International Journal of Mathematics and
Computer Science, **16**(2021), no. 2, 705–712

On the number of lattice points in n-dimensional space with an application

Shatha A. Salman

Mathematics and Computer Applications
Faculty of Applied Science
University of Technology
Baghdad, Iraq

email: 100178@uotechnology.edu.iq

(Received November 2, 2020, Accepted December 3, 2020)

Abstract

The principal aim of this work is to provide a proof of a theorem that computes the coefficients of the Ehrhart polynomial in general form. An application for this computation in any dimension is given along with the procedure to calculate the number of lattice points in n-dimensional space with the aid of the Ehrhart polynomial of the output PQ, for two polytopes P and Q whose dimensions are n and m, respectively.

1 Introduction

A polyhedron is a geometrical object used in many topics in pure and applied mathematics. There are two representations of polytopes: the V-polytope and the H-polytope. Any polytope can be represented by one of them [12]. A polytope is a generalized figure in d dimensions, including polygons in two dimensions, polyhedrons in three dimensions, polycells or polychora in four dimensions, and so on. A four-dimensional polytope is sometimes given the special name polychoron. A polytope is presented as the underlying space of a simplicial complex, especially in algebraic topology [5]. There is

Key words: Polytope, Earhart polynomial, product.
AMS (MOS) Subject Classifications: 52B05, 05C30,05C76.
ISSN 1814-0432, 2021, http://ijmcs.future-in-tech.net

a lot of work related to the computation of the number of lattice points in high dimensions; e.g., Salman [6] used the Ehrhart polynomial to find the number of lattice points on a four-dimensional ball. In [7], another tool, the Tutte polynomial, was used to find the number of lattice points on a four-dimensional ball. Salman [8] used solid angle polynomials to find the number of lattice points. Salman et al. [9] applied Fourier transformation to calculate the number of lattice points in high dimensions. Salman [10] computed the number of lattice points, which broke the RSA cryptosystem. Recently, the open problem of finding the number of lattice points on a polytope in high dimensions was proposed. There are many reasons to explore structures in higher dimensions, some of them practical, some simply interesting. The basis of this research can be summed up in steps: first, find the general form for the product of two polytopes; then, any other polytope in high dimensions can be acquired from the obtained polytopes. On the basis of the general form of the theorem, we created an algorithm, without many steps, that works for any dimension, as explained in Section 3. The remainder of the paper is organized as follows: in Section 2, we review several definitions of geometric combinatorics. Section 3 presents the technique together with the proof of the new theorem. In Section 4, the connected calculation with some illustrative applications are given.

2 Ehrhart polynomials and their properties

This section includes the definitions of polytopes, Ehrhart polynomials, and the product of two polytopes.

Definition 1: Geometrically speaking, a polyhedron is simply a three-dimensional solid that consists of an aggregation of polygons, whose edges are joined.

Definition 2: A finite set of points that is a convex hull (which are always bounded) is called a convex polytope, which can also be defined as a bounded intersection of a finite collection of points.

Definition 3: For a convex lattice polytope, the Ehrhart polynomial counts the integer points in an integral dilated polytope, the function of which counts the lattice points in the n-fold dilated copy. Recently, the open problem of finding the number of lattice points on a polytope in high dimen-

sions was proposed. There are many reasons to explore structures in higher dimensions. $L_P : N \to N, L_P(n) = \sharp(n_P \cap Z^d)$ is a polynomial in n, called an Ehrhart polynomial.

Definition 4: Given two convex lattice polytopes $P \subset R_{d_P}$ and R_{d_Q} of dimensions d_P and d_Q, respectively, the product polytope $P \times Q$ is described as follows: $P \times Q = \{(p, q)$, where $p \in P, q \in Q\}$.

Theorem 1: The Ehrhart polynomial for the product of two lattice polytopes is equal to the product of the Ehrhart polynomial of these polytopes separately.

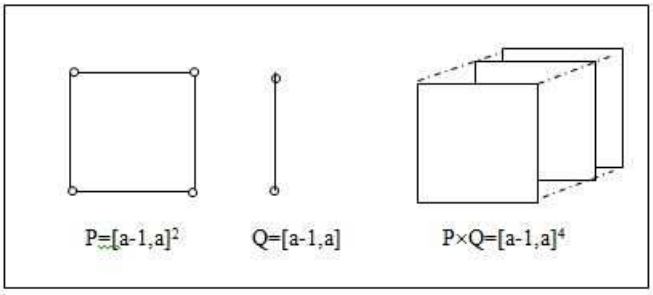

Figure 1: The product of a cube with a line in four dimensions.

