

1 Anwendungen der Linearen Algebra

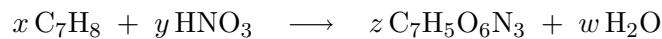
In der Mathematik und insbesondere in allen Naturwissenschaften haben wir es mit linearen Gleichungssystemen zu tun.

1.1 Chemische Reaktion

Angenommen, man interessiert sich für die Synthese des Giftes und Sprengstoffs TNT.

Unter kontrollierten Bedingungen ergibt Toluol C_7H_8 und Salpetersäure HNO_3 das Produkt TNT (Trinitrotoluol) $C_7H_5O_6N_3$ und das Nebenprodukt Wasser.

Wie sind die Mischungsverhältnisse von Toluol und Salpetersäure? Hierzu wird ein Chemiker folgende Gleichung aufstellen:



Da es sich um eine chemische Reaktion (und nicht etwa um eine Kernreaktion) handelt, muss die Anzahl der Atome der Elemente C, H, N und O vor und nach der Reaktion gleich sein. Mathematisch löst man also das LGS:

$$7x = 7z \quad \text{(Gleichung für C)}$$

$$8x + 1y = 5z + 2w \quad \text{(Gleichung für H)}$$

$$1y = 3z \quad \text{(Gleichung für N)}$$

$$3y = 6z + 1w \quad \text{(Gleichung für O)}$$

z.B. mit dem Gauß-Verfahren und folgender erweiterter Koeffizientenmatrix

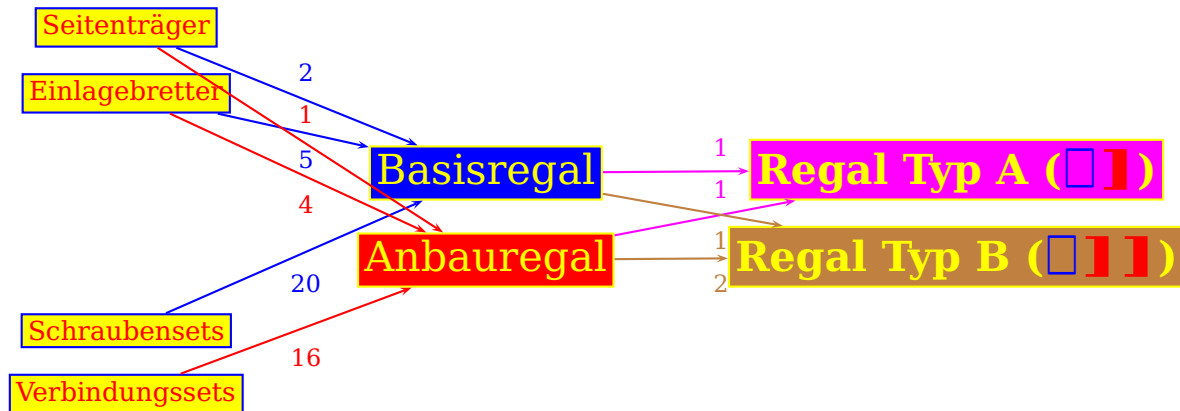
$$\left(\begin{array}{cccc|c} 0 & 7 & 0 & -7 & 0 \\ -2 & 8 & 1 & -5 & 0 \\ 0 & 0 & 1 & -3 & 0 \\ -1 & 0 & 3 & -6 & 0 \end{array} \right) \Leftrightarrow \left(\begin{array}{cccc|c} 1 & 0 & 0 & -3 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & -3 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

Es gibt hier unendlich viele Lösungen. Natürlich ist das LGS nicht eindeutig lösbar, denn wir haben z.B. nicht fest gelegt, wie viele Moleküle TNT hergestellt werden. Insbesondere ist die triviale Lösung ($w = x = y = z = 0$) möglich, d.h. wir stellen am besten gar nichts von diesem Sprengstoff her (obwohl es z.B. im Berg- oder Tunnelbau sinnvolle Anwendungen von Sprengstoff gibt; man könnte also $z = 1$ fordern und eine eindeutige Lösung erhalten).

