PERIODICA POLYTECHNICA SER. MECH. ENG. VOL. 36, NOS. 3-4, PP. 251-264 (1992)

CODES AND LATTICES

Á. G. HORVÁTH[1]

Department of Geometry
Faculty of Mechanical Engineering
Technical University of Budapest

Received: November 16, 1992

Abstract

One of the most important questions in the theory of N-dimensional Euclidean lattices is: How many minima can be found in an N-lattice? As first result G. F. Voronoi proved in [1] that this number is not greater than $2^{N+1}-2$. On the other hand, for the well-known classical extremal lattices, this number is not 'enough large', in these lattices there are only $O(N^2)$ minimal vectors. The first lattices with a lot of minima were constructed by E. S. Barnes and G. E. Wall. They proved in [1] that in the dimensions $N = 2^n$ there exists such an N-lattice in which the number of minima is $s(f_N) = c \cdot (N^{\frac{1}{2}(\log_2 N+1)}) = c \cdot (2^{\frac{1}{2}[(\log_2 N)^2+\log_2 N]})$. (The assymptotic formula was given by J.Leech in [3].) The above mentioned lattice for dimension $N = 2^3$ is the well-known lattice E_8. Using the base properties of the Reed-Muller code, in this paper we give the characterization of the minima of this lattice and determine the number of minima of the $2^n - 2$-dimensional lattice that is a generalization of the extremal lattice E_6. We note that the author proved some similar results in the paper [4] but the precise value of the above number was not known yet.

Keywords: N-lattice, minimal vector, code.

Some Lattices with a Lot of Minima

Let $\mathbf{e}_1, \cdots, \mathbf{e}_N$ be N independent points in E^N. Then the set Λ of points

$$\mathbf{z} = \sum_{i=1}^{n} x_i \mathbf{e}_i, \quad x_1, \cdots, x_n \in Z \quad \text{integers}$$

is called a lattice. The lattice Λ^* is a sublattice of Λ if and only if $\Lambda^* \subset \Lambda$. The vector $\mathbf{m}$ is a minimum of Λ if for every lattice-vector $\mathbf{v} \in \Lambda$, $|\mathbf{m}| \leq |\mathbf{v}|$. The number of the minima of Λ is denoted by $s(\Lambda)$. Now we describe some important lattices with a lot of minima. These lattices are extremals and in the lower dimension cases ($N \leq 8$) they have the most minimum vector.

[1]Supported by Hung. Nat. Found.for Sci. Research (OTKA) No. 1615 (1991).

The Lattice A_N

$$A_N = \{\sum_{i=1}^{N+1} x_i \mathbf{e}_i \mid \mathbf{x} = (x_1, \dots, x_{N+1}) \in \mathbf{Z}^{N+1} \quad \sum_{i=1}^{N+1} x_i = 0\}.$$

Minimum vectors: vectors $\mathbf{e}_i - \mathbf{e}_j$ $(i \neq j)$. Number of minima: $N(N+1)$.

The Lattice D_N

$$D_N = \{\sum_{i=1}^{N} x_i \mathbf{e}_i \mid \mathbf{x} = (x_1, \dots, x_N) \in \mathbf{Z}^N \quad \sum_{i=1}^{N} x_i \equiv 0(2)\}.$$

Minimum vectors: vectors $\pm\mathbf{e}_i \pm \mathbf{e}_j$ $(i \neq j)$. Number of minima: $2N(N-1)$.

The Lattice E_N $(N = 6, 7, 8)$

$$E_8 = \{\sum_{i=1}^{8} x_i \mathbf{e}_i \mid \mathbf{x} = (x_1, \dots, x_8) \in \mathbf{Z}^8 \text{ or } \mathbf{x} \in (\mathbf{Z} + \frac{1}{2})^8 \quad \sum_{i=1}^{8} x_i \equiv 0(2)\}.$$

$$E_7 = \{\sum_{i=1}^{8} x_i \mathbf{e}_i \mid \mathbf{x} = (x_1, \dots, x_8) \in E^8 \quad \sum_{i=1}^{8} x_i = 0\},$$

$$E_6 = \{\sum_{i=1}^{8} x_i \mathbf{e}_i \mid \mathbf{x} = (x_1, \dots, x_8) \in E^8 \quad x_1 + x_8 = \sum_{i=2}^{7} x_i = 0\}.$$

Minimum vectors:

E_8: vectors $(\pm\mathbf{e}_i \pm \mathbf{e}_j)$ $(i \neq j)$ and vectors $\frac{1}{2}\sum_{i=1}^{8}(\pm\, \mathbf{e}_i)$. Number of minima: 240.

