

# Counting Lattice Points in Pyramids

Patrick Solé \*

## Abstract

The old problem of counting lattice points in euclidean spheres leads to use Jacobi Theta functions and its relatives as generating functions. Important lattices (root systems, the Leech lattice) can be constructed from algebraic codes and analogies between codes and lattices have been extensively studied by coding theorists and number theorists alike . In this dictionnary, the MacWilliams formula is the finite analog of the Poisson formula.

The new problem of counting lattice points in spheres for the  $L^1$  distance leads to hyperbolic trigonometric functions. The same analogy exists but the  $L^1$  counterpart of the Poisson formula is missing. The MacWilliams formula lead to such a duality formula for those lattices which are constructed from codes via Construction A. A connection with Ehrhart's enumerative theory of polytopes is pointed out. Both problems have important applications in multidimensional vector quantization.

## 1 Motivation

An  $n$ -dimensional lattice  $\Lambda_n$  is defined as a set of vectors

$$\Lambda_n = \{X \in \mathbb{R}^m | X = u_1 a_1 + \dots + u_n a_n\}$$

where  $a_1, \dots, a_n$  are linearly independent vectors in  $m$ -dimensional real Euclidean space  $\mathbb{R}^m$  with  $m \geq n$ , and  $u_1, \dots, u_n$  are in  $\mathbb{Z}$ . A well known result of Lloyd-Max is that, for quantizing an uniform distribution on the real line, the decision intervals have to be taken of the form  $[n - \frac{1}{2}, n + \frac{1}{2}]$ . The centers of the intervals constitute a one dimensional lattice ( $n = 1$ ). In the general  $n$ -dimensional case, the role of the integers is played by the lattice points, and the role of the decision intervals is played by the so-called Voronoi region of the Lattice [2]. It was shown by Zador [9], extending pionner work of Schützenberger [6], that the quadratic error depended crucially on the geometry of the lattice by a term called the second moment of the lattice [6]. If  $G_n$  denotes the average mean squared error per dimension for the best quantizing lattice in  $n$  dimensions, then Zador showed that:  $\lim(G_n) = \frac{1}{2\pi e} < \frac{1}{12}$  for large  $n$ . This demonstrates the interest of using multidimensionnal lattices. As Conway and Sloane put it : "it pays to procrastinate". In general, finding the best

---

\*CNRS, I3S , 250, rue A. Einstein, 06 560 Valbonne, FRANCE. Work supported in part by PRC Math-Info.

quantizing lattices in  $n$  dimensions is a difficult task. They are only known for some integers  $n \leq 24$ . More applicative information can be found in the companion paper [1].

When using an infinite lattice for source coding one needs to truncate it according to a shape suited to the probability law of the source to be encoded : euclidean spheres for a Gaussian distribution, pyramids (or hyperoctahedra) for an exponential distribution. It is of practical importance to know how many lattice points remain in the truncated lattice. This task is performed with the help of generating functions

- the old theta functions for spheres
- the new nu function for pyramids

This work emphasizes two analogies:

- codes vs lattices
- spheres vs pyramids

The paper is organized as follows. After reviewing the first analogy in section 1, we develop the second in section 2. In section 3 we derive the generating functions associated with the problem of counting lattice points for pyramids. In particular we treat root systems  $D_n, E_8$ . A few numerical results are presented in section 4. We highlight differences, in particular the non-invariance of pyramids by rotations of  $\mathbb{R}^n$ , and the absence of a Poisson summation formula (subsection 3.3). The connection with Ehrhart's enumerative theory of Polytopes is developed in section 5.

