

Typen von algebraischen Gleichungen und Gleichungssystemen

Unter einer algebraischen Gleichung verstehen wir eine Gleichung, die wir aus endlich vielen unbekannten Größen $x_1, \dots, x_n$ in einem vorgegebenen Rechenbereich durch endlich viele Anwendungen der algebraischen Grundoperationen $+$ und $\cdot$ gewinnen können. Bspw. ist

$$x_2^4 + \frac{x_1 x_2}{2} - \frac{x_1^3}{3} + x_1 x_2^2 - x_2^2 + \frac{1}{7} = 0$$

eine algebraische Gleichung über dem Rechenbereich $\mathbb{Q}$.

Durch geeignete Umformungen können wir immer erreichen, dass auf der rechten Seite der Gleichung eine 0 steht. Spezialformen:

- Lineare Gleichung $3x_1 + \frac{x_2}{2} - 5 = 0$
- Univariate polynomiale Gleichung $x_1^4 - 3x_1^2 + x_1 - \frac{1}{3} = 0$
- Monomiale Gleichung $x_1^4 x_2^2 x_4 = 0$
- Multivariate polynomiale Gleichung $x_2^4 + \frac{x_1 x_2}{2} - \frac{x_1^3}{3} + x_1 x_2^2 - x_2^2 + \frac{1}{7} = 0$

Wenn man endlich viele algebraische Gleichungen gleichzeitig betrachtet so spricht man von einem Gleichungssystem.

Lineare und univariate Gleichungssysteme

Lineare Gleichungssysteme

- Ein allgemeines Verfahren zum Lösen linearer Gleichungssysteme ist der Gauß-Algorithmus, der darauf basiert, mehrere abgeleitete Gleichungen aus den gegebenen Gleichungen zu berechnen, die alle mit unterschiedlichen Variablen beginnen.

$$\left| \begin{array}{ccc} x_1 + x_2 & +x_3 & = 0 \\ x_1 & +2x_3 & = 0 \end{array} \right| \rightsquigarrow \left| \begin{array}{ccc} x_1 + x_2 + x_3 & = 0 \\ -x_2 + x_3 & = 0 \end{array} \right|$$

- Die Lösungsmenge kann man dann effizient berechnen.

Univariate Gleichungssysteme

- Es gibt Lösungsformeln für $\mathbb{R}$ und $\mathbb{C}$ wenn der Grad jeder Gleichung ≤ 4 ist.
- Für höhere Grade gibt es keine allgemeine Formel. Lösungen können aber durch numerische Verfahren wie bspw. das Newton-Verfahren approximiert werden.
- Bei einem Gleichungssystem mit mehreren univariaten Polynomgleichungen (in derselben Unbekannten) können wir Polynomdivision benutzen, um weitere Gleichungen abzuleiten (ohne die Lösungsmenge zu verändern). Die Reste der Divisionen sind die neuen abgeleiteten Gleichungen. Durch Polynomdivision kann man jedes solches Gleichungssystem auf eine einzige Gleichung reduzieren: Den größten gemeinsamen Teiler.

$$\left| \begin{array}{c} x^2 + x - 2 = 0 \\ x^3 - 2x^2 - x + 2 = 0 \end{array} \right| \rightsquigarrow |x - 1 = 0|$$

- Diese Anwendung der Polynomdivision ist nichts anderes als der Euklidische Algorithmus.

Allgemeine polynomiale Gleichungssysteme

Wie kann man nun im allgemeinsten Fall der multivariaten polynomialen Gleichungssysteme vorgehen?

- Gesucht:** Allgemeines Rechenverfahren, das die speziellen Rechenverfahren für lineare und univariate Gleichungssysteme beinhaltet.
- Das erreicht man, indem man die Ideen kombiniert:
 - Linearkombinationen $\rightsquigarrow$ Multiplikation mit Variablen
 - „erste“ Variable in Gleichung $\rightsquigarrow$ Leitterm
 - Polynomdivision $\rightsquigarrow$ multivariate Polynomdivision
- Ziel:** Abgeleitetes Gleichungssystem, dessen Leiterte alle Leiterte beschreiben, die man überhaupt bei diesem System als Leiterte abgeleiteter Gleichungen erhalten kann.
- Nenne die Menge der Gleichungen in diesem abgeleiteten System Gröbnerbasis.

