Komplexität des Erfüllbarkeitsproblems von Kreuzprodukt-Termen

On the Complexity of Satisfiability over Vector Product Terms

Diplomarbeit von Johanna Sokoli

Februar 2013

TECHNISCHE UNIVERSITÄT DARMSTADT

Fachbereich Mathematik
Arbeitsgruppe Logik

Komplexität des Erfüllbarkeitsproblems von Kreuzprodukt-Termen
On the Complexity of Satisfiability over Vector Product Terms

Vorgelegte Diplomarbeit von Johanna Sokoli

1. Gutachten: Prof. Dr. Martin Ziegler
2. Gutachten: Prof. Dr. Christian Herrmann

Tag der Einreichung:

Erklärung zur Diplomarbeit

Hiermit versichere ich, die vorliegende Diplomarbeit ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den 06. Februar 2013

(Johanna Sokoli)

Zusammenfassung

In der folgenden Arbeit soll die Komplexität des Erfüllbarkeitsproblems von Kreuzprodukt-Termen untersucht werden.
Ein zentrales Problem der Komplexitätstheorie ist das Erfüllbarkeitsproblem SAT boolscher Formeln. SAT liegt in $\mathcal{NP}$, und Cook und Levin haben unabhängig voneinander 1971 bzw. 1973 zeigen können, dass SAT $\mathcal{NP}$-vollständig ist, d.h. dies ist eines der schwersten Probleme, die eine nichtdeterministische Turingmaschine in polynomieller Zeit lösen kann. Um ein beliebiges anderes Problem aus $\mathcal{NP}$ zu lösen, braucht eine Turingmaschine höchstens polynomiell viel mehr Zeit.
Als ein alternatives Modell zur Turingmaschine, welche über dem Alphabet $\{0, 1\}$ arbeitet, wurde 1989 von Blum, Shub und Smale die BSS-Maschine, welche über einem Ring R arbeitet, eingeführt. Laut diesem Modell kann eine BSS-Maschine über $\mathbb{R}$ in jedem Schritt eine der Operationen Addition, Multiplikation, Division oder den Vergleich zweier reeller Zahlen exakt durchführen.
Da zur Berechnung von Kreuzprodukten nur diese Operationen notwendig sind, stellt sich die Frage, ob man ein zu SAT analoges Problem für Terme von Kreuzprodukten sinnvoll definieren kann, in welcher Komplexitätsklasse sich dieses befindet und ob auch dieses Problem vollständig bezüglich der entsprechenden Komplexitätsklasse ist.
In Kapitel 1 der vorliegenden Arbeit wird gezeigt, dass mehrere ähnliche Definitionen möglich sind. Dadurch ergeben sich die Fragestellungen, ob diese Probleme polynomialzeitäquivalent sind oder ob eines der Probleme echt schwerer ist als alle anderen, welche in Kapitel 2 behandelt werden. Im dritten Kapitel wird gezeigt, dass diese Probleme in $BP\left(\mathcal{NP}_{\mathbb{R}}^{0}\right)$ liegen, und die Vollständigkeit bezüglich dieser Klasse für einige der Probleme bewiesen.

Inhaltsverzeichnis

1 Grundlegende Definitionen und Eigenschaften von Kreuzprodukt-Termen 4

2 Reduzierbarkeit zwischen verschiedenen Erfüllbarkeitproblemen von Kreuzprodukt-Termen 10
2.1 Reduktionen zwischen reellwertigen Erfüllbarkeitsproblemen 10
2.2 Reduktionen zwischen projektiven Erfüllbarkeitsproblemen 12
2.3 Reduktionen zwischen reellwertigen und projektiven Erfüllbarkeitsproblemen 12
2.4 Übersicht über die bisherigen Reduktionen 21

3 Einordnung der Erfüllbarkeitsprobleme in Komplexitätsklassen 23
3.1 Einordnung der reellwertigen Erfüllbarkeitsprobleme 23
3.2 Einordnung der projektiven Erfüllbarkeitsprobleme 27
3.3 Untersuchen der Erfüllbarkeitsprobleme auf Vollständigkeit 28
3.3.1 Grundlagen der Verbandstheorie 28
3.3.2 Weitere Hilfsmittel zum Beweis von Theorem 3.21 35
3.3.3 Vollständigkeit einiger der betrachteten Erfüllbarkeitsprobleme 37

1 Grundlegende Definitionen und Eigenschaften von Kreuzprodukt-Termen

Das erste, von Alan Turing 1936 definierte Model eines Computers, wird heute Turingmaschine genannt und bildet eine der wichtigsten Grundlagen der Komplexitätstheorie. Alan Turing bezog sich in seinem Model noch auf eine Person (die ersten Computer gab es erst ab etwa 1940), welche beliebig viel Papier, einen Bleistift und einen Radiergummi zur Verfügung hat, und damit in jedem Schritt eine Ziffer lesen und in Abhängigkeit davon eine andere Ziffer schreiben, die gelesene Ziffer ausradieren oder überschreiben und anschließend entweder die gleiche Ziffer oder eine der beiden Ziffern rechts bzw. links davon bearbeiten kann, wobei die Ziffern aus $\{0,1\}$ sein müssen.
Damit stellte sich die Frage, welche Berechnungen von einer Turingmaschine durchgeführt und welche Probleme von ihr entschieden werden können, und wie viel Zeit und Platz sie dafür benötigt. Um Probleme, die eine solche Turingmaschine lösen kann, besser vergleichen zu können, wurden Komplexitäsklassen definiert. So bezeichnet $\mathscr{P}$ die Klasse all der Sprachen, die eine (deterministische) Turingmaschine in polynomieller Zeit entscheiden kann, während in $\mathscr{NP}$ diejenigen Entscheidungsprobleme liegen, die eine nichtdeterministische Turingmaschine, d.h. eine Turingmaschine, die zusätzlich zu den obigen erlaubten Arbeitsanweisungen raten kann, in polynomieller Zeit entscheiden kann. Weiter wurde der Begriff der sogenannten „Vollständigkeit“ definiert, der aussagt, dass ein Problem für die Komplexitätsklasse, in der es enthalten ist, zu den schwersten Problemen gehört.
So haben Cook und Levin unabhängig voneinander 1971 bzw. 1973 zeigen können, dass das in der Komplexitätstheorie zentrale Erfüllbarkeitsproblem SAT boolscher Formeln $\mathscr{NP}$-vollständig ist, d.h. dass eine Turingmaschine zum Entscheiden eines beliebigen anderen Entscheidungsproblems aus $\mathscr{NP}$ höchstens polynomiell viel mehr Zeit benötigt.
Da eine solche Turingmaschine nur mit dem Alphabet $\{0,1\}$ arbeitet, also eine Zahl aus $\mathbb{R}\backslash\mathbb{Q}$ in endlicher Zeit nicht einmal exakt lesen und somit auch nicht exakt mit ihr rechnen kann, wurde 1989 von Blum, Shub und Smale das sogenannte BSS-Modell eingeführt. Eine solche BSS-Maschine arbeitet über einem Ring R, der oft als $\mathbb{R}$ oder $\mathbb{C}$ festgelegt wird, und kann in jedem Schritt eine Addition, Multiplikation, Subtraktion oder Division oder den Vergleich zweier gegebener (oder berechneter) Zahlen exakt durchführen. Analog zu den zu einer Turingmaschine gehörenden Komplexitätsklassen wurden die Komplexitätsklassen $\mathscr{P}_{\mathbb{R}}$ und $\mathscr{NP}_{\mathbb{R}}$ definiert, die am Beginn des dritten Kapitels noch einmal wiederholt werden sollen.
Da zur Berechnung von Kreuzprodukten von Elementen aus $\mathbb{R}^3$, gelesen als Tripel reeller Zahlen, nur die einer BSS-Maschine erlaubten Rechenoperationen Multiplikation und Subtraktion benötigt werden, soll nun untersucht werden, ob ein zum Erfüllbarkeitsproblem SAT boolscher Formeln analoges Erfüllbarkeitsproblem für Kreuzprodukt-Terme definiert werden kann, in welcher Komplexitätsklasse sich dieses befindet und ob dieses ebenfalls ein vollständiges Entscheidungsproblem ist.
Dazu muss zunächst definiert werden, was man unter einem Kreuzprodukt-Term versteht, und was das Erfüllbarkeitsproblem von Kreuzprodukt-Termen sein soll. Diese Kreuzprodukt-Terme sollen nicht nur in $\mathbb{R}^3$, sondern auch über $\mathbb{P}^2$ untersucht werden, wobei unter $\mathbb{P}^2$ die Menge der Geraden in $\mathbb{R}^3$ verstanden wird, welche durch Richtungsvektoren $x \in \mathbb{R}^3\backslash\{0\}$ repräsentiert werden. Die von x erzeugte Gerade wird hierbei mit $[x]$ bezeichnet. Damit wird die Definition einer dem Kreuzprodukt ähnlichen Verknüpfung zweier Punkte aus $\mathbb{P}^2$ notwendig. Diese soll zur Vereinfachung ebenfalls als „Kreuzprodukt“ bezeichnet werden, obwohl es sich streng genommen im mathematischen Sinne nicht um ein Kreuzprodukt handelt. Dieses ist u.a. definiert als eine bilineare Abbildung eines Vektorraums auf sich selbst, projektive Räume tragen jedoch keine Vektorraumstruktur.

In diesem 1. Kapitel sollen diese für diese Arbeit zentralen Begriffe definiert und einige einfache Lemmata, die in den folgenden Kapiteln Verwendung finden sollen, gezeigt werden.

Wenden wir uns zunächst der Bildung von Kreuzprodukten in projektiven Räumen zu. Es erscheint sinnvoll, dieses Kreuzprodukt durch die Gerade zu definieren, welche durch das gewöhnliche Kreuzprodukt der Richtungvektoren zweier Ausgangsgeraden erzeugt wird.

Definition 1.1. *Seien $a, b \in \mathbb{R}^3 \backslash \{0\}$ und $[a], [b]$ die zugehörigen Äquivalenzklassen in $\mathbb{P}^2$. Das Kreuzprodukt von $[a]$, $[b]$ sei definiert als*

$$[a] \times [b] := [a \times b]$$

falls es existiert, d.h. falls $a \times b \neq 0$.