E_7: vectors $\mathbf{e}_i \pm \mathbf{e}_j$ $\frac{1}{2}(\mathbf{e}_{i_1} + \mathbf{e}_{i_2} + \mathbf{e}_{i_3} + \mathbf{e}_{i_4} \pm \mathbf{e}_{i_5} \pm \mathbf{e}_{i_6} \pm \mathbf{e}_{i_7} \pm \mathbf{e}_{i_8})$, where $1 \leq i, j \leq 8$ $\{i_1, \cdots, i_8\}$ are a permutation of the numbers $\{1, \cdots, 8\}$. Number of minima: 126.

E_6: vectors $\mathbf{e}_i - \mathbf{e}_j$ $(2 \leq i \neq j \leq 7)$ and vectors $\pm\frac{1}{2}(\mathbf{e}_1 + \mathbf{e}_{i_2} + \mathbf{e}_{i_3} + \mathbf{e}_{i_4} - \mathbf{e}_{i_5} - \mathbf{e}_{i_6} - \mathbf{e}_{i_7} - \mathbf{e}_8)$, where $\{i_2, \cdots, i_7\}$ are a permutation of the numbers $\{2, \cdots, 7\}$ and the vectors $\pm(\mathbf{e}_1 - \mathbf{e}_8)$. Number of minima: 72.

2.The Barnes–Wall Construction

Let V be an n-dimensional vector space over the Galois field GF(2) ; in terms of a basis $\varepsilon_1, \ldots, \varepsilon_n$, we may write the elements as $\alpha = \sum \alpha_i \varepsilon_i$ with coordinates α_i which are integers taken modulo 2. The additive group of V, which we shall also denote by V, is the elementary Abelian group of order $N = 2^n$. Subgroups and cosets of dimension r will be denoted generically by V_r and C_r, respectively. In N-dimensional Euclidean space E.S.BARNES and G. E. WALL (Barnes and Wall) consider integral vectors $\mathbf{x} = (x_\alpha)$ with coordinates x_α indexed by the N elements α of V. If W is any subset of V, $[W]$ will denote the characteristic vector $\mathbf{x}$ defined by :

$$x_\alpha = \begin{cases} 1 & \text{if} \quad \alpha \in W \\ 0 & \text{if} \quad \alpha \notin W \end{cases}$$

Barnes and Wall denoted by Λ the sublattices of Z^N generated by all vectors $2^{[\frac{n-r}{2}]}[C_r]$, where C_r runs over all cosets in V. They proved the following theorems:

Theorem 2.1. *Let $\varepsilon_1, \ldots, \varepsilon_n$ be any basis of V. Then a basis of Λ is given by the N vectors $2^{[\frac{n-r}{2}]}[C_r]$, where V_r runs through the subgroups of V which have a subset of $\varepsilon_1, \ldots, \varepsilon_n$ as basis. (see* [2] T.3.1)

Theorem 2.2. *Λ is invariant under the following orthogonal transformations:*

i. the permutation of the coordinates x_α induced by the transformation $\alpha \longmapsto \tau\alpha + \gamma$ of V, where τ is a non-singular matrix over GF(2) and γ is any fixed element of V,

ii. the involution

$$y_\alpha = \begin{cases} x_\alpha & \text{if} \quad \alpha \in W \\ -x_\alpha & \text{if} \quad \alpha \notin W \end{cases}$$

where W is any fixed subgroup of V of dimensionn $- 1$.

Barnes and Wall defined the rank of a point $\mathbf{x} \neq 0$ of Λ to be the largest $r (0 \leq r \leq n)$ for which all coordinates x_α are divisible by $2^{[\frac{r}{2}]}$ and proved:

Theorem 2.3. *A point $\mathbf{x} \neq 0$ of Λ is a minimal vector if and only if R is odd, and for some coset C_{n-R} of dimension $n - R$*

$$|x_\alpha| = \begin{cases} 2^{[\frac{R}{2}]} & \text{if} \quad \alpha \in C_{n-R} \\ 0 & \text{if} \quad \alpha \notin C_{n-R} \end{cases}$$

(see T.3.2 and (5.2) in [2])

Theorem 2.4. *For the lattice Λ the number of minima*

$$s(\Lambda) = 2^{n+1} \sum_{R \text{ odd}} 2^{\binom{n-R}{2}} K_{n,R} \quad \text{where} \quad K_{n,R} = \frac{(2^n-1)\cdots(2^{n-R+1}-1)}{(2^R-1)\cdots(2-1)}.$$

J.LEECH in [3] determined this sum, he gave the following form:

$$s(\Lambda) = (2+2)(2+2^2)\cdots(2+2^n) \sim l \cdot N^{\frac{1}{2}(\log_2 N+1)},$$

where $l = 4,7684\ldots$ is a constant.