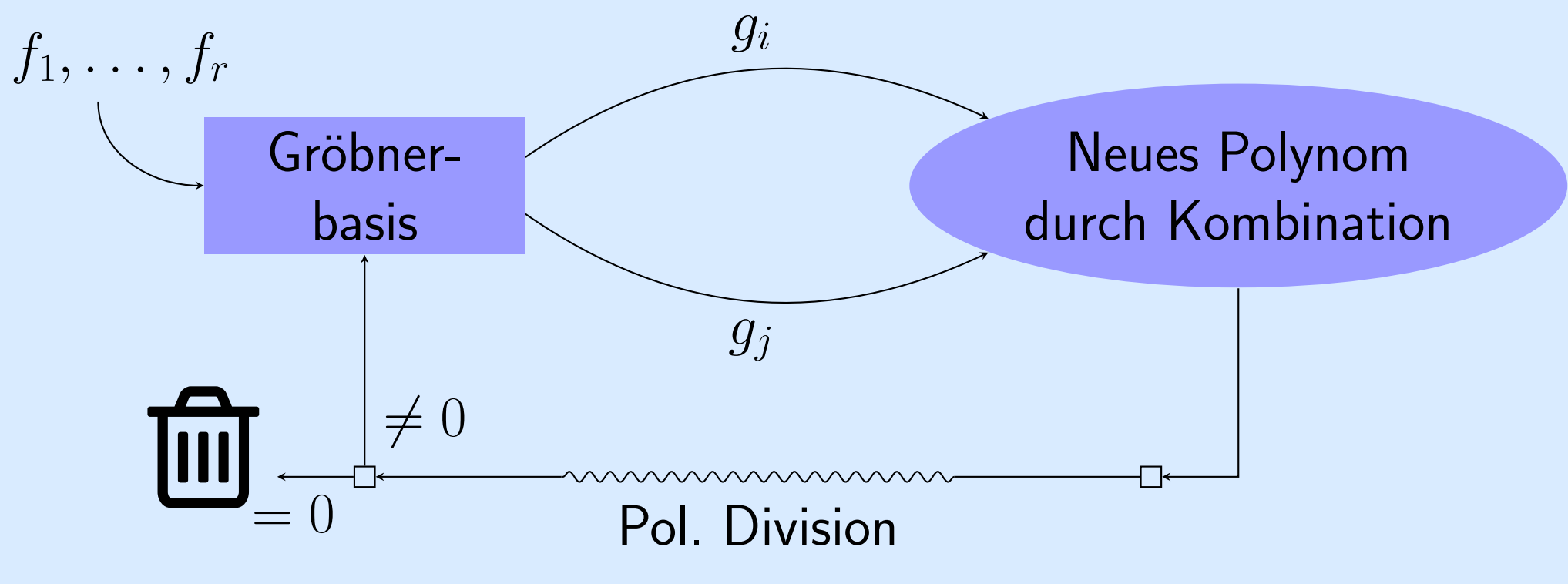
Ein Beispielgleichungssystem

$$\left| \begin{array}{c} xy - z = 0 \\ yz = 0 \end{array} \right| \rightsquigarrow \left| \begin{array}{c} xy - z = 0 \\ yz = 0 \\ z^2 = 0 \end{array} \right|$$

