Computing The Number of Integral Points in4-dimensional Ball Using Tutte Polynomial

Dr.Shatha Assaad Salman Al-Najjar
Applied Mathematics Department, University of Technology/ Baghdad.
Email: drshatha.alnajar@gmail.com

Received on:4/5/2014 & Accepted on:17/9/2015

ABSTRACT

In recent years, the uses of high dimensional appear in a large and a lot of applications appear within it. So, we study these applications and take one of them that play a central role in the factoring of prime number which is an application especially in cryptography. Our main purpose is to introduce another procedure which make the operation of computing the factoring of N = p.q as more easy as the direct computation fast, therefore, an approach is working on for finding the number of integral points(lattice points) make benefit from the concept of the Tutte polynomial and its application on integral points of a polytope. Polytopes which are taken are the Platonic solid, and a map is making between a ball and a polytope in four dimensions, then discusses the relation between the numbers of integral points of them from dimension one to n dimension. We found a relation between the radiuses of the ball, the edge of the cube which is one of the Platonic solid and the dimension together with Pascal triangle, the rhombic dodecahedron, octahedron, and icosahedrons are also taken.

Keywords: Polytope, lattice point, Tutte polynomial.

حساب عدد النقاط ذات الاحداثيات الصحيحة فيالكرة ذات الاربعة الأبعاد باستخدام متعدد الحدود(تات)

الخلاصة

في السنوات الأخيرة ،ظهرت استخدامات الأبعاد العالية في مجموعة واسعة وكبيرة من التطبيقات. لذلك درسنا هذه التطبيقات واتخذنا احداها التي تلعب دورا محوريا في ايجاد عوامل الاعداد الاولية الذي هو تطبيق مهم وخاصة في الترميز . هدفنا الرئيسي هو أن نقدم تقنية آخرى التي تجعل من عملية ايجاد العوامل أكثر سهولة عن الحساب المباشر ، لذلك قدمنا تقريبين ، وهو نهج يعمل على إيجاد عدد النقاط ذات p.q=N وتطبيقه على متعدد الاضلاع والزوايا . تم اخذ الابعاد الصحيحة بالاستفادة من مفهوم متعدد الحدود تات الاشكال الأفلاطونية ، ووجدنا تطبيق بين الكرة و متعدد الاضلاع والزوايا في البعد الرابع ، ثم ناقشنا وجدنا علاقة بين أنصاف أقطار الكرة و حرف nالعلاقة بين أعداد النقاط بينهما من البعد الاول إلى البعد المكعب حيث ان المكعب هو واحد من الاشكال الأفلاطونية مع البعد و مثلث باسكال ، أيضا تم اخذ الاشكال Rhombic ,dodecahedron , octahedron, icosahedrons.

INTRODUCTION

Convex bounded polyhedrons are fundamental geometric objects that have been investigated since antiquity. The beauty of their theory is now a day complemented by their importance for many other objects, ranging from the integration theory, algebraic topology, and algebraic geometry (toric varieties) to the linear and combinatorial optimization, and another applications given in [6,7,14,15].
The main reason of this paper is to make use of Platonic solids which are cube, tetrahedron, octahedron, icosahedrons and dodecahedron. And use the concepts of Ehrhart polynomials for them depends on the Tutte polynomials to get the number of integral points and make use of it with the solutions of equation that compute the number of integral points on a ball in four dimension. We approximately cover the entire sphere with the dodecahedron which is one of the Platonic solid rather than a cube that we use it in the previous paper, [12,13].

Fukuda in [5] shows that every arrangement of spheres (and hence every central arrangements of hyperplanes) is combinatorial equivalent to some convex polytope. Also Mazo in [9] proved that there is a relationship between the number of integral point on a sphere and the volume of it. Although a four - dimensional Euclidean geometry with time as the fourth dimension was already known since Galileo Galilei's time, it was Einstein who showed that the fourth dimension, time, is essentially different from the other three dimensions. Therefore, his early creations were unrealistic. And yet, real 4d-objects have to exist, if the relativistic geometry is real.

Shatha in [13] proved that there is a relation between the number of integral points and the edge of cube together with Pascal triangle.

