Chicken McNuggets

Square magic

Polyhedra

The art of bookkeeping

The magic unravelled

Barvinok's algorithm

Closing the circle

Fast-food, square magic and polyhedra.

Benjamin Nill

(& Christian Haase)

Research Group Lattice Polytopes - FU Berlin

IMA Minneapolis, October 2, 2007

$=$

^{11} $\cdot$

^{6} $\cdot$

^{4}

Chicken McNuggets

Square magic

Polyhedra

The art of bookkeeping

The magic unravelled

Barvinok's algorithm

Closing the circle

1. Chicken McNuggets

How many ways are there to order 200 Chicken McNuggets?
(Available: 6, 9, 20.)

$$
\begin{array}{rllll}
= & t^{10}, & n^{20}t, & sn^{6}t^{7}, & s^{2}n^{12}t^{4} \\
 & s^{3}n^{18}t, & s^{4}n^{4}t^{7}, & s^{5}n^{10}t^{4}, & s^{6}n^{16}t \\
 & s^{7}n^{2}t^{7}, & s^{8}n^{8}t^{4}, & s^{9}n^{14}t, & s^{10}t^{7} \\
 & s^{11}n^{6}t^{4}, & s^{12}n^{12}t, & s^{14}n^{4}t^{4}, & s^{15}n^{10}t \\
 & s^{17}n^{2}t^{4}, & s^{18}n^{8}t, & s^{20}t^{4}, & s^{21}n^{6}t \\
 & s^{24}n^{4}t, & s^{27}n^{2}t, & s^{30}t &
\end{array}
$$

…twenty three possibilities.

Exercise. Determine the largest impossible order (Frobenius number).

Chicken McNuggets
Square magic
Polyhedra
The art of bookkeeping
The magic unravelled
Barvinok's algorithm
Closing the circle

On planet Qkargogg they have Value Menus with
12'223, 12'224, 36'674, 61'119, and 85'569
Chicken McNuggets each.

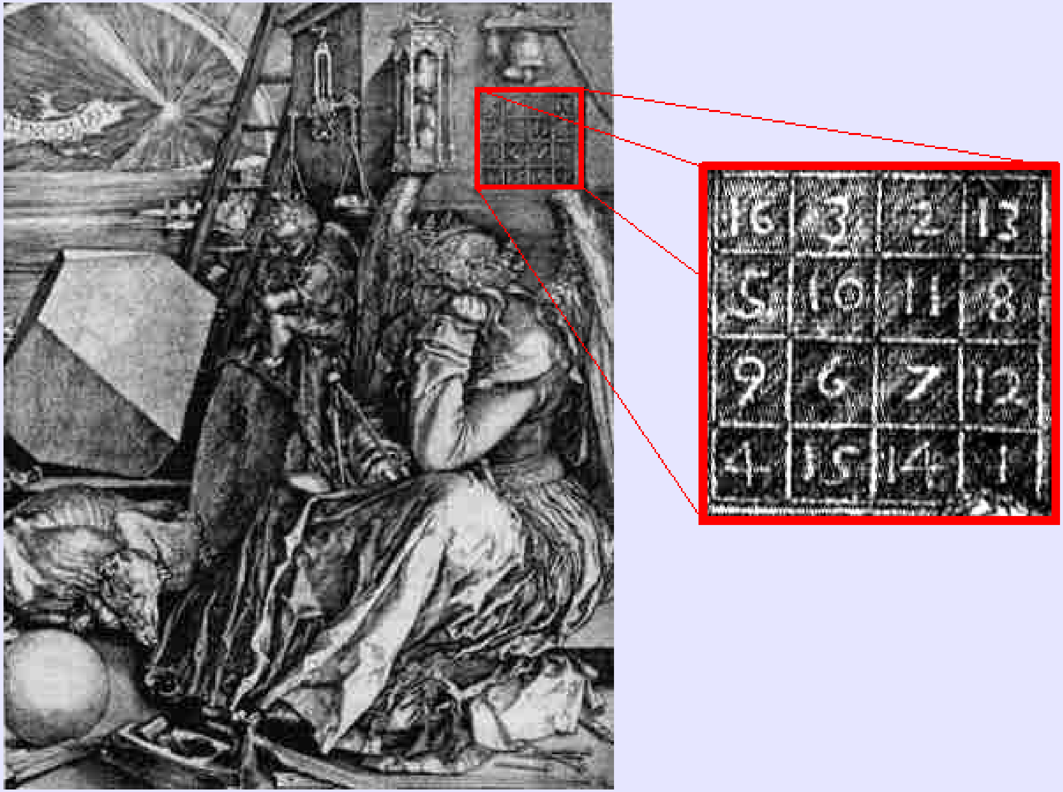
How many ways are there to order 89'643'482 Chicken McNuggets?

$$12223x_1+12224x_2+36674x_3+61119x_4+85569x_5 = 89643482$$

How many NON-NEGATIVE, INTEGRAL solutions?