Second-Order Reed–Muller Code and the Barnes–Wall Lattices

A binary code C of length N is a subset of F_2^N, where F_2^N is the N-dimensional vector space over the Galois field GF(2). The *Hamming distance* between two vectors

$$\mathbf{u} = (u_1, \ldots, u_N), \mathbf{v} = (v_1, \ldots, v_N)$$

$u_i, v_i \in GF(2)$, to be the number of coordinates where they differ:

$$d(u,v) = |\{i : u_i \neq v_i\}|.$$

The *minimal distance* d of a code is

$$d := \min\{d(u,v) \mid u,v \in C\}.$$

A code of length N containing M codewords and with minimal distance d is said to be an (N,M,d) code. A linear code C is a linear subspace of F_2^N: the set of codewords is closed under vector addition and coordinate-wise multiplication by elements of F_2^N. The *dimension* k is the dimension of this subspace, and there are 2^k codewords. A linear code of length N, dimension k and minimal distance d is said to be an $[N,k,d]$ code. The minimal distance of a linear code is the minimal nonzero weight (the number of the nonzero coordinates) of any codeword. Let $A_i(c)$ denote the number of codewords at Hamming distance i from a codeword $c \in C$. The numbers $\{A_i(c)\}$ are called the *weight distribution* of C with respect to c. For linear codes $\{A_i(c)\}$ is independent of c and will be denoted by $\{A_i\}$.(See for example [6] or [5].) Assume now that $N = 2^n$. Denote by $X = \{P_0, \ldots, P_{2^n-1}\}$ the set of the points of the n-dimensional Euclidean geometry $EG(n,2)$ over $GF(2)$. Any subset S of the points of $EG(n,2)$ has

associated with it a binary incidence (or characteristic) vector of length N, containing 1' in the components $s \in S$, and zeros elsewhere. This gives us another way of thinking about codewords, namely as (characteristic vectors of) subsets of $EG(n,2)$. If we fix a coordinate system and the points of $EG(n,2)$ are column-vectors in this system, then this geometry corresponds with a binary matrix which has n rows and N columns. For example, in the case of $n = 3$ we have the incidence-matrix:

	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7
$\overline{w}_3$	1	1	1	1	0	0	0	0
$\overline{w}_2$	1	1	0	0	1	1	0	0
$\overline{w}_1$	1	0	1	0	1	0	1	0

It is clear that the complements of the rows of this matrix are the characteristic vectors of hyperplanes which pass through the origin, so these are subspaces of dimension $n-1$. Let's denote by $V^1, \ldots, V^n$ these subspaces and denote by $[S]$ the characteristic vector of the subset S. (At this time the corresponding codewords are $[V^1], \ldots, [V^n]$.) Since the coordinatewise multiplication of two codewords is also a codeword, for which

$$[S] * [G] = [S \cap G]$$

holds, we get that $[V^i] * [V^j]$ is the characteristic vector of a $n-2$-dimensional subspaces. For example in the three dimensional case the rows of this matrix are the characteristic vectors of the three 2-dimensional subspaces of F_2^N $\{\varepsilon_i, \varepsilon_j\}$, where $i \neq j$ .The characteristic vectors of the subspaces of dimension 1 (or 0, resp.) are the collection of vectors formed by componentwise multiplying these vectors two at a time (or three at a time, resp.):

$$\begin{aligned}
[1\,0\,0\,0\,1\,0\,0\,0] &\longleftrightarrow \{0, \varepsilon_3\} \\
[1\,0\,1\,0\,0\,0\,0\,0] &\longleftrightarrow \{0, \varepsilon_2\} \\
[1\,1\,0\,0\,0\,0\,0\,0] &\longleftrightarrow \{0, \varepsilon_1\} \\
[1\,0\,0\,0\,0\,0\,0\,0] &\longleftrightarrow \{0\}
\end{aligned}$$

In this paper the set of indices of the N-dimensional space E^N will correspond with the space $EG(n,2)$, so we regard it as an algebraic structure.

