cup_{\dim \Lambda = n} \mathcal{I}(\Lambda)$.
(Notation: 4 for "cyclic", 2^2 for "2-elementary", ...)

Examples

(1) $\mathcal{I}_4 = \mathcal{I}(\mathbb{D}_4) = \{1, 2\}$;
(2) $\mathcal{I}_7 = \mathcal{I}(\mathbb{E}_7) = \{1, 2, 3, 4, 2^2, 2^3\}$;
(3) $\mathcal{I}_8 = \mathcal{I}(\mathbb{E}_8) = \{1, 2, 3, 4, 2^2, 2^3, 5, 6, 4 \cdot 2, 2^3, 3^2, 2^4\}$.
(4) For $n = 6$, $\imath(\Lambda) = 4 \Longleftrightarrow \Lambda \sim \mathbb{D}_6$, but $\mathcal{I}(\mathbb{D}_6) = \{1, 2, 2^2\}$,
whereas $\mathcal{I}(\mathbb{E}_6) = \{1, 2, 3\}$. $\Longrightarrow$ "No *universal lattice* in dimension 6".

Numerical results and conjectures ($n = 9, 10, 11$)

n	9	10	11
$\lfloor \gamma_n^{n/2} \rfloor \leq$	30.2...	59.4...	121.48...
$\lfloor \gamma_n^{n/2} \rfloor \leq$ (??) *	22.62...	36.95...	65.6...
$\ell_{\max}$	16	32 ??	64 ??

(*): $\Lambda_9, \Lambda_{10}, K_{11}$

Numerical results and conjectures ($n = 9, 10, 11$)

n	9	10	11
$\lfloor \gamma_n^{n/2} \rfloor \leq$	30.2...	59.4...	121.48...
$\lfloor \gamma_n^{n/2} \rfloor \leq$ (??) *	22.62...	36.95...	65.6...
$\imath_{\max}$	16	32 ??	64 ??

(*): $\Lambda_9, \Lambda_{10}, K_{11}$

Some results for dimension 9:

$$\mathcal{I}(\Lambda_9) = \{1, 2, 3, 4, 2^2, 5, 6, 7, 8, 4.2, 2^3, 9, 3^2, 10, 12, 6 \cdot 2, 4 \cdot 2^2, 2^4\};$$

$$\mathcal{I}_9 = \mathcal{I}(\Lambda_9) \cup \{4^2\}.$$

Three perfect lattices play a special rôle: Λ_9, and two up to now not noticed lattices we name L_{81} and L_{99} (the index is s, the number of pairs of minimal vectors).

Computation of $\mathcal{I}(\Lambda)$

(1) *Naive calculation.* Consider all sets of n minimal vectors, keep those of rank n, and calculate the structure of the corresponding quotient Λ/Λ'.

Complexity: roughly $\binom{s}{n}$. Works for $n \leq 8$ except $\mathbb{E}_8$. $\left(\binom{s}{n} \leq \binom{75}{8}\#1.7 \cdot 10^{10}.\right)$

(2) $\mathbb{E}_8$. Classification of root systems. $\left(\binom{s}{n} = \binom{120}{8}\#1.8 \cdot 10^{11} >>.\right)$

(3) Λ_9. **Luck** ! In the course of the classification of codes, all quotients except 4^2 either exist for $n \leq 8$ or occur with Λ_9, and $4^2 \in \mathcal{I}(L) \Longleftrightarrow L \sim L_{81}$.

(4) L_{81}, L_{99}. Solved by Mathieu DUTOUR SIKIRIĆ in Zagreb.
(Note that $\binom{99}{9}\#1.7 \cdot 10^{12}$, but that for Λ_9, we have $\binom{136}{9}\#3.3 \cdot 10^{13}$.)

General computations

In [K-M-S], we made use of linear programming packings under *MAGMA* and of *PARI* for various complements. Codes over $\mathbb{F}_2$, $\mathbb{F}_3$, and $\mathbb{Z}/4\mathbb{Z}$ were dealt with using essentially hand calculations. For cyclic quotients of order $m \in [6, 30]$ as well as for codes over $\mathbb{F}_5$, we made use of *MAGMA*. Calculations were often shortened using convenient identities, notably of WATSON.