Chicken McNuggets
Square magic
Polyhedra
The art of bookkeeping
The magic unravelled
Barvinok's algorithm
Closing the circle

2. Square magic



A magic square is a matrix with all row sums, column sums and diagonal sums equal to the magic constant.

$$\begin{bmatrix} 3 & 3 \\ 3 & 3 \end{bmatrix} \quad \begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix} \quad \begin{bmatrix} 1 & 30 & 41 & 54 & 23 & 12 & 63 & 36 \\ 47 & 52 & 7 & 28 & 57 & 38 & 17 & 14 \\ 21 & 10 & 61 & 34 & 3 & 32 & 43 & 56 \\ 59 & 40 & 19 & 16 & 45 & 50 & 5 & 26 \\ 42 & 53 & 2 & 29 & 64 & 35 & 24 & 11 \\ 8 & 27 & 48 & 51 & 18 & 13 & 58 & 37 \\ 62 & 33 & 22 & 9 & 44 & 55 & 4 & 31 \\ 20 & 15 & 60 & 39 & 6 & 25 & 46 & 49 \end{bmatrix}$$

Exercise. Determine the magic constant, if all entries are different.

$$\begin{bmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{bmatrix}$$

$$x_1 + x_2 + x_3 = \mathrm{mc} \quad x_4 + x_5 + x_6 = \mathrm{mc} \quad x_7 + x_8 + x_9 = \mathrm{mc}$$
$$x_1 + x_4 + x_7 = \mathrm{mc} \quad x_2 + x_5 + x_8 = \mathrm{mc} \quad x_3 + x_6 + x_9 = \mathrm{mc}$$
$$x_1 + x_5 + x_9 = \mathrm{mc} \quad x_3 + x_5 + x_7 = \mathrm{mc}$$

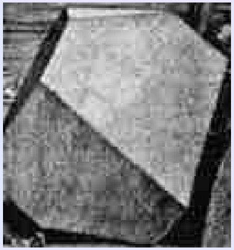
How many NON-NEGATIVE, INTEGRAL solutions?

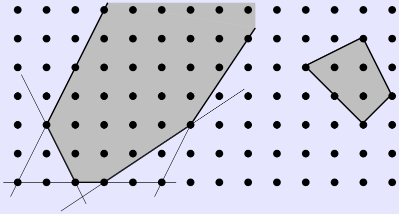
Chicken McNuggets
Square magic
Polyhedra
The art of bookkeeping
The magic unravelled
Barvinok's algorithm
Closing the circle

3. Polyhedra

3.1. Definition

The set of (real) solutions to finitely many linear (in)equalities is a **polyhedron**. The convex hull of finitely many points is a **polytope**.





Theorem. bounded polyhedron = polytope

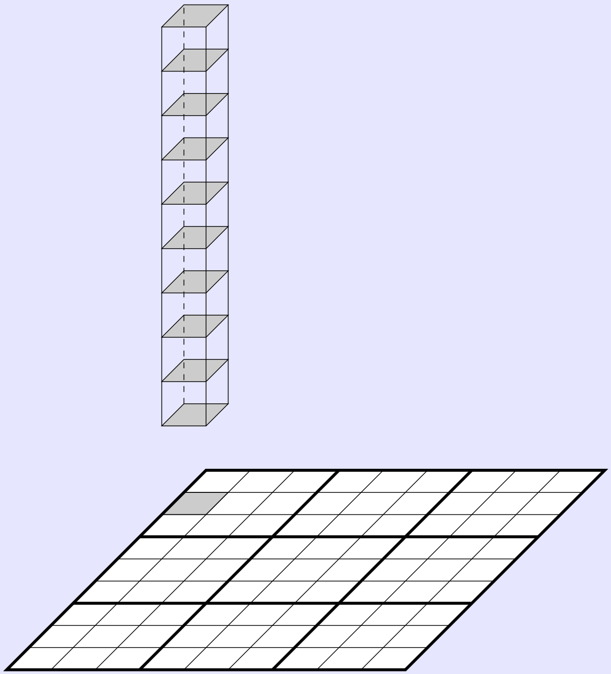
Lattice points in $\mathbb{R}^n$ are elements in the lattice $\mathbb{Z}^n$.

3.2. Polytope of Sudokus

5	8	4	1	7	3	2	9	6
6	9	3	5	4	2	7	1	8
7	1	2	8	6	9	5	3	4
4	5	8	7	2	1	9	6	3
1	3	9	6	5	4	8	2	7
2	7	6	9	3	8	4	5	1
8	2	5	3	1	7	6	4	9
3	6	7	4	9	5	1	8	2
9	4	1	2	8	6	3	7	5

Counting number of Sudokus
= counting lattice points in a polytope?!