The binary r^{th} order *Reed–Muller code* of length $N = 2^n$ (R(r,n)) is the linear code generated by the codewords:

$$[V], [V^1], \ldots, [V^n], [V^n]*[V^{n-1}], \ldots, [V^2]*[V^1], \ldots, [V^r]*[V^{r-1}]*\cdots*[V^1].$$

It can be proved that this code is a $[2^n, \sum_{i=0}^{r} \binom{n}{i}, 2^{n-r}]$ one, so its minimal distance is 2^{n-r} (see [5],[6]). We use the following theorems:

Theorem 3.1. *By an invertible linear transformation of the space $EG(n,2)$, arbitrary codewords in the second-order Reed–Muller code can be transformed to one of the following forms:*

a) $$\sum_{i=1}^{\sigma}[V^{2i-1}]*[V^{2i}],$$

b) $$\sum_{i=1}^{\sigma}[V^{2i-1}]*[V^{2i}]+[V],$$

c) $$\sum_{i=1}^{\sigma}[V^{2i-1}]*[V^{2i}]+L_{2\sigma+1},$$

where the linear part of the third case $L_{2\sigma+1}=\sum_{i=2\sigma+1}^{n}a_i[V^i]$ is not identically zero, and for σ $\sigma\leq[\frac{n}{2}]$ holds.

This theorem can be found in the books [6] and [7].

Theorem 3.2. *Let A_i^n be the number of codewords of weight i in $R(2,n)$. Then $A_i^n=0$ unless $i=0,2^n,2^{n-1}$ or $2^{n-1}\pm 2^{n-1-\sigma}$ for some σ, $0<\sigma\leq[\frac{n}{2}]$. Furthermore*

$$A_0^n=A_{2^n}=1,$$

$$A_{2^{n-1}\pm 2^{n-1-\sigma}}=2^{\sigma(\sigma+1)}\frac{(2^n-1)\cdots(2^{n-2\sigma+1}-1)}{(4^\sigma-1)\cdots(4-1)},\qquad 0<\sigma\leq[\frac{n}{2}],$$

$$A_{2^{n-1}}^n=2^{1+\binom{n}{1}+\binom{n}{2}}-\sum_{i\neq 2^{n-1}}A_i^n.$$

We now give the precise characterization of the minima of the lattice defined by Barnes and Wall. We prove the following statement:

Theorem 3.3. *Regard the following $n-R$-dimensional subspace of V: $W_{n-R}=V^{n-R+1}\cap\ldots\cap V^n$ and denote by $\mathbf{m}$ such a vector of Λ whose support is the coset W_{n-R} and the absolute values of its coordinates are $2^{[\frac{n-r}{2}]}$. Let W_{n-R}^+ be the set of such indices of $\mathbf{m}$ where the corresponding coordinates are positives. Then the vector $\mathbf{m}$ is a minimum vector if and only if the vector $[\mathbf{W}_{n-R}^+]$ is a codeword of the second-order Reed–Muller code of length 2^{n-R} which is defined over the subspace W_{n-R}.*

Before proving this theorem, we have to verify an interesting lemma about the incidence vectors of subspaces of the space $EG(n,2)$.

Lemma 3.1. *Let $G_i<EG(n,2)$ $i=1,\ldots,h$ be distinct subspaces in $EG(n,2)$. Regard the codewords $c=\sum_{i=1}^{h}(mod2)[G_i]$.*

Then the following equality holds:

$$c = \sum_{i=1}^{h}[G_i] - 2\sum_{i_1\neq i_2}[G_{i_1}]*[G_{i_2}] + 4\sum_{i_1\neq i_2\neq i_3}[G_{i_1}]*[G_{i_2}]*[G_{i_3}] - \ldots + (-2)^{h-1}[G_1]*\cdots*[G_h].$$

Proof. The above-mentioned equality is an identity if $h = 1$. Assume that the statement is true if the number of the components of the sum is less than or equals h. Regard now the following decomposition of the codewords c:

$$c = \sum_{i=1}^{h}\mathrm{mod}2[G_i] = c' + [G_i]\mathrm{mod}2.$$

Since if $\alpha \notin G_i$ then $0 = [G_i]_\alpha$ so we can see that:

$$c_\alpha = c'_\alpha = \Big(\sum_{\substack{j=1\\ i\neq j}}^{h}[G_j] - 2\sum_{\substack{i_1\neq i_2\\ i_1,i_2\neq i}}[G_{i_1}]*[G_{i_2}] + 4\sum_{\substack{i_1\neq i_2\neq i_3\\ i_1,i_2,i_3\neq i}}[G_{i_1}]*[G_{i_2}]*[G_{i_3}] - \ldots + (-2)^{h-1}[G_1]*\cdots*[G_{i-1}]*[G_{i+1}]*\cdots*[G_h]\Big)_\alpha =$$