Bemerkung 1.2 Das Kreuzprodukt zweier projektiver Punkte ist wohldefiniert, d.h. unabhängig von den gewählten Repräsentanten:
Seien $[a], [a'], [b], [b'] \in \mathbb{P}^2$ mit $[a] = [a']$ und $[b] = [b']$, d.h. es gibt $\lambda, \mu \in \mathbb{R} \backslash \{0\}$, sodass $a = \lambda a'$ und $b = \mu b'$. Damit ist

$$\begin{aligned} & 0 \neq a \times b = (\lambda a') \times (\mu b') = \underbrace{\lambda\mu}_{\neq 0} \cdot (a' \times b') \\ \Leftrightarrow \quad & 0 \neq a' \times b' \end{aligned}$$

d.h. $[a \times b]$ existiert genau dann, wenn auch $[a' \times b']$ existiert, und es folgt

$$[a \times b] = [(\lambda a') \times (\mu b')] = [\lambda\mu \cdot (a' \times b')] = [a' \times b'].$$

Definition 1.3.

1. *Sei X eine $\mathbb{R}^3$-wertige Variable. Dann ist X ein Kreuzprodukt-Term über $\mathbb{R}^3$.*
2. *Sei X eine $\mathbb{P}^2$-wertige Variable. Dann ist X ein Kreuzprodukt-Term über $\mathbb{P}^2$.*
3. *Sind s, t Kreuzprodukt-Terme über $\mathbb{R}^3$, so ist auch $(s \times t)$ ein Kreuzprodukt-Term über $\mathbb{R}^3$.*
4. *Sind s, t Kreuzprodukt-Terme über $\mathbb{P}^2$, so ist auch $(s \times t)$ ein Kreuzprodukt-Term über $\mathbb{P}^2$.*

Bemerkung 1.4 Im Folgenden wird von einem Kreuzprodukt-Term statt von einem Kreuzprodukt-Term über $\mathbb{R}^3$ bzw. $\mathbb{P}^2$ gesprochen. Es wird sich aus dem Sinnzusammenhang ergeben, ob Terme über $\mathbb{R}^3$ oder $\mathbb{P}^2$ betrachtet werden.

Beispiel 1.5 Seien $X_1, \ldots, X_4$ $\mathbb{R}^3$- (oder $\mathbb{P}^2$-) wertige Variablen. Dann gilt:

a) X_1 ist ein Kreuzprodukt-Term.

b) $X_1 \times X_2$ ist ein Kreuzprodukt-Term.

c) $(X_1 \times X_3) \times (X_4 \times (X_2 \times X_1))$ ist ein Kreuzprodukt-Term.

d) $X_1 \times X_2 + X_3 \times X_4$ ist kein Kreuzprodukt-Term.

e) $\langle X_1, X_3 \rangle$ ist kein Kreuzprodukt-Term.

f) $5 \cdot X_1 \times X_2$ ist kein Kreuzprodukt-Term.

Für Kreuzprodukte in $\mathbb{R}^3$ gilt folgende nützliche Rechenregel, die man leicht durch Nachrechnen beweist:

Lemma 1.6 Seien $a, b, c \in \mathbb{R}^3$. Es gilt

$$a \times (b \times c) = \langle a, c \rangle \cdot b - \langle a, b \rangle \cdot c.$$

Eine weitere einfache, aber wichtige Eigenschaft des Kreuzprodukts in $\mathbb{R}^3$ ist seine Vertauschbarkeit mit Drehungen:

Lemma 1.7 Seien $a, b \in \mathbb{R}^3$ und $\mathscr{D} \in SO(3)$. Dann gilt

$$\mathscr{D}(a \times b) = \mathscr{D}(a) \times \mathscr{D}(b).$$

Beweis: Seien e_1, e_2, e_3 die Standardbasisvektoren von $\mathbb{R}^3$. Es gilt

$$\begin{aligned}
\mathscr{D}(a \times b) &= \mathscr{D}\left(\left(\sum_{i=1}^{3} a_i e_i\right) \times \left(\sum_{j=1}^{3} b_j e_j\right)\right) \\
&= \mathscr{D}\left(\sum_{i=1}^{3}\sum_{j=1}^{3} a_i b_j \left(e_i \times e_j\right)\right) \\
&= \sum_{i=1}^{3}\sum_{j=1}^{3} a_i b_j \mathscr{D}\left(e_i \times e_j\right).
\end{aligned}$$

Damit genügt es, die Behauptung für $e_i \times e_j$ $(i, j \in \{1, 2, 3\})$ zu zeigen.
Da $\{e_1, e_2, e_3\}$ eine Orthonormalbasis ist, gilt dies auch für $\{\mathscr{D}(e_1), \mathscr{D}(e_2), \mathscr{D}(e_3)\}$, und damit gilt

$$\begin{aligned}
\mathscr{D}(e_i \times e_j) &= \mathscr{D}(e_i) \times \mathscr{D}(e_j) \\
&\Leftrightarrow \\
\langle \mathscr{D}(e_i \times e_j), \mathscr{D}(e_k) \rangle &= \langle \mathscr{D}(e_i) \times \mathscr{D}(e_j), \mathscr{D}(e_k) \rangle \quad \forall\, k \in \{1, 2, 3\}.
\end{aligned}$$

Sei also $k \in \{1, 2, 3\}$ beliebig. Da Drehungen das Skalarprodukt invariant lassen, gilt dann

$$\begin{aligned}
\langle \mathscr{D}(e_i) \times \mathscr{D}(e_j), \mathscr{D}(e_k) \rangle &= \det(\mathscr{D}(e_i), \mathscr{D}(e_j), \mathscr{D}(e_k)) \\
&= \det(\mathscr{D}(e_i, e_j, e_k)) \\
&= \underbrace{\det(\mathscr{D})}_{=1} \cdot \det(e_i, e_j, e_k) \\
&= \det(e_i, e_j, e_k) \\
&= \langle e_i \times e_j, e_k \rangle \\
&= \langle \mathscr{D}(e_i \times e_j), \mathscr{D}(e_k) \rangle,
\end{aligned}$$

wobei mit $\det(a, b, c)$ die Determinante der Matrix gemeint ist, die entsteht, wenn man die Vektoren a, b, c in die Spalten einer Matrix schreibt. □

Als einfache Konsequenz dieses Resultats ergibt sich, dass auch beliebige Kreuzprodukt-Terme mit Drehungen vertauschen:

Korollar 1.8 Für einen beliebigen Kreuzprodukt-Term $t(X_1, \ldots, X_n)$ und $x_1, \ldots, x_n \in \mathbb{R}^3 \backslash \{0\}$ gilt

$$\mathscr{D}(t(x_1, \ldots, x_n)) = t(\mathscr{D}(x_1), \ldots, \mathscr{D}(x_n)).$$

Beweis: Mit Induktion über die Anzahl der Kreuzprodukte. □

Im Folgenden soll ebenfalls von der Drehung eines projektiven Punktes gesprochen werden können.

Definition 1.9. *Sei $\mathscr{D} \in SO(3)$, $a \in \mathbb{R}^3\backslash\{0\}$ und $[a]$ die zugehörige Äquivalenzklasse in $\mathbb{P}^2$. Die Drehung von $[a]$ sei definiert als*

$$\mathscr{D}([a]) := [\mathscr{D}(a)].$$

Bemerkung 1.10 Auch dieses Konzept ist wohldefiniert:
Seien dazu $a, b \in \mathbb{R}^3\backslash\{0\}$ mit $[b] = [a]$, d.h. es gibt ein $\lambda \in \mathbb{R}\backslash\{0\}$, sodass $a = \lambda b$. Dann gilt

$$[\mathscr{D}(a)] = [\mathscr{D}(\lambda b)] = [\lambda \mathscr{D}(b)] = [\mathscr{D}(b)],$$

d.h.

$$\mathscr{D}([a]) = \mathscr{D}([b]),$$

sodass die Drehung einer Äquivalenzklasse unabhängig vom gewählten Repräsentanten ist.

Analog zu Lemma 1.7 gilt

Lemma 1.11 Seien $[a], [b] \in \mathbb{P}^2$ und $\mathscr{D} \in SO(3)$. Dann gilt

$$\mathscr{D}([a]) \times \mathscr{D}([b]) = \mathscr{D}([a] \times [b]),$$

d.h. Kreuzprodukte und Drehungen vertauschen auch im projektiven Fall.

Beweis:

$$\begin{aligned}
\mathscr{D}([a]) \times \mathscr{D}([b]) &\overset{Def}{=} [\mathscr{D}(a)] \times [\mathscr{D}(b)] \\
&\overset{Def}{=} [(\mathscr{D}(a)) \times (\mathscr{D}(b))] \\
&\overset{1.7}{=} [\mathscr{D}(a \times b)] \\
&\overset{Def}{=} \mathscr{D}([a \times b]) \\
&\overset{Def}{=} \mathscr{D}([a] \times [b])
\end{aligned}$$

□

Korollar 1.12 Auch hier folgt damit für einen beliebigen Kreuzprodukt-Term $t(X_1, \ldots, X_n)$ und $[x_1], \ldots, [x_n] \in \mathbb{P}^2$

$$\mathscr{D}(t([x_1], \ldots, [x_n])) = t(\mathscr{D}([x_1]), \ldots, \mathscr{D}([x_n])).$$

Beweis: Mit Induktion über die Anzahl der Kreuzprodukte. □

Mit Hilfe der bisherigen Vorbereitung kann man verschiedene Erfüllbarkeitsprobleme von Kreuzprodukt-Termen definieren:

Definition 1.13.