1.2 Produktionsprozess

In einem Produktionsprozess gibt es typischerweise Zwischenprodukte, die in einem oder mehrere Endprodukte münden. Evtl. werden sogar Rohstoffe verarbeitet. Die verschiedenen Produktionsprozesse und die Lagerung von Rohstoffen, Zwischen- und Endprodukten verursachen Kosten. Die Rohstoffe oder Vorprodukte müssen eingekauft werden. Der Verkauf von End- und eventuell auch von Zwischenprodukten dagegen bringt Einnahmen. Unter Berücksichtigung all dieser Faktoren wird betriebswirtschaftlich versucht, einen maximalen Gewinn zu erzielen. Es wäre auch denkbar, bei vorgegebener Produktion die Kosten, die Produktionszeit oder die

Umweltbelastung zu minimieren. Dies sind mathematisch alles so genannte Extremwertprobleme, die in der Analysis behandelt werden. Hier konzentrieren wir uns auf die Aspekte, die mit linearer Algebra gelöst werden können. Betrachten wir das konkrete Beispiel einer Regalproduktion:



Anhand obiger Materialfluss-Darstellung lässt sich der Materialbedarf für die Herstellung von z.B. 10 Regalen vom Typ A und 5 Regalen vom Typ B bestimmen. So benötigt man allein für 5 Regale vom Typ B $5 \cdot 2 + 5 \cdot 2 = 20$ Seitenträger. Erhöht man nun die Zahl der möglichen Regaltypen, so wird der Rechenaufwand schnell sehr hoch. Professionell wird man dies mittels Linearer Algebra (PC-technisch mit sog. supply chain management Programmen) behandeln.

Die Bestellung der Endprodukte (Typ A $\square \blacksquare$, Typ B $\square \blacksquare \blacksquare$) schreibt man in einen Bestellvektor $\vec{x} = \begin{pmatrix} 10 \\ 5 \end{pmatrix}$. Den hierfür nötigen Bedarf an Zwischenprodukten entnimmt man dem obigen Materialfluss-Diagramm:

Anzahl der benötigten Basisregale: $y_1 = 10 \cdot \underline{1} + 5 \cdot \underline{1} = 15$

Anzahl der benötigten Anbauregale: $y_2 = 10 \cdot \underline{1} + 5 \cdot \underline{2} = 20$

Die unterstrichenen Werte lassen sich in einer Matrix zusammenfassen.

$$P_1 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

Diese Produktionsmatrix P_1 veranschaulicht die Geschehnisse in der letzten Produktionsstufe. Die Anzahl der Zwischenprodukte (Basis-, Anbauregale) schreiben wir auch als Vektor $\vec{y} = \begin{pmatrix} 15 \\ 20 \end{pmatrix}$, entstanden aus der Matrixmultiplikation:

$$\vec{y} = P_1 \cdot \vec{x} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 10 \\ 5 \end{pmatrix} = \begin{pmatrix} 15 \\ 20 \end{pmatrix}$$

Analog beantworten wir die Frage nach den benötigten Rohstoffen (bzw. Vorprodukten) bei nun vorgegebenen Zwischenprodukten. Aus dem Materialfluss-Diagramm bestimmt man die entsprechende Produktionsmatrix P_2 :

$$P_2 = \begin{pmatrix} 2 & 1 \\ 5 & 4 \\ 20 & 0 \\ 0 & 16 \end{pmatrix}$$

Der Rohstoffbedarf (Bretter, Schrauben) \vec{z} ist somit:

$$\vec{z} = P_2 \cdot \vec{y} = \begin{pmatrix} 2 & 1 \\ 5 & 4 \\ 20 & 0 \\ 0 & 16 \end{pmatrix} \cdot \begin{pmatrix} 15 \\ 20 \end{pmatrix}$$