Chicken McNuggets
Square magic
Polyhedra
The art of bookkeeping
The magic unravelled
Barvinok's algorithm
Closing the circle



Polytope in $\mathbb{R}^{9\times 9\times 9}$ given by :

- Any entry between 0 and 1.
- Sum over each tower equals 1.
- Sum over each floor of row/column/square equals 1.

Chicken McNuggets

Square magic

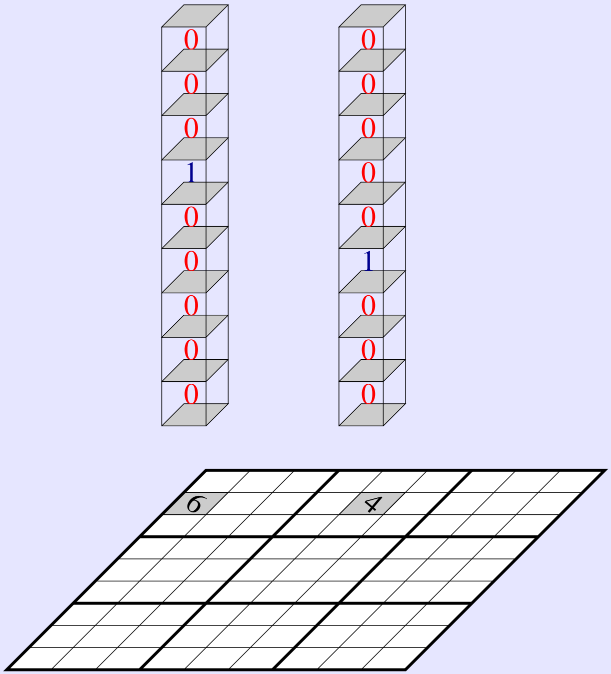
Polyhedra

The art of bookkeeping

The magic unravelled

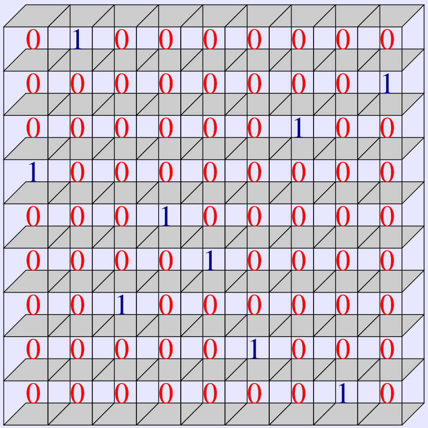
Barvinok's algorithm

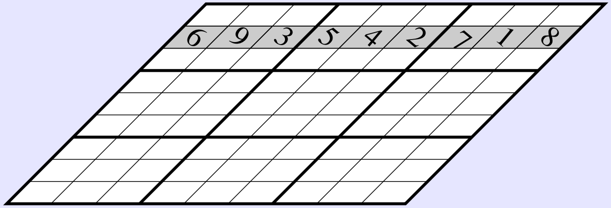
Closing the circle



Polytope in $\mathbb{R}^{9\times 9\times 9}$ given by :

- Any entry between 0 and 1.
- Sum over each tower equals 1.
- Sum over each floor of row/column/square equals 1.





Polytope in $\mathbb{R}^{9\times 9\times 9}$ given by :

- Any entry between 0 and 1.
- Sum over each tower equals 1.
- Sum over each floor of row/column/square equals 1.

3.3. Ehrhart polynomials

Theorem. [Ehrhart 1967]
Let P be a polytope whose vertices have rational coordinates. Define for a natural number k

$$L(k) := \text{ number of lattice points in } kP.$$

Then $k \mapsto L(k)$ is a **quasi-polynomial** (of period N), i.e., it becomes polynomial on the set of numbers with the same remainder modulo N.

Example:
The number of 4×4 magic squares with magic constant c equals

$$\begin{cases} \frac{1}{480}c^7 + \frac{7}{240}c^6 + \frac{89}{480}c^5 + \frac{11}{16}c^4 + \frac{49}{30}c^3 + \frac{38}{15}c^2 + \frac{71}{30}c + 1 & \text{if } c \text{ is even,} \\ \frac{1}{480}c^7 + \frac{7}{240}c^6 + \frac{89}{480}c^5 + \frac{11}{16}c^4 + \frac{779}{4800}c^3 + \frac{593}{240}c^2 + \frac{1051}{480}c + \frac{13}{16} & \text{if } c \text{ is odd.} \end{cases}$$

3.4. Other applications

Chicken McNuggets

Square magic

Polyhedra

The art of bookkeeping

The magic unravelled

Barvinok's algorithm

Closing the circle

Counting lattice points in polyhedra

turns up in

- graph theory/integer linear programming (colorings and flows)
- statistics (contingency tables)
- representation theory (Kostka and Littlewood-Richardson coefficients, saturation conjecture)
- algebraic geometry (global sections, Todd classes)
- string theory (stringy Hodge numbers)

Chicken McNuggets
Square magic
Polyhedra
The art of bookkeeping
The magic unravelled
Barvinok's algorithm
Closing the circle

4. The art of bookkeeping

Throughout all polyhedra are given by *rational* inequalities.