a) $SAT_1 := \{\langle t(X_1,\dots,X_n)\rangle \mid t(X_1,\dots,X_n)$ *ist ein Kreuzprodukt-Term, es gibt* $x_1,\dots x_n \in \mathbb{R}^3\backslash\{0\}$, *sodass* $t(x_1,\dots,x_n) = e_3\}$

b) $SAT_2 := \{\langle t(X_1,\dots,X_n), s(X_1,\dots,X_n)\rangle \mid t(X_1,\dots,X_n), s(X_1,\dots,X_n)$ *sind Kreuzprodukt-Terme, es gibt* $x_1,\dots x_n \in \mathbb{R}^3\backslash\{0\}$, *sodass* $t(x_1,\dots,x_n) = s(x_1,\dots,x_n) \neq 0\}$

c) $SAT_3 := \{\langle t_1(X_1,\dots,X_n), s_1(X_1,\dots,X_n),\dots, t_m(X_1,\dots,X_n), s_m(X_1,\dots,X_n)\rangle \mid$
$t_1(X_1,\dots,X_n),\dots,t_m(X_1,\dots,X_n), s_1(X_1,\dots,X_n),\dots,s_m(X_1,\dots,X_n)$
sind Kreuzprodukt-Terme, es gibt $x_1,\dots x_n \in \mathbb{R}^3\backslash\{0\}$, *sodass*
$t_i(x_1,\dots,x_n) = s_i(x_1,\dots,x_n) \neq 0 \ \ \forall i \in \{1,\dots,m\}\}$

d) $SAT_4 := \{\langle t_1(X_1,\dots,X_n), s_1(X_1,\dots,X_n)\square\dots\square t_m(X_1,\dots,X_n), s_m(X_1,\dots,X_n)\rangle \mid$
$t_1(X_1,\dots,X_n),\dots,t_m(X_1,\dots,X_n), s_1(X_1,\dots,X_n),\dots,s_m(X_1,\dots,X_n)$
sind Kreuzprodukt-Terme, es gibt $x_1,\dots x_n \in \mathbb{R}^3\backslash\{0\}$, *sodass*
$t_1(x_1,\dots,x_n) = s_1(x_1,\dots,x_n) \neq 0 \quad \square\dots\square$
$t_m(x_1,\dots,x_n) = s_m(x_1,\dots,x_n) \neq 0\}$
wobei $\square \in \{\vee,\wedge\}$, *und in den Eingabetermen die Priorität der logischen Verknüpfungen* $\wedge$ *und* $\vee$ *durch Klammerung eindeutig festgelegt ist.*

e) $SAT_5 := \{\langle t_1(X_1,\dots,X_n)\diamond s_1(X_1,\dots,X_n)\square\dots\square t_m(X_1,\dots,X_n)\diamond s_m(X_1,\dots,X_n)\rangle \mid$
$t_1(X_1,\dots,X_n),\dots,t_m(X_1,\dots,X_n), s_1(X_1,\dots,X_n),\dots,s_m(X_1,\dots,X_n)$
sind Kreuzprodukt-Terme, es gibt $x_1,\dots x_n \in \mathbb{R}^3\backslash\{0\}$, *sodass*
$0 \neq t_1(x_1,\dots,x_n)\diamond s_1(x_1,\dots,x_n) \neq 0 \quad \square\dots\square$
$0 \neq t_m(x_1,\dots,x_n)\diamond s_m(x_1,\dots,x_n) \neq 0\}$
wobei $\square \in \{\vee,\wedge\}$, $\diamond \in \{=,\neq\}$ *und in den Eingabetermen die Priorität der logischen Verknüpfungen* $\wedge$ *und* $\vee$ *durch Klammerung eindeutig festgelegt ist.*

f) $SAT_{1^P} := \{\langle t(X_1,\dots,X_n)\rangle \mid t(X_1,\dots,X_n)$ *ist ein Kreuzprodukt-Term, es gibt* $[x_1],\dots[x_n] \in \mathbb{P}^2$, *sodass* $t([x_1],\dots,[x_n]) = [e_3]\}$

g) Wie in f) sei SAT_{i^P} *analog zu b) bis e) definiert als das jeweilige Erfüllbarkeitsproblem, wobei nun nach der Existenz von* $[x_1],\dots,[x_n] \in \mathbb{P}^2$ *gefragt wird, und die Bedingung, dass die ausgewerteten Terme nicht* 0 *sein dürfen, durch die Bedingung der Existenz aller ausgewerteten Kreuzprodukt-Terme ersetzt wird.*

h) $SAT_{2^{P^*}} := \{\langle t(X_1,\dots,X_n), s(X_1,\dots,X_n)\rangle \mid t(X_1,\dots,X_n), s(X_1,\dots,X_n)$
sind Kreuzprodukt-Terme, es gibt $[x_1],\dots[x_n] \in \mathbb{P}^2$
sodass $t([x_1],\dots,[x_n]) \neq s([x_1],\dots,[x_n])$ *und*
$t([x_1],\dots,[x_n]), s([x_1],\dots,[x_n])$ *existieren*$\}$

Beispiel 1.14 Es gilt $t(X_1,X_2) := (((X_1 \times (X_1 \times X_2)) \times X_1) \times (X_1 \times X_2)) \notin \mathrm{SAT}_1$, denn für beliebige $a, b \in \mathbb{R}^3\backslash\{0\}$ folgt mit Lemma 1.6

$$\begin{aligned} t(a,b) &= ((a \times (a \times b)) \times a) \times (a \times b) \\ &= -(a \times (a \times (a \times b))) \times (a \times b) \\ &\overset{1.6}{=} -(a \cdot \underbrace{\langle a, a \times b\rangle}_{=0} - (a \times b) \cdot \underbrace{\langle a, a\rangle}_{=:\lambda}) \times (a \times b) \\ &= \lambda \cdot (a \times b) \times (a \times b) \\ &= 0 \\ &\neq e_3. \end{aligned}$$

Bemerkung 1.15 Für alle Kreuzproduktgleichungen in SAT_i für $i \in \{1,\dots,4\}$ folgt, dass diese auch in SAT_{i^p} liegen: Gibt es eine Variablenbelegung $x_1,\dots,x_n \in \mathbb{R}^3\backslash\{0\}$, sodass die Auswertung der Terme gleich, aber ungleich 0 ist, so sind die Terme mit dieser Variablenbelegung insbesondere linear abhängig, und das Einsetzen von $[x_1],\dots,[x_n] \in \mathbb{P}^2$ führt zur Gleichheit der Terme über $\mathbb{P}^2$. Wegen der Bedingung, dass sie über $\mathbb{R}^3$ betrachtet nicht 0 sein dürfen, existieren diese auch in $\mathbb{P}^2$.

Dies könnte zu dem Schluss verleiten, dass (eine) Kreuzproduktgleichung(en) genau dann in SAT_i (für $i \in \{1,\dots,4\}$) liegt, wenn diese auch in SAT_{i^p} enthalten ist. Folgendes Beispiel zeigt, dass dies jedoch nicht der Fall ist.

Beispiel 1.16 Sei $t(X_1,X_2) := (X_1 \times X_2)$ und $s(X_1,X_2) := (X_2 \times X_1)$. Dann gilt

$$(t(X_1,X_2), s(X_1,X_2)) \in \mathrm{SAT}_{2^p} \quad \text{und} \quad (t(X_1,X_2), s(X_1,X_2)) \notin \mathrm{SAT}_2,$$

denn $x_1 \times x_2 = -x_2 \times x_1$ für alle $x_1, x_2 \in \mathbb{R}^3$, sodass die Gleichheit der Terme über $\mathbb{R}^3\backslash\{0\}$ nur im ausgeschlossenen Fall $x_1 \times x_2 = 0 = -x_2 \times x_1$ erfüllt wird. Über $\mathbb{P}^2$ gilt jedoch

$$[x_1 \times x_2] = [x_1] \times [x_2] = [-x_2] \times [x_1] = [x_2] \times [x_1] = [x_2 \times x_1]$$

für alle $[x_1], [x_2] \in \mathbb{P}^2$, sodass insbesondere eine erfüllende Variablenbelegung existiert.

Somit sind diese Erfüllbarkeitsprobleme von Kreuzprodukt-Termen echt verschieden, und es stellt sich die Frage, ob sie polynomialzeitäquivalent sind oder eines der Probleme echt schwerer ist als die anderen. Im folgenden Kapitel werden die Beziehungen zwischen diesen verschiedenen Erfüllbarkeitsproblemen untersucht.

2 Reduzierbarkeit zwischen verschiedenen Erfüllbarkeitproblemen von Kreuzprodukt-Termen

Betrachtet man die Definitionen der verschiedenen Erfüllbarkeitsprobleme, so fällt auf, dass zunehmend kompliziertere Kreuzprodukt-Terme bzw. immer mehr logische Verknüpfungen von aus Kreuzprodukt-Termen bestehenden Gleichungen zugelassen werden. Dies führt zu der Vermutung, dass diese auch entsprechend polynomiell reduzierbar sein sollten. Um dies im Folgenden zeigen zu können, wird noch einmal die Definition der polynomiellen Reduzierbarkeit wiederholt.

Definition 2.1. *Seien A, B Entscheidungsprobleme. Man nennt A polynomiell reduzierbar auf B, wenn es eine von einer deterministischen Turingmaschine in polynomieller Zeit (gemessen in der Länge der Eingabe) berechenbare Funktion f gibt, für die*

$$x \in A \qquad \Leftrightarrow \qquad f(x) \in B$$

gilt. Man schreibt hierfür $A \leq_p B$.

2.1 Reduktionen zwischen reellwertigen Erfüllbarkeitsproblemen

Proposition 2.2 Es gilt:

$$\mathrm{SAT}_1 \leq_P \mathrm{SAT}_2 \leq_P \mathrm{SAT}_3 \leq_P \mathrm{SAT}_4 \leq_P \mathrm{SAT}_5.$$

Beweis:

a) $\mathrm{SAT}_1 \leq_P \mathrm{SAT}_2$:
Sei $f(t(X_1,\ldots,X_n)) := (t(X_1,\ldots,X_n),X_{n+1})$, wobei X_{n+1} mit keiner der Variablen aus $t(X_1,\ldots,X_n)$ übereinstimmt. f ist offensichtlich in polynomieller Zeit berechenbar.

Sei $t(X_1,\ldots,X_n) \in \mathrm{SAT}_1$, d.h. es gibt $x_1,\ldots,x_n \in \mathbb{R}^3\backslash\{0\}$, sodass $t(x_1,\ldots,x_n) = e_3$ gilt. Dann gilt für diese $x_1,\ldots,x_n$ und $x_{n+1} := e_3 \in \mathbb{R}^3\backslash\{0\}$ $t(x_1,\ldots,x_n) = x_{n+1}$, und damit folgt $(t(X_1,\ldots,X_n),X_{n+1}) \in \mathrm{SAT}_2$.