## 2 Theta functions of Lattices

### 2.1 Lattices

The theta function of a lattice  $\Lambda$  is defined as the formal power series:

$$\theta_\Lambda(q) = \sum_{x \in \Lambda} q^{\|x\|^2},$$

where  $\|x\|^2 = x \cdot x$ , the squared standard euclidean norm. In words the coefficient  $N_m$  of  $q^{m^2}$  in  $\theta_\Lambda(q)$  counts the number of lattice points at distance  $m$  from the origin in  $\mathbb{R}^n$ . The classical Jacobi theta function is

$$\Theta(\xi|z) = \sum_{m=-\infty}^{+\infty} e^{2mi\xi + \pi izm^2}.$$

The sum converges for  $\Im(z) > 0$  (the so-called Poincaré upper half-plane). It is classical to set  $q = e^{\pi iz}$ . For us,  $q$  will be, however an indeterminate. Special instances of this formula which will be of use here are

$$\theta_3(q) = \Theta(0|z) = \sum_{m=-\infty}^{+\infty} q^{m^2},$$

the theta function of  $\mathbb{Z}$ , and

$$\theta_2(q) = e^{\frac{2\pi z}{4}} \Theta\left(\frac{\pi z}{2} | z\right) = \sum_{m=-\infty}^{+\infty} q^{(m+\frac{1}{2})^2}.$$

If we extend the definition of theta functions from lattices to cosets of lattices we see that  $\theta_{2\mathbb{Z}+1}(q) = \theta_2(q^4)$ . It will also be noticed that  $\theta_{2\mathbb{Z}}(q) = \theta_3(q^4)$ . Finally, we will also need the relation

$$\theta_4(q) = \theta_3(q^4) - \theta_2(q^4), \quad (1)$$

where

$$\theta_4(q) = \Theta\left(\frac{\pi}{2} | z\right) = \sum_{m=-\infty}^{+\infty} (-q)^{m^2}.$$

as well as the simpler

$$\theta_3(q) = \theta_3(q^4) + \theta_2(q^4), \quad (2)$$

which follows from the coset decomposition  $\mathbb{Z} = 2\mathbb{Z} + (2\mathbb{Z} + 1)$ .

## 2.2 Algebraic Codes

For us a binary linear *code* of length  $n$  will be a linear subspace of  $\mathbb{F}_2^n$  coordinatized w.r.t. a special basis of  $\mathbb{F}_2^n$ . The *weight* of a binary vector  $u$ , henceforth denoted by  $|u|$  is the number of its nonzero coordinates on this basis. The weight enumerator of a code  $C$  is defined as

$$W_C(x, y) = \sum_{u \in C} x^{n-|u|} y^{|u|}.$$

We denote by  $|C|$  the cardinality of  $C$ . For more details on block codes we refer to [2].

## 2.3 Construction A

The most simple way to associate a lattice with a code is construction A.

$$A(C) := \{(x_1, \dots, x_n) \in \mathbb{Z}^n | \exists c \in C, x \equiv c \pmod{2}\}.$$

Then the following result is classical (Theorem 3 of Chapter 7 of [2]).

$$\theta_{A(C)} = W_C(\theta_3(q^4), \theta_2(q^4)).$$

Denoting by  $U_n$  the universe code  $\mathbb{F}_2^n$ , we see that  $W_{U_n}(x, y) = (x + y)^n$ , and that  $A(U_n) = \mathbb{Z}^n$ , so that

$$\theta_{\mathbb{Z}^n}(q) = (\theta_3(q^4) + \theta_2(q^4))^n = \theta_3(q)^n,$$

(by equation (2)) which was to be expected by the product rule for ordinary generating functions since  $\mathbb{Z}^n$  is a cartesian product.

The root lattice  $D_n$  (dubbed checkerboard lattice in [2]) is defined as follows

$$D_n = \{(x_1, \dots, x_n) \in \mathbb{Z}^n \mid \sum_{i=1}^n x_i \equiv 0(2)\}.$$

Clearly,  $D_n = A(EW_n)$  where  $EW_n$  is the even weight code of dimension  $n - 1$ . Its weight enumerator collects the even powers of  $y$  in the w.e. of  $U_n$ .

