

COMPUTERALGEBRA

Freie Universität Berlin

Kompaktskript

İrem Portakal

9-15 März 2018

1 Termordnungen

Definition 1. Sei $k[x_1, \dots, x_n]$ ein Polynomring. Ein *Term* in $k[x_1, \dots, x_n]$ ist ein Potenzprodukt $x_1^{a_1} \dots x_n^{a_n}$ mit $a_1, \dots, a_n \in \mathbb{N}$.

Die Terme in $k[x_1, \dots, x_n]$ werden folglich mit \mathbb{N}^n identifiziert. Ein *Monom* ist ein Term mit einem nichtnullen Koeffizient von k . Man beachtet, dass ein Term ein Monom mit $c = 1$ (monisches Monom) ist. Der *Totalgrad* eines nichtnull Monoms $c.x_1^{a_1} \dots x_n^{a_n}$ ist die naturale Zahl $\deg(m) := a_1 + \dots + a_n$. Wir bezeichnen den Träger des Polynom $f = c_1 m_1 + \dots + c_r m_r$ mit $c_1 \in k \setminus \{0\}$ als die Menge

$$\text{supp}(f) := \{m_1, \dots, m_r\}.$$

Der Totalgrad eines nichtnull Polynoms f ist die naturale Zahl

$$\deg(f) = \max\{\deg(m) \mid m \in \text{supp}(f)\}$$

Bezeichne $\text{Mon}(S)$ als das Monoid aller Terme in $S := k[x_1, \dots, x_n]$. Dann gibt es die folgende Monoidabbildung

$$\log: \text{Mon}(S) \rightarrow \mathbb{N}^n$$

$$\exp: \text{Mon}(S) \leftarrow \mathbb{N}^n$$

mit $\log(x_1^{a_1} \dots x_n^{a_n}) = (a_1, \dots, a_n)$ und $\log^{-1} = \exp$.

Definition 2 (Monoidordnung und Termordnung \leq auf \mathbb{N}^n). Seien $a, b, c \in \mathbb{N}^n$. Eine Relation \leq auf \mathbb{N}^n wird eine *Monoidordnung* genannt, falls gilt

1. $a \leq a$ (Reflexivität)

2. $a \leq b$ und $b \leq a \Rightarrow a = b$ (Antisymmetrie)

3. $a \leq b$ und $b \leq c \Rightarrow a \leq c$ (Transitivität)
4. $a \leq b$ oder $b \leq a$ (Totalität)
5. $a \leq b \Rightarrow a + c \leq b + c$ (Verträglich mit +)

Eine *Termordnung* (oder eine Monomordnung) ist eine Monoidordnung, falls gilt

- $0 \leq a, \forall a \in \mathbb{N}^n$

Beispiel 1. 1. [Lexikographische Ordnung] $a \leq_{lex} b$, falls der am weitesten links stehende nichttriviale Eintrag von $b - a \in \mathbb{Z}^n$ positiv ist. **Singular:** lp.

2. [Reverse lexikographische Ordnung] $a \leq_{revlex} b$, falls der am weitesten rechts stehende nichttriviale Eintrag $b - a \in \mathbb{Z}^n$ negativ ist. **Singular:** ls. Das ist eine Monoidordnung aber **keine Termordnung**.

3. [Graduierte lexikographische Ordnung] $a \leq_{grlex} b \Leftrightarrow \sum_{i=1}^n a_i < \sum_{i=1}^n b_i$ oder $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$ und $a \leq_{lex} b$. **Singular:** dp.

4. [Ordnungsmatrix] Sei W ein Matrix mit den Zeilen $w_1, \dots, w_k \in \mathbb{Q}^n$. Dann gibt es eine Monoidordnung \leq_W zu W

$$a \leq_W b \Leftrightarrow W.a \leq_{lex} W.b$$

In **Singular**, $\mathbb{Wp}(w_1, \dots, w_n)$ ist definiert wie dp aber mit $\deg(x^a) = w_1 a_1 + \dots + w_n a_n$ und w_i 's sind positive ganze Zahle. Ausserdem kann man ein Matrix W in **Singular** definieren und schreibt man die Ordnung zu W als $\mathbb{M}(W)$.