Sei nun umgekehrt $(t(X_1,\ldots,X_n),X_{n+1}) \in \mathrm{SAT}_2$. Dann gibt es $x_1,\ldots x_{n+1} \in \mathbb{R}^3\backslash\{0\}$, sodass $t(x_1,\ldots,x_n) = x_{n+1}$. Sei $\mathscr{D}$ die Drehung, die x_{n+1} auf e_3 dreht, d.h. $\mathscr{D}(x_{n+1}) = e_3$. Dann folgt mit Korollar 1.8

$$\begin{aligned} t(\mathscr{D}(x_1),\ldots,\mathscr{D}(x_n)) &\overset{1.8}{=} \mathscr{D}(t(x_1,\ldots,x_n)) \\ &\overset{Vor.}{=} \mathscr{D}(x_{n+1}) \\ &\overset{Ann.}{=} e_3 \end{aligned}$$

sodass $t(X_1,\ldots,X_n) \in \mathrm{SAT}_1$ gilt.

b) $\text{SAT}_2 \leq_P \text{SAT}_3$:
Sei $f((t(X_1,\ldots,X_n), s(X_1,\ldots,X_n))) := (t(X_1,\ldots,X_n), s(X_1,\ldots,X_n))$, d.h. f ist die Identitätsfunktion. Diese ist trivialerweise in polynomieller Zeit berechenbar.

Sei $(t(X_1,\ldots,X_n), s(X_1,\ldots,X_n)) \in \text{SAT}_2$, d.h. es gibt $x_1,\ldots,x_n \in \mathbb{R}^3\backslash\{0\}$, sodass $t(x_1,\ldots,x_n) = s(x_1,\ldots,x_n) \neq 0$. Diese $x_1,\ldots,x_n \in \mathbb{R}^3\backslash\{0\}$ erfüllen somit auch $t_i(x_1,\ldots,x_n) = s_i(x_1,\ldots,x_n) \neq 0$ für alle $i \in \{1\}$, und damit folgt $f(t(X_1,\ldots,X_n), s(X_1,\ldots,X_n)) \in \text{SAT}_3$.

Gilt $f(t(X_1,\ldots,X_n), s(X_1,\ldots,X_n)) = (t(X_1,\ldots,X_n), s(X_1,\ldots,X_n)) \in \text{SAT}_3$, so gibt es $x_1,\ldots,x_n \in \mathbb{R}^3\backslash\{0\}$, sodass $t(x_1,\ldots,x_n) = s(x_1,\ldots,x_n) \neq 0$, und damit $(t(X_1,\ldots,X_n), s(X_1,\ldots,X_n)) \in \text{SAT}_2$.

c) $\text{SAT}_3 \leq_P \text{SAT}_4$:
Sei

$$\begin{aligned} &f(t_1(X_1,\ldots,X_n), s_1(X_1,\ldots,X_n),\ldots,t_m(X_1,\ldots,X_n), s_m(X_1,\ldots,X_n)) \\ &\quad := (t_1(X_1,\ldots,X_n), s_1(X_1,\ldots,X_n) \wedge \ldots \wedge t_m(X_1,\ldots,X_n), s_m(X_1,\ldots,X_n)). \end{aligned}$$

Eine Turingmaschine kann dies in polynomieller Zeit berechnen.

Gilt $(t_1(X_1,\ldots,X_n), s_1(X_1,\ldots,X_n),\ldots,t_m(X_1,\ldots,X_n), s_m(X_1,\ldots,X_n)) \in \text{SAT}_3$, so gibt es $x_1,\ldots,x_n \in \mathbb{R}^3\backslash\{0\}$, sodass $t_i(x_1,\ldots,x_n) = s_i(x_1,\ldots,x_n) \neq 0$ für alle $i \in \{1,\ldots,m\}$. Dann gilt für diese $x_1,\ldots,x_n \in \mathbb{R}^3\backslash\{0\}$ auch $t_1(x_1,\ldots,x_n) = s_1(x_1,\ldots,x_n) \neq 0 \wedge \ldots \wedge t_m(x_1,\ldots,x_n) = s_m(x_1,\ldots,x_n) \neq 0$, und somit $f(t_1(X_1,\ldots,X_n), s_1(X_1,\ldots,X_n),\ldots,t_m(X_1,\ldots,X_n), s_m(X_1,\ldots,X_n)) \in \text{SAT}_4$.

Ist $f(t_1(X_1,\ldots,X_n), s_1(X_1,\ldots,X_n),\ldots,t_m(X_1,\ldots,X_n), s_m(X_1,\ldots,X_n)) \in \text{SAT}_4$, so gibt es $x_1,\ldots,x_n \in \mathbb{R}^3\backslash\{0\}$, sodass $t_1(x_1,\ldots,x_n) = s_1(x_1,\ldots,x_n) \neq 0 \wedge \ldots \wedge t_m(x_1,\ldots,x_n) = s_m(x_1,\ldots,x_n) \neq 0$. Damit gilt $t_i(x_1,\ldots,x_n) = s_i(x_1,\ldots,x_n) \neq 0$ für alle $i \in \{1,\ldots,m\}$, und es folgt $(t_1(X_1,\ldots,X_n), s_1(X_1,\ldots,X_n),\ldots,t_m(X_1,\ldots,X_n), s_m(X_1,\ldots,X_n)) \in \text{SAT}_3$.

d) $\text{SAT}_4 \leq_P \text{SAT}_5$:
Sei

$$\begin{aligned} &f(t_1(X_1,\ldots,X_n), s_1(X_1,\ldots,X_n) \square \ldots \square t_m(X_1,\ldots,X_n), s_m(X_1,\ldots,X_n)) \\ &\quad := (t_1(X_1,\ldots,X_n) = s_1(X_1,\ldots,X_n) \square \ldots \square t_m(X_1,\ldots,X_n) = s_m(X_1,\ldots,X_n)), \end{aligned}$$

wobei die notwendige Klammerung zur eindeutigen Festlegung der Prioritäten der logischen Verknüpfungen $\wedge$ und $\vee$ unverändert übernommen wird.
Auch diese Funktion kann eine Turingmaschine in polynomieller Zeit berechnen.

Für $(t_1(X_1,\ldots,X_n), s_1(X_1,\ldots,X_n) \square \ldots \square t_m(X_1,\ldots,X_n), s_m(X_1,\ldots,X_n)) \in \text{SAT}_4$ gibt es $x_1,\ldots,x_n \in \mathbb{R}^3\backslash\{0\}$ mit $t_1(x_1,\ldots,x_n) = s_1(x_1,\ldots,x_n) \neq 0 \square \ldots \square t_m(x_1,\ldots,x_n) = s_m(x_1,\ldots,x_n) \neq 0$ unter Einhaltung der durch die Klammerung eindeutig vorgegebenen Prioritäten der logischen Verknüpfungen $\wedge$ und $\vee$. Damit folgt direkt

$$f(t_1(X_1,\ldots,X_n), s_1(X_1,\ldots,X_n) \square \ldots \square t_m(X_1,\ldots,X_n), s_m(X_1,\ldots,X_n)) \in \text{SAT}_5.$$

Gilt $f(t_1(X_1,\ldots,X_n), s_1(X_1,\ldots,X_n) \square \ldots \square t_m(X_1,\ldots,X_n), s_m(X_1,\ldots,X_n)) \in \text{SAT}_5$, so gibt es $x_1,\ldots,x_n \in \mathbb{R}^3\backslash\{0\}$ mit $t_1(x_1,\ldots,x_n) = s_1(x_1,\ldots,x_n) \neq 0 \square \ldots \square t_m(x_1,\ldots,x_n) = s_m(x_1,\ldots,x_n) \neq 0$ unter Einhaltung der durch die Klammerung eindeutig vorgegebenen Prioritäten der logischen Verknüpfungen $\wedge$ und $\vee$, sodass

$$(t_1(X_1,\ldots,X_n), s_1(X_1,\ldots,X_n) \square \ldots \square t_m(X_1,\ldots,X_n), s_m(X_1,\ldots,X_n)) \in \text{SAT}_4.$$

□

2.2 Reduktionen zwischen projektiven Erfüllbarkeitsproblemen

Da die entsprechenden projektiven Erfüllbarkeitsprobleme sehr ähnlich definiert sind, kann man vermuten, dass die entsprechenden polynomiellen Reduktionen ebenfalls möglich sind. Dies ist tatsächlich der Fall.

Proposition 2.3 Es gilt:

$$\mathrm{SAT}_{1^p} \leq_p \mathrm{SAT}_{2^p} \leq_p \mathrm{SAT}_{3^p} \leq_p \mathrm{SAT}_{4^p} \leq_p \mathrm{SAT}_{5^p}.$$

Beweis:

a) $\mathrm{SAT}_{1^p} \leq_p \mathrm{SAT}_{2^p}$:
Sei $f(t(X_1,\ldots,X_n)) := (t(X_1,\ldots,X_n),X_{n+1})$ mit $X_{n+1} \neq X_i$ für alle $i \in \{1,\ldots,n\}$. Dies kann eine Turingmaschine in polynomieller Zeit berechnen.

Sei $t(X_1,\ldots,X_n) \in \mathrm{SAT}_{1^p}$. Dann gibt es $[x_1],\ldots,[x_n] \in \mathbb{P}^2$, sodass $t([x_1],\ldots,[x_n]) = [e_3]$ gilt. Für diese $[x_1],\ldots,[x_n] \in \mathbb{P}^2$ und $[x_{n+1}] = [e_3]$ gilt dann auch $t([x_1],\ldots,[x_n]) = [x_{n+1}]$, sodass $f(t(X_1,\ldots,X_n)) \in \mathrm{SAT}_{2^p}$.