- Betrachte obiges multivariates polynomiales Gleichungssystem in den drei Variablen x, y, z . Ordne dabei die Terme lexikographisch, wobei $x > y > z$.
- Obwohl beide Gleichungen unterschiedliche Leitterme haben, xy und yz , bilden sie noch keine Gröbnerbasis.
- Entscheidend ist, dass diese beiden Terme einen gemeinsamen Teiler, y , haben.
- Wenn wir die erste Gleichung mit z multiplizieren und die zweite mit x und dann die Differenz bilden, erhalten wir eine abgeleitete Gleichung $z^2 = 0$ mit einem neuen Leitterm z^2 .
- Durch Hinzufügen dieser dritten Gleichung entsteht ein System, dessen linke Seiten eine Gröbnerbasis bilden.
- Diese Form eignet sich sogar besonders gut zum Bestimmen der Lösungsmenge: Für jede Lösung (a, b, c) muss gelten $c = 0$ (gemäß der dritten Gleichung); es gibt keine Einschränkungen für b (siehe zweite Gleichung nach Einsetzen $z = 0$); aus erster Gleichung: $a = 0$, falls $b \neq 0$, und a beliebig, falls $b = 0$ (siehe erste Gleichung nach Einsetzen der entsprechenden Werte für b und c).
- Die Lösungsmenge ist also die Vereinigung der x - und y -Achsen in der $(z = 0)$ -Ebene.

Algorithmik

Es gibt einen Algorithmus für die Berechnung einer Gröbnerbasis aus einer gegebenen Menge von Polynomen.