5. [Graduierte Reverse lexikographische Ordnung] $a \leq_{grevlex} b$ wird durch W mit $w_1 = (1, \dots, 1)$ und $w_i = -e^{n+1-i}$ dargestellt. **Singular:** dp.

6. **Singular:** $\mathbb{wp}(w_1, \dots, w_n)$ ist analog zu \mathbb{Wp} aber mit grevlex .

$$a \leq_W b \Leftrightarrow W.a \leq_{grevlex} W.b$$

Angenommen, in jede W -Spalte ist der erste nicht-triviale Eintrag positiv. Dann ist \leq_W ist eine Termordnung.

Die partielle komponent-weise Ordnung auf \mathbb{N}^n ist

$$(a_1, \dots, a_n) \leq_{\mathbb{N}^n} (b_1, \dots, b_n) \Leftrightarrow a_i \leq b_i, \forall i = 1, \dots, n$$

Lemma 1 (Dickson's Lemma). *Jedes $M \subseteq \mathbb{N}^n$ enthält bez. \mathbb{N}^n nur endliche viele minimale Elemente.*

Beweis. Wir beweisen per Induktion über die Anzahl der Variablen n . Für $n = 1$ ist es klar. Angenommen, das Lemma gilt für $n - 1$. Wir verwenden die Variablen x_1, \dots, x_{n-1}, y . Sei M' die Menge der Monome m in x_1, \dots, x_{n-1} , so dass $my^a \in M$ für ein $a \in \mathbb{Z}_{>0}$. Nach der Induktionsverankerung wissen wir, dass es endlich viele Minimale Elemente in M' gibt: m'_1, \dots, m'_r . Wir definieren für $i = 1, \dots, r$

$$a_i = \min\{a \in \mathbb{Z}_{>0} \mid m'_i y^a \in M\}$$

Sei $a = \max\{a_1, \dots, a_r\}$. Für jedes $j = 0, \dots, a$, betrachten wir die Mengen

$$M'_j = \{\text{Monome } m \text{ in } x_1, \dots, x_{n-1} \mid my^j \in M\}$$

Die Minimalelemente in M finden sich in

$$\bigcup_{j=0}^a \{(m_{j,i}, j) \mid m_{j,i} \text{ Minimalelement in } M'_j\}$$

□

2 Divisionsalgorithmus und Gröbner Basis

2.1 Leitmonome und der Divisionsalgorithmus

Definition 3. Seien $0 \neq f \in k[x_1, \dots, x_n]$ ein Polynom und τ eine Monoidordnung. Wir definieren

$$\text{LT}_\tau(f) = \max_\tau \text{supp}(f) \text{ - den Leitterm von } f \text{ bez. } \tau,$$

$$\text{LC}_\tau(f) = \text{Koeffizient von } \text{LT}_\tau(f) \text{ in } f \text{ - den Leitkoeffizient von } f \text{ bez. } \tau.$$

$$\text{in}_\tau(f) = \text{LC}_\tau(f) \text{LT}_\tau(f) \text{ - den Leitmonom von } f \text{ bez. } \tau.$$

In Singular bezeichnet man sie als: `leadmonom(f)`, `leadcoef(f)`, `lead(f)`.

In der ersten Woche haben wir gesehen, dass der Polynomring in einer Variable $k[x]$ ein euklidischer Ring ist. Das heisst für $f, g \in k[x]$, findet man eindeutige $q, r \in k[x]$, so dass $f = q \cdot g + r$ mit $\deg(r) < \deg(g)$. Alle Ideale in $k[x]$ sind von einem einzigen Element in $k[x]$ erzeugt, i.e. $k[x]$ ist ein Hauptidealring. Um die Idealzugehörigkeit zu bestimmen, brauchen wir nur durch ein Polynom zu teilen. Im Fall von mehreren Variablen geht das nicht: $k[x_1, \dots, x_n]$ ist kein euklidischer Ring und kein Hauptidealring. Deswegen für die Idealzugehörigkeit, sollen wir erstmal die Division durch eine Menge von Polynomen definieren.