4.1. Why rational functions are nice

List all lattice points in the polyhedron $[0,3]$.

- 0,1,2,3
- $g_{[0,3]} = 1 + x + x^2 + x^3$
- $g_{[0,3]} = \dfrac{1 - x^4}{1 - x}$

List all lattice points in the polyhedron $[0, 10000]$.

- 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,2
- $1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} +$
- $g_{[0,10000]} = \dfrac{1 - x^{10001}}{1 - x}$

Chicken McNuggets

Square magic

Polyhedra

The art of bookkeeping

The magic unravelled

Barvinok's algorithm

Closing the circle

Chicken McNuggets
Square magic
Polyhedra
The art of bookkeeping
The magic unravelled
Barvinok's algorithm
Closing the circle

List all lattice points in the polyhedron $[0, 10000]$.

- 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,2
- $1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} +$
- $g_{[0,10000]} = \dfrac{1 - x^{10001}}{1 - x}$

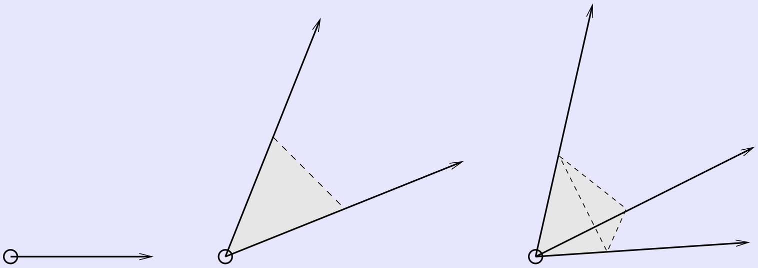
...in the polyhedron $[0, \infty)$

-
-
- $g_{[0,\infty)} = \dfrac{1}{1 - x}$

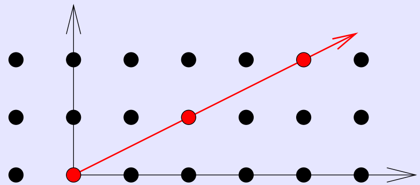
Chicken McNuggets
Square magic
Polyhedra
The art of bookkeeping
The magic unravelled
Barvinok's algorithm
Closing the circle

4.2. Why simple cones are *simple*

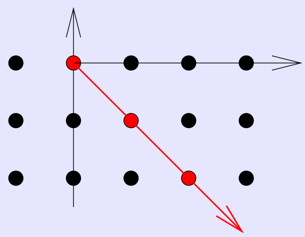
Simple cones in dimension 1,2,3:



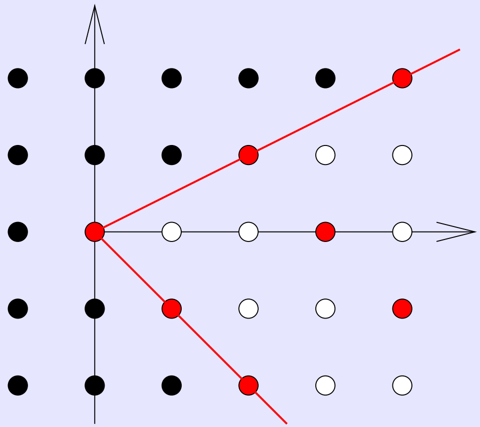
How to enumerate lattice points?



$$1 + x^2y + x^4y^2 + \ldots = \sum_{k \geq 0} (x^2y)^k = \frac{1}{1 - x^2y}$$



$$1 + x/y + x^2/y^2 + \ldots = \sum_{k \geq 0} (x/y)^k = \frac{1}{1 - x/y}$$



$$(x^2y)^2 \cdot 1$$

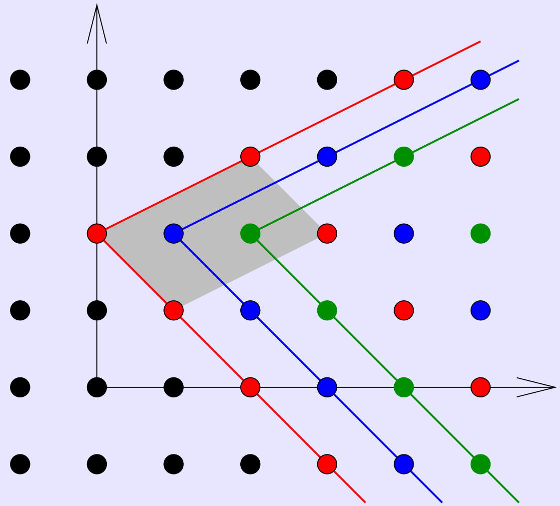
$$x^2y \cdot 1$$

$$\frac{1}{1-x^2y} \cdot \frac{1}{1-x/y} = 1 \cdot 1 \qquad x^2y \cdot x/y$$

$$1 \cdot x/y \qquad x^2y \cdot (x/y)^2$$

$$1 \cdot (x/y)^2$$

Chicken McNuggets
Square magic
Polyhedra
The art of bookkeeping
The magic unravelled
Barvinok's algorithm
Closing the circle