There are 137 *codes in dimension* 9*, whereas only* 42 *codes exist in dimensions* $n \leq 8$ *all together.*

Cyclic quotients

d	generator	s	r	s'
2	(1,1,1,1,1,1,1,1,1)	9	9	9
3	(1,1,1,1,1,1,1,1,1)	9	9	9
4	(1,1,1,1,1,1,1,1,1)	9	9	9
4	(1,1,1,1,1,1,1,1,2)	9	9	9
4	(1,1,1,1,1,1,1,2,2)	9	9	9
4	(1,1,1,1,1,1,2,2,2)	9	9	9
4	(1,1,1,1,1,2,2,2,2)	9	9	9
4	(1,1,1,1,2,2,2,2,2)	17	15	9
5	(1,1,1,1,1,1,1,1,2)	18	17	9
5	(1,1,1,1,1,1,1,2,2)	9	9	9
5	(1,1,1,1,1,1,2,2,2)	9	9	9
5	(1,1,1,1,1,2,2,2,2)	9	9	9
6	(1,1,1,1,1,1,2,2,2)	18	17	9
6	(1,1,1,1,1,2,2,2,2)	9	9	9
6	(1,1,1,1,2,2,2,2,2)	23	20	9
6	(1,1,1,1,1,1,1,2,3)	27	25	9
6	(1,1,1,1,1,1,2,2,3)	9	9	9
6	(1,1,1,1,1,2,2,2,3)	9	9	9
6	(1,1,1,1,2,2,2,2,3)	9	9	9
6	(1,1,1,2,2,2,2,2,3)	17	15	9
6	(1,1,1,1,1,1,1,3,3)	9	9	9
6	(1,1,1,1,1,1,2,3,3)	9	9	9
6	(1,1,1,1,1,2,2,3,3)	9	9	9
6	(1,1,1,1,2,2,2,3,3)	9	9	9
6	(1,1,1,2,2,2,2,3,3)	9	9	9
6	(1,1,2,2,2,2,2,3,3)	17	15	9
6	(1,1,1,1,1,1,3,3,3)	15	14	9
6	(1,1,1,1,1,2,3,3,3)	23	20	9
6	(1,1,1,1,2,2,3,3,3)	15	14	9
6	(1,1,1,2,2,2,3,3,3)	15	14	9
6	(1,1,2,2,2,2,3,3,3)	15	14	9
6	(1,2,2,2,2,2,3,3,3)	23	20	9
7	(1,1,1,1,1,2,2,2,3)	33	31	9
7	(1,1,1,1,2,2,2,2,3)	18	17	9
7	(1,1,1,1,1,1,2,3,3)	136	45	24
7	(1,1,1,1,1,2,2,3,3)	9	9	9
7	(1,1,1,1,2,2,2,3,3)	9	9	9
7	(1,1,1,1,1,2,3,3,3)	30	26	9
7	(1,1,1,1,2,2,3,3,3)	9	9	9

d	generator	s	r	s'
7	(1,1,1,2,2,2,3,3,3)	18	17	9
8	(1,1,1,1,2,2,2,3,3)	136	45	18
8	(1,1,1,2,2,2,2,3,3)	9	9	9
8	(1,1,2,2,2,2,2,3,3)	35	28	9
8	(1,1,1,2,2,2,3,3,3)	50	37	12
8	(1,1,1,1,1,2,2,3,4)	136	45	19
8	(1,1,1,1,2,2,2,3,4)	40	34	9
8	(1,1,1,2,2,2,2,3,4)	37	32	9
8	(1,1,1,1,2,2,3,3,4)	25	24	9
8	(1,1,1,2,2,2,3,3,4)	9	9	9
8	(1,1,2,2,2,2,3,3,4)	17	15	9
8	(1,1,1,1,2,3,3,3,4)	31	29	9
8	(1,1,1,2,2,3,3,3,4)	27	25	9
8	(1,1,1,1,3,3,3,3,4)	34	30	9
8	(1,1,1,1,2,2,3,4,4)	32	28	9
8	(1,1,1,2,2,2,3,4,4)	38	29	9
8	(1,1,1,1,2,3,3,4,4)	42	34	10
8	(1,1,1,2,2,3,3,4,4)	9	9	9
8	(1,1,2,2,2,3,3,4,4)	33	27	9
8	(1,1,1,2,3,3,3,4,4)	23	21	9
9	(1,1,1,2,2,2,3,3,4)	84	43	13
9	(1,1,1,2,2,3,3,3,4)	50	37	10
9	(1,1,1,1,2,3,3,4,4)	136	45	16
9	(1,1,1,2,2,3,3,4,4)	53	37	10
9	(1,1,1,2,3,3,3,4,4)	31	27	9
9	(1,1,2,2,3,3,3,4,4)	15	14	9
10	(1,1,2,2,2,2,3,3,5)	136	45	16
10	(1,1,2,2,2,2,3,4,5)	136	45	16
10	(1,1,2,2,2,3,3,4,5)	64	40	10
10	(1,1,1,2,2,3,4,4,5)	136	45	13
10	(1,1,2,2,2,3,4,4,5)	51	36	9
10	(1,1,2,2,3,3,4,4,5)	43	39	9
10	(1,1,1,2,3,4,4,4,5)	84	43	12
10	(1,1,2,2,3,4,4,4,5)	53	37	9
12	(1,1,2,3,3,4,4,5,6)	136	45	12
12	(1,1,3,3,4,4,5,5,6)	136	45	12
12	(1,2,2,3,3,3,4,4,5)	136	45	13
12	(1,2,2,3,3,4,4,5,6)	87	42	10