Satz 1 (Divisionsalgorithmus). *Seien $f, g_1, \dots, g_s \in k[x_1, \dots, x_n]$ Polynome ungleich Null und τ eine Termordnung. Dann lässt sich jedes $f \in k[x_1, \dots, x_n]$ schreiben als $f = q_1 g_1 + \dots + q_s g_s + r$ mit $(q_1, \dots, q_s, r) \in k[x_1, \dots, x_n]^{s+1}$, so dass*

- *Kein Element in $\text{supp}(r)$ liegt im Ideal $(\text{in}_\tau(g_1), \dots, \text{in}_\tau(g_s))$.*

- Für nicht-null q_i hat man $\text{in}_\tau(q_i g_i) \leq_\tau \text{in}_\tau(f)$.
- $\forall i = 1, \dots, s$ und $\forall m \in \text{supp}(q_i)$, es gilt dass $m \text{in}_\tau(g_i) \notin (\text{in}_\tau(g_1), \dots, \text{in}_\tau(g_{i-1}))$

Weiterhin sind (q_1, \dots, q_s, r) vom Tupel (f, g_1, \dots, g_s) eindeutig bestimmt.

Beweis. Wir präsentieren hier den Algorithmus der das Tupel $(q_1, \dots, q_s, r) \in k[x_1, \dots, x_n]^{s+1}$ zurückgibt.

Schritt 1. Seien $q_1 = \dots = q_s = r = 0$ und $v = f$.

Schritt 2. Finde das kleinste $i \in \{1, \dots, s\}$, so dass $\text{in}_\tau(v)$ ein Vielfaches von $\text{in}_\tau(g_i)$ ist. Falls so ein i existiert, ersetze:

$$q_i \rightsquigarrow q_i + \frac{\text{in}_\tau v}{\text{in}_\tau g_i} \text{ und } v \rightsquigarrow v - \frac{\text{in}_\tau(v)}{\text{in}_\tau(g_i)} \cdot g_i$$

Schritt 3. Wiederhole **Schritt 2** bis kein solches i existiert. Danach ersetze:

$$r \rightsquigarrow r + \text{in}_\tau(v) \text{ und } v \rightsquigarrow v - \text{in}_\tau(v)$$

Schritt 4. Wenn $v \neq 0$, springe zu **Schritt 2**. an. Wenn $v = 0$, gib (q_1, \dots, q_s, r) zurück. \square

Falls der Divisionsalgorithmus für $f, g_1, \dots, g_s \in k[x_1, \dots, x_n]$ das Tupel $(q_1, \dots, q_s, r) \in k[x_1, \dots, x_n]^{s+1}$ zurückgibt, sagen wir “ f wird mittels (g_1, \dots, g_s) zu r reduziert” oder im Kürze “ $f \mapsto_{(g_1, \dots, g_s)} r$ ”.

2.2 Gröbner Basis

Seien $f \in k[x_1, \dots, x_n]$ ein Polynom über einen Körper k und $I = (g_1, \dots, g_s)$ ein Ideal in $k[x_1, \dots, x_n]$. Aus Hilbert Basissatz folgt, dass alle Ideale $I \subseteq k[x_1, \dots, x_n]$ endlich erzeugt sind. Unsere Ziel ist zu entscheiden ob f in I ist. Wir haben versucht dies Analog zum Fall von einer Variable zu machen, d.h. wir haben f durch (g_1, \dots, g_s) geteilt (Divisionsalgorithmus). Obwohl aus $f \mapsto_{(g_1, \dots, g_s)} 0$ folgt $f \in I$, gilt Umkehrung nicht. Ein Beispiel sind das Polynom $f = y - z \in k[x, y, z]$ und das Ideal $I = (xy - 1, xz - 1)$. Deswegen brauchen wir hier Gröbner Basis.

