Algebraische Algorithmen (Timo Fleischfresser und Deepak Chavan)

Teil 1: Matrizen

Matrizenmultiplikation

Sei A eine m x n Matrix und B eine n x p Matrix.

Dann ist A * B = W = [w_{ij} mit i = 0 .. m-1, j = 0 .. n-1]

Für i = 0 bis m-1
Für j = 0 bis n -1

$$w_{ij} = \sum_{k=0}^{n-1} a\ (i\ ,k\ ) * b\ (k\ ,j\ )$$

Laufzeit berechnet sich durch Anzahl an arithmetischen Rechenschritten.
Diese ist hier 2mn – mp ops.

Mit m = n = p für quadratische Matrizen ist somit die Laufzeit $O(n^3)$.

Der vorgestellte Algorithmus benötigt für 2 x 2 Matrizen 8 Multiplikation.

Die Idee ist nun, dass man eine n x n Matrix mit $n = 2^i$ für i aus N, in (n/2) x (n/2) Matrizen aufteilt. Dieser Schritt soll rekursiv stattfinden, so dass am Ende 2 x 2 Matrizen bestehen.

Der ***Strassen-Algorithum*** benötigt für das Produkt zweier 2 x 2 Matrizen nur 7 Multiplikation.

Und zwar seien A und B zwei 2 x 2 Matrizen.

Dann ist A * B = $\begin{pmatrix} a\ 11 & a\ 12 \\ a\ 21 & a\ 22 \end{pmatrix} * \begin{pmatrix} b\ 11 & b\ 12 \\ b\ 21 & b\ 22 \end{pmatrix} = \begin{pmatrix} c\,11 & c\,12 \\ c\,21 & c\,22 \end{pmatrix}$

Die benötigten 7 Multiplikationen sind:

$m_1 = (a_{12} – a_{22}) * (b_{21} + b_{22})$
$m_2 = (a_{11} + a_{22}) * (b_{11} + b_{22})$
$m_3 = (a_{11} – a_{21}) * (b_{11} + b_{12})$
$m_4 = (a_{11} + a_{12}) * b_{22}$
$m_5 = a_{11} * (b_{21} - b_{11})$
$m_6 = a_{22} * (b_{21} – b_{11})$
$m_7 = (a_{21} + a_{22}) * b_{11}$

Dann sind:
$c_{11} = m_1 + m_2 – m_4 + m_6$
$c_{12} = m_4 + m_5$
$c_{21} = m_6 + m_7$
$c_{22} = m_2 – m_3 + m_5 – m_7$

↙ Durch Rekursion gilt:
$T(n) = 7 * T(n/2) + a * n^2 = O(n^{lg\ 7}) = O(n^{2,81})$

PLU Zerlegung

Sei A eine n x n Matrix, dann gilt

P * A = L * U, wobei

P = Permutationsmatrix (pro Zeile und Spalte eine 1)
L = Einheits-„lower“ Matrix (d.h. oberes Dreieck ist 0 und Diagonalen enthalten 1)
U = „upper“ Matrix (unteres Dreieck ist 0)

Motivation für die Zerlegung:

1. lineare Gleichungssysteme
2. Determinantenbestimmung

Algorithmus für die PLU- Zerlegung:

- Erste Spalte betrachten
- Zeilen so tauschen, dass größtes Element oben steht, dieses sei Pivot Element
- Zahlen unter dem Pivot-Element teilen durch Pivot-Element
- In der Untermatrix (ohne Zeile und Spalte, zu dem das Pivot-Element gehört) äußeres Produkt bilden
- Rekursiv die Diagonale durchlaufen.

Obere Hälfte der Diagonalen entspricht U, untere Hälfte der Diagonalen mit 1 als Diagonale entspricht L.

Inversenbildung
Bildung der Inversen ist zurückzuführen auf die Matrizenmultiplikation, so dass dieses Problem ebenfalls in $O(n^{\lg 2})$ gelöst wird.