As we discussed before the difficult factorization problem for N = p.q with p and q large primes, presented as follows: For an integer number N=p.q consider the 4-dimensional convex body $B(N) = \{x \in R^4 : x_1^2+x_2^2+x_3^2+x_4^2 \leq N\}$, thus if we know that N = p.q, and B(N) denotes the number of lattice points in B(N). The fast factorization of n is based on fast computing of B (N). And the application for this problem relates to RSA cryptosystems.

Many optimization techniques involving a sub step that counts the number of integral points in a set S, which can be described by a set of linear constraints, i.e. S is the intersection of z^d and a rational polyhedron [11]. The problem of counting the number of elements in S is therefore equivalent to count the number of integral points in a polytope which implies that the count is finite (since the polytope is bounded polyhedron). Different algorithms are used to find the number of integral points since 1980, all of them depend on the concept of integer programming for more see [1,2].

Definitions and theorems

Firstly some of the basic definitions are given to consolidate results, which are given as follows:

Definition 2.1, [10]:

Let $Ax \leq b$ where $A \in R^{m\times d}$ is a given real matrix, and $b \in R^m$ is a known real vector. A set $P = \{x \in R^d : Ax \leq b\}$ is said to be a polyhedron. Every bounded polyhedron is said to be a polytope.

Definition 2.2, [4]:

Let $P \subset R^d$ be a lattice d-polytope, for a positive integer t, $tP = \{tx : x \in P\}$ is said to be the dilated polytope.

Definition 2.3, [16]:

Let $P \subset R^d$ be a lattice d-polytope. a map $L : N \rightarrow N$ is defined by $L(P, t) = card(tP \cap Z^d)$, where card means the cardinality of $(tP \cap Z^d)$ and N is the set of natural numbers. It is seen that L(P, t) can be represented as, $L(P, t) = 1 + \sum c_i t^i$, this polynomial is said to be the Ehrhart polynomial of a lattice d-polytope P.

Theorem 2.1, **[16]**(Pick's theorem):

For d = 2, $P \subset R^d$ and P is an integral polyhedron. The famous formula, states that: The number of integral points in an integral polyhedron is equal to the area of the polyhedron plus half the number of integral points on the boundary of the polyhedron plus one,

$$|P \cap Z^2| = \text{area}(P) + |\partial P \cap Z^2|/2 + 1 \quad \ldots(1)$$

Formula (1) is useful because it is much more efficient than the direct enumeration of integral points in a polyhedron. The area of P is computed by triangulating the polyhedron. Furthermore, the boundary P is a union of finitely many straight-line intervals, and counting integral points in intervals.

Theorem 2.2, [**1**](Ehrhart's theorem):

Let P be a convex lattice polygon and let t be a positive integer, the following equality always holds.

$|P \cap Z^2| = \text{area}(P) + |\partial P \cap Z^2|/2 + 1$.

Theorem 2.3, [1](Ehrhart - Macdonald reciprocity):

Let P be a d-polytope in R^d with integer vertices, let L(P, t) be the number of integer points in tP , and $L(P_o, t)$ be the number of integer points in the relative interior of tP . Then let L(P, t) and $L(P_o, t)$ are polynomial functions in t of degree d that satisfy L(P, 0) = 1 and $L(P_o, t) = (-1)^d L(P,-t)$.

Theorem 2.4, [8](Jacobi 1829):

The number of representations of N as a sum of four squares equates 8 times the sum of all divisors of N that are not divisible by 4.

Tutte Polynomial

In this section some definitions and theorems that are related to Tutte polynomial are given.

Tutte polynomial is a polynomial in two variables x and y which can be defined for a graph, matrix or, more generally a matroid, most of the interesting applications arise when the underlying structure is a graph or a matrix, but matroids are an extremely useful vehicle for unifying the concepts and definitions, for example, the all terminal reliability probability of a network. Now we must define the Tutte polynomial for matroids which is the main polynomial in this work.

Definition 3.1, [17]:

Let $X \subset Z^n$, for every $A \subseteq X$, let r (A) be the rank of A that is the number of all spanned subspace of $\mathbb{R}^n$ .The Tutte polynomial of the matroid is defined as:

$$T_x(x,y) = \sum_{A \subseteq X} (x-1)^{n-r(A)} \ (y-1)^{|A|-r(A)}$$

where,
n means the dimension of the lattice n-dimensional space Z^n.
|A| means the maximal cardinality of an independent subset of A.

