Periodica Mathematica Hungarica Vol. 31 (2), (1995), pp. 131-138

ON THE SUBLATTICES OF THE BARNES-WALL LATTICE

ÁKOS G.HORVÁTH* (Budapest)

Abstract

This paper is connected with the fundamental work of E.S. Barnes and G.E. Wall [1] in which the authors defined the so-called Barnes-Wall lattice. We shall determine the number of minima of some special sublattices of dimension $2^n - k$ of this lattice, where $1 \leq k \leq n$.

1. Introduction

Let Λ be the Barnes-Wall lattice of dimension 2^n as it was defined in [1]. The construction which gives this lattice is very important because for this lattice the number of minima is not a polynomial function of the dimension. The author of the present paper worked out a method for the calculation of the number of minima of some sublattices of dimensions $2^n - 1$ and $2^n - 2$ based on the second-order Reed–Muller code, see [3] and [4].

In this paper we show a combinatorial calculation for the determination of the precise number of minima of $(2^n - k)$-sublattices of the Barnes–Wall lattice of special types. In the case of $k = 2$ and $n \geq 4$ this method gives a sublattice which has more minima than that in [4], where the sublattice was the generalization of the lattice E_6.

2. Definitions and theorems

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

*Supported by Hung. Nat. Found for Sci. Research (OTKA) grant no. 1615 (1992)
Mathematics subject classification numbers, 1991. Primary 11H50; Secondary 52C07.
Key words and phrases. n-lattice, minimum vector.

0031-5303/95/$5.00

Akadémiai Kiadó, Budapest
Kluwer Academic Publishers, Dordrecht

denote by V, is the elementary Abelian group of order $N = 2^n$. Subgroups and cosets of dimension r will be denoted generally by V_r and C_r, respectively. In N-dimensional Euclidean space E.S. Barnes and G.E. Wall [1] consider integral vectors $\underline{x} = (x_\alpha)$ 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 $\underline{x}$ defined by

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

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 that the collection of characteristic vectors with suitable coefficients corresponding to the "coordinate" subspaces (the subspaces spanned by a subset of the fixed basis $\varepsilon_1, \ldots, \varepsilon_n$ of V) is a basis of the lattice Λ (see [1] T.3.1). They showed that Λ is invariant under 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. (See T.3.2 in [1].) Finally, they proved the following theorem which characterises the elements of the lattice Λ having minimal Euclidean norm (shortly, minimal elements).

THEOREM 1. *A point $\underline{x} \neq 0$ of Λ is a minimal vector if and only if there is an odd number R, $0 \leq R \leq n$ and some coset C_{n-R} of dimension $n - R$ so that*

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

(see (5.2) *in* [1]*).*

From this result they gave the number of minima of Λ.

THEOREM 2. *For the lattice Λ the number of minima is*

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

where

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

is the well-known number of the $(n - R)$-dimensional subspaces of V.

J. Leech in [5] determined this sum, showed that

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

where $l = 4.7684\ldots$ is a constant.

3. The result of this paper

In this section we shall define some sublattices of the Barnes–Wall lattice of dimension $N = 2^n - k$, where the positive integer k is less than or equal to n.

DEFINITION 1. Let $\Lambda_{\mathcal{H}}$ be the following lattice:

$$\Lambda_{\mathcal{H}} = \{\underline{v} \,|\, \underline{v} \in \Lambda \text{ and } (\underline{v})_\alpha = 0 \text{ if } \alpha \in \cup\mathcal{H}\}$$

where $\mathcal{H}$ is a family of such subspaces of the space $V = EG(n, 2)$ which are spanned by subsets of a fixed base of V.