$$W_{EW_n}(x, y) = \frac{1}{2}((x + y)^n + (x - y)^n).$$

By equations (1) and (2) we see that

$$\theta_{D_n}(q) = \frac{1}{2}(\theta_3(q)^n + \theta_4(q)^n).$$

A slightly more advanced example is obtained for the root lattice  $E_8$  which is produced by construction  $A$  applied to the Hamming code  $H_8$  of length 8 of weight enumerator

$$W_{H_8} = x^8 + 14x^4y^4 + y^8.$$

This yields equation (101) of Chapter 4 of [9]

$$\theta_{E_8} = \theta_2(q)^8 + 14\theta_2(q)^4\theta_3(q)^4 + \theta_3(q)^8.$$

## 2.4 Construction B

Construction  $B$  of [2] is defined as follows. Let  $C$  denote a binary linear code with weights multiple of 4. (Such a code is usually called “doubly even”). With this code construction  $B$  associates a lattice  $B(C)$  by the formula

$$B(C) := \{(x_1, \dots, x_n) \in \mathbb{Z}^n \mid \exists c \in C, x \equiv c(2) \sum_{i=0}^n x_i \equiv 0((4))\}.$$

The following result is classical (Theorem 15 of Chapter 7 of [2]).

$$\theta_{B(C)}(q) = \frac{1}{2}W_C(\theta_3(q^4), \theta_2(q^4)) + \frac{1}{2}\theta_4(q^4)^n.$$

## 2.5 Poisson and MacWilliams

The dual of a code  $C$  is its dual w.r.t to the standard inner product  $x \cdot y = \sum_{i=1}^n x_i y_i$ , and is usually denoted by  $C^\perp$ . The celebrated MacWilliams formula connects the w.e. of a code with the w.e. of its dual.

$$W_{C^\perp}(x, y) = \frac{1}{|C|}W_C(x + y, x - y).$$

The dual of a lattice  $\Lambda$  is defined w.r.t. to the same inner product as

$$\Lambda^* = \{x \in \mathbb{R}^n \mid \forall y \in \Lambda \ x \cdot y \in \mathbb{Z}\}$$

The Poisson formula connects the theta function of a lattice with the theta function of its dual. We denote by  $|L|$  the elementary volume of the lattice  $L$ . Letting  $q = e^{\pi iz}$ , we have

$$\theta_{L^*}(e^{\pi iz}) = |L| \left(\frac{i}{z}\right)^{n/2} \theta_L(e^{-(i\pi)/z}).$$

Construction  $A$  and  $B$  behave nicely w.r.t. duality

$$A(C)^* = \frac{1}{2} A(C^\perp) \tag{3}$$

$$B(C)^* = \frac{1}{2} B(C^\perp). \tag{4}$$

Indeed one could derive the MacWilliams formula from the Poisson formula by using relation 3 and construction  $A$ .

### 3 The Nu function of Lattices

For  $x \in \mathbf{R}^n$ , let  $\|x\|_1 = \sum_{i=1}^n |x_i|$ , and  $\|x\| = \sqrt{\sum_{i=1}^n |x_i|^2}$ . For a lattice  $\Lambda$ , we define its function Nu by the relation

$$\nu_\Lambda(z) = \sum_{y \in \Lambda} z^{\|y\|_1} = \sum_{n=0}^{+\infty} z^n |\{y \in \Lambda \mid \|y\|_1 = n\}|.$$

Note the analogies and differences with the definition of the theta function [2]

$$\theta_\Lambda(q) = \sum_{y \in \Lambda} q^{\|y\|^2} = \sum_{n=0}^{+\infty} q^{n^2} |\{y \in \Lambda \mid \|y\| = n\}|.$$

**Caution** Unlike the euclidean norm, the norm  $\|\cdot\|_1$  depends on the chosen orthogonal basis. Different bases may yield different functions  $\nu_\Lambda$  for the same lattice  $\Lambda$ . An example of this situation will be given for  $\Lambda = E_8$ , where construction  $A$  and construction  $B$  yield different Nu functions.