Sei $f(t(X_1,\ldots,X_n)) \in \mathrm{SAT}_{2^p}$, d.h. es gibt $[x_1],\ldots,[x_{n+1}] \in \mathbb{P}^2$, sodass $t([x_1],\ldots,[x_n]) = [x_{n+1}]$ gilt. Sei $\mathscr{D}$ eine Drehung mit $\mathscr{D}([x_{n+1}]) = [e_3]$. Es folgt

$$\begin{aligned} t(\mathscr{D}([x_1]),\ldots,\mathscr{D}([x_n])) &\overset{1.12}{=} \mathscr{D}(t([x_1],\ldots,[x_n])) \\ &\overset{Ann.}{=} \mathscr{D}([x_{n+1}]) \\ &= [e_3], \end{aligned}$$

d.h. es gibt $[x_1],\ldots,[x_n] \in \mathbb{P}^2$, sodass $t([x_1],\ldots,[x_n]) = [e_3]$, und damit $t(X_1,\ldots,X_n) \in \mathrm{SAT}_{1^p}$.

b), c) und d) zeigt man analog zu den Beweisen von Proposition 2.2 b), c) und d). Hier wird nur exemplarisch die Reduktion von SAT_{2^p} auf SAT_{3^p} gezeigt:

Sei $f((t(X_1,\ldots,X_n), s(X_1,\ldots,X_n))) := (t(X_1,\ldots,X_n), s(X_1,\ldots,X_n))$, d.h. f ist wie im Beweis von Proposition 2.2b) die Identitätsfunktion. Auch der Beweis, dass dies die gewünschte Reduktionsfunktion ist, verläuft analog:

Sei $(t(X_1,\ldots,X_n), s(X_1,\ldots,X_n)) \in \mathrm{SAT}_{2^p}$, d.h. es gibt $[x_1],\ldots,[x_n] \in \mathbb{P}^2$, sodass $t([x_1],\ldots,[x_n])$ und $s([x_1],\ldots,[x_n])$ existieren, und $t([x_1],\ldots,[x_n]) = s([x_1],\ldots,[x_n])$ gilt. Für diese $[x_1],\ldots,[x_n] \in \mathbb{P}^2$ existieren somit $t_i([x_1],\ldots,[x_n])$ und $s_i([x_1],\ldots,[x_n])$, und es gilt $t_i([x_1],\ldots,[x_n]) = s_i([x_1],\ldots,[x_n])$ für alle $i \in \{1\}$, sodass
$f(t(X_1,\ldots,X_n), s(X_1,\ldots,X_n)) \in \mathrm{SAT}_{3^p}$ folgt.

Gilt $f(t(X_1,\ldots,X_n), s(X_1,\ldots,X_n)) = (t(X_1,\ldots,X_n), s(X_1,\ldots,X_n)) \in \mathrm{SAT}_{3^p}$, so gibt es
$[x_1],\ldots,[x_n] \in \mathbb{P}^2$, sodass $t([x_1],\ldots,[x_n]) = s([x_1],\ldots,[x_n])$ gilt und die Auswertung der Terme wohldefiniert ist, und damit folgt $(t(X_1,\ldots,X_n), s(X_1,\ldots,X_n)) \in \mathrm{SAT}_{2^p}$.

□

2.3 Reduktionen zwischen reellwertigen und projektiven Erfüllbarkeitsproblemen

Die obigen Resultate sind aufgrund der Definition der jeweiligen Erfüllbarkeitsprobleme zu erwarten gewesen und stellen in einem gewissen Sinne „triviale“ Reduktionen dar. Im Folgenden wird klar werden,

dass man auch eine ganze Reihe nichttrivialer Aussagen dieser Art erhalten kann. Das folgende Theorem stellt erstmals eine Verbindung zwischen einem der Erfüllbarkeitsprobleme von Kreuzprodukt-Termen über $\mathbb{R}^3$ und zwei projektiven Erfüllbarkeitsproblemen her.

Theorem 2.4 Es gilt:

$$\mathrm{SAT}_{2^{p*}} \equiv_P \mathrm{SAT}_1 \equiv_P \mathrm{SAT}_{1^p}.$$

Beweis:

a.1) $\mathrm{SAT}_{2^{p*}} \leq_P \mathrm{SAT}_1$:
Die gesuchte Reduktionsfunktion ist gegeben durch

$$f((s(X_1,\ldots,X_n),\, t(X_1,\ldots,X_n))) := s(X_1,\ldots,X_n) \times t(X_1,\ldots,X_n).$$

Sie ist in linearer Zeit berechenbar und liefert das richtige Ergebnis, denn es gilt:

$$\begin{array}{l}
\exists [x_1],\ldots,[x_n] \in \mathbb{P}^2 : s([x_1],\ldots,[x_n]), t([x_1],\ldots,[x_n]) \text{ existieren,} \\
s([x_1],\ldots,[x_n]) \neq t([x_1],\ldots,[x_n]) \\
\qquad\qquad \Leftrightarrow \\
\exists [x_1],\ldots,[x_n] \in \mathbb{P}^2 : [s(x_1,\ldots,x_n)], [t(x_1,\ldots,x_n)] \text{ existieren,} \\
[s(x_1,\ldots,x_n)] \neq [t(x_1,\ldots,x_n)] \\
\qquad\qquad \Leftrightarrow \\
\exists x_1,\ldots,x_n \in \mathbb{R}^3\backslash\{0\} : s(x_1,\ldots,x_n) \neq 0 \neq t(x_1,\ldots,x_n), \\
s(x_1,\ldots,x_n) \neq \lambda t(x_1,\ldots,x_n) \quad \forall \lambda \in \mathbb{R}\backslash\{0\} \\
\qquad\qquad \Leftrightarrow \\
\exists x_1,\ldots,x_n \in \mathbb{R}^3\backslash\{0\} : s(x_1,\ldots,x_n) \times t(x_1,\ldots,x_n) \neq 0 \\
\qquad\qquad \Leftrightarrow \\
\exists x_1,\ldots,x_{n+1} \in \mathbb{R}^3\backslash\{0\} : s(x_1,\ldots,x_n) \times t(x_1,\ldots,x_n) = x_{n+1} \\
\qquad\qquad \Leftrightarrow \\
\exists x_1,\ldots,x_{n+1} \in \mathbb{R}^3\backslash\{0\}, \exists \mathscr{D} \text{ Drehung: } \mathscr{D}(s(x_1,\ldots,x_n) \times t(x_1,\ldots,x_n)) = \mathscr{D}(x_{n+1}) = e_3 \\
\qquad\qquad \Leftrightarrow \\
\exists x_1,\ldots,x_{n+1} \in \mathbb{R}^3\backslash\{0\}, \exists \mathscr{D} \text{ Drehung: } s(\mathscr{D}(x_1),\ldots,\mathscr{D}(x_n)) \times t(\mathscr{D}(x_1),\ldots,\mathscr{D}(x_n)) = e_3 \\
\qquad\qquad \Leftrightarrow \\
\exists x_1,\ldots,x_n \in \mathbb{R}^3\backslash\{0\} : s(x_1,\ldots,x_n) \times t(x_1,\ldots,x_n) = e_3.
\end{array}$$

a.2) $\mathrm{SAT}_1 \leq_P \mathrm{SAT}_{2^{p*}}$:
Sei

$$f(t(X_1,\ldots,X_n)) := \begin{cases} (u(X_1,\ldots,X_n),\, v(X_1,\ldots,X_n)), & \text{falls es zwei Kreuzprodukt-Terme } u(X_1,\ldots,X_n),\, v(X_1,\ldots,X_n) \text{ gibt, sodass } t(X_1,\ldots,X_n) = u(X_1,\ldots,X_n) \times v(X_1,\ldots,X_n) \\ (t(X_1,\ldots,X_n), X_{n+1}), & \text{falls } t(X_1,\ldots,X_n) \text{ nur aus einer Variablen besteht, } X_{n+1} \text{ neue Variable} \end{cases}$$

Da die Klammerung eines Kreuzprodukt-Terms eindeutig festlegt, in welcher Reihenfolge die Kreuzprodukte ausgeführt werden, kann eine Turingmaschine, indem sie den Term einmal liest und dabei die geöffneten und wieder geschlossenen Klammern mitzählt, feststellen, welches Kreuzprodukt zuletzt ausgeführt wird. Damit ist diese Funktion in polynomieller Zeit berechenbar.

Durch Rückwärtslesen des Beweises aus a.1) folgt, dass sie das richtige Ergebnis liefert.

b.1) $\mathrm{SAT}_1 \leq_P \mathrm{SAT}_{1^P}$:
Sei $f(t(X_1,\ldots,X_n)) := t(X_1,\ldots,X_n)$ die Identitätsfunktion. Diese ist trivialerweise in polynomieller Zeit berechenbar.

Ist $t(X_1,\ldots,X_n) \in \mathrm{SAT}_1$, so gibt es $x_1,\ldots,x_n \in \mathbb{R}^3\backslash\{0\}$, sodass $t(x_1,\ldots,x_n) = e_3$ gilt. Dann existieren $[x_1],\ldots,[x_n]$, und es gilt $t([x_1],\ldots,[x_n]) = [e_3]$. Insbesondere ist $t([x_1],\ldots,[x_n]) = [t(x_1,\ldots,x_n)] \in \mathbb{P}^2$. Insgesamt folgt $t(X_1,\ldots,X_n) \in \mathrm{SAT}_{1^P}$.

Sei nun $t(X_1,\ldots,X_n) \in \mathrm{SAT}_{1^P}$. Dann gibt es $[x_1],\ldots,[x_n] \in \mathbb{P}^2$, sodass $t([x_1],\ldots,[x_n]) = [e_3]$. Damit gilt $t(x_1,\ldots,x_n) = \lambda e_3$ für beliebige Repräsentanten $x_1 \in [x_1],\ldots,x_n \in [x_n]$ und ein zugehöriges $\lambda \in \mathbb{R}\backslash\{0\}$. Skaliert man diese $x_1,\ldots,x_n$ entsprechend, so erhält man $x_1',\ldots,x_n' \in \mathbb{R}^3\backslash\{0\}$ mit $t(x_1',\ldots,x_n') = e_3$. Also gilt $t(X_1,\ldots,X_n) \in \mathrm{SAT}_1$.

b.2) $\mathrm{SAT}_{1^P} \leq_P \mathrm{SAT}_1$:
Setzt man wieder $f(t(X_1,\ldots,X_n)) := t(X_1,\ldots,X_n)$, so folgt die Behauptung mit dem unveränderten Beweis aus b.1).