In what follows let $\mathcal{H}$ be the following family:

$$\mathcal{H} = \{< \underline{0} >, < \underline{e}_i > \text{ where } i = 1, \ldots, k \text{ for a number } k, \quad 1 \leq k \leq n\}.$$

The theorem is the following:

THEOREM 3. *Let k be an integer ($1 \leq k \leq n$) and consider the $N = 2^n - k$-sublattice $\Lambda_{\mathcal{H}}$ of the Barnes–Wall lattice Λ. (This is the intersection of the lattice Λ and an $N = 2^n - k$-dimensional coordinate-subspace.) Then the number of minima of $\Lambda_{\mathcal{H}}$ is equal to the number:*

$$s(\Lambda_{\mathcal{H}}) = 2^{\frac{n(n+1)}{2}} \left\{ \prod_{l=0}^{n-1} \left(1 + \frac{1}{2^l}\right) - \binom{k}{1} \left[\prod_{l=1}^{n} \left(1 + \frac{1}{2^l}\right) - \prod_{l=1}^{n} \left(1 - \frac{1}{2^l}\right) \right] + \right.$$
$$\left. + \cdots + (-1)^k \binom{k}{k} \left[\prod_{l=k}^{n} \left(1 + \frac{1}{2^l}\right) - \prod_{l=k}^{n} \left(1 - \frac{1}{2^l}\right) \right] \right\}.$$

Unfortunately, at the moment we could not give for this sum a nice form similar to the one appearing in Theorem 2. (See also Remark 3.)

4. Proof of the theorem

Denote by A_0 the set of those minimum vectors of Λ which have zero coordinate above the position $\underline{0} \in V$. Similarly, let A_i be the set of those minimum lattice-vectors which have zero coordinate above the position $\underline{e}_i \in V$. The following lemma plays an important role in the proof of the theorem:

LEMMA 1. *If the sets of indices $\{i'_j\}$, $\{i_j\}$ are two subsets of the set $I = \{0, 1, \ldots, k-1\}$ of the same cardinality, then the following equality holds for every integer l for which $1 \leq l \leq k-1$:*

$$|A_{i_1} \cap \ldots \cap A_{i_l}| = |A_{i'_1} \cap \ldots \cap A_{i'_l}|.$$

PROOF. It is clear, that the set $A_{i_1} \cap \ldots \cap A_{i_l}$ is the set of those minima of Λ, which have zero coordinate above the position of the set of indices $\{\underline{e}_{i_1}, \ldots, \underline{e}_{i_l}\}$.

1. If $0 \notin \{i_j\} \cup \{i'_j\}$ then there is a regular linear map L of V for which the conditions
$$L : \underline{e}_{i_j} \longmapsto \underline{e}_{i'_j}, \qquad j = 1, \ldots, l$$
hold. By this transformation, the set $A_{i_1} \cap \ldots \cap A_{i_l}$ corresponds to the set $A_{i'_1} \cap \ldots \cap A_{i'_l}$. This means that in this case the statement is true.
2. The case when the condition $0 \in \{i_j\} \cap \{i'_j\}$ holds can be treated similarly. (Now the image of the zero is zero.)
3. So we have to examine only that case when $0 \in \{i_j\}$ and $0 \notin \{i'_j\}$. But the translation with the vector $\underline{e}_{i'_j}$ takes the set $\{\underline{e}_{i'_j}\}$ into the set $\{0, \underline{e}_{i'_2} + \underline{e}_{i'_1}, \ldots, \underline{e}_{i'_l} + \underline{e}_{i'_1}\}$. Omitting the element zero from this system we get a linearly independent one which has $l-1$ elements. This means that the statement is true because the last system can be taken into the system $\{\underline{e}_{i_j}\}$ with a regular linear transformation, so the original systems are affine-equivalent. So we get that the congruence induced by this permutation of the indices takes one of the examined sets into the other. ■

REMARK 1. We get from the proof of the lemma that the sets $A_{i_1} \cap \ldots \cap A_{i_l}$ and $A_{i'_1} \cap \ldots \cap A_{i'_l}$ are congruent.

We now give the proof of the theorem.

PROOF OF THEOREM 3. Let S be the set of the minima of the lattice Λ. Using the combinatorial inclusion-exclusion formula we see that:

$$|S \setminus \{A_0 \cup \ldots \cup A_{k-1}\}| = |S| - \sum_{i=0}^{k-1} |A_i| + \sum_{i,j} |A_i \cap A_j| + \ldots + (-1)^k |A_0 \cap \ldots \cap A_{k-1}|.$$

According to Lemma 1 this formula can be written in the form:

$$|S \setminus \{A_0 \cup \ldots \cup A_{k-1}\}| = |S| - k|A_0| + \binom{k}{2} |A_0 \cap A_1| + \ldots + (-1)^k \binom{k}{k} |A_0 \cap \ldots \cap A_{k-1}|.$$