The problem of Louis Michel

Question (Louis MICHEL, circa 1990): *Does a lattice which is generated by its minimal vectors have a basis of minimal vectors?*

Counter-example (CONWAY and SLOANE,1995). *In all dimensions $n \geq 11$, there exist lattices generated by their minimal vectors, but without any basis of minimal vectors.*

Theorem (J.M., 2007). *Assume that Λ is generated by its minimal vectors, and that either $n \leq 8$, or $n \leq 10$ and $\imath(\Lambda) \leq 4$.*
Then Λ has a basis of minimal vectors.

The proof is by examination of all possible codes associated with pairs (Λ, Λ') as above. Easy for "small" and for "large" index!

$$\Longrightarrow \text{Counter-examples need } n \geq 9 \text{ and } \imath \geq 5.$$

The problem of Louis Michel

Question (Louis MICHEL, circa 1990): *Does a lattice which is generated by its minimal vectors have a basis of minimal vectors?*

Counter-example (CONWAY and SLOANE,1995). *In all dimensions $n \geq 11$, there exist lattices generated by their minimal vectors, but without any basis of minimal vectors.*

Theorem (J.M., 2007). *Assume that Λ is generated by its minimal vectors, and that either $n \leq 8$, or $n \leq 10$ and $\imath(\Lambda) \leq 4$.*
Then Λ has a basis of minimal vectors.

The proof is by examination of all possible codes associated with pairs (Λ, Λ') as above. Easy for "small" and for "large" index!

$$\Longrightarrow \text{Counter-examples need } n \geq 9 \text{ and } \imath \geq 5.$$

Theorem (J.M. & Achill SCHÜRMANN, 2009).

1. *Every lattice of dimension $n \leq 9$ which is generated by its minimal vectors has a basis of minimal vectors.*
2. *There exist a 10-dimensional lattice of maximal index $\imath = 5$, generated by its minimal vectors, but without a basis of minimal vectors.*

The problem of Louis Michel (continuation)

The **Proof** is again a case-by-case proof, using the classification of 9-dimensional $\mathbb{Z}/d\mathbb{Z}$-codes.

- $i \leq 4$: nothing to prove.
- $i \geq 10$: the existence of a basis of minimal vectors is automatic.
- $i = 9, 8, 7$: we use the existence of generators.
- $i = 5$: thanks to a computer calculation, we were able to guess an identity which allowed us to write down a "by hand" proof.
- Taking for granted the classification, we were thus able to write down a handy-computational proof for any $i \neq 6$.
- Finally only the case of index 6 was dealt with in a purely computational way. Main problem: 6 is not a prime power !

Hermite vs Minkowski. 1. The question

We return to the comparison of bases and successive minima, that is we want to compare the product $m(\Lambda)$:

$$N(f_1)\dots N(f_n)$$

of successive minima with the minimum value $h(\Lambda)$ of the product

$$N(e_1)\dots N(e_n)$$

on a basis $(e_1,\dots,e_n)$ for Λ. Set

$$\mathrm{hm}_n = \inf_{\dim \Lambda = n} \frac{h(\Lambda)}{m(\Lambda)}\,.$$

Up to $n=4$, we may choose representatives of the successive minima which constitute a basis for Λ, so that $\mathrm{hm}_n = 1$. This is no longer true in higher dimensions.

From now on, let $n \geq 4$ *.*

Example

For the centred cubic lattice C_n, $\mathrm{hm}_n = \dfrac{n}{4}$.

Hermite vs Minkowski. 2. van der Waerden's inequality

In his 1956 paper in Acta Mathematica, van der Waerden proves that the first two optimal values for hm_n are

$$\mathrm{hm}_4 = 1 \quad \text{and} \quad \mathrm{hm}_5 = \mathrm{hm}(C_5) = \frac{5}{4},$$

and gives a recursive formula to calculate an upper bound V_n of hm_n.

Hermite vs Minkowski. 2. van der Waerden's inequality

In his 1956 paper in Acta Mathematica, van der Waerden proves that the first two optimal values for hm_n are

$$\mathrm{hm}_4 = 1 \quad \text{and} \quad \mathrm{hm}_5 = \mathrm{hm}(C_5) = \frac{5}{4},$$

and gives a recursive formula to calculate an upper bound V_n of hm_n.

