

Kapitel II Gitterpunkt-Enumeration

Hier immer: $\mathbb{Z}^n$ als Gitter

Grundproblem: Sei $M \subseteq \mathbb{R}^n$. Wie können wir die Punkte $\mathbb{Z}^n \cap M$ aufzählen? Können wir sie so darstellen dass die Anzahl leicht abzulesen ist?

§1 Polytope und Polyeder

Def 1: Eine Menge $M \subseteq \mathbb{R}^n$ heißt Konvex falls gilt:
 $x, y \in M, \alpha \in [0, 1] \Rightarrow \alpha x + (1 - \alpha)y \in M$

Def 2: Eine Menge $P \subseteq \mathbb{R}^n$ heißt (konvexes) Polytop falls es eine endliche Menge $\{v_1, \dots, v_N\}$ gibt, so dass P die kleinste konvexe Menge ist, die $\{v_1, \dots, v_N\}$ enthält.

$$\rightarrow P = \left\{ \lambda_1 v_1 + \dots + \lambda_N v_N : \sum_{i=1}^N \lambda_i = 1, \lambda_i \geq 0 \forall i \in [N] \right\}$$

Notation: $P = \text{conv}\{v_1, \dots, v_N\}$

Def 3: Die Dimension einer Menge $M \subseteq \mathbb{R}^n$ ist die Dimension des kleinsten affinen Unterraums, der M enthält, d.h.

$$\dim M = \dim \operatorname{span} M = \dim \{x + \lambda(y-x) : x, y \in M, \lambda \in \mathbb{R}\}.$$

Thm 4 (Caratheodory): Sei $A \subseteq \mathbb{R}^n$, $y \in \operatorname{conv} A$.

Dann existieren $x_1, \dots, x_N \in A$ affin unabh. mit

$$y \in \operatorname{conv}\{x_1, \dots, x_N\}, \text{ und } N \leq \dim A + 1 \leq n + 1.$$

→ OR

Def 5: $H \subseteq \mathbb{R}^n$ heißt (affine) Hyperebene, falls es ein $c \in \mathbb{R}^n$ und $\delta \in \mathbb{R}$ gibt mit

$$H = \{x \in \mathbb{R}^n : c^T x = \delta\}.$$

Falls $c \neq 0$, so sind

$$H^+ = \{x \in \mathbb{R}^n : c^T x \geq \delta\} \quad \text{und} \quad H^- = \{x \in \mathbb{R}^n : c^T x \leq \delta\}$$

Halbräume.

Def 6: $P \subseteq \mathbb{R}^n$ heißt Polyeder, falls es eine Matrix $A \in \mathbb{R}^{m \times n}$ und einen Vektor $b \in \mathbb{R}^m$ gibt, so dass

$$P = \{x \in \mathbb{R}^n : Ax \leq b\} \quad \text{gilt.}$$

Thm 7 (Minkowski-Weyl) Sei $P \subseteq \mathbb{R}^n$. Dann gilt
 P ist beschränktes Polyeder $\Leftrightarrow P$ ist Polytop.

→ OR

Notation/Eigenschaften:

- Falls $P \subseteq H^+$ oder $P \subseteq H^-$, dann ist $P \cap H$ eine Seite von P .
- 0-dim. Seiten heißen Ecken.
- 1- — " — Kanten.
- $(n-1)$ - — " — Facetten.
- Falls $\dim P = n$, dann hat P mindestens $n+1$ Ecken.
- Falls $\dim P = n$ und $P = \text{conv}\{v_1, \dots, v_{n+1}\}$, so heißt P n -Simplex.
- Falls alle Ecken von P ganzzahlig sind, so heißt P ganzzahlig.

§2 Erste Beispiele

Wollen also bestimmen, wieviele ganzzahlige Punkte in einem Polytop P liegen.

Dazu: Betrachte zu P die Familie der Dilatationen

$$t \cdot P = \{(t \cdot x_1, \dots, t \cdot x_n) : x \in P\}.$$

Konvention: Seien (zunächst) alle Polytope ganzzahlig.

1. Würfel

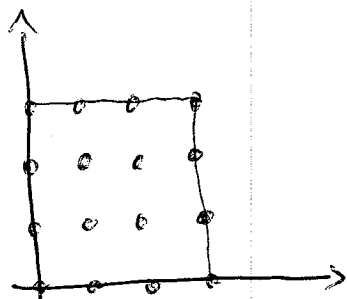
Der Einheitswürfel ist gegeben durch

$$Q = \{x \in \mathbb{R}^n : 0 \leq x_i \leq 1 \quad \forall i \in [n]\}$$

Dann ist für $t \in \mathbb{Z}, t > 0$

$$t \cdot Q = \{t \cdot x \in \mathbb{R}^n : 0 \leq x_i \leq 1 \quad \forall i \in [n]\}$$

der Würfel mit Kantenlänge t .