$$= \Big(\sum_{j\neq i} - 2\sum_{\substack{i_1\neq i_2\\ i_1,i_2\neq i}} + 4\sum\cdots\Big)_\alpha + [G_i]_\alpha - 2\sum_{j\neq i}([G_i]*[G_j])_\alpha + \ldots =$$

$$= \Big(\sum_{i=1}^{h}[G_i] - 2\sum_{i_1\neq i_2}[G_{i_1}]*[G_{i_2}] + 4\sum_{i_1\neq i_2\neq i_3}[G_{i_1}]*[G_{i_2}]*[G_{i_3}] - \ldots + (-2)^{h-1}[G_1]*\cdots*[G_h]\Big)_\alpha.$$

For this reason in this case for the index α the statement of the lemma is true. This means that if there exists such an index i for which $\alpha \notin G_i$ then in the index α the desired equality holds. Assume now that $\alpha \in \cap\{G_i \mid i = 1, \ldots, h\}$. Then the value of the left hand side in this index is:

$$(c)_\alpha = (\sum_{i=1}^{h}\mathrm{mod}2[G_i])_\alpha = \begin{cases} 0 & \text{if } h \text{ is even} \\ 1 & \text{if } h \text{ is odd.} \end{cases}$$

At the same time the value of the other side is:

$$h - 2\binom{h}{2} + 4\binom{h}{3} - \ldots + (-2)^{h-1}\binom{h}{h} = \frac{1}{2} - \frac{(1-2)^h}{2} = (c)_\alpha.$$

Thus, the statement of the lemma in this case holds, too.

Proof of Theorem 3.3. BARNES and WALL in [2] proved that the number of the minima supporting the fixed subspace W_{n-R} was not greater than the number $2^{1+\binom{n-R}{1}+\binom{n-R}{2}}$. Let $\alpha_0, \alpha_i, \alpha_{i,j}$ be elements of $GF(2)$ and denoted by $W^i = W_{n-R} \cap V_i$ for all index $1 \leq i \leq n-R$. Regard now the following vector:

$$\mathbf{m} = 2^{[\frac{R+1}{2}]}\Big(\Big\{\alpha_0[W_{n-R}] + \sum_{1\leq i\leq n\text{-}R} \mathrm{mod}2\alpha_i[W^i] + \sum_{1\leq i\neq j\leq n\text{-}R} \mathrm{mod}2\alpha_{i,j}[W^i] * [W^j]\Big\}\Big) - 2^{[\frac{R}{2}]}[W_{n-R}],$$

where the plus in the bracket means the $(mod2)$ sum of those binary vectors which can be found there. It is clear that $\mathbf{m}$ is in the lattice Λ if and only if the first member is in Λ. In this case the vector $\mathbf{m}$ satisfies the conditions of Theorem (2.3), so it is a minimum one. Since the linear combination in the bracket is a codeword of the code $R(2, n-R)$, so the number of the distinguished vectors $\mathbf{m}$, which can be stated in the above form, is $2^{1+\binom{n-R}{1}+\binom{n-R}{2}}$. This means that we only have to prove that every codeword as an N-dimensional (0-1)-vector (the coordinates which are not in W_{n-R} are equal to zero) is in Λ. We now prove that this binary vector is a linear combination with integer coefficients of the lattice vectors with support W^i. Note that under a coordinate permutation of E^N induced by an invertible linear transformation of the space W_{n-R} the lattice Λ is invariant (see Theorem (2.2)), so the image vector and the original one are in the lattice at the same time. By virtue of the Theorem (Dickson) it may be assumed that the examined vector is in one of the following forms:

a) $\sum_{i=1}^{h} [W^{2i-1}] * [W^{2i}],$

b) $\sum_{i=1}^{h} [W^{2i-1}] * [W^{2i}] + [W^{n-R}]$

c) $\sum_{i=1}^{h} [W^{2i-1}] * [W^{2i}] + L_{2h+1}$

where the sum $L_{2h+1} = \sum_{i=2h+1}^{n-R} a_i[W^i]$ is not identically zero.

