

不変式論と格子点ソフトウェア LattE

中本和典氏（山梨大学）との共同研究

奥山 真吾

香川高等専門学校
情報工学科

数学ソフトウェアとフリードキュメント X

Outline

- 1 Brute force method ~ 苦難の歴史の物語
- 2 Math.
- 3 LattE ~ 新しい時代の幕開け
 - 前回までのあらすじ
 - 時代は LattE
- 4 Barvinok's algorithm

登場人物

- N氏... 数学 段、計算機 級
- O氏... 数学 段、計算機 級

N氏の要求

問題

次の行列の個数はいくつか？

$$0 \leq r \leq 150$$

$$\begin{pmatrix} a_{11} & \cdots & a_{15} \\ \vdots & & \vdots \\ a_{51} & \cdots & a_{55} \end{pmatrix} \in M_5(\mathbb{Z})$$

- $a_{ij} \geq 0$
- $\sum_{i,j} a_{ij} = r$
- $\sum_{i=1}^5 a_{ik} = \sum_{i=1}^5 a_{ki}, k = 1, \dots, 5$

$$M(n, r) = \left\{ A = (a_{ij}) \in M_n(\mathbb{Z}) \left| \begin{array}{l} a_{ij} \geq 0, \\ \sum_{i,j} a_{ij} = r, \\ \sum_i a_{ik} = \sum_i a_{ki} \forall k \end{array} \right. \right\}$$

$$h_n(r) = \#M(n, r), \quad F_n(t) = \sum_{r \geq 0} h_n(r) t^r$$

- $M(1, r) = \{(r)\}$, $F_1(t) = 1 + t + t^2 + \dots = \frac{1}{1-t}$
- $M(n, 0) = *$, $h_n(1) = n$, $F_n(t) = 1 + nt^r + \dots$

• $n = 2$

$$M(2, 1) = \left\{ \begin{pmatrix} 1 & \\ & \end{pmatrix}, \begin{pmatrix} & \\ & 1 \end{pmatrix} \right\}$$

$$M(2, 2) = \left\{ \begin{pmatrix} 2 & \\ & \end{pmatrix}, \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} & \\ 2 & \end{pmatrix}, \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} \right\}$$

$$M(2, 3) = \left\{ \begin{pmatrix} * & \\ & * \end{pmatrix} (4 \text{ 個}), \begin{pmatrix} 1 & 1 \\ 1 & \end{pmatrix}, \begin{pmatrix} & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

⋮

- $n = 3$

$$M(3, 1) = \{ \text{対角行列 (3 個)} \}$$

$$M(3, 2) = \{ \text{対角行列 (6 個), “互換に対応する物”(3 個)} \}$$

$$M(3, 3) = \left\{ \begin{array}{l} \text{対角行列 (10 個),} \\ \left(\begin{array}{ccc} 1 & 1 & \\ 1 & 0 & \\ & & 0 \end{array} \right), \dots, \left(\begin{array}{ccc} 0 & & \\ & 0 & 1 \\ & 1 & 1 \end{array} \right) \text{ (9 個),} \\ \text{長さ 3 の巡回置換 (2 個)} \end{array} \right\}$$

⋮

$M(n, r)$ の部分集合 $D(n, r) = \{ \text{成分の和が } r \text{ の対角行列} \}$ および
 $T(n, r) = \langle \text{成分の和が } r \text{ の“互換に対応する物”} \rangle$ を考えると、

$$\#M(n, r) = \sum_{s+t+u=n}^n \#D(n, s) \#T(n, t) g_n(u)$$

と表せる。

Simplified Problem

問題

次の行列の個数はいくつか？

$$0 \leq r \leq 150$$

$$\begin{pmatrix} a_{11} & \cdots & a_{15} \\ \vdots & & \vdots \\ a_{51} & \cdots & a_{55} \end{pmatrix} \in M_5(\mathbb{Z})$$