In a visit to Bordeaux (October, 2007), Achill Schürmann pointed out to me *FIRST*, that van der Waerden's V_n is simply $\left(\frac{5}{4}\right)^{n-4}$ (!!!!), ...

Hermite vs Minkowski. 2. van der Waerden's inequality

In his 1956 paper in Acta Mathematica, van der Waerden proves that the first two optimal values for hm_n are

$$\mathrm{hm}_4 = 1 \quad \text{and} \quad \mathrm{hm}_5 = \mathrm{hm}(C_5) = \frac{5}{4},$$

and gives a recursive formula to calculate an upper bound V_n of hm_n.

In a visit to Bordeaux (October, 2007), Achill Schürmann pointed out to me *FIRST*, that van der Waerden's V_n is simply $\left(\frac{5}{4}\right)^{n-4}$ (!!!!), ...

... *NEXT*, that one could probably take $\mathrm{hm}(C_n) = \frac{n}{4}$ $\boxed{\text{for } n = 6, 7, 8.}$

Hermite vs Minkowski. 3. A conjecture of Schürmann

Warning. hm_n is not expected to be polynomial in n!

Schürmann's idea was that the bound $\frac{n}{4}$ could be proved using a computer exploration of the edges of the Voronoi domains of the various perfect forms (33 in dimension 7, but 10916 in dimension 8).

Hermite vs Minkowski. 3. A conjecture of Schürmann

Warning. hm_n is not expected to be polynomial in n!

Schürmann's idea was that the bound $\frac{n}{4}$ could be proved using a computer exploration of the edges of the Voronoi domains of the various perfect forms (33 in dimension 7, but 10916 in dimension 8).

It turned out that I could quickly solve the problem using the classification of codes, known up to dimension 8.

Theorem

For $n = 5, 6, 7, 8$, one has $\mathrm{hm}_n \leq \frac{n}{4}$. This bound is optimal, and equality holds only on the centred cubic lattices.

$n = 6 : \frac{3}{2} = 1.5 < 1.56\ldots$; $n = 7 : \frac{7}{4} = 1.75 < 1.95\ldots$; $n = 8 : 2 < 2.44\ldots$.

Hermite vs Minkowski. 4. Binary codes

Let Λ be a lattice of maximal index $\imath = 2$, written as $\Lambda = \Lambda' \cup e + \Lambda'$, where Λ' has a basis $(f_1, \ldots, f_n)$ made of representatives of the successive minima of Λ, and

$$e = \frac{f_{i_1} + \cdots + f_{i_m}}{2} \quad \text{for some } m \in [4, n] .$$

[$\imath = 2$ is necessary, for otherwise, the coefficients of the f_i could be ≥ 3.]

Then we have $\mathrm{hm}_n \leq \frac{n}{4}$ and equality holds if and only if

the f_i have equal norms and are pairwise orthogonal, and $m = n$.

Hermite vs Minkowski. 4. Binary codes

Let Λ be a lattice of maximal index $\imath = 2$, written as $\Lambda = \Lambda' \cup e + \Lambda'$, where Λ' has a basis $(f_1, \ldots, f_n)$ made of representatives of the successive minima of Λ, and

$$e = \frac{f_{i_1} + \cdots + f_{i_m}}{2} \quad \text{for some } m \in [4, n] .$$

[$\imath = 2$ is necessary, for otherwise, the coefficients of the f_i could be ≥ 3.]

Then we have $\mathrm{hm}_n \leq \dfrac{n}{4}$ and equality holds if and only if

the f_i have equal norms and are pairwise orthogonal, and $m = n$.

This extends to binary codes of weight $w \geq 4$ and dimension $k \geq 2$.

The bound is then $\mathrm{hm}_n \leq \min \dfrac{w_1 \cdots w_k}{4^k}$ where the w_i are the weights of an $\mathbb{F}_2$-basis for the code.

Hermite vs Minkowski. 4. Binary codes (end)

Examples

We consider binary codes in dimensions n from 6 to 10 with the highest possible value for hm.

$n = 6$: $w_1 = w_2 = 4$, $\mathrm{hm} = 1$.

$n = 7$: $w_1 = 4, w_2 = 5$, $\mathrm{hm} = 1.25$.

$n = 8$: $w_1 = w_2 = 5$, $\mathrm{hm} = 1.5625 < \frac{n}{4} = 2$.

$n = 9$: $w_1 = w_2 = 6$, $\mathrm{hm} = 2.25 = \frac{n}{4}$.

$n = 10$: $w_1 = 6, w_2 = 7$, $\mathrm{hm} = 2.625 > \frac{n}{4} = 2.5$.