The cases of a, and b are easy to see from the Lemma 3.1 because for every odd number R the following equality holds $\left[\frac{R+2}{2}\right] = \left[\frac{R+1}{2}\right]$. Hence

we get that :

$$2^{[\frac{R+1}{2}]}\Big\{\sum_{i=1}^{h}[W^{2i-1}]*[W^{2i}](mod2)\Big\} = \sum_{i=1}^{h}2^{[\frac{R+1}{2}]}[W^{2i-1}]*[W^{2i}]-$$

$$-\sum_{\substack{i_1,i_2=1\\ i_1\neq i_2}}^{h}2\cdot 2^{[\frac{R+1}{2}]}[W^{2i_1-1}]*[W^{2i_1}]*[W^{2i_2-1}]*[W^{2i_2}]+$$

$$+\ldots+(-1)^{h-1}\sum 2^{h-1}2^{[\frac{R+1}{2}]}[W^1]*\cdots*[W^{2h}]=$$

$$=\sum_{i=1}^{h}2^{[\frac{R+1}{2}]}[W^{2i-1}]*[W^{2i}]-$$

$$-\sum_{\substack{i_1,i_2=1\\ i_1\neq i_2}}^{h}2^{[\frac{R+1}{2}]+1}[W^{2i_1-1}]*[W^{2i_1}]*[W^{2i_2-1}]*[W^{2i_2}]+\ldots$$

Here every element of the right hand side is in Λ, so this is true for the left hand side, too.

In the case of c, we have to apply such an affine transformation $\mathcal{T}$ which does not modify the first part of the sum c, and at the same time for which the equality $\mathcal{T}(L_{2h+1}) = [W^{2h+1}]$ holds. (There exists such a transformation, see for example in [8] the formula (16.352).) Regard now the following notes: $G_i = [W^{2i-1}]*[W^{2i}]$ $G_{h+1} = [W^{2h+1}]$ and apply the Lemma 3.1. It is easy to verify that the statement of the theorem is true in this case, too.

Sublattices of the Barnes–Wall Lattice

Let H be an arbitrary subgroup of V. Let Λ_H denote the set of those vectors of Λ for which $\sum_{\alpha\in H} x_\alpha = 0$. Then Λ_H is a sublattice of Λ . The author in [4] proved the following basic theorem:

Theorem 4.1. *Let dimH be the dimension of the subspace H.*
1. If dimH = dimG, where H and G are subgroups of V, then, the lattices Λ_H and Λ_G are congruents.

2. For every subgroup H of V the minimal value of the sublattice Λ_H is equal to the minimal value of the original lattice Λ.

In this paragraph let the dimension r of the subgroup H be fixed $(0 \leq r \leq n)$. According to the notations of the paper [2] let N_R be the

number of minimal vectors of the lattice Λ with support C_{n-R}, where C_{n-R} is a coset of dimension $n-R$. (It can be seen from the theorem 2.2 that this number is the same for all cosets of dimension $n-R$.) Denote by $N_{R,k}$ the number of those minima of Λ_H with support C_{n-R} for which $\dim(C_{n-R} \cap H) = k$. It is easy to see that $N_{R,k}$ is also independent of the choice of the coset C_{n-R}. From Theorem 3.3 it is clear that this number is equal to the number of those codewords of an $R(2, n-R)$ code which have 2^{k-1} 0's and 2^{k-1} 1's coordinates over a k-dimensional subspace V_k of the original vector space V. In [9] the author determined this number and proved that:

$$N_{R,k} = \sum_{\delta=1}^{\left[\frac{k+1}{2}\right]} (2^k - 1)\cdots(2^{k-2\delta+2} - 1)2^{\binom{n-R+1}{2}-\binom{k+1}{2}+\binom{k-2\delta+1}{2}+1}.$$

In the same paper the following recursive formula was verified:

Theorem 4.2. *If $1 \le k \le n-R$ holds for the number k, then:*

$$2^k N_{R,k} = (2^k - 1)\left[2^{\binom{n-R+1}{2}+1} - N_{R,k-1}\right].$$

By the help of these formulas the asymptotic one was given in [4] for the number Λ_H when $H =< \{0\} >$. It was proved that in this lattice the number of minima was equal to $O(N^{\frac{1}{2}(\log_2 N+1)})$. In this paper we shall prove a similar result.

Theorem 4.3. *Regard the lattice $\Lambda_H \cap \Lambda_G$, where H, G are the subgroups V_{n-1} and $< \{0\} >$, respectively. Then for the number of minima of this lattice the following inequality holds:*

$$s(\Lambda_{V_{n-1},<\{0\}>}) \ge c^* s(\Lambda_{<\{0\}>}),$$

where the constant c^* is independent of the dimension N.