Def 1: Sei $L_P: \mathbb{Z}_{>0} \rightarrow \mathbb{Z}_{>0}$ die Funktion, die für ein festes Polytop dem Dilationsfaktor t die Anzahl der Gitterpunkte in $t \cdot P$ zuordnet, also

$$L_P(t) = |t \cdot P \cap \mathbb{Z}^n|$$

Hier also: $L_Q(t) = |t \cdot Q \cap \mathbb{Z}^n| = |[0, t]^n \cap \mathbb{Z}^n| = (t+1)^n$

Bem: L_Q ist ein Polynom in t und lässt sich als solches auf $t \in \mathbb{R}$ erweitern.

Genauer: $L_Q(t) = (t+1)^n = \sum_{k=0}^n \binom{n}{k} t^k$

$$\overbrace{(t+1) \cdot \dots \cdot (t+1)}^{n\text{-Mal}}$$

$\nwarrow \nearrow$
k-Mal ersten Eintrag wählen

Da wir L_P auch für nicht-ganzzahlige Mengen definieren können:

$$L_{Q^0}(t) = |t \cdot Q^0 \cap \mathbb{Z}^n| = |(0, t)^n \cap \mathbb{Z}^n| = (t-1)^n$$

Bem: Auch L_{Q^0} ist ein Polynom und wir können

umformen: $L_{Q^0}(t) = (t-1)^n = (-1)^n (-t+1)^n = (-1)^n L_Q(-t).$

2. Strecken im $\mathbb{R}^2$

Seien $a, b \in \mathbb{Z}_{>0}$ rel. prim und definiere

$$P = \{(k, l) \in \mathbb{R}^2 : k, l \geq 0, \underline{ka + lb = 1}\}.$$

$$\begin{aligned} \Rightarrow tP &= \{(k, l) \in \mathbb{R}^2 : k, l \geq 0, \underline{\frac{k}{t}a + \frac{l}{t}b = 1}\} \\ &= \{(k, l) \in \mathbb{R}^2, k, l \geq 0, \underline{ka + lb = t}\} \end{aligned}$$

$$\Rightarrow L_P(t) = |\{(k, l) \in \mathbb{Z}_{\geq 0}^2 : \underline{ka + lb = t}\}|$$

D.h.: $L_p(t)$ zählt die Möglichkeiten, t als nichtnegative (ganzzahlige) Linearkombination von a und b zu schreiben.

Methode der erzeugenden Funktion:

Betrachte die Reihen

$$1 + z^a + z^{2a} + \dots = \frac{1}{1-z^a} \quad \text{und}$$

$$1 + z^b + z^{2b} + \dots = \frac{1}{1-z^b}.$$

Im Produkt dieser Reihen zählt der Koeffizient von z^t dann ebenfalls alle Möglichkeiten, t als nichtneg. Linearkomb. von a und b zu schreiben.

$$\Rightarrow \left(\frac{1}{1-z^a} \right) \cdot \left(\frac{1}{1-z^b} \right) = \sum_{t \geq 0} L_p(t) z^t.$$

Anders gesagt: $L_p(t)$ ist der konstante Term der Reihenschreibweise von

$$\frac{1}{(1-z^a)(1-z^b)} z^t.$$

Vorsicht: In dieser Reihe kommen negative Exponenten vor, weshalb wir nicht einfach $z=0$ einsetzen können um den konstanten Term zu bestimmen.

Notation:

$$L_p(t) = \text{const} \left(\frac{1}{(1-2^a)(1-2^b)2^t} \right)$$

Bem: Mit ein paar Tricks lässt sich dieser Term explizit bestimmen:

Popoviciu 1953: Sei $b^{-1} \in \mathbb{Z}$ so dass $b^{-1}b = 1 \bmod a$ und $a^{-1} \in \mathbb{Z}$ so dass $a^{-1}a = 1 \bmod b$. Dann ist

$$L_p(t) = \frac{t}{a \cdot b} - \left\{ \frac{b^{-1}t}{a} \right\} - \left\{ \frac{a^{-1}t}{b} \right\} + 1$$

(wobei für $x \in \mathbb{R}$ gilt: $\{x\} = x - \lfloor x \rfloor$)