Algorithmus anwendbar auf symmetrische und positiv-definierte Matrix.
Für eine ist symmetrisch und positiv-definierte n x n Matrix A und $n = 2^i$ mit i aus N gilt:

$$A = \begin{pmatrix} B & C^T \\ C & D \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} B^{-1} + B^{-1} * C^T * S^{-1} * C * B^{-1} & -B^{-1} * C^T * S^{-1} \\ -S^{-1} * C * B^{-1} & S^{-1} \end{pmatrix}$$

mit S als der Konvulutionsmatrix

Angewandt auf alle invertierbaren Matrizen A mit n x n, gilt:
$A^T * A$ ergibt eine symmetrische und positiv-definierte Matrix, also lässt sich davon die Inverse mit diesem Algorithmus bestimmen.
Um schließlich Inverse zu A zu berechnen, rechnet man: $A^{-1} = (A^T * A) * A^T$
Da nur Matrizenmultiplikationen beteiligt sind, ist die Laufzeit auch hier $O(n^{\lg 2})$

Eigenwertbestimmung von Matrizen
Eigenwerte einer n x n Matrix A sind die Nullstellen des charakteristischen Polynoms $c_A(x) = \det(x*I - A)$.

Bestimmung der Nullstellen eines Polynoms lässt sich mit dem Newton’sche Näherungsverfahren näherungsweise bestimmen.
Algorithmus: Wähle geeignetes x_i in der Nähe der Nullstelle. Dann ergibt sich die nächste Stelle x_{i+1} durch

$$x_{i+1} = x_i - c_A(x_i) / c_A'(x_i)$$

Zu der Stelle x_i wird die Tangente am Graphen bestimmt, und die Nullstelle der Tangente ist das x_{i+1}.

Die Sylvester Resultante

Ziel

Die Sylvester Resultante ist ein Mittel, um herauszufinden, ob zwei Polynome einen nichttrivialen gemeinsamen Faktor, eine sogenannte gemeinsame Wurzel, besitzen. Die Sylvester Resultante ist die Determinante der sogenannten Sylvester Matrix, die für zwei Polynome f = $\sum_0^n a_i x^i$ und g = $\sum_0^m b_j x^j$ die folgende Form hat

$$S(f,g) := \begin{pmatrix} a_n & a_{n-1} & \dots & a_0 & 0 & \dots & 0 \\ 0 & a_n & \dots & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & \dots & \dots & \dots & a_0 \\ b_m & b_{m-1} & \dots & \dots & \dots & \dots & 0 \\ 0 & b_m & \dots & \dots & \dots & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & \dots & \dots & \dots & b_0 \end{pmatrix}$$

wobei sie aus m ersten Zeilen für die a_i und n Zeilen für die b_j besteht. Die zwei Polynome f und g haben genau dann einen nichttrivialen gemeinsamen Faktor, wenn die Resultante Res(f,g) = det(S(f,g)) gleich null ist.

Erweiterung

Die Sylvester Resultante ist nur anwendbar auf zwei Polynome. Um die Lösbarkeit eines Gleichungssystems mit mehr als zwei Gleichungen zu untersuchen, kann das Verfahren rekursiv angewendet werden. Dabei wird in jedem Rekursionsschritt eine Variable eleminiert bis nur noch ein univariates Polynom vorhanden ist, das dann auf seine Nullstellen untersucht werden kann. Der Nachteil dieses Verfahrens ist, dass der Grad der entstehenden Polynome exponentiell wächst, so dass es nur für eine geringe Zahl von Gleichungen praktisch realisierbar ist.

Beispiel

f(x) = x² + xy + 2x + y - 1 = 0
g(x) = x² + + 3x – y² + 2y – 1 = 0

$$S(f,g) = \begin{pmatrix} x+1 & x^2+2x-1 & 0 \\ 0 & x+1 & x^2+2x-1 \\ -1 & 2 & x^2+3x-1 \end{pmatrix}$$

$$\det(S(f,g)) = \mathrm{Re}s(S(f,g)) = -x^3-2x^2+3x$$

Die Resultante wird 0 für x=0, x=-3 und x=1. In f oder g eingesetzt ergibt das die Lösungsmengen {-3,1}, {0,1} und {1,-1}.