#### 3.1 Easy Examples: $\mathbb{Z}$ , $2\mathbb{Z}$ and $\mathbb{Z}^n$ .

First we start with dimension 1, where the well-known uniform quantifier (lattice  $\mathbb{Z}$ ) has Nu function

$$\nu_{\mathbb{Z}}(z) = 1 + 2 \sum_{n=0}^{+\infty} z^n = 1 + \frac{2z}{1-z} = \frac{1+z}{1-z},$$

a geometric series. The lattice of even integers has Nu function (by scaling)

$$\nu_{2\mathbb{Z}}(z) = \sum_{y \in 2\mathbb{Z}} z^{2\|y\|_1} = \nu_{\mathbb{Z}}(z^2) = \frac{1+z^2}{1-z^2},$$

and the set of odd integers, which is a coset of the preceding into  $\mathbb{Z}$  (by difference)

$$\nu_{1+2\mathbb{Z}}(z) = \nu_{\mathbb{Z}}(z) - \nu_{2\mathbb{Z}}(z) = \frac{2z}{1-z^2}.$$

Since the cubic lattice is a cartesian product of  $n$  linear lattices, we get

$$\nu_{\mathbb{Z}^n}(z) = (\nu_{\mathbb{Z}}(z))^n = \left(\frac{1+z}{1-z}\right)^n.$$

Since  $D_n$  consists of those vectors of  $\mathbb{Z}^n$  whose  $L_1$  norm is even, we see that its Nu function is the even part of  $\nu_{\mathbb{Z}^n}(z)$  that is

$$\nu_{D_n}(z) = \frac{1}{2}(\nu_{\mathbb{Z}^n}(z) + \nu_{\mathbb{Z}^n}(-z)).$$

### 3.2 Connection with block codes

The next result generalizes to the  $L^1$  metric the Theorem 3 of Chapter 7 of [2].

**Theorem 1** *Let  $C$  be a binary linear block code with weight enumerator  $W_C(x, y)$ . Then*

$$\nu_{A(C)} = W(\nu_{2\mathbb{Z}}(z), \nu_{1+2\mathbb{Z}}(z)) = W_C(1+z^2, 2z)(1-z^2)^{-n}.$$

*Alternatively, for an indeterminate  $\alpha$ , we have*

$$\nu_{A(C)}(\tanh(\frac{\alpha}{2})) = W(\cosh(\alpha), \sinh(\alpha)).$$

**Proof:** Let  $c \in C$  and  $\bar{c}$  denote the following lattice

$$\{y \in \mathbb{Z}^n \mid y \equiv c[2]\}$$

Then  $A(C)$  is a disjoint union of such  $\bar{c}$  for  $c \in C$ . This entails

$$\nu_{A(C)} = \sum_{c \in C} \nu_{\bar{c}}(q).$$

To compute each summand, observe that  $\bar{c}$  is a cartesian product  $(2\mathbb{Z})^{n-|c|}(1+2\mathbb{Z})^{|c|}$ . Therefore

$$\nu_{\bar{c}}(q) = \nu_{(2\mathbb{Z})^{n-|c|}}(q) \nu_{(1+2\mathbb{Z})^{|c|}}(q).$$

The result follows. □

Let  $R_n := \{0, 1\}$  denote the repetition code. Clearly  $W_{R_n}(x, y) = x^n + y^n$ . From the dual of the repetition code, we get  $\nu_{D_n} = \frac{1}{2}(\nu_{\mathbb{Z}^n}(z) + \nu_{\mathbb{Z}^n}(-z))$ , as was expected from section 3.1. The dual code yields the  $\nu$  function of the dual lattice.

$$\nu_{D_n^*} = 2((1+z^2)^n + 2^n z^n)/(2-2z^2)^n.$$

From the Hamming code of length 8, we get

$$\begin{aligned} \nu_{E_8}(z) &= [(1+z^2)^8 + 224z^4(1+z^2)^4 + 256z^8]/(1-z^2)^8 = \\ &= 1 + 16z^2 + 352z^4 + 3376z^6 + 19648z^8 + 82256z^{10} + O(z^{12}). \end{aligned}$$

Applying the complex variable techniques of [4] yields the following asymptotic estimate ( a more elementary and more tedious proof can be obtained by partial fraction expansion)