Da \vec{y} selbst das Produkt aus Matrix mit Vektor ist, lässt sich obige Gleichung auch schreiben als $\vec{z} = P_2 \cdot \vec{y} = P_2 \cdot P_1 \cdot \vec{x}$. Der zweistufige Produktionsprozess lässt sich auch durch die Produktionsmatrix $P = P_2 \cdot P_1$ beschreiben:

$$P = P_2 \cdot P_1 = \begin{pmatrix} 2 & 1 \\ 5 & 4 \\ 20 & 0 \\ 0 & 16 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 9 & 13 \\ 20 & 20 \\ 16 & 31 \end{pmatrix}$$

1.3 Codierung von Nachrichten

Klartexte sollen in Geheimtexte codiert werden, so dass sie nicht gelesen werden können. Eine einfache Form der Codierung ist zunächst, den Buchstaben des Klartextes in eine Zahl umzuwandeln, was die Rechnung in Verschlüsselungsverfahren erheblich vereinfacht. Hierbei kann man z.B. eine ASCII-Tabelle oder folgende Tabelle benutzen.

	A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.
14	15	16	17	18	19	20	21	22	23	24	25	26	27

Demnach setzt man für ein Leerzeichen die Null, für das A die Eins, usw., und für das Z die Zahl 26. Außerdem kann man für einen Punkt (STOP) noch zusätzlich die Zahl 27 benutzen.

Eine relativ sichere Verschlüsselung einer solchen in Zahlen umgesetzten Nachricht benutzt Lineare Algebra. Dazu wird der Klartext, z.B. „MATHE IST SUPER.“, zunächst in Zahlen umgesetzt: „13 1 20 8 5 0 9 19 20 0 19 21 16 5 18 27“ und diese werden in eine 2-zeilige Matrix eingetragen:

$$W = \begin{pmatrix} 13 & 20 & 5 & 9 & 20 & 19 & 16 & 18 \\ 1 & 8 & 0 & 19 & 0 & 21 & 5 & 27 \end{pmatrix}$$

Diese Wortmatrix wird nun mit einer Verschlüsselungsmatrix V verschlüsselt. Nach dem Prinzip von Kerckhoffs („Die Sicherheit eines Kryptosystems beruht allein auf der Geheimhaltung des Schlüssels, nicht auf der Geheimhaltung des Kryptosystems.“) sollte diese Verschlüsselungsmatrix V möglichst geheim bleiben. So dass der unberechtigte Leser nur durch Raten („brute force attack“ mit Ausprobieren einer Vielzahl von Schlüsseln) bzw. mit einer Häufigkeitsanalyse der in deutschen Texten vorkommenden Buchstaben (siehe folgende Tabelle) der codierten Nachricht auf die Schliche kommt.

A	B	C	D	E	F	G	H	I	J	K	L	M	
6,5%	1,9%	3,1%	5,1%	17,4%	1,7%	3,0%	4,8%	7,6%	0,3%	1,2%	3,4%	2,5%	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	ß
9,8%	2,5%	0,8%	0,0%	7,0%	7,3%	6,2%	4,4%	0,7%	1,9%	0,0%	0,0%	1,1%	0,3%

Nehmen wir einmal an, die geheime Verschlüsselungsmatrix V sei:

$$V = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

so dass die codierte Matrix C schließlich:

$$C = V \cdot W = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 13 & 20 & 5 & 9 & 20 & 19 & 16 & 18 \\ 1 & 8 & 0 & 19 & 0 & 21 & 5 & 27 \end{pmatrix} = \begin{pmatrix} 15 & 36 & 5 & 47 & 20 & 61 & 26 & 72 \\ 43 & 92 & 15 & 103 & 60 & 141 & 68 & 162 \end{pmatrix}$$

wird.

Bis hierhin wurde codiert. Ohne Kenntnis des geheimen Schlüssels ist es fast unmöglich den Klartext wieder heraus zu lesen. Wenn durch günstige Umstände aber die Verschlüsselungstechnik mittels Matrixmultiplikation und auch noch der Schlüssel bekannt sind, so kann nun die codierte Nachricht C decodiert werden.