□

Um den Beweis des nachfolgenden Theorems übersichtlicher zu machen, wird die folgende Hilfsaussage benötigt:

Lemma 2.5 Sei $\{a_1,a_2,a_3\}$ eine Orthonormalbasis von $\mathbb{R}^3$ und $s \in \mathbb{R}^3\backslash\{0\}$. Dann gibt es Drehungen $\mathscr{D}_i$, sodass

$$a_i \times s = (\mathscr{D}_i \circ P_{jk})(s) \qquad \text{für alle } i \in \{1,2,3\} \text{ und } i \neq j \neq k \neq i,$$

wobei $P_{jk}(s)$ die orthogonale Projektion von s auf die a_j-a_k-Ebene ist.

Beweis: Sei $a_i \in \{a_1,a_2,a_3\}$, $\mathscr{D}$ eine Drehung mit $\mathscr{D}(a_i) = e_3$ und P_{12}' die orthogonale Projektion auf die e_1-e_2-Ebene. Dann gilt

$$\begin{aligned}
a_i \times s &= \mathscr{D}^{-1}\mathscr{D}(a_i \times s) \\
&\overset{1.7}{=} \mathscr{D}^{-1}(\mathscr{D}(a_i) \times \underbrace{\mathscr{D}(s)}_{=:s'}) \\
&= \mathscr{D}^{-1}(e_3 \times s') \\
&= \mathscr{D}^{-1}\begin{pmatrix} -s_2' \\ s_1' \\ 0 \end{pmatrix} \\
&= \mathscr{D}^{-1}\underbrace{\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{=:\widehat{\mathscr{D}}}\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}}_{=P_{12}'} s' \\
&= \mathscr{D}^{-1}\widehat{\mathscr{D}}P_{12}'\mathscr{D}(s) \\
&= \underbrace{\mathscr{D}^{-1}\widehat{\mathscr{D}}\mathscr{D}}_{=:\widetilde{\mathscr{D}}}\underbrace{\mathscr{D}^{-1}P_{12}'\mathscr{D}}_{=:\widetilde{P}}(s) \\
&= \widetilde{\mathscr{D}}\widetilde{P}(s),
\end{aligned}$$

wobei $\widetilde{\mathscr{D}}$ wieder eine Drehung und $\widetilde{P}$ die gewünschte orthogonale Projektion ist:
Wegen

$$\begin{aligned}(\mathscr{D}^{-1}P'_{12}\mathscr{D})^2 &= \mathscr{D}^{-1}P'_{12}\mathscr{D}\mathscr{D}^{-1}P'_{12}\mathscr{D}\\ &= \mathscr{D}^{-1}P'_{12}P'_{12}\mathscr{D}\\ &= \mathscr{D}^{-1}P'_{12}\mathscr{D}\end{aligned}$$

und

$$\begin{aligned}(\mathscr{D}^{-1}P'_{12}\mathscr{D})^T &= \mathscr{D}^T P'^T_{12}(\mathscr{D}^{-1})^T\\ &= \mathscr{D}^{-1}P'_{12}\mathscr{D}^{TT}\\ &= \mathscr{D}^{-1}P'_{12}\mathscr{D}\end{aligned}$$

ist $\widetilde{P}$ eine orthogonale Projektion. Weiter gilt

$$\widetilde{P}(a_i) = \mathscr{D}^{-1}P'_{12}\mathscr{D}(a_i) = \mathscr{D}^{-1}\underbrace{P'_{12}e_3}_{=0} = 0,$$

und mit

$$\{a_i\}^\perp = \{\mathscr{D}^{-1}\mathscr{D}\,a_i\}^\perp = \{\mathscr{D}^{-1}e_3\}^\perp = \mathscr{D}^{-1}\{e_3\}^\perp = \mathscr{D}^{-1}(span\{e_1,e_2\})$$

folgt für $c = \mathscr{D}^{-1}(d_1e_1 + d_2e_2) \in \{a\}^\perp$

$$\begin{aligned}\widetilde{P}c &= \mathscr{D}^{-1}P'_{12}\mathscr{D}\mathscr{D}^{-1}(d_1e_1 + d_2e_2)\\ &= \mathscr{D}^{-1}P'_{12}(d_1e_1 + d_2e_2)\\ &= \mathscr{D}^{-1}(d_1e_1 + d_2e_2)\\ &= c,\end{aligned}$$

sodass $\widetilde{P} = P_{jk}$ mit $i \neq j \neq k \neq i$ für $a_i \in \{a_1, a_2, a_3\}$ gilt. □

Wir sind nunmehr in der Lage, das folgende Resultat zu beweisen, welches erstmals einen Zusammenhang zwischen komplizierteren reellen und projektiven Erfüllbarkeitsproblemen herstellt.

Theorem 2.6 Es gilt:

$$\mathrm{SAT}_{2^p} \leq_P \mathrm{SAT}_3.$$

Beweis:
Die Reduktion basiert auf der Tatsache, dass die Auswertungen von zwei Kreuzprodukt-Termen genau dann linear abhängig (und ungleich null) sind, wenn es eine Orthonormalbasis $\{a_1, a_2, a_3\}$ von $\mathbb{R}^3$ sowie zu diesen Basisvektoren parallele Vektoren b_1, b_2, b_3 gibt, sodass

$$a_i \times s(x_1,\ldots,x_n) = b_i \times t(x_1,\ldots,x_n) \quad \text{für alle } i \in \{1,2,3\} \qquad (*)$$

gilt und alle diese Kreuzprodukte nicht 0 sind.

Die Existenz einer Orthonormalbasis kann durch die Kreuzproduktgleichungen

$$\exists\, a_1, a_2, a_3 \in \mathbb{R}^3\backslash\{0\}: \quad a_1 = a_2 \times a_3 \quad \wedge \quad a_2 = a_3 \times a_1 \quad \wedge \quad a_3 = a_1 \times a_2 \qquad (**)$$

ausgedrückt werden:
Es ist klar, dass für beliebige $i,j,k \in \{1,2,3\}$ mit $i \neq j \neq k \neq i$ a_i senkrecht auf a_j und a_k steht. Normiert man nun die 3 Gleichungen, erhält man

$$\begin{aligned}
\|a_1\| = \|a_2 \times a_3\| = \|a_2\| \cdot \|a_3\| - \|\langle a_2, a_3\rangle\| = \|a_2\| \cdot \|a_3\| \\
\|a_2\| = \|a_3 \times a_1\| = \|a_3\| \cdot \|a_1\| - \|\langle a_3, a_1\rangle\| = \|a_3\| \cdot \|a_1\| \\
\|a_3\| = \|a_1 \times a_2\| = \|a_1\| \cdot \|a_2\| - \|\langle a_1, a_2\rangle\| = \|a_1\| \cdot \|a_2\|
\end{aligned}$$

und es folgt

$$\|a_1\| = \|a_2\| = \|a_3\| = 1,$$

sodass die Vektoren a_1, a_2, a_3 eine Orthonormalbasis bilden.

Die Existenz der dazu parallelen Vektoren b_1, b_2, b_3 erhält man durch die Bedingungen

$$\begin{aligned}
\exists\, c_1,c_2,c_3,d_1,d_2,d_3 \in \mathbb{R}^3\backslash\{0\}: \quad & b_1 = c_1 \times a_2 \quad \wedge \quad b_1 = d_1 \times a_3 \\
\wedge \quad & b_2 = c_2 \times a_1 \quad \wedge \quad b_2 = d_2 \times a_3 \qquad (***) \\
\wedge \quad & b_3 = c_3 \times a_1 \quad \wedge \quad b_3 = d_3 \times a_2
\end{aligned}$$

Sie stellen sicher, dass b_i für jedes $i \in \{1,2,3\}$ und $i \neq j \neq k \neq i$ senkrecht auf a_j und a_k steht. Da $\{a_1, a_2, a_3\}$ eine Orthonormalbasis ist, stehen diese Vektoren paarweise senkrecht aufeinander, sodass $b_i \in \{a_j, a_k\}^\perp = span(a_i)$, und damit ist b_i parallel zu a_i.

Insgesamt ergibt sich folgende Reduktionsfunktion:

$$\begin{aligned}
f(s(X_1,\ldots,X_n),\, t(X_1,\ldots,X_n)) \quad := \quad & a_1 = a_2 \times a_3 \quad \wedge \quad a_2 = a_3 \times a_1 \quad \wedge \quad a_3 = a_1 \times a_2 \\
\wedge \quad & b_1 = c_1 \times a_2 \quad \wedge \quad b_1 = d_1 \times a_3 \quad \wedge \quad b_2 = c_2 \times a_1 \\
\wedge \quad & b_2 = d_2 \times a_3 \quad \wedge \quad b_3 = c_3 \times a_1 \quad \wedge \quad b_3 = d_3 \times a_2 \\
\wedge \quad & a_1 \times s(X_1,\ldots,X_n) = b_1 \times t(X_1,\ldots,X_n) \neq 0 \\
\wedge \quad & a_2 \times s(X_1,\ldots,X_n) = b_2 \times t(X_1,\ldots,X_n) \neq 0 \\
\wedge \quad & a_3 \times s(X_1,\ldots,X_n) = b_3 \times t(X_1,\ldots,X_n) \neq 0
\end{aligned}$$

Die Berechnung dieser Funktion ist in polynomieller Zeit möglich (wobei die Turingmaschine eigentlich $X_{n+1},\ldots,X_{n+9}$ anstelle der a_i, b_i und c_i verwendet, diese werden hier nur zur besseren Lesbarkeit des Beweises beibehalten), und es bleibt nur die Äquivalenz zu zeigen:

Sei also $(s(X_1,\ldots,X_n),\, t(X_1,\ldots,X_n)) \in \mathrm{SAT}_{2^P}$. Dann gibt es $[x_1],\ldots,[x_n] \in \mathbb{P}^2$, sodass $[s(x_1,\ldots,x_n)] = [t(x_1,\ldots,x_n)]$, d.h. es gibt $x_1,\ldots,x_n \in \mathbb{R}^3\backslash\{0\}$ und ein $\lambda \in \mathbb{R}\backslash\{0\}$, sodass $s(x_1,\ldots,x_n) = \lambda t(x_1,\ldots,x_n)$ gilt.
Sei $\{a_1, a_2, a_3\}$ eine beliebige Orthonormalbasis des $\mathbb{R}^3$, für die weder a_1 noch a_2 noch a_3 parallel zu $s(x_1,\ldots,x_n)$ ist, damit alle Kreuzprodukte in $(*)$ ungleich 0 sind, und sei $b_1 := \lambda a_1$, $b_2 := \lambda a_2$ sowie $b_3 := \lambda a_3$. Setzt man $c_1 := -\lambda a_3$, $d_1 := \lambda a_2$, $c_2 := \lambda a_3$, $d_2 := -\lambda a_1$, $c_3 := -\lambda a_2$, $d_3 := \lambda a_1$, so sind $(*), (**)$ und $(***)$ erfüllt und es folgt $f(s(X_1,\ldots,X_n),\, t(X_1,\ldots,X_n)) \in \mathrm{SAT}_3$.