$$\frac{y^2 + xy^2 + x^2y^2}{(1 - x/y)(1 - x^2y)}$$

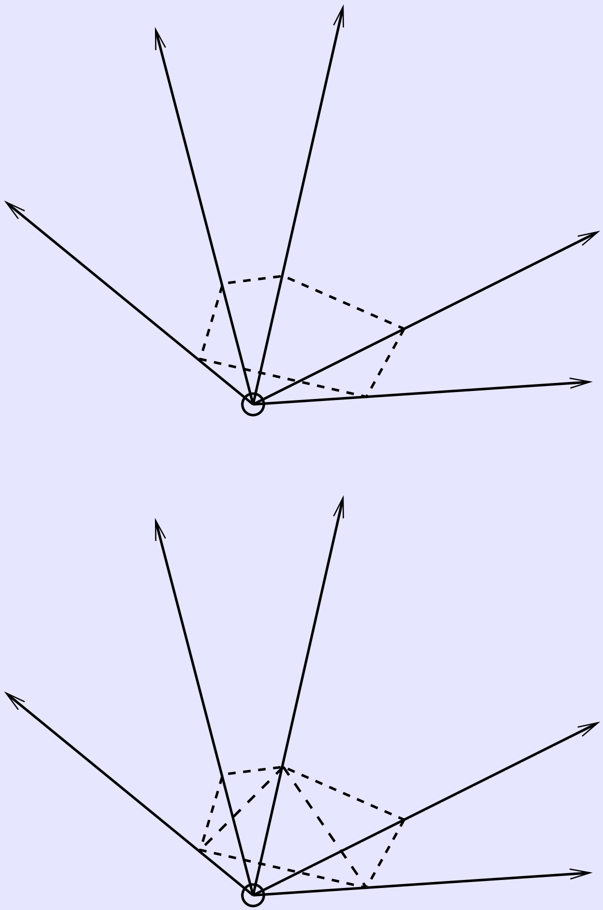
C a simple cone in $\mathbb{R}^n$ $\quad\Rightarrow$

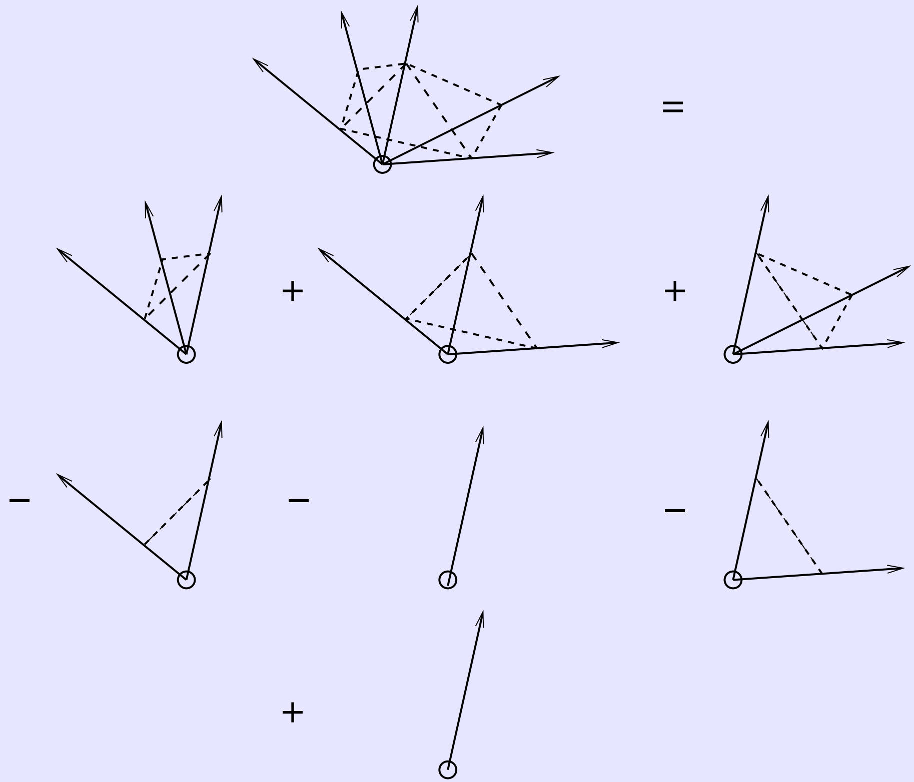
$$g_C = \sum_{x \in C \cap \mathbb{Z}^n} x$$

rational function of this form.