**Corollary 1**

$$[z^m] \frac{\nu_{A(C)}(z)}{1-z} \sim |C| \frac{m^n}{n!}.$$

**Proof:** From Theorem 1 we see that  $\nu_{A(C)}(z)$  has a singularity in  $z = 1$  where it is equivalent to  $\frac{|C|}{(1-z)^n}$ , since  $W$  being homogeneous  $W(2, 2) = 2^n$ . Now the term in  $z^m$  in  $\frac{1}{(1-z)^n}$  is  $\binom{n+m-1}{m-1}$ . The result follows by the transfer Theorems of Flajolet-Odlyzko.  $\square$

Since the volume of the elementary parallelotope of  $A(C)$  is  $\frac{2^n}{|C|}$ , and the volume of the unit  $L^1$  sphere is  $\frac{2^n}{n!}$ , Corollary 1 says that the number of lattice points at  $L^1$  distance  $m$  from the origin is asymptotically equivalent to the volume of the  $L^1$  sphere of radius  $m$  divided by the volume of the lattice. This intuitive result is known as ‘‘Gauss counting principle’’[5].

**Theorem 2** *Let  $C$  be a doubly even binary code of length  $n$ , and weight enumerator  $W$ . Its Nu function is*

$$\nu_{B(C)}(z) = \frac{1}{2}W\left(\frac{1+z^2}{1-z^2}, \frac{2z}{1-z^2}\right) + \frac{1}{2}\left(\frac{1-z^2}{1+z^2}\right)^n.$$

**Proof:** Let  $f(q, a)$  denote the bivariate generating function

$$(\nu_{4z}(q) + a\nu_{4z+2}(q))^{n-|c|}(\nu_{4z+1}(q) + a\nu_{4z-1}(q))^{|c|}$$

We claim that, with the notations of the proof of Theorem 1, we have

$$\nu_{\bar{c}}(q) = \frac{1}{2}(f(q, 1) + f(q, -1))$$

Since  $\nu_{4z+1}(q) = \nu_{4z-1}(q)$ , the only contribution of  $f(q, -1)$  comes from the term in  $|c| = 0$ . Then the values of  $\nu_{4z}(q)$  and  $\nu_{4z+2}(q)$  are easily computed by scaling from the values of  $\nu_{(2z)}$  and  $\nu_{(2z+1)}$  calculated in section (4.1). The result follows.

To prove the claim, let  $c \in B(C)$  and  $y \in \bar{c}$  and let  $N_i, i = 0, \pm 1, 2$ , denote the number of coordinates of  $y$  congruent to  $i \pmod 4$ . Since  $|c|$  is a multiple of 4 we see that  $N_1 + N_{-1} \equiv 0[4]$ . From there it follows that the sum  $\sum_i y_i$ , which is  $N_1 + 2N_2 - N_{-1}$ , is congruent to 0 modulo 4. as it should in construction B, iff  $N_2 + N_{-1}$  is even. But this latter term is obtained by summing up the even terms in  $a$  in  $f(q, a)$ .  $\square$

We are indebted to Dr. Sloane for the  $L^2$  version of this proof.

Applied to the code  $R_8$  this theorem yields a different result for the nu function of  $E_8$ .

$$\nu_{E_8}(z) = \frac{1}{2} \frac{(1+z^2)^8 + 256z^8}{(1-z^2)^8} + \frac{1}{2} \frac{(1-z^2)^8}{(1+z^2)^8} = 1 + 128z^4 + 2944z^8 + 1024z^{10} + O(z^{12})$$

This could be expected from asymptotic considerations since we have by [4]

**Corollary 2**

$$[z^m] \frac{\nu_{B(C)}(z)}{1-z} \sim \frac{|C|}{2} \frac{m^n}{n!}.$$

**Proof:** From Theorem 2 we see that  $\frac{\nu_{B(C)}(q)}{1-q}$  has a singularity at  $z = 1$  where it is equivalent to  $\frac{|C|}{2(1-q)^{n+1}}$ , since  $W(2, 2) = 2^n$ . The rest is analogous to the proof of Corollary 1. □

This shows that if a lattice can be constructed both by construction A and construction B, they will yield different orientations, and, in addition, orientation B will have half as many points in pyramids, which is interesting in quantizing applications.

**3.3 Nu Functions of Dual lattices**

There is no known analog of the Poisson-Jacobi formula. The combination of MacWilliams formula and of the relation 3 for construction A leads to the following conjecture.