Sei nun $f(s(X_1,\ldots,X_n),\, t(X_1,\ldots,X_n)) \in \mathrm{SAT}_3$. Dann gibt es (wegen $(**)$) eine Orthonormalbasis $\{a_1, a_2, a_3\}$ und (wegen $(***)$) dazu parallele $b_1, b_2, b_3 \in \mathbb{R}^3\backslash\{0\}$, sodass

$$a_i \times s(x_1,\ldots,x_n) = b_i \times t(x_1,\ldots,x_n) = \lambda_i a_i \times t(x_1,\ldots,x_n) = a_i \times \lambda_i t(x_1,\ldots,x_n) \quad \forall i \in \{1,2,3\}$$

mit $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}\backslash\{0\}$ gilt. Nach Lemma 2.5 gibt es dann Drehungen $\mathscr{D}_i$, sodass dies äquivalent ist zu

$$\mathscr{D}_i P_{jk}(s(x_1,\ldots,x_n)) = \mathscr{D}_i P_{jk}(\lambda_i t(x_1,\ldots,x_n)) \qquad \forall i \in \{1,2,3\},\ i \neq j \neq k \neq i$$

mit P_{jk} wie im Lemma. Durch Multiplikation der Gleichungen mit dem jeweiligen $\mathscr{D}_i^{-1}$ erhält man

$$P_{jk}(s(x_1,\ldots,x_n)) = P_{jk}\lambda_i(t(x_1,\ldots,x_n)) \qquad \forall i \in \{1,2,3\},\ i \neq j \neq k \neq i.$$

Seien nun $s^i(x_1,\ldots,x_n)$, $t^i(x_1,\ldots,x_n)$ für $i = 1,2,3$ die Koordinaten von $s(x_1,\ldots,x_n)$ bzw. $t(x_1,\ldots,x_n)$ bezüglich der Basis $\{a_1,a_2,a_3\}$. Dann kann man die obigen Gleichungen schreiben als

$$\begin{aligned}
s^1(x_1,\ldots,x_n)a_1 + s^2(x_1,\ldots,x_n)a_2 &= \lambda_3(t^1(x_1,\ldots,x_n)a_1 + t^2(x_1,\ldots,x_n)a_2),\\
s^1(x_1,\ldots,x_n)a_1 + s^3(x_1,\ldots,x_n)a_3 &= \lambda_2(t^1(x_1,\ldots,x_n)a_1 + t^3(x_1,\ldots,x_n)a_3), \qquad (\dagger)\\
s^2(x_1,\ldots,x_n)a_2 + s^3(x_1,\ldots,x_n)a_3 &= \lambda_1(t^2(x_1,\ldots,x_n)a_2 + t^3(x_1,\ldots,x_n)a_3).
\end{aligned}$$

Durch Bilden der Skalarprodukte mit a_1, a_2 und a_3 folgt

$$\begin{aligned}
s^1(x_1,\ldots,x_n) &= \lambda_3 t^1(x_1,\ldots,x_n), & s^2(x_1,\ldots,x_n) &= \lambda_3 t^2(x_1,\ldots,x_n),\\
s^1(x_1,\ldots,x_n) &= \lambda_2 t^1(x_1,\ldots,x_n), & s^3(x_1,\ldots,x_n) &= \lambda_2 t^3(x_1,\ldots,x_n),\\
s^2(x_1,\ldots,x_n) &= \lambda_1 t^2(x_1,\ldots,x_n), & s^3(x_1,\ldots,x_n) &= \lambda_1 t^3(x_1,\ldots,x_n),
\end{aligned}$$

und damit

$$t^1(x_1,\ldots,x_n)\cdot(\lambda_3-\lambda_2) = 0, \qquad t^2(x_1,\ldots,x_n)\cdot(\lambda_3-\lambda_1) = 0, \qquad t^3(x_1,\ldots,x_n)\cdot(\lambda_1-\lambda_2) = 0.$$

Nun ist höchstens eines der $t^i(x_1,\ldots,x_n)$ gleich 0:
Angenommen, es wäre $t^i(x_1,\ldots,x_n) = t^j(x_1,\ldots,x_n) = 0$ und $i \neq j$. Dann würde

$$0 = t^i(x_1,\ldots,x_n)a_i + t^j(x_1,\ldots,x_n)a_j = P_{ij}t(x_1,\ldots,x_n)$$

und mit $\mathscr{D}_k$, $i \neq k \neq j$, aus Lemma 2.5

$$0 = \mathscr{D}_k P_{ij} t(x_1,\ldots,x_n) = a_k \times t(x_1,\ldots,x_n) = \lambda_k a_k \times t(x_1,\ldots,x_n) = b_k \times t(x_1,\ldots,x_n)$$

folgen, im Widerspruch zur Annahme.
Also sind mindestens zwei der drei Gleichungen nichttrivial und es gilt $\lambda_1 = \lambda_2 = \lambda_3 =: \lambda$. Setzt man dies in die Gleichungen (†) ein und addiert diese, erhält man

$$2 \cdot s(x_1,\ldots,x_n) = 2 \cdot \lambda \cdot t(x_1,\ldots,x_n),$$

also

$$[s(x_1,\ldots,x_n)] = [t(x_1,\ldots,x_n)],$$

und damit $(s(X_1,\ldots,X_n),\ t(X_1,\ldots,X_n)) \in SAT_{2^p}$.

□

Auf analoge Weise erhält man nun die folgenden weiteren Reduktionen zwischen abermals komplizierteren Erfüllbarkeitsproblemen.

Theorem 2.7 Es gilt:

$$\mathrm{SAT}_{3^p} \leq_P \mathrm{SAT}_3 \quad \text{und} \quad \mathrm{SAT}_{4^p} \leq_P \mathrm{SAT}_4.$$

Beweis: a) Für $(s_1(X_1,\ldots,X_n),\, t_1(X_1,\ldots,X_n),\ldots,s_m(X_1,\ldots,X_n),\, t_m(X_1,\ldots,X_n)) \in \mathrm{SAT}_{3^p}$ definiert man die Reduktionsfunktion folgendermaßen:

$$\begin{aligned}
&f(s_1(X_1,\ldots,X_n),\, t_1(X_1,\ldots,X_n),\ldots,s_m(X_1,\ldots,X_n),\, t_m(X_1,\ldots,X_n)) := \\
&\qquad a_1 = a_2 \times a_3 \quad \wedge \quad a_2 = a_3 \times a_1 \quad \wedge \quad a_3 = a_1 \times a_2 \\
&\wedge \quad b_1^1 = c_1^1 \times a_2 \quad \wedge \quad b_1^1 = d_1^1 \times a_3 \quad \wedge \quad b_2^1 = c_2^1 \times a_1 \\
&\wedge \quad b_2^1 = d_2^1 \times a_3 \quad \wedge \quad b_3^1 = c_3^1 \times a_1 \quad \wedge \quad b_3^1 = d_3^1 \times a_2 \\
&\qquad\qquad\qquad \vdots \\
&\wedge \quad b_1^m = c_1^m \times a_2 \quad \wedge \quad b_1^m = d_1^m \times a_3 \quad \wedge \quad b_2^m = c_2^m \times a_1 \\
&\wedge \quad b_2^m = d_2^m \times a_3 \quad \wedge \quad b_3^m = c_3^m \times a_1 \quad \wedge \quad b_3^m = d_3^m \times a_2 \\
&\wedge \quad a_1 \times s_1(x_1,\ldots,x_n) = b_1^1 \times t_1(x_1,\ldots,x_n) \neq 0 \\
&\wedge \quad a_2 \times s_1(x_1,\ldots,x_n) = b_2^1 \times t_1(x_1,\ldots,x_n) \neq 0 \\
&\wedge \quad a_3 \times s_1(x_1,\ldots,x_n) = b_3^1 \times t_1(x_1,\ldots,x_n) \neq 0 \\
&\qquad\qquad\qquad \vdots \\
&\wedge \quad a_1 \times s_m(x_1,\ldots,x_n) = b_1^m \times t_m(x_1,\ldots,x_n) \neq 0 \\
&\wedge \quad a_2 \times s_m(x_1,\ldots,x_n) = b_2^m \times t_m(x_1,\ldots,x_n) \neq 0 \\
&\wedge \quad a_3 \times s_m(x_1,\ldots,x_n) = b_3^m \times t_m(x_1,\ldots,x_n) \neq 0
\end{aligned}$$

Gilt nun $(s_1(X_1,\ldots,X_n),\, t_1(X_1,\ldots,X_n),\ldots,s_m(X_1,\ldots,X_n),\, t_m(X_1,\ldots,X_n)) \in \mathrm{SAT}_{3^p}$, so gibt es (analog zum Beweis von Theorem 2.6) $x_1,\ldots,x_n \in \mathbb{R}^3$ und $\lambda^1,\ldots,\lambda^m \in \mathbb{R}\backslash\{0\}$, sodass

$$s_i(x_1,\ldots,x_n) = \lambda^i t_i(x_1,\ldots,x_n) \qquad \forall i \in \{1,\ldots,m\}.$$

Wählt man nun eine beliebige Orthonormalbasis $\{a_1,a_2,a_3\}$ des $\mathbb{R}^3$, für die keiner der Basisvektoren parallel zu einem der $s_1(X_1,\ldots,X_n),\ldots,s_m(X_1,\ldots,X_n)$ ist (da $m \in \mathbb{N}$ endlich ist, aber überabzählbar viele Orthonormalbasen existieren, gibt es eine solche Orthonormalbasis immer), und definiert

$$\begin{aligned}
&b_1^i := \lambda^i a_1, \quad && b_2^i := \lambda^i a_2, \quad && b_3^i := \lambda^i a_3, \\
&c_1^i := -\lambda^i a_3, \quad && c_2^i := \lambda^i a_3, \quad && c_3^i := -\lambda^i a_2, \\
&d_1^i := \lambda^i a_2, \quad && d_2^i := -\lambda^i a_1, \quad && d_3^i := \lambda^i a_1 \qquad (\text{für } i \in \{1,\ldots,m\}),
\end{aligned}$$

so folgt $f((s_1(X_1,\ldots,X_n),\, t_1(X_1,\ldots,X_n),\ldots,s_m(X_1,\ldots,X_n),\, t_m(X_1,\ldots,X_n))) \in \mathrm{SAT}_3$.