- $a_{ij} \geq 0$
- $\sum_{i,j} a_{ij} = r$
- $\sum_{i=1}^5 a_{ik} = \sum_{i=1}^5 a_{ki}, k = 1, \dots, 5$
- $a_{ij} \cdot a_{ji} = 0, i, j = 1, \dots, 5$

計算時間 (推計)

	$r = 20$	$0 \leq r \leq 150$
Maple	1 min.	80 years
GAP	11 sec.	17 years
C+NTL	0.3 sec.	5 months

「百五十物語」

Reduced Poincaré series

$$f_5(t) = \frac{g_5(t)}{(1-t)^5(1-t^2)^{10}} \text{ を用いて計算すると、}$$

定理 (Nakamoto-O.)

$$f_5(t) = \frac{R_5(t)}{(1-t)^5(1-t^2)^9(1-t^3)^4(1-t^4)^2(1-t^5)}$$

ここで、

$$\begin{aligned} R_5(t) = & 1 + t^2 + 16t^3 + 29t^4 + 39t^5 + 95t^6 + 187t^7 + 254t^8 \\ & + 307t^9 + 386t^{10} + 461t^{11} + 461t^{12} + 386t^{13} + 307t^{14} \\ & + 254t^{15} + 187t^{16} + 95t^{17} + 39t^{18} + 29t^{19} + 16t^{20} \\ & + t^{21} + t^{23} \end{aligned}$$

次の問題

問題

次の行列の個数はいくつか？

$$0 \leq r \leq 960$$

$$\begin{pmatrix} a_{11} & \cdots & a_{16} \\ \vdots & & \vdots \\ a_{61} & \cdots & a_{66} \end{pmatrix} \in M_6(\mathbb{Z})$$

- $a_{ij} \geq 0$
- $\sum_{i,j} a_{ij} = r$
- $\sum_{i=1}^6 a_{ik} = \sum_{i=1}^6 a_{ki}, k = 1, \dots, 6$
- $a_{ij} \cdot a_{ji} = 0, i, j = 1, \dots, 6$

次の問題の計算時間（推計）

	$r = 20$	$r = 70$	$0 \leq r \leq 70$	$0 \leq r \leq 960$
C	1min.	18 days	4 months	1.7×10^{16} years

Impossible!

「九百六十物語」

一年が過ぎて

N: 「 $r = 70$ の結果を送ります。ところで、LattE というソフトを試してみてください。」

O: 「インストールできませんでした。」

Cで直接書く以上に早い方法があるのだろうか？

行列の不変式環

- $M_n^m = M_n(\mathbb{C}) \times \cdots \times M_n(\mathbb{C})$
- $GL_n(\mathbb{C}) \curvearrowright M_n^m$
- $GL_n(\mathbb{C}) \curvearrowright \mathbb{C}[x_{ij}^{(1)}; x_{ij}^{(2)}; \dots; x_{ij}^{(m)}]$
- $C(n, m) = \mathbb{C}[x_{ij}^{(1)}; \dots; x_{ij}^{(m)}]^{GL_n(\mathbb{C})}$

$C(n, m)$ の生成元

予想-Artin(1969)

$C(n, m)$ は $Tr(X_{i_1} \cdots X_{i_r})$ で生成される。

Procesi によって肯定的に解決された。(1976)

$C(n, m)$ の構造

- $C(2, 2)$ の構造 (Formanek-Halpin-Li 1981)
- $C(3, 2)$ の構造 (Formanek 1987)
- $\mathbb{Z}[M_3 \times M_3]^{PGL_3}$ の構造 (Nakamoto 2002)
- $C(4, 2)$ の Poincaré級数 (Teranishi 1987)

$F(s, t)$ を $\mathbb{C}[M_n \times M_n]^{GL_n}$ の Poincaré級数とする。このとき、 $F(t) = ((1-s)^n F(s, t))|_{s=1}$ とおくと、 $F(t) = F_n(t)$

Teranishi's Theorem

定理 (Teranishi)