Die Macaulay Resultante

Ziel

Das Ziel der Macaulay Resultanten ist ebenfalls die Überprüfung eines Gleichungssystems auf seine Lösbarkeit. Der Vorteil der Macaulay Resultanten besteht darin, dass sie auch für mehr als zwei Gleichungen anwendbar ist und dass sie alle Variablen auf einmal eleminiert. Allerdings ist der Grad der Determinanten entsprechend höher.

Definitionen

Homogene Polynome : Homogene Polynome sind Polynome, bei denen der Gesamtgrad ihrer einzelnen Summanden gleich ist (die Grade verschiedener Variablen innerhalb eines Summanden werden dabei addiert)

Bsp.: f(x) = x² + y² + xy ist homogen.

Reduzierte Polynome : Ein Polynom P heißt reduziert in x^i für ein $1 \leq i \leq n+1$, falls kein Monom von P durch x^{d_i} teilbar ist, wobei d_i der totale Grad des Polynoms f_i ist. Es heißt reduziert in ¿ $x_{i_1}, \ldots x_{i_n}$ ¿ mit $1 \leq i_1 \ldots i_n \leq n+1$ reduziert ist.
¿
¿

Bsp.:
$$g_1 = 4x^2 + 3x + y^2$$
$$g_2 = 3x + 2y^2$$
$$g_3 = 2xy - 3x + y - 15$$

g_1 ist weder in x noch in y reduziert
g_2 ist in x reduziert
g_3 ist in x und y reduziert

Algorithmus zur Berechnung der Macaulay-Matrix

Gegeben : Polynomsystem $f_1 \ldots f_{n+1}$ mit n Variablen

1) Erzeugen des homogenen Polynomsystems $F_1 \ldots F_{n+1}$ durch Einführung einer Homogenisierungsvariablen x_{n+1} und $F_i = x_{n+1}^{d_i} f_i\left(\frac{x_1}{x_{n+1}} \ldots \frac{x_n}{x_{n+1}}\right)$ für i = 1...n+1
2) Definition von (n+2) Vektorräumen, wobei
   - V = Vektorraum aller homogenen Polynome vom Grad
     $t = \sum_{i=1}^{n+1} (d_i - 1) + 1 = \sum_{i=1}^{n+1} d_i - n$

- V_i = Vektorraum aller in $\{x_1 \ldots x_{i-1}\}$ reduzierten homogenen Polynome vom Grad $t - d_i$ einschließlich des Nullpolynoms (i = 1...n+1)
- B = Menge aller Monome aus V (Basis von V)
- B_i = Menge aller Monome von V_i (Basis von V_i)

3) Bildung der Macaulay-Matrix nach dem folgenden Schema :
   - Sei B = $\{b_1 \ldots b_\mu\}$ und B_i = $\{b_1 \ldots b_\mu\}$, dann ist die Matrix M bestimmt durch
   -
$$
\begin{array}{c|ccccccccc|}
 & b_1 & b_2 & b_3 & .. & .. & .. & .. & .. & b_\mu \\
b_{11}F_1 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
b_{1\mu_1} & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
b_{21}F_2 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
b_{2\mu_2}F_2 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
b_{(n+1)1}F_{n+1} & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
b_{(n+1)\mu_{(n+1)}}F_{n+1} & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots
\end{array}
$$
   -

4) Aufgrund der Homogenisierung der Polynome $f_1 \cdots f_{n+1}$ entspricht die Determinante dieser Matrix noch nicht der Resultanten der Matrix, sondern eines Vielfachen der Resultante. Deshalb kann es sein, dass obwohl die Determinante gleich 0 ist, das Gleichungssystem lösbar ist, nämlich wenn der Faktor 0 ist. Folglich muss dieser sogenannte „außerwesentliche Faktor" noch berechnet werden, um die Resultante zu erhalten. Der außerwesentliche Faktor ist die Determinante der Teilmatrix von M, die man erhält, wenn man alle Spalten streicht, bei denen die Elemente von B in n der Variablen $x_1 \ldots x_{n+1}$ reduziert sind und alle Zeilen streicht, die aus Multiplikationen von F_i mit Monomen, die in { $x_{i+1}, x_{i+2} \ldots x_{n+1}$ } für i = 1...n+1 reduziert sind, herrühren.