Definition 4. Seien $I \subseteq k[x_1, \dots, x_n]$ ein Ideal und τ eine Termordnung. Wir definieren das Leitideal von I bezüglich τ als

$$\text{in}_\tau(I) = (\text{in}_\tau(f) \mid f \in I)$$

Beobachtung 1. Das ist nicht immer ausreichend nur die Leitmonome der Erzeuger zu berechnen. Sei $I = (xy - 1, y^2 - 1) \subset k[x, y]$. Wir haben bezüglich Termordnung grevlex, dass $(xy, y^2) \subsetneq \text{in}(I)$ da $x - y = y(xy - 1) - x(y^2 - 1) \in I$ aber $x \notin (xy, y^2)$.

Definition 5. Eine Menge von Polynome $\{g_1, \dots, g_r\}$ ist eine *Gröbner Basis* von I wenn

$$\text{in}_\tau(I) = (\text{in}_\tau(g_1), \dots, \text{in}_\tau(g_r))$$

Satz 2. *Ein Gröbner Basis von I erzeugt das Ideal I .*

Beweis. Wählen wir ein Polynom $f \in I \setminus (g_1, \dots, g_r)$ so dass $\text{in}_\tau(f)$ minimal ist. Da $\text{in}(f) \in \text{in}(I)$, existiert es ein g_i mit $\text{in}(g_i) \mid \text{in}(f)$. Dann hat $f - \frac{\text{in}(f)}{\text{in}(g_i)}g_i \in I$ ein kleineres Leitmonom aber es liegt nicht in (g_1, \dots, g_r) . \square

Gröbner Basen lösen das Problem der Idealzugehörigkeit:

Satz 3. *Seien $f \in k[x_1, \dots, x_n]$ ein Polynom und $I \subseteq k[x_1, \dots, x_n]$ ein Ideal. Fall G eine Gröbner Basis von I ist und $f \mapsto_G r$, dann*

$$f \in I \Leftrightarrow r = 0$$

3 Buchberger Algorithmus und reduzierte Gröbner Basis

Definition 6. Seien $f, g \in k[x_1, \dots, x_n]$ und $m_{f,g} = \text{ggT}(\text{in}(f), \text{in}(g))$. Wir definieren das *S-Polynom* von f und g als

$$S(f, g) := \frac{\text{in}(f)}{m_{f,g}} \cdot g - \frac{\text{in}(g)}{m_{f,g}} \cdot f \in (f, g)$$

Satz 4. *Sei $I = (g_1, \dots, g_r) \subseteq k[x_1, \dots, x_n]$. Dann sind die folgende Bedingungen äquivalent:*

1. (g_1, \dots, g_r) ist eine Gröbner Basis.
2. $\forall i, j, S(g_i, g_j) \mapsto_{(g_1, \dots, g_r)} 0$.

Die Suche wird dadurch vereinfacht, dass teilfremde Paare nicht überprüft werden müssen:

Satz 5. *Falls $\text{in}(f)$ und $\text{in}(g)$ teilerfremd sind, so gilt $S(f, g) \mapsto_{(f,g)} 0$.*

Seien $x^a = \text{in}_\tau(f)$ und $y^b = \text{in}_\tau(g)$. Dann gilt $S(f, g) = y^b f - x^a g = (f - x^a g) - (g - y^b f)$. Andererseits treten wir in $S(f, g)$ die Monome beider Summanden auf. Damit gilt $\text{in}_\tau((f - x^a g) - (g - y^b f)) = \text{in}_\tau((f - x^a)y^b) \leq \text{in}_\tau(S(f, g))$.

Buchberger Algorithmus

Sei $I = (f_1, \dots, f_k)$:

1. Setze $G := \{f_1, \dots, f_k\}$ und $P := \{(f_i, f_j) \mid i < j, \text{ggT}(\text{in}(f_i), \text{in}(f_j)) \neq 1\}$.
2. Solang $P \neq \emptyset$:
 - (a) $(f, g) = P[1]$.
 - (b) $P := P \setminus \{(f, g)\}$.
 - (c) Falls $\text{ggT}(\text{in}(f), \text{in}(g)) \neq 1$, reduziere $S(f, g) \mapsto_G r$.