- 1 $F_n(t)$ は関数方程式 $F_n\left(\frac{1}{t}\right) = -t^{n^2} F_n(t)$ を満たす。
- 2 整数係数の多項式 $R_n(t)$ が存在して、

$$F_n(t) = \frac{R_n(t)}{(1-t)^n \prod (1-t^{|\sigma|})}$$

が成り立つ。ここで、 σ は全ての巡回置換 $\sigma \in S_n$ を動く。
($|\sigma|$ は巡回置換の長さ。)

$$F(t) = \frac{R(t)}{(1-t)^n \prod (1-t^{|\sigma|})} \text{ とおく。}$$

$$N_k = \#\{\text{長さ } k \text{ の巡回置換} \in S_n\}$$

さらに、 $L = n + \sum_{k=2}^n kN_k$ とおくと、

$$\begin{aligned} F(t^{-1}) &= \frac{R(t^{-1})}{(1-t^{-1})^n \prod (1-t^{-|\sigma|})} \\ &= t^L \frac{R(t^{-1})}{(t-1)^n \prod (t^{|\sigma|}-1)} \\ &= (-t)^L \frac{R(t^{-1})}{(1-t)^n \prod (t^{|\sigma|}-1)} \end{aligned}$$

よって、関数方程式より

$$-t^{n^2} R(t) = (-t)^L R(t^{-1})$$

つまり

$$R(t) = (-1)^{L-1} t^{L-n^2} R(t^{-1})$$

よって

$$R(t) \text{ の次数は } m = L - n^2$$

であり、 $R(t) = a_0 + a_1 t + \cdots + a_m t^m$ とおくと、

$$a_i = (-1)^{L-1} a_{m-i}$$

である。

$N_k = (k-1)! \binom{n}{k}$ より、

$$L = \sum_{k=1}^n \frac{n!}{k!}$$

よって、 $L_n = n(1 + L_{n-1})$, $L_1 = 1$

$n = 5$ のとき、 $L_5 = 325$, $m = 300$

$n = 6$ のとき、 $L_6 = 1956$, $m = 1920$

$n = 7$ のとき、 $L_7 = 13699$, $m = 13650$

⋮

百五十物語の計算時間

	$r = 20$	$0 \leq r \leq 150$
Maple	1 min.	80 years
GAP	11 sec.	17 years
C+NTL	0.3 sec.	5 months

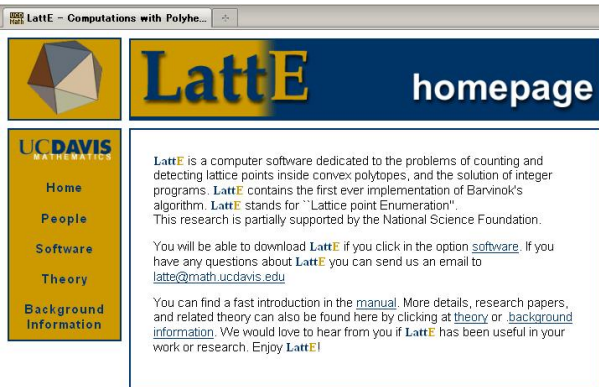
九百六十物語の計算時間

	$r = 20$	$r = 70$	$0 \leq r \leq 70$	$0 \leq r \leq 960$
C	1min.	18 days	4 months	1.7×10^{16} years

Impossible!


N : 「LattE というソフトを試してみてください。」

LattE



UCD
Math

LattE - Computations with Polyhe...



LattE homepage

UC DAVIS
MATHEMATICS

- Home
- People
- Software
- Theory
- Background Information

LattE is a computer software dedicated to the problems of counting and detecting lattice points inside convex polytopes, and the solution of integer programs. LattE contains the first ever implementation of Barvinok's algorithm. LattE stands for "Lattice point Enumeration". This research is partially supported by the National Science Foundation.