Definition 2.2, [18]:
A multiplicity (arithmetic) Tutte polynomial (X,I,m) is called representable, means that the multiplicity (arithmetic) matroid is realized by a list of elements in a finitely generated abelian group.

The proposed method
The proposed method is given in this section is to give a procedure for computing the number of integral points in 4-dimensional ball which is depending on the Ehrhart polynomials of a polytope (cube) and its properties.

procedures I:
In this procedure we cover a ball in four dimension by a cube with edges a, and make use of the Ehrhart polynomial for the cube in 4-dimension. Approximately computing the number of integral points depend on the Ehrhart polynomials of the cube. First imagine a circle putting in first quadrant in a square with the same center with dimension two and get a general formula for the number of integral points include the radius of the circle and the edge of the cube which as follows: In dimension two
Let a = the edge of the square.
r = radius of the circle.
N-cube=number of integral points on a cube.
N-circle=number of integral points on a circle.
Now if a = 2 then r = 1 and N-cube=1.
if a = 3 then r = 3/2 and N-cube=4.
Combinatorial, the number of integral points on a circle is computed. This is similar to the number of integral points on a cube. Continue in this computation until we reach to the general formula as follow:
From the general formula of the Ehrhart polynomial for a cube, Which is $L(P, t) = (t+1)^n$
We have the number of integral points in a cube is $(a-1)^2$, where a is the edge of the square. We didn't stop at this point but we want to of our computation and try to compute using Ehrhart polynomial for the square and then number of integral points by putting 1 in the Ehrhart polynomial as follows using theorem (2.1)
$|P \cap Z^2| = \text{area}(P) + |\partial P \cap Z^2|/2 + 1$.
$L(P, t) = 4t^2 + 4t + 1$
The number of integral points is 9.
The number that entirely in P, can be found by using
$L(P_0, t) = (-1)^d L(P,-t) = (-1)^2[4-12 + 4-1 + 1] = 1$
And so on. For dimension 3, we put a ball in a cube also we get a general formula as we are obtained it in dimension two, and the results are compared with the Ehrhart polynomial.

$L(P, t) = (t + 1)^d$,$L(P_0, t) = (t - 1)d$
$L(P_0, 2t) = (2t - 1)^3$,$L(P_0, 2) = 1$
$L(P_0, 3t) = (3t - 1)^3$,$L(P_0, 3) = 8$
$L(P_0, 4t) = (4t - 1)^4$,$L(P_0, 4) = 27$
$L(P_0, nt) = (nt - 1)^3$ = number of lattice points in a sphere.
For dimension four, the general formula
$L(P_0, t) = (t - 1)^d$
$L(P_0, nt) = (nt - 1)^4$

Table(1). Number of lattice points in dimension 2

n	a	r	N-cube	N-circle
1	2	1	1	1
	3	3/2	4	4
	4	2	9	9
	5	5/2	16	16
	6	3	25	25
	7	7/2	36	36
	8	4	49	49
	9	9/2	64	64

Table (2). Number of lattice points in dimension 3

n	a	r	N-cube	N-circle
1	2	1	1	1
	3	3/2	8	8
	4	2	27	27
	5	5/2	64	64
	6	3	5^3	5^3
	7	7/2	6^3	6^3
	8	4	7^3	7^3
	9	9/2	8^3	8^3

Table (3). Number of lattice points in dimension 4

n	a	r	N-cube	N-circle
1	2	1	1	1
	3	3/2	2^4	2^4
	4	2	3^4	3^4
	5	5/2	4^4	4^4
	6	3	5^4	5^4
	7	7/2	6^4	6^4
	8	4	7^4	7^4
	9	9/2	8^4	8^4

Remark 2.1

Before we take the second procedure, the Tutte polynomial for the Platonic solid is given as follows:

Example 2.1

Let the six pair of octahedron is{(1,1,0), (1,-1,0),(1,0,1),(1,0,-1),(0,1,1),(0,1,-1)}. This shape can fill space without leaving any gaps, now let{(1,1,0),(1,0,1),(0,1,1)} be the generators and compute the other vertices as a linear combination of them. After some calculations, get the Ehrhart polynomial the same as of a cube. For tetrahedron the rotation will preserve the number of integral points, which is the aim of a lot of papers concerning this work.