(d) Falls $r \neq 0$, $P := P \cup (G, r)$ und $G := G \cup \{r\}$.

3. `return(G)`.

Satz 4 und Satz 5 führt uns zu der Beobachtung, dass G eine Gröbner Basis ist, falls schließlich $P = \emptyset$. Andererseits gilt $(\text{supp}(r)) \cap (\text{in}(G)) = \emptyset$ und $(\text{in}(G)) \subsetneq (\text{in}(G \cup \{r\}))$, falls $r \neq 0$.

Definition 7. Ein Gröbner Basis $\{g_1, \dots, g_r\}$ heisst reduziert, falls

1. $LC(g_i) = 1$, für alle $i = 1, \dots, r$.
2. $(\text{in}(g_1), \dots, \text{in}(g_r))$ sind die minimale Erzeuger von $\text{in}(I)$.
3. $\text{supp}(g_i - \text{in}(g_i)) \cap \text{in}(I) = \emptyset$, $\forall i = 1, \dots, r$.

Für jedes Ideal und jede Termordnung gibt es eine eindeutige reduzierte Gröbner Basis.

$S = k[x_1, \dots, x_n]$ ist ein unendlichdimensionaler Vektorraum. Da Ideale $I \subset S$ Unterräume von S sind, ist S/I auch ein Vektorraum.

Satz 6. (Macaulay) Sei $I \subset S$ ein Ideal, dann ist für jede Termordnung τ , die Menge:

$$\{\hat{m} \mid m \text{ Monom mit } m \notin \text{in}_\tau(I)\}$$

eine Basis von S/I als Vektorraum. Diese Monome heissen Standardmonome.

Mit Gröbnerbasen kann man Ideale mit Unterringen schneiden: Für $I \subset k[x_1, \dots, x_n, y_1, \dots, y_m]$, berechnen $I \cap k[y_1, \dots, y_m]$. Wir brauchen dafür eine Termordnung die folgende Bedingung erfüllt:

$$\text{in}_\tau(f) \in k[y_1, \dots, y_m] \Rightarrow f \in k[y_1, \dots, y_m]$$

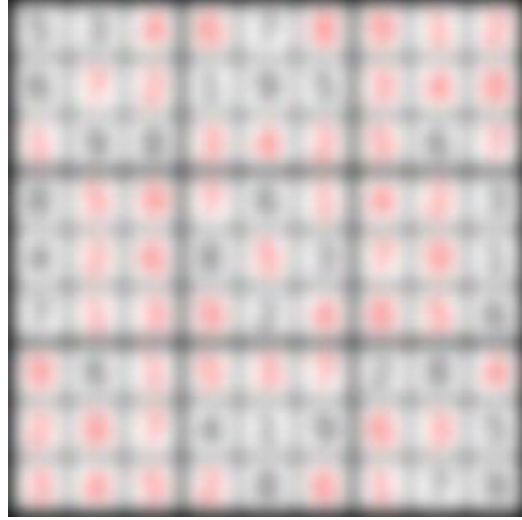
So eine Termordnung heisst *Eliminationsordnung* für x_1, \dots, x_n .

Satz 7. (Elimination) Sei $I \subset k[x_1, \dots, x_n, y_1, \dots, y_m]$ ein Ideal und sei τ eine Eliminationsordnung für x_1, \dots, x_n . Falls $\{f_1, \dots, f_r\}$ eine Gröbnerbasis von I bez. τ ist, dann ist $\{f_1, \dots, f_r\} \cap k[y_1, \dots, y_m]$ eine Gröbnerbasis von $I \cap k[y_1, \dots, y_m]$.

4 Eine Anwendung von Gröbner Basen: Sudoku

Sudoku wird von Howard Garns (USA) erfunden. Das Spiel wurde jedoch erst nach seinem Erfolg in Japan bekannt.