Proof. The precise value of the number of minima of this lattice was determined in [4], this is the following:

$$s(\Lambda_{V_{n-1},<\{0\}>}) = \sum_{R \text{ odd}} \Big\{(2^R - 1)N_{R,n-R-1}2^R K_{n-1,R} + (2^{R-1}N_R + (2^{R-1} - 1)N_{R,n-R})K_{n-1,R-1}\Big\}.$$

Substitute the value $k = n - R$ into the recursion formula (see Theorem 4.2) and arrange the equality into the following form:

$$(2^{n-R} - 1)N_{R,n-R-1} = \left[(2^{n-R} - 1)2^{\binom{n-R+1}{2}+1} - 2^{n-R}N_{R,n-R}\right].$$

Then we get:
$s(\Lambda_{V_{n-1},<\{0\}>}) =$

$$= \sum_{R\,\text{odd}} \Big\{ (2^R - 1)2^R \Big[2^{\binom{n-R+1}{2}+1} - \frac{2^{n-R}}{(2^{n-R}-1)} N_{R,n-R} \Big] K_{n-1,R} + \\ + (2^{R-1} N_R + (2^{R-1} - 1) N_{R,n-R}) K_{n-1,R-1} \Big\}.$$

However, from the definition of the number $K_{n-1,R-1}$ it is clear that:

$$\frac{2^R - 1}{(2^{n-R} - 1)} K_{n-1,R} = K_{n-1,R-1},$$

so we have that:
$s(\Lambda_{V_{n-1},<\{0\}>}) =$

$$= \sum_{R\ \text{odd}} \Big\{ 2^R \Big[2^{\binom{n-R+1}{2}+1} (2^{n-R} - 1) - 2^{n-R} N_{R,n-R} \Big] K_{n-1,R-1} + \\ + (2^{R-1} N_R + (2^{R-1} - 1) N_{R,n-R}) K_{n-1,R-1} \Big\} =$$

$$= \sum_{R\ \text{odd}} \Big\{ (2^n - 2^R + 2^{R-1}) N_R + (-2^n + 2^{R-1} - 1) N_{R,n-R} \Big\} K_{n-1,R-1}.$$

Here we use the equality: $N_R = 2^{\binom{n-R+1}{2}+1}$. If we take into consideration the equality

$$\frac{2^R - 1}{(2^n - 1)} K_{n,R} = K_{n-1,R-1},$$

too, we get that:

$$s(\Lambda_{V_{n-1},<\{0\}>}) =$$

$$= \sum_{R\ \text{odd}} \Big\{ (2^n - 2^{R-1}) + (-2^n + 2^{R-1} - 1) \frac{N_{R,n-R}}{N_R} \Big\} N_R \frac{2^R - 1}{(2^n - 1)} K_{n,R} =$$

$$= \sum_{R\ \text{odd}} \Big\{ \frac{(2^n - 2^{R-1})}{(2^n - 1)} - \frac{(2^n - 2^{R-1} + 1)}{(2^n - 1)} \frac{N_{R,n-R}}{N_R} \Big\} (2^R - 1) N_R K_{n,R} =$$

$$= \frac{1}{2^n - 1} \sum_{R\ \text{odd}} \Big\{ (2^n - 2^{R-1}) \Big[1 - \frac{N_{R,n-R}}{N_R} \Big] - \frac{N_{R,n-R}}{N_R} \Big\} (2^R - 1) N_R K_{n,R}.$$

If we can give a good upper bound for the number $\frac{N_{R,n-R}}{N_R}$, we get a lower one for the number of the minima. Take now the sum-form of the number $N_{R,n-R}$. This is the following:

$$N_{R,n-R} = \sum_{\delta=1}^{\left[\frac{n-R+1}{2}\right]} (2^{n-R}-1)\cdots(2^{n-R-2\delta+2}-1)2^{\binom{n-R-2\delta+1}{2}+1}.$$

Since $N_R = 2^{\binom{n-R+1}{2}+1}$, we have that:

$$\frac{N_{R,n-R}}{N_R} = \sum_{\delta=1}^{\left[\frac{n-R+1}{2}\right]} \left(1-\frac{1}{2^{n-R}}\right)\cdots\left(1-\frac{1}{2^{n-R-2\delta+2}}\right)\frac{1}{2^{n-R-2\delta+1}} =: L_{n-R}.$$

It is easy to verify the following recursion formula for the number L_{n-R}:

$$L_{n-R} = \left(1-\frac{1}{2^{n-R}}\right)\left[\frac{1}{2^{n-R-1}} + \left(1-\frac{1}{2^{n-R-1}}\right)L_{n-R-2}\right].$$