Determine first the value $|S \setminus \{A_0 \cup \ldots \cup A_{k-1}\}|$. It is clear that the elements of $S \setminus \{A_0 \cup \ldots \cup A_{k-1}\}$ are those minima of Λ the supports of which include the elements $\underline{0}, \underline{e}_1, \ldots, \underline{e}_{k-1}$. Since the support of a minimum vector of Λ is a coset, the support of such a minimum vector is a subspace of V and contains the subspace generated by the elements $\{\underline{e}_1, \ldots, \underline{e}_{k-1}\}$. But the number of these subspaces in V of dimension m (where $k-1 \leq m \leq n$) is equal to the number of the $m-k+1$-dimensional subspaces of a vectorspace V_{n-k+1} of dimension $n-k+1$ over the Galois field $GF(2)$, for this reason this common value is $K_{n-k+1,n-m}$. We know from the Theorem 1 that the support of a minima of the lattice Λ is a coset of dimension $n-R$, where R is odd. So if m is the dimension of the support of a minimum then for an odd number R we have $n-R=m$ hence $n-m=R$ so $n-m$ is odd. It

is known (see [1]) that there are $2^{1+\binom{m}{1}+\binom{m}{2}}$ minima with such an m-dimensional support so according to the condition $k-1 \leq n-R \leq n$ we have the formula

$$|S \setminus \{A_0 \cup \ldots \cup A_{k-1}\}| = \sum_{\substack{R=1 \\ R \in I}}^{n-k+1} 2^{1+\binom{n-R}{1}+\binom{n-R}{2}} \cdot K_{n-k+1,R},$$

where I is the set of odd numbers. A simple calculation shows that the formula

$$\begin{aligned} &|S\setminus\{A_0 \cup \ldots \cup A_{k-1}\}| = \\ &= \sum_{\substack{R=1 \\ R \in I}}^{n-k+1} 2^{n(k-1)-\binom{k-1}{2}} \cdot 2^{1+\binom{n-k+1-R}{1}+\binom{n-k+1-R}{2}} \cdot K_{n-k+1,R} \cdot \left(2^{-(k-1)}\right)^R = \\ &= 2^{n(k-1)-\binom{k-1}{2}} \cdot \sum_{\substack{R=1 \\ R \in I}}^{n-k+1} 2^{1+\binom{n-k+1-R}{1}+\binom{n-k+1-R}{2}} \cdot K_{n-k+1,R} \cdot \left(2^{-(k-1)}\right)^R \end{aligned}$$

holds. In the paper [3] it was proved that the generator function

$$g_n(x) = \sum_{n-R} 2^{1+\binom{n-R}{1}+\binom{n-R}{2}} \cdot K_{n,R} \cdot x^{n-R}$$

can be also written in the following form

$$g_n(x) = 2(1+2x)(1+2x^2)\cdots(1+2^n x).$$

From this the product form of the function

$$f_n(x) = \sum_{n-R} 2^{1+\binom{n-R}{1}+\binom{n-R}{2}} \cdot K_{n,R} \cdot x^R$$

can be calculated, hence we get that

$$f_n(x) = x^n g_n\left(\frac{1}{x}\right) = x^n \cdot 2\left(1+\frac{2}{x}\right)\left(1+\frac{2^2}{x}\right)\cdots\left(1+\frac{2^n}{x}\right).$$

If we perform the substitutions $n \longmapsto n-k+1, x = 2^{-(k-1)}$, then the value of the function $|S \setminus \{A_0 \cup \ldots \cup A_{k-1}\}|$ can be computed. Since

$$\begin{aligned} f_{n-k+1}\left(2^{-(k-1)}\right) &= 2^{-n(k-1)+(k-1)^2} \cdot 2(1+2^k)(1+2^{k+1}\cdots(1+2^n) \\ &= \left(2^{-(k-1)}\right)^{n-k+1} \cdot 2^{\binom{n+1}{2}-\binom{k}{2}+1} \cdot \prod_{l=k}^{n}\left(1+\frac{1}{2^l}\right) \end{aligned}$$