Chicken McNuggets
Square magic
Polyhedra
The art of bookkeeping
The magic unravelled
Barvinok's algorithm
Closing the circle

4.3. Cones triangulate into simple ones



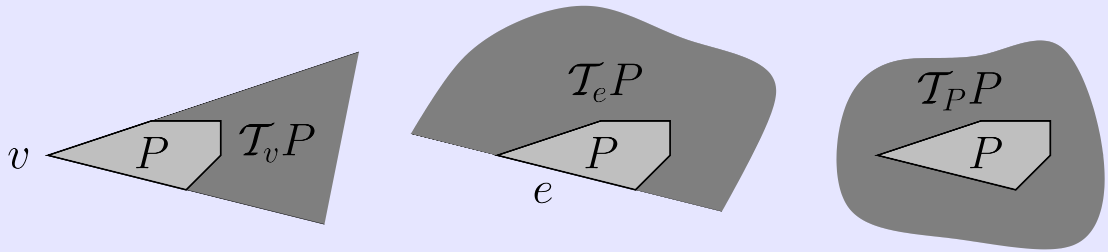


C cone $\Rightarrow$ g_C rational function!

4.4. So, what about polytopes?

For a face F of a polytope P, define the tangent cone

$$\mathcal{T}_F P = \{f + x \in \mathbb{R}^d \;:\; f \in F \text{ and } f + \epsilon x \in P \text{ for some } \epsilon > 0\}$$



Chicken McNuggets

Square magic

Polyhedra

The art of bookkeeping

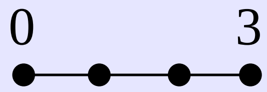
The magic unravelled

Barvinok's algorithm

Closing the circle

Our favourite example:

$$P = [0, 3]$$



$$g_P = x^0 + x^1 + x^2 + x^3 = \frac{1 - x^4}{1 - x}$$

Chicken McNuggets

Square magic

Polyhedra

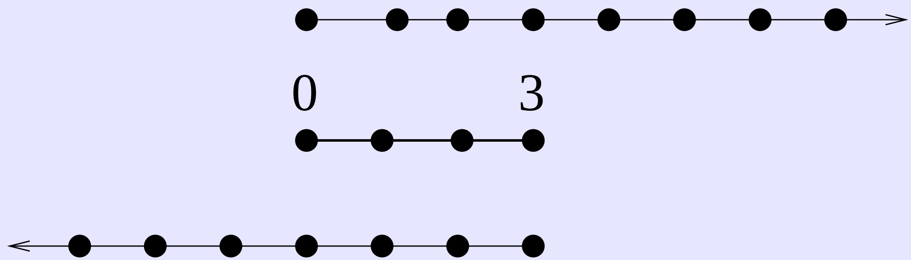
The art of bookkeeping

The magic unravelled

Barvinok's algorithm

Closing the circle

Look at the tangent cones:



$$g_{\mathcal{T}_0 P} \;=\; x^0 + x^1 + x^2 + x^3 + x^4 + x^5 + \cdots \;=\; \frac{1}{1-x}$$

$$g_{\mathcal{T}_3 P} \;=\; \cdots + x^{-2} + x^{-1} + x^0 + x^1 + x^2 + x^3 \;=\; \frac{x^3}{1-1/x}$$

Chicken McNuggets
Square magic
Polyhedra
The art of bookkeeping
The magic unravelled
Barvinok's algorithm
Closing the circle

A magic sum:

$$
\begin{array}{rcc}
g_{\mathcal{T}_0 P} & = & \dfrac{1}{1-x} \\
+ \quad g_{\mathcal{T}_3 P} & = & \dfrac{x^3}{1-1/x} \\
\hline
g_P & = & \dfrac{1-x^4}{1-x}
\end{array}
$$

Chicken McNuggets

Square magic

Polyhedra

The art of bookkeeping

The magic unravelled

Barvinok's algorithm

Closing the circle

Theorem. [Brion 1988]
P polytope with rational vertex coordinates

$$\Rightarrow \quad g_P = \sum_{v \text{ vertex of } P} g_{\mathcal{T}_v P}.$$

In particular, g_P is a rational function.