Beispiel

$f_1 = x^2 + xy + x + y$
$f_2 = 2x^2 + 3xy + y^2 + 3x + 3y + 1$
$f_3 = 2x + 3y + 4$

Dieses Gleichungssystem ist inhomogen, es muss also zunächst homogenisiert werden.

$F_1 = x^2 + xy + xz + yz$
$F_2 = 2x^2 + 3xy + y^2 + 3xz + 3yz + z^2$
$F_3 = 2x + 3y + 4z$

Der Grad der Basiselemente von V beträgt somit t = 2 + 2 + 1 – 2 = 3

B = $\{x^3, x^2y, xz^2, z^3, y^3, y^2z, yz^2, x^2z, xy^2, xyz\}$

Seien B'_i die Mengen aller homogenen Monome vom Grad t - d_i für i = 1...n+1

B'_1 ={x,y,z}
B'_2 ={x,y,z}
B'_3 ={x^2,xz,z^2,y^2,yz,xy}

Dann sind die Mengen B_i der in $\{ x_1 \dots x_{i-1} \}$ reduzierten Monome in B'_i für i = 1...3

B_1 ={x,y,z}
B_2 ={x,y,z}
B_3 ={xz,z^2,yz,xy}

Die eingerahmte Matrix sieht dann wie folgt aus

	x^3	x^2z	xz^2	z^3	y^3	y^2z	yz^2	x^2y	xy^2	xyz
xF_1	1	1	0	0	0	0	0	1	0	1
yF_1	0	0	0	0	0	1	0	1	1	1
zF_1	0	1	1	0	0	0	1	0	0	1
xF_2	2	3	1	0	0	0	0	3	1	3
yF_2	0	0	0	0	1	3	1	2	3	3
zF_2	0	2	3	1	0	1	3	0	0	3
xzF_3	0	2	4	0	0	0	0	0	0	3
z^2F_3	0	0	2	4	0	0	3	0	0	0
yzF_3	0	0	0	0	0	3	4	0	0	2
xyF_3	0	0	0	0	0	0	0	2	3	4

Um nun den außerwesentlichen Faktor zu bestimmen, untersuchen wir die Spalten- und Zeilenmonome auf ihre Reduziertheit :

Monom	x^3	x^2z	xz^2	z^3	y^3	y^2z	yz^2	x^2y	xy^2	xyz
Red. in	{y,z}	{y}	{x,y}	{x,y}	{x,z}	{x}	{x,y}	{y,z}	{x,z}	{x,y}

Monom	x	y	z	xz	z^2	yz	xy
Red. in	{x,y,z}	{x,y,z}	{x,y}	{x,y}	{x,y}	{x,y}	{x,y,z}

Der außerwesentliche Faktor ist folglich die Determinante der Matrix

$$A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \Rightarrow \det(A) = 1$$

Gröbner Basen

Was ist eine Gröbner Basis

Eine Gröbner Basis ist ein Generatorsystem für die Menge aller Linearkombinationen (das Ideal) der Polynome $f_1 \dots f_m$ mit einigen zusätzlichen Eigenschaften :

(1) G ist eine Gröbner Basis (unter Berücksichtigung der vorgegebenen Ordnung), wenn und nur wenn die Normalform normalf(g,G) = 0 für alle g, die im Ideal liegen, dass von G generiert wird
(2) Ein polynomisches Gleichungssystem $f_1(x_1 \dots x_n)=0 \dots f_m(x_1 \dots x_m)=0$ ist lösbar, wenn und nur wenn die Gröbner Basis von $f_1 \dots f_m$ ungleich {1} ist.
(3) Wenn das GS lösbar ist, sind die Nullstellen des GS sind auch Nullstellen der Polynome der Gröbner Basis

Definitionen

Multidegree : Multideg $(f)=\max(\alpha \in Z_{¿0}^n | a_\alpha \neq 0)$

Leading coefficient : LC $(f)=a_{multi\deg(f)} \in k$

Leading Monomial : LM $(f)=x^{multi\deg(f)}$ (mit Koeffizienten 1)