You will be able to download LattE if you click in the option [software](#). If you have any questions about LattE you can send us an email to latte@math.ucdavis.edu

You can find a fast introduction in the [manual](#). More details, research papers, and related theory can also be found here by clicking at [theory](#) or [background information](#). We would love to hear from you if LattE has been useful in your work or research. Enjoy LattE!

<http://www.math.ucdavis.edu/latte/>
次世代版は“LattE macchiato”

開発者

- LattE
 - J.A. De Loera
 - R. Hemmecke
 - Ruriko Yoshida
 - Jeremy Tauzer...and so on.
- LattE macchiato
 - E.Köppe

LattE にできること

ポリトープ $P \subset \mathbb{R}^d$ に対して

- P の内部にある格子点を数えること。
 - `count filename ... filename` に P の定義を記述。
 - `count n filename ... nP` 内の格子点を数える。
- P の “Ehrhart 級数” を求めること。
 - `ehrhart filename`
 - $Ehr(t) = \sum \#(nP \cap \mathbb{Z}^d) t^n$
- 線型関数の P 内の格子点における最適化。
 - `maximize filename`
 - `minimize filename`

再チャレンジ

- Cygwin ... ×
- Fedora Core 12 ... ×
- Fedora Core 6 ... !!
- Knoppix Math 2008...

連立線型方程式

変数の番号 $\begin{pmatrix} - & 1 & 2 \\ 3 & - & 4 \\ 5 & 6 & - \end{pmatrix}$

$$\begin{pmatrix} 1 & 1 & -1 & 0 & -1 & 0 \\ -1 & 0 & 1 & 1 & 0 & -1 \\ 0 & -1 & 0 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ r \end{pmatrix}$$

LattE input

ポリトープ P が $Ax \leq b$; $A \in M_{m,d}$, $b \in \mathbb{Z}^m$ で定義されているとき、

$$\begin{array}{|l} m & d + 1 \\ b & -A \end{array}$$

というファイルを用意してやればよい。

LattE input

```
6 21
0 1 1 1 1 -1 0 0 0 -1 0 0 0 -1 0 0 0 -1 0 0 0
0 -1 0 0 0 1 1 1 1 0 -1 0 0 0 -1 0 0 0 -1 0 0
0 0 -1 0 0 0 -1 0 0 1 1 1 1 0 0 -1 0 0 0 -1 0
0 0 0 -1 0 0 0 -1 0 0 0 -1 0 1 1 1 1 0 0 0 -1
0 0 0 0 -1 0 0 0 -1 0 0 0 -1 0 0 0 -1 1 1 1 1
-150 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
linearity 6 1 2 3 4 5 6
nonnegative 20 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
```

計算時間 ($n = 5$)

	$r = 20$	$0 \leq r \leq 150$
Maple	1 min.	80 years
GAP	11 sec.	17 years
C+NTL	0.3 sec.	5 months
LattE (CPU:600MHz)	5 min.	13 hours

計算時間 ($n = 6$)

	$r = 20$	$r = 70$	$0 \leq r \leq 960$
C	1min.	18 days	1.7×10^{16} years
LattE (CPU:3GHz)	2.8 hours	2.8 hours	112 days

$\mathbb{R}^d \supset P$: rational polyhedron

$$P = \{x \in \mathbb{R}^d \mid Ax \leq b\}, \quad A : m \times d \text{ 行列}, \quad b \in \mathbb{Z}^m$$

$$f_P = \sum_{a \in P \cap \mathbb{Z}^d} z^a \quad (z^a = z_1^{a_1} \cdots z_d^{a_d})$$

例 1

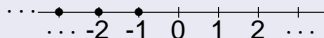
$$P : x \geq 0$$



$$1 + z + z^2 + \cdots = \frac{1}{1 - z} \quad (z \ll +\infty)$$

例 2

$$P : x \leq -1$$



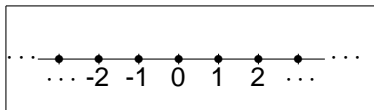
$$z^{-1} + z^{-2} + \dots = \frac{z^{-1}}{1 - z^{-1}} \quad (z \gg 1)$$