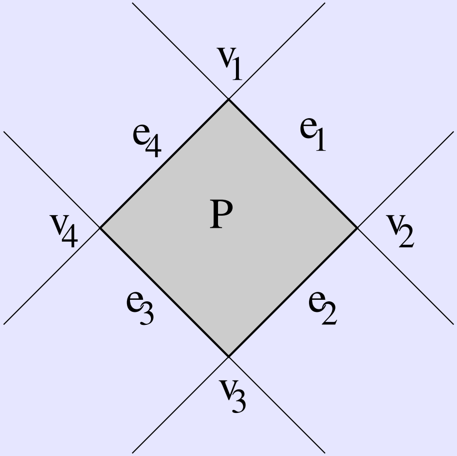
5. The magic unravelled

Theorem. [Brianchon 1837, Gram 1874]

$$g_P = \sum_v g_{\mathcal{T}_v P} + \sum_F (-1)^{\dim F} g_{\mathcal{T}_F P}$$

where F are faces of P with $\dim F > 0$.

Illustration:



$$g_P = \sum_{i=1}^4 g_{\mathcal{T}_{v_i} P} - \sum_{j=1}^4 g_{\mathcal{T}_{e_j} P} + g_{\mathcal{T}_P P}.$$

Chicken McNuggets

Square magic

Polyhedra

The art of bookkeeping

The magic unravelled

Barvinok's algorithm

Closing the circle

Chicken McNuggets

Square magic

Polyhedra

The art of bookkeeping

The magic unravelled

Barvinok's algorithm

Closing the circle

The magic trick:

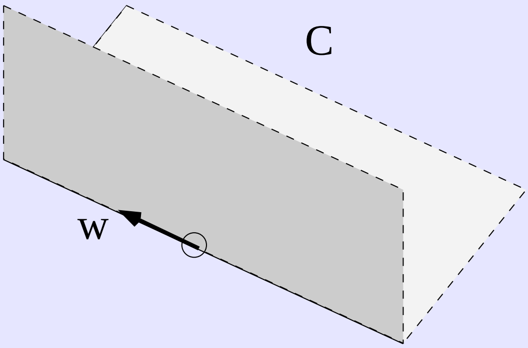
Claim:

C cone containing a line $\Rightarrow$ $g_C = 0$ (as a rational function).

Corollary:

F is a face of positive dimension $\Rightarrow$ $g_{\mathcal{T}_F P} = 0.$

Thus, Brion's theorem follows from Brianchon-Gram.



Proof of claim:

Exists lattice point w:

$$w + C = C.$$

$$\Rightarrow \quad x^w g_C = g_C.$$

$$\Rightarrow \quad (1 - x^w) g_C = 0.$$

$$\Rightarrow \quad g_C = 0,$$

since rational function $f \neq 0$ times polynomial $p \neq 0$ is rational function $f \cdot p \neq 0$.

$\square$

6. Barvinok's algorithm

6.1. Our algorithm so far

Given a linear (in-)equality description of polytope P in $\mathbb{R}^n$.

1. Calculate vertices v.
2. Calculate $\mathcal{T}_v P$.
3. Triangulate $\mathcal{T}_v P$ into simple cones C_i.
4. Calculate rational function g_{C_i}.
5. Calculate rational function $g_{\mathcal{T}_v P}$.
6. Calculate rational function g_P by Brion's theorem.
7. Evaluate rational function

$$g_P(1, \ldots, 1) = \sum_{x \in P \cap \mathbb{Z}^n} 1$$

to get number of lattice points in P.

Chicken McNuggets
Square magic
Polyhedra
The art of bookkeeping
The magic unravelled
Barvinok's algorithm
Closing the circle

Fix the dimension n. Given P with input size α.

Bit input size: $\log(\alpha)$.

Goal: Enumeration complexity polynomial in $\log(\alpha)$.

6.2. Analyzing the algorithm

1. Calculate vertices v - polynomial
2. Calculate $\mathcal{T}_v P$ - polynomial
3. Triangulate $\mathcal{T}_v P$ into simple cones C_i - polynomial
4. Calculate rational function g_{C_i} - unclear

Possibly MANY lattice points in parallelepiped!

Chicken McNuggets
Square magic
Polyhedra
The art of bookkeeping
The magic unravelled
Barvinok's algorithm
Closing the circle

5. Calculate rational function $g_{\mathcal{T}_v P}$ - polynomial

   This can be done via inclusion-exclusion.

   Nowadays, via *irrational decomposition* even disjoint union of lattice points in **full-dimensional** cones.

Chicken McNuggets
Square magic
Polyhedra
The art of bookkeeping
The magic unravelled
Barvinok's algorithm
Closing the circle

6. Calculate rational function g_P by Brion's theorem - polynomial

7. Evaluate $g_P(1,\ldots,1)$ to get number of lattice points - polynomial

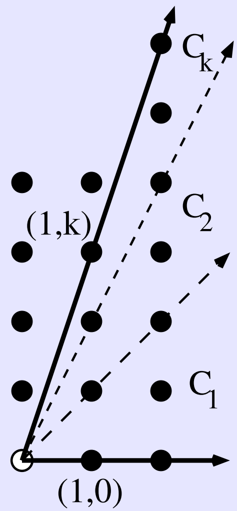
$(1,\ldots,1)$ is a pole of rational function g_P.
Evaluation via complex methods.