and

$$\begin{aligned} f_{n-k+1}\left(-2^{-(k-1)}\right) &= \left(-2^{-(k-1)}\right)^{n-k+1} \cdot 2^{\binom{n+1}{2}-\binom{k}{2}+1} \cdot \prod_{l=k}^{n}\left(1-\frac{1}{2^l}\right) \cdot (-1)^{n-k+1} \\ &= \left(2^{-(k-1)}\right)^{n-k+1} \cdot 2^{\binom{n+1}{2}-\binom{k}{2}+1} \cdot \prod_{l=k}^{n}\left(1-\frac{1}{2^l}\right), \end{aligned}$$

hence the above sum is:

$$|S\setminus\{A_0\cup\ldots\cup A_{k-1}\}| = 2^{n(k-1)-\binom{k-1}{2}}\frac{f_{n-k+1}\left(2^{-(k-1)}\right)-f_{n-k+1}\left(-2^{-(k-1)}\right)}{2}$$
$$= 2^{n(k-1)-\binom{k-1}{2}}\cdot 2^{-(k-1)(n-k+1)+\binom{n+1}{2}-\binom{k}{2}}\cdot\Big[\prod_{l=k}^{n}\left(1+\tfrac{1}{2^l}\right)-\prod_{l=k}^{n}\left(1-\tfrac{1}{2^l}\right)\Big]$$
$$= 2^{\frac{n(n+1)}{2}}\cdot\Big[\prod_{l=k}^{n}\left(1+\tfrac{1}{2^l}\right)-\prod_{l=k}^{n}\left(1-\tfrac{1}{2^l}\right)\Big].$$

This calculation is valid in the case when $1\le k\le n$, so with the trivial equality $|S| = |S|$ for the determination of the unknown values $|A_0|, |A_0\cap A_1|, \ldots, |A_0\cap\ldots\cap A_{k-1}|$ we have an $n+1$-dimensional linear equation array with the following matrix.

$$A = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & \cdots & 0 \\ 1 & -1 & 0 & \cdots & 0 & \cdots & 0 \\ 1 & -2 & 1 & \cdots & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdots & \cdot \\ 1 & -\binom{k}{1} & \binom{k}{2} & \cdots & (-1)^k\binom{k}{k} & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdots & \cdot \\ 1 & -\binom{n}{1} & \binom{n}{2} & \cdots & (-1)^k\binom{n}{k} & \cdots & (-1)^n\binom{n}{n} \end{pmatrix}$$

The inverse of this matrix coincides with itself. This follows from the fact that the product of the j-th column and i-th row of this matrix is equal to

$$\Big[\sum_{k=i-1}^{j-1}(-1)^k\ \binom{j-1}{k}(-1)^{i-1}\binom{k}{i-1}\Big]_j^k = (-1)^{i-1}\sum_{k=i-1}^{j-1}(-1)^k\binom{j-1}{k}\binom{k}{i-1}$$
$$= (-1)^{i-1}\binom{j-1}{i-1}\sum_{k=i-1}^{j-1}(-1)^k\binom{j-i}{k-i+1} = \begin{cases} 0, & \text{if } j>i, \\ (-1)^{i+j-2}=1, & \text{if } j=i. \end{cases}$$

Since in the case of $j<i$ the examined product is zero, we have that this matrix is its own inverse. So the statement of the theorem results from the inversion of this equation array. We get the following:

$$|A_0\cap\ldots\cap A_{k-1}| =$$
$$= |S| - k|S\setminus\{A_0\}| + \binom{k}{2}|S\setminus\{A_0\cup A_1\}| + \ldots + (-1)^k\binom{k}{k}|S\setminus\{A_0\cup\ldots\cup A_{k-1}\}|.$$

From this we have for the number of minima of the examined lattice:

$$s(\Lambda_{\mathcal{H}}) = 2^{\frac{n(n+1)}{2}}\left\{\prod_{l=0}^{n-1}\left(1+\tfrac{1}{2^l}\right) - \binom{k}{1}\left[\prod_{l=1}^{n}\left(1+\tfrac{1}{2^l}\right)-\prod_{l=1}^{n}\left(1-\tfrac{1}{2^l}\right)\right]+\right.$$
$$\left.+\cdots+(-1)^k\binom{k}{k}\left[\prod_{l=k}^{n}\left(1+\tfrac{1}{2^l}\right)-\prod_{l=k}^{n}\left(1-\tfrac{1}{2^l}\right)\right]\right\}.$$