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



Jede Zelle enthält ganze Zahlen aus der Menge $\{1,2,3,4,5,6,7,8,9\}$. Es darf keine Wiederholung von Zahlen in denselben Zeilen, Spalte und 3×3 Box geben. Wir markieren die Zelle mit x_i , wo $i \in \{1, \dots, 81\}$. Wir definieren die Menge

$$E = \{(i, j) \mid i < j \text{ and } i, j \text{ in denselben Zeil, Spalte oder } 3 \times 3 \text{ Box}\}$$

Wir definieren die folgende Polynome

- $F(x_j) = \prod_{a=1}^9 (x_j - a) = 0, \forall j \in \{1, \dots, 81\}$
- $G(x_i, x_j) = \frac{F(x_i) - F(x_j)}{x_i - x_j} = 0$, für $\forall (i, j) \in E$
- $x_i - a_i = 0$, mit gegebenen Ziffern a_i der unvollständigen Lösung.

Die Polynome $F(x_j)$ spiegeln wider, dass jede Zelle eine Zahl aus $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ enthält. $G(x_i, x_j)$ codiert die Regel, dass $x_i \neq x_j$ für $(i, j) \in E$. Die lineare Polynome $x_i - a_i = 0$ lassen sich mit dem gegebenen Zahlen des Spiels identifizieren z.B. für obiges Sudoku, haben wir $x_1 - 5, x_2 - 3, x_5 - 7, x_{10} - 6, x_{13} - 1, x_{14} - 9, x_{15} - 5$, usw.

Wir definieren das Ideal $I \subset k[x_1, \dots, x_{81}]$ erzeugt von diesen 891 Polynomen. Die Aufgabe ist es die gemeinsamen Nullstellen der Polynome zu finden, d.h die *affine Varietät* $V(I)$

$$V(I) := \{x \in k^n \mid f(x) = 0, \text{ für } x \in I\}$$

Proposition 1. $a = (a_1, \dots, a_{81}) \in V(I)$ genau dann, wenn $a_i \in [9]$ and $a_i \neq a_j$ für $(i, j) \in E$.

Nehmen wir an, dass ein gegebenes Sudoku S genau eine Lösung hat.

Proposition 2. Sei $L \subset \{1, \dots, 81\}$ die Menge von Indizes von gegebene Zahlen $\{a_i\}_{i \in L}$ von einem Sudoku Spiel S . Dann ist $I_S = I + \langle x_i - a_i \rangle_{i \in L}$ das Ideal von S . Die reduzierte Gröbner Basis von I_S bezüglich der lexikalischen Ordnung ist $\langle x_1 - a_1, \dots, x_{81} - a_{81} \rangle$ und woraus folgt (a_1, \dots, a_{81}) die Lösung von S ist.

Beispiel 2. Diese Aussagen können wir in Singular implementieren.

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

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

Wir machen das Sudoku schwieriger und löschen 8 von der 62. Zelle.

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

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

Sei $L \subset \{1, \dots, 81\}$ die Menge von Indizes von gegebenen Zahlen im zweiten Bild. Dann erhalten wir die folgende Gröbner Basis

$$\langle x_{62} + x_{63} - 12, x_{17} - x_{63}, x_{12} + x_{18} + x_{63} - 14, x_9 + x_{18} + x_{63} - 14, x_3 - x_{18} - x_{63} + 8, \\ x_{63}^2 - 12x_{63} + 32, x_{18}x_{63} - 8x_{18} - 8x_{63} + 64, x_{18}^2 - 6x_{18} + 6x_{63} - 40 \rangle + \langle \{x_i - a_i\}_{i \in L} \rangle.$$

Man kann zeigen, dass es drei verschiedene Lösungen gibt.

Literatur

- [1] Franziska Hinkelmann, Lars Kastner and Mike Stillman, *Singular Online*, The official web-interface of Singular based on the InteractiveShell package, <https://www.singular.uni-kl.de:8003/>.
- [2] *A Computer Algebra System for Polynomial Computations*, HTML User Manual for Singular Version 4-1-0, 2016, University of Kaiserslautern Department of Mathematics Centre for Computer Algebra, <https://www.singular.uni-kl.de/Manual/latest/index.htm>
- [3] Michael Kaplan, *Computeralgebra*, Springer, 2005, DOI 10.1007/b137968.