We prove by induction with respect to the number $n-R$ that the inequality holds:

$$L_{n-R} \le \frac{2^{n-R+2}-1}{\frac{3}{2}2^{n-R+2}-1}.$$

If $n-R$ is equal to 1 or 2, then the above number L_{n-R} is $\frac{1}{2}$ or $\frac{3}{8}$, respectively, so the statement is true. Assume now that

$$L_{n-R-2} \le \frac{2^{n-R}-1}{\frac{3}{2}2^{n-R}-1}.$$

Then

$$\begin{aligned} L_{n-R} &= \left(1-\frac{1}{2^{n-R}}\right)\left[\frac{1}{2^{n-R-1}} + \left(1-\frac{1}{2^{n-R-1}}\right)L_{n-R-2}\right] \le \\ &\le \left(1-\frac{1}{2^{n-R}}\right)\left[\frac{1}{2^{n-R-1}} + \left(1-\frac{1}{2^{n-R-1}}\right)\frac{2^{n-R}-1}{\frac{3}{2}2^{n-R}-1}\right] = \\ &= \frac{2^{n-R}-1}{2^{n-R}}\left[\frac{\frac{3}{2}2^{n-R}-1+(2^{n-R-1}-1)(2^{n-R}-1)}{2^{n-R-1}(\frac{3}{2}2^{n-R}-1)}\right] = \\ &= \frac{2^{n-R}-1}{\frac{3}{2}2^{n-R}-1} \le \frac{2^{n-R+2}-1}{\frac{3}{2}2^{n-R+2}-1}, \end{aligned}$$

so the inequality holds. Here we used the trivial inequality :

$$\frac{2^{n-R}-1}{\frac{3}{2}2^{n-R}-1} \leq \frac{2^{n-R+2}-1}{\frac{3}{2}2^{n-R+2}-1}.$$

Although the limit of the above sequence is $\frac{2}{3}$ for this reason we have the same upper bound for the number L_{n-R}, too. So

$$s(\Lambda_{V_{n-1},<\{0\}>}) =$$
$$= \frac{1}{2^n-1}\sum_{R \text{ odd}}\left\{(2^n-2^{R-1})[1-\frac{N_{R,n-R}}{N_R}]-\frac{N_{R,n-R}}{N_R}\right\}(2^R-1)N_R K_{n,R} \geq$$
$$\geq \frac{1}{2^n-1}\sum_{R \text{ odd}}\left[\frac{2^n-2^{R-1}-2}{3}\right](2^R-1)N_R K_{n,R} =$$
$$= \frac{2^{n-1}-2}{3(2^n-1)}\sum_{R \text{ odd}}(2^R-1)N_R K_{n,R} \geq c^* s(\Lambda_{<\{0\}>}),$$

where the non-zero constant c^* is equal to $\inf\left\{\frac{2^{n-2}-1}{6(2^n-1)} \quad n \geq 3\right\}$. So we proved the theorem.

We remark that the statement of Theorem 4.3 means that the $N = (2^n-2)$-dimensional sublattice $\Lambda_{V_{n-1},<\{0\}>}$ of the Barnes–Wall lattice Λ has at least $O(2^{\frac{1}{2}[(\log_2 N)^2+\log_2 N]})$ minima.

Acknowledgement

I would like finally to express my thanks to my wife Prof. Á.P.Horváth for helping me to sharpen the mean estimation of this paper which was given for the number $s(\Lambda_{V_{n-1},<\{0\}>})$.

References

1. Voronoi, G. F. (1952): Selected papers. Complete edition, Akad.Nauk. Ukr. SSR, Kiev
2. Barnes, E. S.– Wall, G. E.(1959): Some Extreme Forms Defined in Terms of Abelian Groups, *Journal of the Australian Math. Soc.* pp. 47–63.
3. Leech, J.(1964): Some Sphere Packings in Higher Space, *Canadian J. Math.* Vol. 16 .
4. Horváth, Á. G. (1991): On the Number of the Minima of N-Lattices, *Conference on Intuitive Geometry*,Szeged, (to appear).
5. Conway,J. M. – Sloane, N. J. A. (1988): Sphere Packings, Lattices and Groups, Springer-Verlag.
6. MacWilliams, F. J. – Sloane, N. J. A. (1978): The Theory of Errorcorrecting Codes, North Holland, Amsterdam.

7. PETERSON, W. W. – WELDON, E. J. (1972): Error-Correcting Codes, MIT Press, Cambridge, MA.
8. BERLEKAMP, E. R. (1968): Algebraic Coding Theory, McGraw-Hill.
9. HORVÁTH, Á. G. : On the Second-Order Reed-Muller Code, (submitted).

Address:
Ákos G. HORVÁTH
Department of Geometry
Faculty of Mechanical Engineering
Technical University of Budapest
H–1521 Budapest, Hungary