Ideal : $f_1, \dots, f_s$ sind Polynome über k[$x_1, \dots, x_n$], dann ist

$¿ f_1, \dots, f_s > = \left\{ \sum_{i=1}^{s} h_i f_i, h_1 \dots h_s \in k\ [x_1 \dots x_n] \right.$ ein Ideal, wenn es folgende Bedingungen erfüllt :

(a) $0 ¿ I$
(b) Wenn $f, g \underset{¿}{\in} I$, dann ist auch $f+g \underset{¿}{\in} I$
(c) Wenn $f \underset{¿}{\in} I$ und $h \underset{¿}{\in}$ k[$x_1, \dots, x_n$], dann ist auch $hf \underset{¿}{\in} I$

Gröbner Basis : Ein Generatorsystem G eines Ideals I wird eine Standard- oder Gröbner Basis genannt, wenn jede Reduktion von $f \underset{¿}{\in} I$ auf ein reduziertes Polynom immer null als Rest ergibt.

S-Polynom : Seien $f, g \underset{¿}{\in}$ k[$x_1, \dots, x_n$] zwei Polynome (ungleich null). Wenn mulideg(f)= α und multideg(g)= β , dann ist $\chi = \chi_1 \dots \chi_n$, wobei $\chi_i = \max\{\alpha_i, \beta_i\}$ für jedes i. x^χ wird *Least Common Multiple* (LCM) von LM(f) und LM(g) genannt. Das S-Polynom von f und g ist gegeben durch

$$S(f,g)=\frac{x^{\chi}}{LT(f)}f-\frac{x^{\chi}}{LT(g)}g\ .$$

Algorithmus zur Berechnung einer Gröbner Basis

Eingabe : Eine endliche Menge G von Polynomen
Ausgabe : Gröbner Basis von G

GB := G
B := $\{(f,g)\mid f,g\in G,\ f\neq g\}$

While ($B\neq\varphi$) {
  Select a pair (f,g) of B
  B := B \ {(f,g)}
  H := normalf(spoly(f,g),GB)

  If ($H\neq 0$) {
    GB := GB ¿ {H}
    B := B ¿ $\{(f,h)\mid f\in GB\}$
  }
}
Return GB

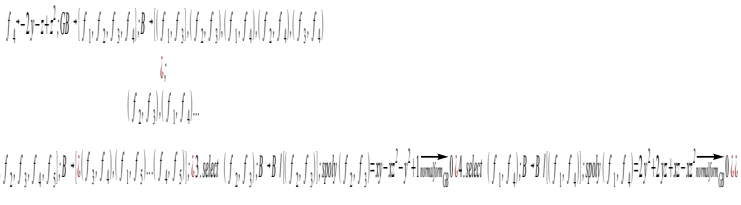
Beispiel

$$f_1=x-y-z$$
$$f_2=x+y-z^2$$
$$f_3=x^2+y^2-1$$

Berechnung der Gröbner Basis nach dem oben vorgestellten Buchberger Algorithmus :

$$1.\ GB\rightarrow\{f_1,f_2,f_3\};B\rightarrow\{(f_1,f_2),(f_1,f_3),(f_2,f_3)\};$$
$$select\ (f_1,f_2);B\rightarrow\{(f_1,f_3),(f_2,f_3)\};spoly(f_1,f_2)=-2y-z+z^2$$

Diese Formel ist bereits in Normalform



Alle weiteren Paare von S-Polynomen ergeben sich zu 0 bei der Normalformbildung.

$$5.\ GB=\{f_1,\ldots,f_5\}=\{x-y-z,x+y-z^2,x^2+y^2-1,-2y-z+z^2,-\frac{1}{2}z^4-\frac{1}{2}z^2+1\};$$

Die Menge GB ist eine Gröbner Basis. Sie enthält ein univariates Polynom, deren Nullstellen man bestimmen kann und durch Rücksubstitution auch die Werte für die restlichen Variablen erhält. So lässt sich folglich die Lösungsmenge des nichtlinearen Gleichungssystem $\{ f_1, f_2, f_3 \}$ bestimmen. Wäre das Gleichungssystem unlösbar, dann hätte sich die Gröbner Basis zu {1} ergeben.