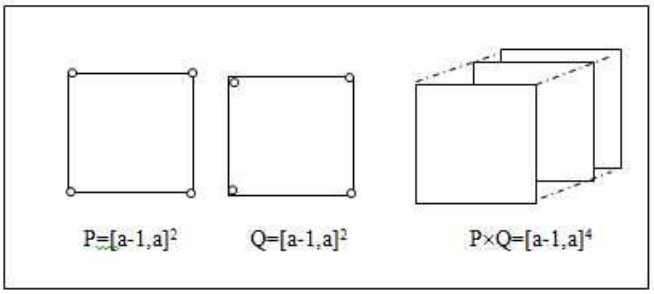

Figure 2: The product of a cube with a square in four dimensions.

3. Formulation of the method

To find the volume of a high-dimensional polytope; i.e., the number of lattice points, the product of two polytopes with their properties is used. Thus, the Ehrhart polynomial for the product of two polytopes is equal to the Ehrhart polynomial for their polytope. We formulate the method as follows:
$P = [a-1, a]^3$ and $Q = [a-1, a], a \geq 1$
$P = \{(a,a,a), (a,a-1,a-1), (a-1,a,a-1), (a-1,a-1,a), (a-1,a-1,a-1)(a-1,a,a), (a,a-1,a)(a,a,a-1)\}$, as given in Figure 1. To find the Ehrhart polynomial for P and Q; that is,
$L_P(t) = t^3 + 3t^2 + 3t + 1$ and $L_Q(t) = t + 1$, we use the cross product
$L_{P\times Q}(t) = L_P(t) \times L_Q(t)$.
Therefore,
$L_{P\times Q}(t) = t^4 + 4t^3 + 6t^2 + 4t + 1$,
and the volume of the polytope $P \times Q$ is 16.

If we take,
$P = [a-1, a]^2$ and $Q = [a-1, a]^2$,
$P = \{(a,a,a), (a,a-1,a-1), (a-1,a,a-1), (a-1,a-1,a), (a-1,a-1,a-1)(a-1,a,a), (a,a-1,a)(a,a,a-1)\}$, as given in Figure 2.

To find the Ehrhart polynomial for P and Q, that is,
$L_P(t) = t^3 + 3t^2 + 3t + 1$ and $L_Q(t) = t^3 + 3t^2 + 3t + 1$,
we use the cross product
$L_{P\times Q}(t) = L_P(t) \times L_Q(t)$.
Hence, the result is
$L_{P\times Q}(t) = t^4 + 4\ t^3 + 6\ t^2 + 4\text{t} + 1$,
and the volume of the polytope $P \times Q$ is 16.
They are equivalent. Simply, the product of two polytopes, the square P and the interval Q, gives a cube, and the product of the squares P and Q also gives a cube. Now, the proof of the theorem, which counts the Ehrhart polynomials for two polytopes, is given.

Theorem 2: The product of two polytopes P and Q gives the polytope W, such that the product of the square P and the interval Q gives a cube, and the squares P and Q also give a cube.

Theorem 3: The Ehrhart polynomial for the product of the d-dimensional simplex with the line polytope Q equal to ; for odd interval N, the Ehrhart

coefficients are $a_3 = N^3/2, a_2 = 2N^2$, and $a_1 = 5N/2$; for even interval N, the Ehrhart coefficients are $a_3 = 4k^3, a_2 = 8k^2$, and $a_1 = 5k, k = 1, 2, 3, 4, \cdots$.
Proof: According to the computation of the Ehrhart polynomial for 2-simplex products of a line, the results of the product for odd and even intervals N are as follows:
$1/2t^3 + 2t^2 + 5/2t + 1$ at $N = 1$
$4t^3 + 8t^2 + 5t + 1$ at $N = 2$
$27/2t^3 + 18t^2 + 15/2t + 1$ at $N = 3$
$32t^3 + 32t^2 + 10t + 1$ at $N = 4$
.
.
.
$243/2t^3 + 162t^2 + 45/2t + 1$ at $N = 9$
$500t^3 + 200t^2 + 25t + 1$ at $N = 10$.
Therefore, for the odd interval, the n-th terms are as follows:
$a_3 = (1/2, 27/2, ...)$ is $N^3/2$,
$a_2 = (2, 18, ...)$ is $2N^2$,
and $a_1 = (5/2, 15/2, ...)$ is $5N/2$.
In addition, for the even interval, the n-th terms are as follows:
$a_3 = (4, 32, ...)$ is $4k^3$,
$a_2 = (8, 32, ...)$ is $8k^2$, and
$a_1 = (5, 10, ...)$ is $5k$,
when $k = 1, 2, 3, ...$
This is given in Table 1. For each interval, the Ehrhart polynomial for the product of two polytopes is obtained. Therefore, any polytope in high dimensions can be decomposed as a product of two polytopes, which means that its volume can be computed.