Also jetzt sind V und C bekannt, sowie dass gilt $VW = C$. Betrachten wir eine beliebige Spalte $c_k = \begin{pmatrix} a \\ b \end{pmatrix}$, die ja bekannt ist, die 2. Spalte von C wäre demnach $c_2 = \begin{pmatrix} 36 \\ 92 \end{pmatrix}$, und die dazu gehörige unbekannte Spalte von W , nennen wir sie $w_k = \begin{pmatrix} x \\ y \end{pmatrix}$, im konkreteren Beispiel gehört hierzu $w_2 = \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$.

$$C = \begin{pmatrix} 15 & \boxed{a} & 5 & 47 & 20 & 61 & 26 & 72 \\ 43 & \boxed{b} & 15 & 103 & 60 & 141 & 68 & 162 \end{pmatrix} \\ = V \cdot W = \begin{pmatrix} \boxed{1} & \boxed{2} \\ \boxed{3} & \boxed{4} \end{pmatrix} \cdot \begin{pmatrix} x_1 & \boxed{x_2} & x_3 & \dots & x_8 \\ y_1 & \boxed{y_2} & y_3 & \dots & y_8 \end{pmatrix}$$

Mittels Gauß-Verfahren können wir diese Unbekannten, nennen wir sie allgemein x und y , ermitteln:

$$1 \cdot x + 2 \cdot y = a \quad (\text{I})$$

$$3 \cdot x + 4 \cdot y = b \quad (\text{II})$$

Aus $II - 3 \cdot I$ folgt: $-2 \cdot y = b - 3 \cdot a$ und somit $y = \frac{3}{2} \cdot a - \frac{1}{2} \cdot b$, hierbei sind ja a und b bekannt. Setzen wir dies in die erste Gleichung ein, folgt: $x = -2 \cdot a + 1 \cdot b$, wie gesagt mit bekannten a , b . In Matrixschreibweise sieht dies entsprechend aus:

$$\left(\begin{array}{cc|c} 1 & 2 & a \\ 3 & 4 & b \end{array} \right) \begin{array}{l} \leftarrow -3 \\ \leftarrow + \end{array} \Leftrightarrow \left(\begin{array}{cc|c} 1 & 2 & a \\ 0 & -2 & b - 3 \cdot a \end{array} \right) \Leftrightarrow \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix}$$

Wir erkennen eine neue Matrix $V^{-1} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}$, die auf die beliebige Spalte von C die unbekannte Spalte von W ermittelt. Diese Matrix V^{-1} ist offenbar die Inverse zu V , denn was immer auch V mit W anstellt, so dass C heraus kommt, die Inverse V^{-1} dreht alles um und macht aus C wieder W zurück.

Wir decodieren nun also die codierte Nachricht, indem wir $V^{-1} \cdot C$ berechnen, den Zahlen der Wortmatrix $W = V^{-1} \cdot C$ wieder Buchstaben zuordnen und schließlich die Buchstaben wieder als Text ordnen, siehe hierzu auch <http://www.warncke-family.de/g12/abisz.ods>.

Wie können wir sicher sein, dass wir uns nicht verrechnet haben, und dass V^{-1} tatsächlich die gesuchte Inverse zur Verschlüsselungsmatrix V ist? Zum einen soll die Inverse V^{-1} ja die codierte Nachricht C wieder entschlüsseln. Wenn dann also das entschlüsselte Wort keinen Sinn macht, bzw. die Elemente der Wortmatrix W keine Zahlen zwischen 0 und 27 sind, sollte man sein Ergebnis nochmals überprüfen. Zum anderen ist wie gesagt eine Inverse die Umkehrung, d.h. mathematisch heben sich V und V^{-1} auf beim Matrixprodukt wie z.B. Vier und Vier⁻¹ = $\frac{1}{4}$ beim gewöhnlichen Multiplizieren mit Zahlen (statt Matrizen). Wenn man also sicher sein will, dass V^{-1} tatsächlich die Inverse zu V ist, dann berechnet man die entsprechenden Matrixprodukte und erhält die Einheitsmatrix E (wenn alles ok ist):

$$V^{-1} \cdot V = V \cdot V^{-1} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E$$