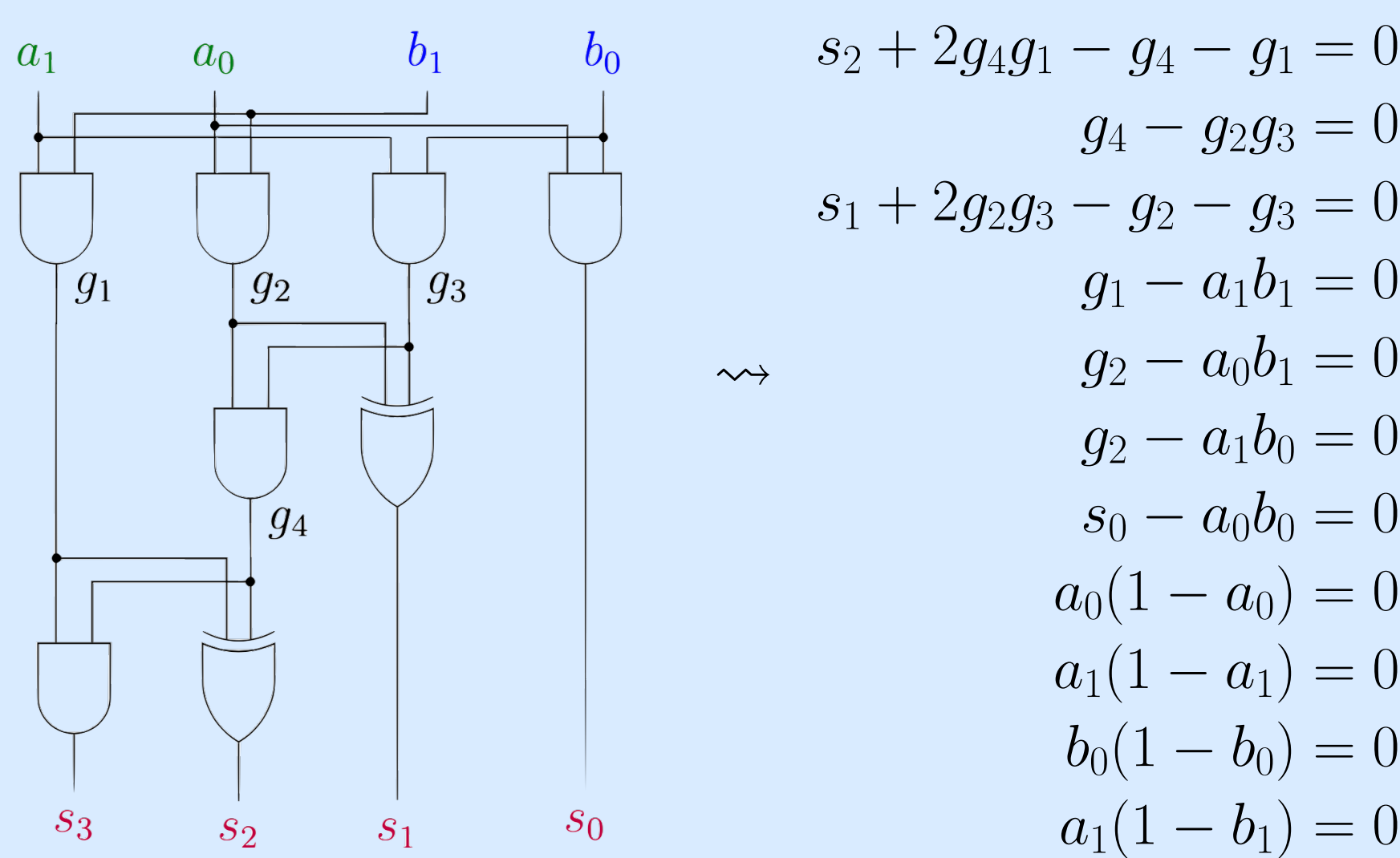
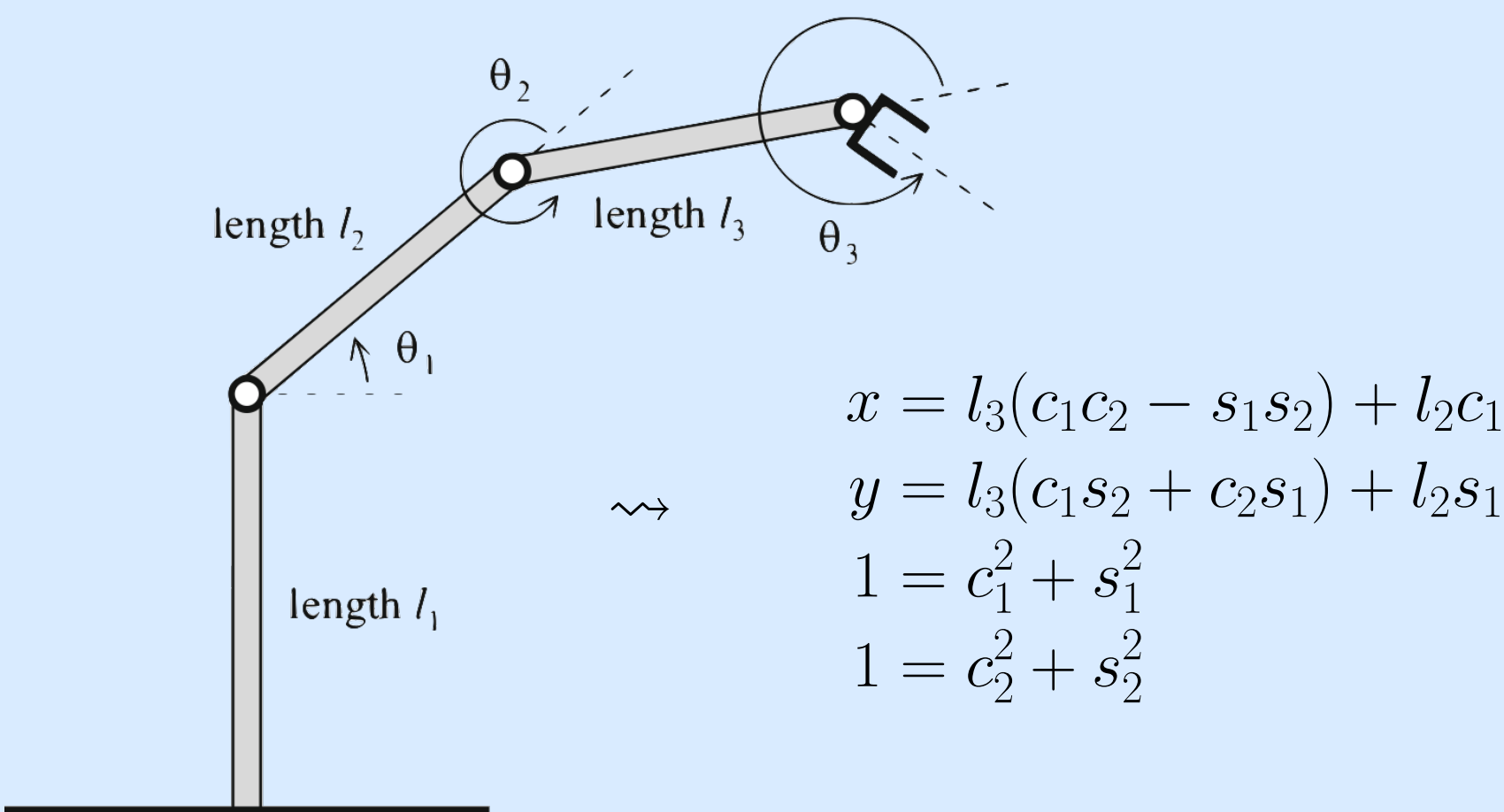
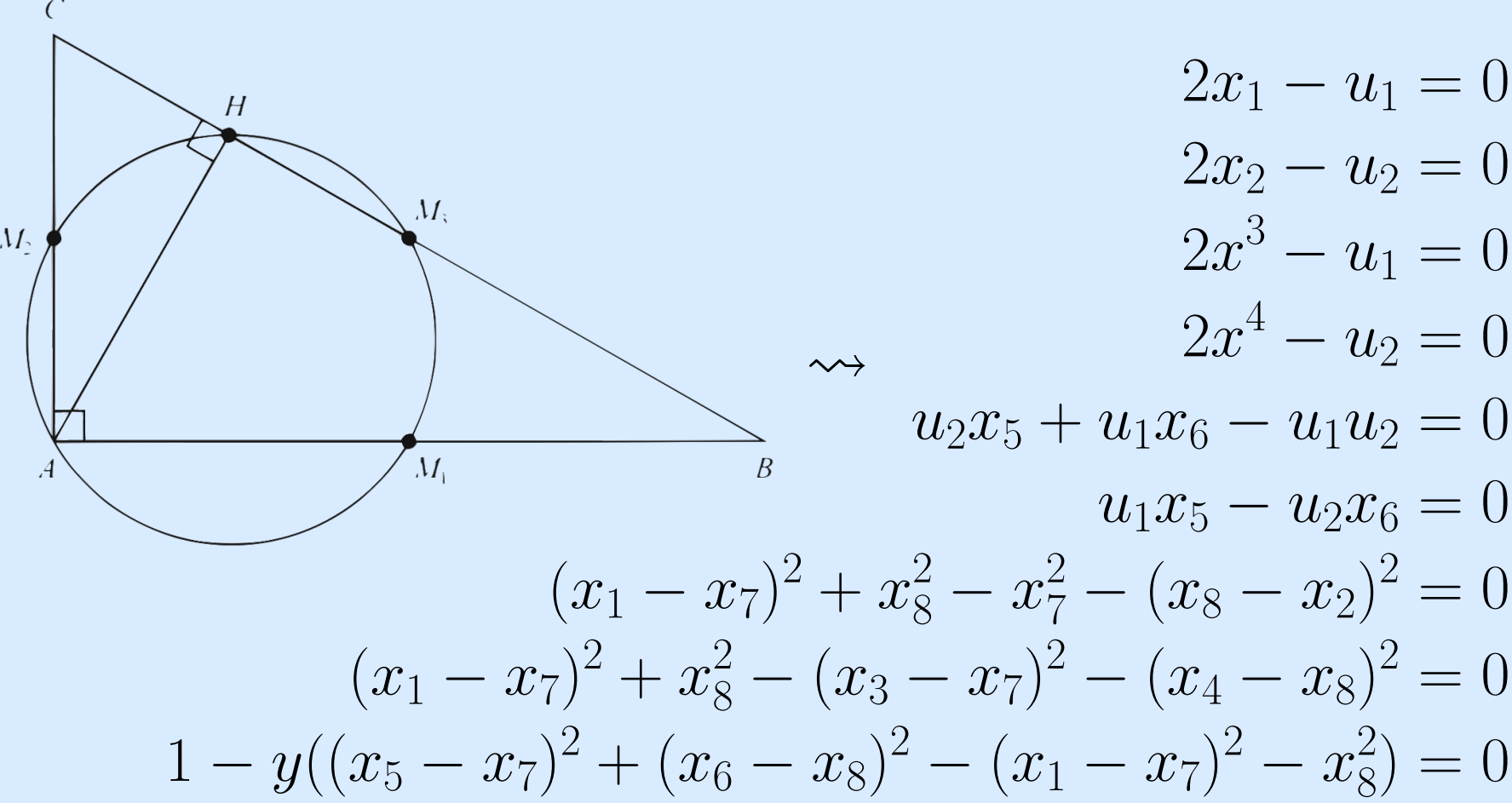
- Worst-case Laufzeit: doppelt exponentiell bzgl. der Größe der Eingabe. Bei vielen praktischen Beispielen aber akzeptabel gering. Trotzdem können Gröbnerbasenberechnungen unter Umständen extrem lange dauern.
- Daher ist es ein aktives Forschungsthema, optimierte Versionen des Algorithmus zu finden, die z.B. auch für bestimmte Typen von Eingaben eine bessere Performance aufweisen.