Example 2.2

Let (0,1,1),(1,0,1),(1,1,0) be the generating vertices of icosahedra(the set of all icosahedrons),when we take the generators and computing the other vertices as a linear combination of them. After computing multiplicity Tutte polynomial and Ehrhart polynomial get the same result of cube, that is:

$M_X(x,y)=(x-1)^3+3(x-1)^2+3(x-1)+1$.

$\mathcal{E}_x(q) = q^3 + 3q^2 + 3q + 1$.

Finally from 3 generators above we get the different multiplicity Tutte polynomial but the same Ehrhart polynomial that is the same Ehrhart polynomial of cube.

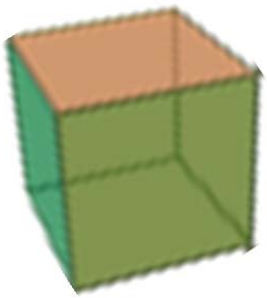

Figure (1) cube

Figure (2) octahedron.

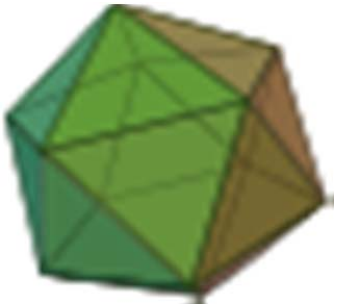

Figure (3) icosahedrons.

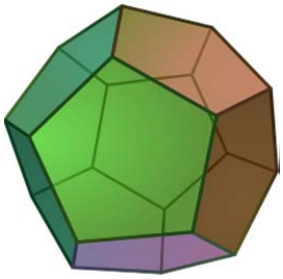

Figure (4) dodecahedron

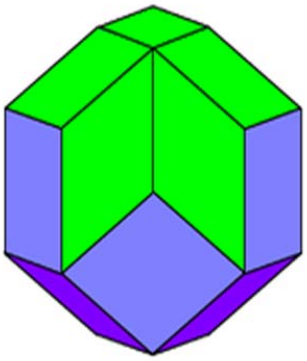

Figure (5) rhombic dodecahedron

Procedure II:

In this procedure we cover a ball in four dimension by a rhombic dodecahedron, and make use of the Tutte polynomials with the Ehrhart polynomial for the rhombic dodecahedron in 4-dimension.

Approximately computing the number of integral points depend on the Ehrhart polynomials of the rhombic dodecahedron. First imagine a circle putting in first quadrant in a cube with the same center with dimension two and get a general formula for the number of integral points include the radius of the circle and the edge of the cube which as follows: In dimension two

Let a^* = the edge of the cube.

r = radius of the circle.

N-cube=number of integral points on a cube.

N-circle=number of integral points on a circle.

Now if $a^* = 2$ then r = 1 and N-cube=1.

if $a^* = 3$ then r = 3/2 and N-cube=4.

Combinatorial the number of integral points on a circle is computed which is similar to the number of integral points on a cube. Continue in this computation until we reach to the general formula as follow:

From the general formula of the Ehrhart polynomial for a cube, Which is $L(P, t) = (t+1)^n$

we have the number of integral points in a cube is $(a^* - 1)^2$, where a is the edge of the square. We didn't stop at this point but we want to of our computation and try to compute using Ehrhart polynomial for the square and then number of integral points by putting 1 in the Ehrhart polynomial as follows using theorem (2.1)

$|P \cap Z^2| = \text{area}|P \cap Z^2| = \text{area}(P) + |\partial P \cap Z^2|/2 + 1.$

$L(P, t) = 4t^2 + 4t + 1$

The number of integral points is 9.

The number that entirely in P, can be found by using

$L(P_0, t) = (-1)^d L(P,-t) = (-1)^2[4-12 + 4-1 + 1] = 1$

And so on. For dimension 3, we put a ball in a cube also we get a general formula as we are obtained it in dimension two, and the results are compared with the Ehrhart polynomial.