例 3

$$P : 2 \leq x \leq 4$$

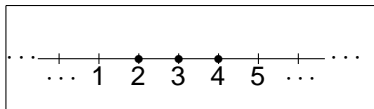


$$\begin{aligned} z^2 + z^3 + z^4 &= \frac{z^2}{1-z} + \frac{z^4}{1-z^{-1}} \\ (\text{RHS}) &= \frac{z^2}{1-z} + \frac{z^5}{z-1} \\ &= \frac{z^2 - z^5}{1-z} = \frac{z^2(1-z^3)}{1-z} \\ &= z^2(1+z+z^2) \end{aligned}$$



$$\sum_{n \in \mathbb{Z}} z^n = \frac{z^{-1}}{1 - z^{-1}} + \frac{1}{1 - z}$$

$$= \frac{1}{z - 1} + \frac{1}{1 - z} = 0$$



$$z^2 + z^3 + z^4 = \frac{z^2}{1-z} + \frac{z^4}{1-z^{-1}}$$

$$(\text{RHS}) = \frac{z^2}{1-z} + \frac{z^5}{z-1}$$

$$= \frac{z^2 - z^5}{1-z} = \frac{z^2(1-z^3)}{1-z}$$

$$= z^2(1+z+z^2)$$

$P \ni v$: vertex

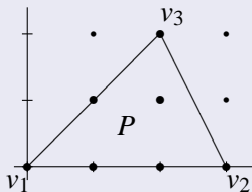
$C(P, v) = v + \{u \in \mathbb{R}^d \mid \text{十分小さな } \forall \delta > 0 \text{ に対して } v + \delta u \in P\}$
 v における P の “supporting cone”

定理

$$f_P = \sum_{v \in V(P)} f_{C(P, v)}$$

$V(P)$: P のすべて頂点の集合

例 4



$$f_C(v_1) = \frac{1}{(1-z_1)(1-z_1z_2)}$$
$$f_C(v_2) = \frac{z_1^3 + z_1^2z_2}{(1-z_1^{-1})(1-z_1^{-1}z_2^2)}$$
$$f_C(v_3) = \frac{z_1^2z_2^2 + z_1^2z_2 + z_1^2}{(1-z_1^{-1}z_2^{-1})(1-z_1z_2^{-2})}$$

$$f_1 + f_2 + f_3 = z_1^2z_2^2 + z_1^3 + z_1^2z_2 + z_1^2 + z_1z_2 + z_1 + 1$$

Proposition

P が直線を含めば $f_P = 0$

Proof.

$$P = \coprod_{\lambda \in \Lambda} l_\lambda$$

$$(\forall \lambda, \nu \in \Lambda, l_\lambda \parallel l_\nu)$$

$f_P = \sum_{\lambda \in \Lambda} f_{l_\lambda}$ なので、 $f_{l_\lambda} = 0$ を示せばよい。

$$f_{l_\lambda} = z^a \sum_{k \in \mathbb{Z}} z^{kb} = 0$$



定義 (Algebra of polyhedra)

部分集合 $S \subset \mathbb{R}^d$ に対して $[S] : \mathbb{R}^d \rightarrow \mathbb{R}$ を

$$[S](x) = \begin{cases} 1 & (x \in S) \\ 0 & (x \notin S) \end{cases}$$

と定義する。

$\mathcal{P}(\mathbb{R}^d) = \mathbb{R}\langle [P] \mid P : \text{polyhedron} \rangle : [P]$ で張られるベクトル空間
 $\mathcal{P}_0(\mathbb{R}^d) \langle [P] \mid P : \text{直線を含む polyhedron} \rangle$

supporting cone の有理関数に帰着

定理 (Brion)