**Conjecture 1** *Let the parameters  $\alpha$  and  $\beta$  be connected by the relation  $e^{-2\beta} = \tanh(\alpha)$ , and let  $L$  be a lattice. The functions  $\nu_L$  and  $\nu_{L^*}$  satisfy the identity*

$$2^{n/2} \nu_{L^*}(\tanh^2(\frac{\beta}{2})) = |L|(\sinh(2\beta))^{n/2} \nu_L(\tanh(\frac{\alpha}{2})).$$

The relation between  $\alpha$  and  $\beta$  is indeed symmetric:  $e^{-2\alpha} = \tanh(\beta)$ .

**4 Numerical Examples**

In the following tables the second line indicates the number of lattice points *within* a pyramid of height  $m$ . The fourth line indicates the number of lattice points *within* a sphere of radius  $m$ . In all examples the pyramids of sufficiently large radius present much fewer lattice points than the euclidean spheres of the same radius. In the case of cubic lattices this can be paralleled with the fact that the volume of the unit  $n$ -sphere is  $2^{n/2}/\Gamma(n/2 + 1)$ , whereas the volume of the unit  $n$ -pyramid is  $2^n/n!$ , which is much smaller for large  $n$ . All calculations were performed in MAPLE on a DEC 500.

**4.1 Plane Cubic Lattice  $\mathbb{Z}^2$**

$m$	1	2	3	4
$[z^m]\nu(z)/(1-z)$	5	13	25	41
$m^2$	1	4	9	16
$[q^{m^2}]\theta(q)/(1-q)$	5	13	25	51



## 4.2 Cubic Lattice in dimension 3: $\mathbb{Z}^3$

$m$	1	2	3	4	5
$[z^m]\nu(z)/(1-z)$	7	25	63	129	231
$m^2$	1	4	9	16	25
$[q^{m^2}]\theta(q)/(1-q)$	7	27	90	224	482

Note that the surpopulation of spheres as compared to pyramids starts earlier ( $m = 2$ ) than in the preceding example.

## 4.3 Lattice $D_4$

$m$	1	2	3	4	5	6	7	8
$[z^m]\nu(z)/(1-z)$	1	33	33	225	225	833	833	2241
$m^2$	1	4	9	16	25	36	49	64
$[q^{m^2}]\theta(q)/(1-q)$	1	49	149	605	1435	3307	5659	9979

## 4.4 Lattice $E_8$

Note the factor 10 between the two entries for  $m = 4$ .

$m$	1	2	3	4
$[z^m]\nu(z)/(1-z)$	1	129	129	3073
$m^2$	1	4	9	16
$[q^{m^2}]\theta(q)/(1-q)$	1	2401	26641	340321

## 5 Nu functions of sub-lattices of $\mathbb{Z}^n$ .

In this section, we shall show that the function  $\nu(z)$  of a full rank sublattice of  $\mathbb{Z}^n$  is always a rational function. We shall rely on a result of Ehrhart [8, Theorem 4.6.25], and will assume some familiarity with polytopes.

**Lemma 1** *Let  $\mathcal{P}$  denote a convex rational polytope of  $\mathbb{R}^n$ , with vertex set  $V$  and let  $p_m = |m\mathcal{P} \cap \mathbb{Z}^n|$ . Then*

$$\sum_{m \geq 0} p_m z^m = \frac{P(z)}{\prod_{a \in V} (1 - z^{d(a)})},$$

where  $d(a)$  is the smallest integer  $q$  such that  $qa \in \mathbb{Z}^n$ . Further,  $\deg(P) < \sum_{a \in V} d(a)$ .

Let  $H_n$  denote the  $n$ -dimensional octahedron, namely

$$H_n = \{x \in \mathbb{R}^n \mid \|x\|_1 = 1\}.$$

Alternatively,  $H_n$  can be thought of as the convex hull of the  $2n$  vectors  $\pm e_i$ , where  $e_i, i = 1, 2, \dots, n$  is the canonical basis. By the multiplicative property of the  $L^1$  norm, for an  $x$  of  $\mathbb{R}^n$ , we have  $\|x\|_1 = m$  iff  $x \in m\mathcal{P}$ . We are now in a position to state the main result of this section.