Only problem left is:
4. Calculate rational function g_{C_i} - unclear

Approach: Triangulate simple cone as far as possible, into *unimodular* cones.

UNIMODULAR CONE $=$
simple cone & parallepiped contains only apex.

Example:
C cone given by directions $(1,0)$ and $(1,k)$.
Decomposition into k unimodular cones:

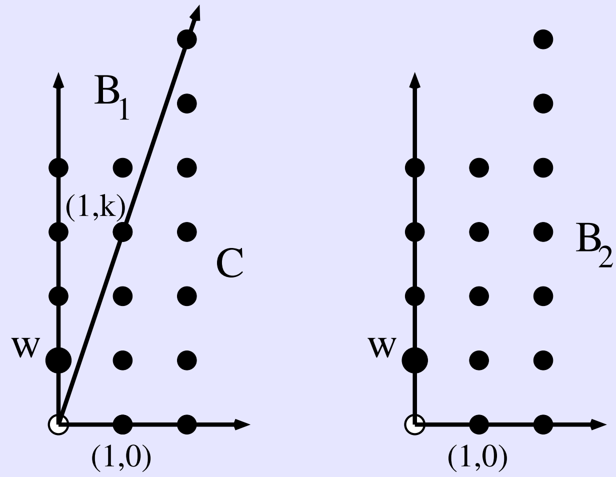


complexity not polynomial $(k = e^{\log(k)})$!

Chicken McNuggets
Square magic
Polyhedra
The art of bookkeeping
The magic unravelled
Barvinok's algorithm
Closing the circle

6.3. Barvinok's trick

Write a **signed decomposition** "$C = B_2 - B_1$" into unimodular cones B_1, B_2:



$$\boxed{g_C = g_{B_2} - g_{B_1}} \quad \pm \sum_F g_F \quad (F \text{ lower dimensional}).$$

Only 2 unimodular cones needed!

This idea works always:

Minkowski's lattice point theorem $\Rightarrow$
exists lattice point w $\rightsquigarrow$ signed decomposition into "smaller" simple cones.

Theorem. [Barvinok 1994] Let n be fixed.
There exists a polynomial-time algorithm for computing the rational generating function g_P of a polyhedron $P \subseteq \mathbb{R}^n$ given by rational inequalities.

Chicken McNuggets
Square magic
Polyhedra
The art of bookkeeping
The magic unravelled
Barvinok's algorithm
Closing the circle

7. Closing the circle

Let N be a natural number.

Theorem. [Jacobi 1829] The number of representations of N as sums of four squares equals 8 times the sum of all divisors of N that are not divisible by 4.

Example: Let $N = p \cdot q$ for different primes p, q.
Number of representations of N as four squares $=$

$$8(1 + p + q + N).$$

Chicken McNuggets
Square magic
Polyhedra
The art of bookkeeping
The magic unravelled
Barvinok's algorithm
Closing the circle

Application:
Let $N = p \cdot q$ for different primes p, q.

Define

$$B(N) := \{x \in \mathbb{Z}^4 \,:\, x_1^2 + x_2^2 + x_3^2 + x_4^2 \leq N\},$$

set of lattice points in 4-dim. ball of radius $\sqrt{N}$.

$$\begin{aligned} & |B(N)| - |B(N-1)| \\ = \;& |\{x \in \mathbb{Z}^4 \,:\, x_1^2 + x_2^2 + x_3^2 + x_4^2 = N\}| \\ = \;& 8(1 + p + q + N). \end{aligned}$$

In other words:
N, $|B(N)| - |B(N-1)|$ known $\quad\Leftrightarrow$
$p \cdot q, p + q$ known $\quad\Leftrightarrow$
p, q known.

Chicken McNuggets

Square magic

Polyhedra

The art of bookkeeping

The magic unravelled

Barvinok's algorithm

Closing the circle

RSA cryptosystem attack. [De Loera 2005]

IF we could count lattice points in 4-dim. balls *fast*,
THEN we could factorize $N = p \cdot q$ *fast*.

References

The many aspects of counting lattice points in polytopes

De Loera, J.A. (Math. Semesterber. 52, 175–195, 2005)

LattE - Computations with Polyhedra

De Loera, J.A.; et.al. (`www.math.ucdavis.edu/~latte/`)

Theorems of Brion, Lawrence, and Varchenko on rational generating functions for cones

Beck, M.; Haase, C.; Sottile, F. (arXiv:math/0506466, 2005)

Computing the Continuous Discretely. Integer-point Enumeration in Polyhedra

Beck, M.; Robins, S. (Undergraduate Texts in Mathematics, Springer, 2007)

Chicken McNuggets

Square magic

Polyhedra

The art of bookkeeping

The magic unravelled

Barvinok's algorithm

Closing the circle