$L(P, t) = (t + 1)^d, L(P_0, t) = (t - 1)d$

$L(P_0, 2t) = (2t - 1)^3, L(P_0, 2) = 1$

$L(P_0, 3t) = (3t - 1)^3, L(P_0, 3) = 8$

$L(P_0, 4t) = (4t - 1)^4, L(P_0, 4) = 27$

$L(P_0, nt) = (nt - 1)^3$ = number of lattice points in a sphere.

For dimension four, the general formula

$L(P_0, t) = (t - 1)^d$

$L(P_0, nt) = (nt - 1)^4$

Table(4). Number of lattice points in dimension 2

n	a*	r	N-cube	N-circle
1	2	1	1	1
	3	3/2	4	4
	4	2	9	9
	5	5/2	16	16
	6	3	25	25
	7	7/2	36	36
	8	4	49	49
	9	9/2	64	64

Table (5). Number of lattice points in dimension 3

n	a*	R	N-cube	N-circle
1	2	1	1	1
	3	3/2	8	8
	4	2	27	27
	5	5/2	64	64
	6	3	5^3	5^3
	7	7/2	6^3	6^3
	8	4	7^3	7^3
	9	9/2	8^3	8^3

Table (6). Number of lattice points in dimension 4

n	a	R	N-cube	N-circle
1	2	1	1	1
	3	3/2	2^4	2^4
	4	2	3^4	3^4
	5	5/2	4^4	4^4
	6	3	5^4	5^4
	7	7/2	6^4	6^4
	8	4	7^4	7^4
	9	9/2	8^4	8^4

REFERENCES

[1] B. J. Braun, Ehrhart thorey for lattice polytopes, Ph.D.thesis, Washington University,(2007).

[2] J. A. De Loera, the many aspects of counting lattice points in polytopes, Mathematische Semesterberichte, vol.52, no.2, (2005), p.175-195.

[3] J. De Loeram, R. Hemmecke, Effective lattice points counting in rational convex polytopes, Journal of symbolic computation vol.53, no.8, (2003).

[4] R. Diaz, S. Robins, the Ehrhart polynomial of a lattice polytope, Annal of Math. 145, (1997),503-518.

[5] K. Fukuda, Lecture notes on oriented matroids and geometric computation, citeseerx.ist.psu.edu/viewdoc/download.

[6] Y. Kim, An algorithm for constracting magic squares, Discrete Applied Mathematics, vol.156, (2008).

[7] P. D. Loly, Franklin squares, A chapters in the scientific studies of magical squares, https://www.wolframscience.com/conference/ 2006/presentations/materials/loly.pdf

[8] L. Long and Y. Yang, A short proof of Milne's formulas for sums of integer squares, International journal of number theory vol. 1, no.4,(2005),533-551.

[9] J. E. Mazo, A. M. odlyzko, lattice points in high-dimensional spheres, citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1....

[10] G. L. Nemhauser and L. A.Wolsey, integer and combinatorial optimization, John wiley and sons, Inc, (1988).

[11] A. Schrijver, theory of linear and integer programming, John wiley and sons,(1998).

[12] A. S. Shatha, G. Adil and G. Ahlam, On the volume and integral points of a polyhedron in R^n, LAP Lambert, Academic publishing GmbH and Co.KG.Germany, (2011).

[13] A. S. Shatha, Computing the number of integral points in 4-dimensional ball,Scientia Magna, Vol.9,No.1,(2013).

[14] A. S. Shatha & A. S. Fatema, The Ehrhart polynomials of the cyclic polytope, Eng & Technology, vol.14, no.27,(2009),p.2624.

[15] A. S. Shatha ,A. R. Nuha &A. A. Fuad, Computation of odd magic square using a new approach with some properties, Eng. & Tech. Journal. vol.30, no. 7, (2012), p.1203-1210.

[16] R. P. Stanley, Enumerative combinatorics, wads worth and Brooks/cole advanced Books and software, California, (1986).
[17] W.T.Tutte, A contribution to the theory of chromatic polynomial, Canadian J.math., 6:80-91, (1954).
[18] D.Welsh, The Tutt polynomial, Mertoncollage, university of Oxford. England, 19march (1999).