**Theorem 3** Let  $\Lambda \subseteq \mathbb{Z}^n$  be a lattice with generating matrix  $A$  of full rank. Let  $a_i$  be the rows of  $A^{-1}$ . Then

$$\nu_\Lambda(z) = \frac{P(z)}{\prod_{i=1}^n (1 - z^{d(a_i)})},$$

where  $P \in \mathbb{Z}[X]$  and  $\deg(P) < \sum_{i=1}^n d(a_i)$ . In particular, the roots of the denominator are complex  $N^{\text{th}}$  roots of unity with  $N = \det(A)$ .

**Proof:** By definition of the Nu function, we have

$$[z^m]\nu_\Lambda(z) = |mH_n \cap \Lambda| = |mH_n A^{-1} \cap \mathbb{Z}^n|.$$

Now, let  $\mathcal{P} = H_n A^{-1}$ , with vectors of  $H_n$  considered as row vectors. Like  $H_n$ , the body  $\mathcal{P}$  is a convex rational polytope with vertices  $\pm e_i A^{-1}$ . By Cramer's rule  $d(a_i)$  divides  $\det(A)$ . The result follows by the preceding Lemma.  $\square$

As an immediate application of the Theorem, we can recover part of Theorem 1. In construction A it is known [2] that, if  $C$  has dimension  $k$ , and binary generating matrix  $(I_k|B)$ , then a generating matrix of  $A(C)$  is

$$A = \left( \begin{array}{c|c} I_k & B \\ \hline 0 & 2I_{n-k} \end{array} \right).$$

It is then easy to see that for this matrix  $d(a_i) = 2$  for every  $i$ . This is consistent with Theorem 1 where the expression  $(1 - z^2)^n$  was found for the denominator of Nu. It would be nice to have a combinatorial interpretation of the numerator in the general case. In view of Gauss counting principle and of the results of the preceding section it is natural to make the following conjecture.

**Conjecture 2** Let  $\Lambda \subseteq \mathbb{Z}^n$  be a lattice with generating matrix of full rank  $A$ . Then, when  $z$  is near 1

$$\frac{\nu_\Lambda(z)}{1 - z} \sim \frac{1}{\det(A)(1 - z)^{n+1}}.$$

In particular, if  $P(1) \neq 0$ , then  $P(1) = 1$ .

## 6 Acknowledgement

The author wishes to thank N.J.A. Sloane for [7] and for helpful discussions and R.A. Calderbank for inviting him to give a talk in Bell Labs on this topic in October 1991. He also thanks Loic Pottier for helpful discussions on polytopes.

## References

- [1] M. Barlaud, P. Solé, M. Antonini, P. Mathieu, T. Gaidon, "A Pyramidal Scheme for Lattice Vector Quantization of Wavelet Transform Coefficients Applied to Image Coding," submitted to IEEE Trans. on Image Processing.
- [2] J.H. Conway, N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Springer (1988).

- [3] E. Ehrhart, *Polynômes Arithmétiques et Méthodes des polyèdres en Combinatoire* Birkhäuser (1977).
- [4] P. Flajolet, A. Odlyzko, "Singularity Analysis of generating Functions", Rapport de Recherche INRIA 826, April 88.
- [5] J. E. Mazo, A.M. Odlyzko, "Lattice Points in High-Dimensional Spheres" Mh. Math. 110, 47-61 (1990).
- [6] M-P. Schützenberger, "On the quantization of finite dimensional messages", Info and control, vol.1, (1958)353-380.
- [7] N.J.A. Sloane, letter to the author, August 1<sup>st</sup>, 1991.
- [8] R.P. Stanley, *Enumerative Combinatorics*, Wadworsth Brooks/ Cole (1986).
- [9] P. Zador, "Asymptotic Quantization Error of Continuous Signals and their Quantization Dimension", IEEE Trans. on Information Theory , vol.IT-28 , 1982.