任意の polyhedron $P \subset \mathbb{R}^d$ に対して $g \in \mathcal{P}_0(\mathbb{R}^d)$ が存在して

$$[P] = g + \sum_{v \in V(P)} [C(P, v)].$$

系

$$f_P = \sum_{v \in V(P)} f_{C(P, v)}$$

定義 (simple rational cone, unimodular cone)

$u_1, \dots, u_d \in \mathbb{Z}^d$: 一次独立
simple rational cone とは

$$K(u_1, \dots, u_d) = \left\{ \sum_i c_i u_i \mid c_i \geq 0 \right\}$$

のこと。その基本平行体とは、

$$\Pi(u_1, \dots, u_d) = \left\{ \sum_i c_i u_i \mid 0 \leq c_i < 1 \right\}$$

のこと。 $\text{vol}(\Pi) = 1$ を満たすとき K を unimodular cone と呼ぶ。

simple rational cone の有理関数

$K = K(u_1, \dots, u_d)$ が simple rational cone、 Π がその基本平行体のとき、

定理

$$\begin{aligned} f_K &= \left(\sum_{a \in \Pi \cap \mathbb{Z}^d} x^a \right) \prod_i \frac{1}{1 - x^{u_i}} \\ &= \text{vol}(\Pi) \prod_i \frac{1}{1 - x^{u_i}} \end{aligned}$$

三角形分割で、一般の cone は simple rational cone に分解できる。

simple rational cone の unimodular cone への分解

定理 (Barvinok)

次元 $d > 0$ を fix する。与えられた polyhedral rational cone $K \subset \mathbb{R}^d$ に対して unimodular cones K_i と $\epsilon_i = \pm 1$ であって

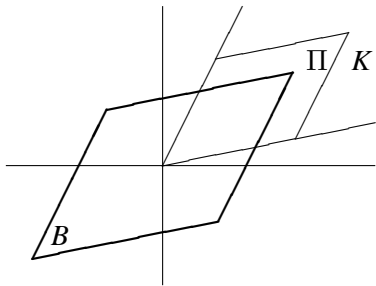
$$[K] = \sum_i \epsilon_i [K_i]$$

となるものを計算する多項式時間のアルゴリズムが存在する。

三角形分割により、 K を simple cone と仮定してよい：

$$K = K(u_1, \dots, u_d) \subset \mathbb{R}^d$$

$$B = \left\{ \alpha_1 u_1 + \dots + \alpha_d u_d \mid |\alpha_j| \leq (\text{vol}(\Pi))^{-\frac{1}{d}} \right\}$$



とおくと、 $\text{vol}(B) = 2^d$ である。

Minkowski's convex body theorem

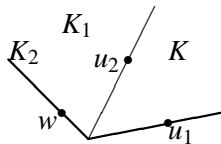
定理 (Minkowski)

A は \mathbb{R}^d のコンパクトな凸部分集合で、原点に関して対称とする。
 $\text{vol}(A) \geq 2^d$ ならば、 A は原点以外の格子点を少なくとも一つ持つ。

$w \in B$: 格子点

$K_j = K(u_1, \dots, u_{j-1}, w, u_{j+1}, \dots, u_n)$ とおく。

$$[K] = \sum_j \epsilon_j [K_j] \pmod{\text{lower dim. faces}}, \quad \epsilon_j = \pm 1$$



$$K_1 = K(w, u_2)$$

$$K_2 = K(u_1, w)$$

$$[K] = -[K_1] + [K_2]$$

$$\text{vol}(\Pi_j) = |u_1 \wedge \cdots \wedge w \wedge \cdots \wedge u_n|$$

$$= |\alpha_j| \text{vol}(\Pi) \leq (\text{vol}(\Pi))^{\frac{d-1}{d}}$$



Summary

- 組合せ論（“ アルゴリズム ”）の威力
… 九百六十物語、完成間近
- 簡約 Poincaré 級数の次のステップ
… 数学的な意味 → 不変式論
- Ehrhart 級数
… $n = 7$ の場合