Syzygien: Abhängigkeiten zwischen Gleichungen

- Gröbnerbasen bieten auch einen Weg, systematisch alle Abhängigkeiten zwischen den Gleichungen in einem vorgegebenen System zu finden.
- Solche Abhängigkeiten heißen *Syzygien*; sie stellen eine Verallgemeinerung des Prinzips der linearen Abhängigkeiten zwischen Vektoren eines Vektorraums dar.
- Syzygien können zur Ermittlung möglichst kompakter Darstellungen von abgeleiteten Gleichungen benutzt werden; eine wiederholte Syzygienberechnung dient zur Aufdeckung wichtiger sogenannter homologischer Invarianten des Gleichungssystems und damit auch geometrischer Daten der zugehörigen Lösungsmenge.
- Außerdem kann eine verflochtene Berechnung von Gröbnerbasis und Syzygien einer Entwicklung von effizienteren Algorithmen dienen, sogenannten signaturbasierten Gröbnerbasisalgorithmen.
- Welche Relationen gibt es zwischen den gegebenen Gleichungen? Dies führt zum Begriff der *freien Auflösung*. (Es kann zwischen den Relationen wieder Relationen geben...)

Anwendungen

Gröbnerbasen finden innerhalb und außerhalb der Mathematik viele Anwendungen, bspw. im Automatischen Beweisen, in der Robotik oder in der Verifikation von Computerchips.



Verallgemeinerungen

Allgemeinere Rechenbereiche

- Klassischerweise betrachtet man Rechenbereiche wie $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$, in denen alle Grundrechnungsarten $(+, -, \cdot, \div)$ ausgeführt werden können. Wir bezeichnen solche Rechenbereiche als *Körper*.
- Manchmal ist man aber auch an Rechenbereichen wie $\mathbb{Z}$ interessiert, wo Division nicht immer möglich ist. Diese Rechenbereiche heißen *Ringe*.
- Auch in solchen Umgebungen können algebraische Gleichungen und Gröbnerbasen definiert werden. Die Theorie wird zwar etwas komplizierter, aber **alles bleibt algorithmisch**.

Gröbnerbasen in der freien Algebra

- In manchen Anwendungen ist es sinnvoll, mit Unbekannten zu arbeiten, die sich bzgl. Multiplikation nicht kommutativ verhalten, wo also $x_i \cdot x_j \neq x_j \cdot x_i$.
- Der allgemeinste geeignete Rechenbereich hierfür ist die sogenannte freie Algebra.
- Auch hier gibt es Gröbnerbasen, die aber nicht unbedingt vollständig berechenbar sind.
- Es stellen sich Fragen der (Semi-)Entscheidbarkeit von gewissen mathematischen Fragestellungen durch geeignete Algorithmen.
- Anwendung finden solche Gröbnerbasen z.B. beim automatisierten Beweisen von mathematischen Sätzen.
- Konkret ist dies besonders hilfreich beim Beweisen von Matrix-Identitäten (Matrizen sind ja bekanntlich i.A. nicht kommutativ bzgl. Multiplikation.)

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$