Table 1. The coefficients of the Ehrhart polynomial.

Interval 1	a3(Volume) 2	a2(Area) 1/2	a1 5/2
2	4	8	5
3	$3^3/2$	18	15/2
4	32	32	10
5	$5^3/2$	50	25/2
6	108	72	15
7	$7^3/2$	98	35/2
8	256	128	20
9	$9^3/2$	162	45/2
10	500	200	25
11	$11^3/2$	242	55/2
.	.	.	.
.	.	.	.
.	.	.	.

Therefore, any polytope in high dimension should be decomposed as a product of two polytopes; this means that its volume can be computed consequently.

Now, an algorithm for the computation is given as follows:
1. Input the vertices of P and Q;
2. compute the volume of the polytopes P and Q;
3. compute the surface area of the polytopes P and Q;
4. compute the number of lattice points of the polytopes P and Q;
5. compute the Ehrhart polynomials for both P and Q;
6. find $L_P(t) \times L_Q(t)$ with $d_P + d_Q$ dimensions;
7. the Earhart polynomial of any polytope in high dimensions can be computed.

4. Applications

Many applications using high-dimensional polytopes have been found. For example, the volume of a polytope is equal to the number of lattice points; this can be done by simply putting the number 1 in the Ehrhart polynomial. This approach, together with the link between the number of lattice points on a four-dimensional ball, was used to break the RSA cryptosystem. More applications related to the computation of lattice points can be found in [13,14].

5. Conclusions

As demonstrated, many real-life applications have difficulty as a result of the huge size of polytopes in high dimensions and the problems associated with counting lattice points. An Ehrhart polynomial is a tolerable limit which processes these points in higher dimensions and can be conceived via the employment of two polytopes. An open problem involves processing the amount of lattice points in four dimensions, which was used to break the RSA cryptosystem. This paper presents a strategy that forms the amount of lattice points in d-dimensions. High-estimation calculations are used in various present-day applications.

References

[1] Benjamin James Braun, Ehrhart theory for lattice polytopes, *Doctoral dissertation, Washington University, 2007.*

[2] Jesús A De Loera, The many aspects of counting lattice points in polytopes, *Mathematische Semesterberichte*, **52,** no. 2, (2005) 175–195.

[3] Ricardo Diaz, Sinai Robins, The Ehrhart polynomial of a lattice polytope, *Annals of Mathematics*, **145,** no. 3, (1997), 503–518.

[4] Jesús A. De Loera,, Raymond Hemmecke, Jeremiah Tauzer, Ruriko Yoshida, Effective lattice point counting in rational convex polytopes, *Journal of symbolic computation*, **38,** no. 4, (2004), 1273–1302.

[5] James R. Munkres, Analysis on manifolds, *Massachusetts Institute of Technology,* 1991.

[6] Shatha Assaad Salman, Computing the number of integral points in 4-dimensional ball, *Scientia Magna*, **9,** no. 1, (2013), 20–26.

[7] Salman Al-Najjar, Shatha Assaad Salman, Computing The Number of Integral Points in 4-dimensional Ball Using Tutte Polynomial, *Engineering and Technology Journal*, **33,** no. 8, (2015), 1420–1429.

[8] Shatha Assaad Salman, Abbas G. Rajij, Solid angle polynomials and its applications in geometric combinatory, *International Conference on Current Research in Computer Science and Information Technology, IEEE, 2017.*

[9] Shatha Assaad Salman, Iman S. Hadeed, Fourier Transform of a Polytope and its Applications in Geometric Combinatorics, *Second Al-Sadiq International Conference on Multidisciplinary in IT and Communication Science and Applications, IEEE, 2017.*

[10] Shatha Assaad Salman, Lattice Point and its Application in RSA Cryptosystem, *Energy Procedia*, **157,** (2019), 39–42.

[11] Richard Stanley, Enumerative Combinatorics, *Vol. I, Wadsworth and Brooks/Cole Math. Ser., Wadsworth and Brooks/Cole, Monterey, CA,* 1986.

[12] Shatha Assaad Salman, Iman S. Hadeed, An algorithm for a modified computation of Dedekind sums,*Journal of Al Qadisiyah for Computer Science and Mathematics*, **12,** no. 1, (2020), 49–53.

[13] Salman Al-Najjar, Shatha Assaad Salman, Israa H. Hassan, Tahani A. Salman, An Ehrhart polynomial for a dual polytope and the number of lattice points, *IOSR Journal of Mathematics*, **3,** no. 2, (2012), 32–36.