■

REMARK 2. For the case $k = 1$ this formula gives the value of $s(\Lambda_{<\underline{0}>})$. This number was determined in the paper [3] using other methods. But the two formulae give the same value, because:

$$|A_0| = 2^{\frac{n(n+1)}{2}} \cdot \{\prod_{l=0}^{n-1}(1+\tfrac{1}{2^l}) - \tbinom{k}{1}[\prod_{l=1}^{n}(1+\tfrac{1}{2^l}) - \prod_{l=1}^{n}(1-\tfrac{1}{2^l})]\}$$

$$= 2^{\frac{n(n-1)}{2}} \cdot \{2 \cdot 2^n \prod_{l=1}^{n-1}(1+\tfrac{1}{2^l}) - 2^n \prod_{l=1}^{n-1}(1+\tfrac{1}{2^l})(1+\tfrac{1}{2^n}) + 2^n \prod_{l=1}^{n-1}(1-\tfrac{1}{2^l})(1-\tfrac{1}{2^n})\}$$

$$= 2^{\frac{n(n-1)}{2}} \cdot \{(2^n-1)\prod_{l=1}^{n-1}(1+\tfrac{1}{2^l}) + (2^n-1)\prod_{l=1}^{n-1}(1-\tfrac{1}{2^l})\}$$

$$= (2^n-1)2^{\frac{n(n-1)}{2}}\{\prod_{l=1}^{n-1}(1+\tfrac{1}{2^l}) + \prod_{l=1}^{n-1}(1-\tfrac{1}{2^l})\}.$$

REMARK 3. It seems to be a hard problem to determine the asymptotic form of the formula of the Theorem 3. The author does not know it in the general

"Kissing number"

n	k	N	$s(\Lambda_{\mathcal{H}})$	$s(\Lambda_{V_{n-1},<\{\underline{0}\}>})$	s'_N
3	0	8	240		240
	1	7	126		126
	2	6	60	72	72
	3	5	26		40
4	0	16	4320		4320
	1	15	2340		2340
	2	14	1260	954	1422
	3	13	696		906
	4	12	392		648
5	0	32	208320		208320
	1	31	80910		
	2	30	45900	45270	
	3	29	27498		
	4	28	17496		
	5	27	11782		
6	0	64	9694080		9694080
	1	63	5386500		
	2	62	3130380	2323080	
	3	61	1940760		
	4	60	1291560		
	5	59	918972		
	6	58	690388		

case. But in the case $k = 1$, this value is known (by virtue of the preceding remark this is the same as the one determined in [4] and in the case $k = 2$ and $n \geq 4$ it can be proved that in the examined lattice there are more minima than in the lattice of dimension $N = 2^n - 2$ which was investigated in the paper [4]. In both of these cases the number of minima is asymptotically not less than $c\left(2^{\frac{1}{2}(\log n^2 + \log n)}\right)$, where the constant c is independent from the dimension. In the cases of lower dimensions we calculated the values of the kissing numbers obtained in [4] and in this work. See the columns 5 and 4 of the table above. In the last column the best results which are known can be found (see for example [2]).

REFERENCES

[1] E.S. BARNES and G.E. WALL, Some extreme forms defined in terms of Abelian groups, *Journal of the Australian Math. Soc.*(1959), 47–63.

[2] J.M. CONWAY and N.J.A. SLOANE, *Sphere Packings, Lattices and Groups*, Springer-Verlag (1988)

[3] Á.G. HORVÁTH, On the number of the minima of N-lattices. *Conference on Intuitive Geometry, Szeged,* (1991) (to appear)

[4] Á.G. HORVÁTH, Codes and lattices. *Periodica Polytechnica Hungarica* (to appear)

[5] J. LEECH, Some sphere packings in higher space. *Canadian J. Math.* 16 (1964)

(Received: October 8, 1993)
(In final form: January 13, 1995)

DEPARTMENT OF GEOMETRY
TECHNICAL UNIVERSITY OF BUDAPEST
H-1521 BUDAPEST
HUNGARY