Der Beweis von

$$\begin{gathered}
f((s_1(X_1,\ldots,X_n),\, t_1(X_1,\ldots,X_n),\ldots,s_m(X_1,\ldots,X_n),\, t_m(X_1,\ldots,X_n)) \in \mathrm{SAT}_3 \\
\Downarrow \\
(s_1(X_1,\ldots,X_n),\, t_1(X_1,\ldots,X_n),\ldots,s_m(X_1,\ldots,X_n),\, t_m(X_1,\ldots,X_n)) \in \mathrm{SAT}_{3^p}
\end{gathered}$$

erfolgt analog zu dem entsprechenden Teil des Beweises von Theorem 2.6, der nun für jeden „Satz von Variablen“ b_1^i, b_2^i, b_3^i, c_1^i, c_2^i, c_3^i, d_1^i, d_2^i, d_3^i, λ_1^i, λ_2^i, λ_3^i mit $i \in \{1,\ldots,m\}$ geführt werden muss.

b) Für $(s_1(X_1,\ldots,X_n),\, t_1(X_1,\ldots,X_n)\square\ldots\square s_m(X_1,\ldots,X_n),\, t_m(X_1,\ldots,X_n)) \in \mathrm{SAT}_{4^P}$ passt man die Reduktionsfunktion folgendermaßen an:

$$
\begin{aligned}
&f((s_1(X_1,\ldots,X_n),\, t_1(X_1,\ldots,X_n)\square\ldots\square s_m(X_1,\ldots,X_n),\, t_m(X_1,\ldots,X_n)) := \\
&\qquad\qquad (a_1 = a_2 \times a_3 \quad\wedge\quad a_2 = a_3 \times a_1 \quad\wedge\quad a_3 = a_1 \times a_2) \\
&\wedge \quad [\quad (\, b_1^1 = c_1^1 \times a_2 \quad\wedge\quad b_1^1 = d_1^1 \times a_3 \quad\wedge\quad b_2^1 = c_2^1 \times a_1 \\
&\qquad\qquad \wedge \quad b_2^1 = d_2^1 \times a_3 \quad\wedge\quad b_3^1 = c_3^1 \times a_1 \quad\wedge\quad b_3^1 = d_3^1 \times a_2) \\
&\qquad \square \\
&\qquad\qquad\qquad\qquad \vdots \\
&\qquad \square \\
&\qquad\qquad (\, b_1^m = c_1^m \times a_2 \quad\wedge\quad b_1^m = d_1^m \times a_3 \quad\wedge\quad b_2^m = c_2^m \times a_1 \\
&\qquad\qquad \wedge \quad b_2^m = d_2^m \times a_3 \quad\wedge\quad b_3^m = c_3^m \times a_1 \quad\wedge\quad b_3^m = d_3^m \times a_2\,) \quad] \\
&\wedge \quad [\quad (a_1 \times s_1(x_1,\ldots,x_n) = b_1^1 \times t_1(x_1,\ldots,x_n) \neq 0 \\
&\qquad\qquad \wedge \quad a_2 \times s_1(x_1,\ldots,x_n) = b_2^1 \times t_1(x_1,\ldots,x_n) \neq 0 \\
&\qquad\qquad \wedge \quad a_3 \times s_1(x_1,\ldots,x_n) = b_3^1 \times t_1(x_1,\ldots,x_n) \neq 0\,) \\
&\qquad \square \\
&\qquad\qquad\qquad\qquad \vdots \\
&\qquad \square \\
&\qquad\qquad (\, a_1 \times s_m(x_1,\ldots,x_n) = b_1^m \times t_m(x_1,\ldots,x_n) \neq 0 \\
&\qquad\qquad \wedge \quad a_2 \times s_m(x_1,\ldots,x_n) = b_2^m \times t_m(x_1,\ldots,x_n) \neq 0 \\
&\qquad\qquad \wedge \quad a_3 \times s_m(x_1,\ldots,x_n) = b_3^m \times t_m(x_1,\ldots,x_n) \neq 0\,) \quad]
\end{aligned}
$$

wobei $\square \in \{\vee, \wedge\}$ mit der jeweiligen logischen Verknüpfung übereinstimmt, die durch den Index festgelegt wird, und die Klammerung entsprechend unverändert bleibt.

Dass diese Reduktionsfunktion das richtige Ergebnis liefert, zeigt man analog zum Beweis von Theorem 2.6 bzw. analog zu dem obigen Teil des Beweises von $\mathrm{SAT}_{3^P} \leq_P \mathrm{SAT}_3$, da nur an den entsprechenden Stellen die logische Verknüpfung $\wedge$ durch $\vee$ bzw. im Fliesstext „und“ durch „oder“ ersetzt und die entsprechende Klammerung mitgeführt werden muss. □

Theorem 2.8 Es gilt:

$$\mathrm{SAT}_{5^P} \leq_P \mathrm{SAT}_4.$$

Beweis: Einen direkten Beweis kann man (nach leichten Änderungen) durch Kombination der Ideen für die Reduktionsfunktionen aus den Beweisen der Theoreme 2.7 ($\mathrm{SAT}_{4^P} \leq_P \mathrm{SAT}_4$) und 2.4 ($\mathrm{SAT}_{2^{P*}} \leq_P \mathrm{SAT}_1$) sowie der Proposition 2.2 ($\mathrm{SAT}_1 \leq_P \mathrm{SAT}_2$) erhalten. Die Aussage folgt aber auch (wegen der Transitivität der Reduktionen) aus $\mathrm{SAT}_{4^P} \leq_P \mathrm{SAT}_4$ (Theorem 2.7) und dem folgenden Theorem 2.9: □

Theorem 2.9 Es gilt:

$$\mathrm{SAT}_{5^P} \leq_P \mathrm{SAT}_{4^P}.$$

Beweis: Die folgende Reduktion besteht aus einer Kombination der Ideen für die Reduktionen von SAT_{4^P} auf SAT_{5^P}, $\mathrm{SAT}_{2^{P*}}$ auf SAT_1, SAT_1 auf SAT_{1^P} und SAT_{1^P} auf SAT_{2^P}.

Sei

$$f(t_1(X_1,\dots,X_n)\diamond s_1(X_1,\dots,X_n)\square\dots\square t_m(X_1,\dots,X_n)\diamond s_m(X_1,\dots,X_n)) \\ := T_1(X_1,\dots,X_{n+m})\square\dots\square T_m(X_1,\dots,X_{n+m})$$

wobei wie bisher $\square \in \{\vee,\wedge\}$ und $\diamond \in \{=,\neq\}$ gilt, die Priorität der logischen Verknüpfungen durch Klammerung eindeutig festgelegt ist und von der Reduktionsfunktion unverändert bleibt, und $T_j(X_1,\dots,X_{n+m})$ folgendermaßen definiert wird:

$$T_j(X_1,\dots,X_{n+m}) := \begin{cases} t_j(X_1,\dots,X_n) = s_j(X_1,\dots,X_n), & \text{falls } \diamond \text{ in } t_j(X_1,\dots,X_n)\diamond s_j(X_1,\dots,X_n) \text{ dem Gleichheitszeichen entspricht} \\ t_j(X_1,\dots,X_n) \times s_j(X_1,\dots,X_n) = X_{n+j}, & \text{sonst} \end{cases}$$

Da die Turingmaschine hierfür nur den Code jedes $\neq$-Zeichens durch den Code des Kreuzproduktzeichens ersetzen, vor der nächsten logischen Verknüpfung den Code eines Gleichheitszeichens und der neuen Variable einfügen und sonst alles unverändert auf das Ausgabeband abschreiben muss, ist diese Reduktionsfunktion in polynomieller Zeit berechenbar.

Sei $f(t_1(X_1,\dots,X_n)\diamond s_1(X_1,\dots,X_n)\square\dots\square t_m(X_1,\dots,X_n)\diamond s_m(X_1,\dots,X_n)) \in \mathrm{SAT}_{4^p}$. Dann gibt es $[x_1],\dots,[x_{n+m}] \in \mathbb{P}^2$, sodass $T_1([x_1],\dots,[x_{n+m}])\square\dots\square T_m([x_1],\dots,[x_{n+m}])$ mit entsprechender Klammerung erfüllt (und die Bedingung der Existenz der Auswertungen der Kreuzprodukt-Terme nicht verletzt) wird. Damit gibt es also eine (von $[x_1],\dots,[x_{n+m}]$ sowie der Klammerung und den logischen Verknüpfungen $\wedge$ und $\vee$ abhängige) Teilmenge $M \subseteq \{1,\dots,m\}$, sodass $[x_1],\dots,[x_{n+m}]$ für alle $T_j(X_1,\dots,X_{n+m})$ mit $j \in M$ eine erfüllende Belegung ist und die Auswertungen der Kreuzprodukt-Terme existieren.
Da die Reduktionsfunktion an der Klammerung und den logischen Verknüpfungen nichts verändert hat, genügt es, eine erfüllende Belegung für alle Gleichungen und Ungleichungen[1] $t_j(X_1,\dots,X_n)\diamond s_j(X_1,\dots,X_n)$ mit $j \in M$ zu finden.
Diese ist durch $[x_1],\dots,[x_n]$ gegeben: Im Fall, dass $\diamond$ dem Gleichheitszeichen entsprach, hat die Reduktionsfunktion nichts verändert, sodass die Bedingungen trivialerweise erfüllt bleiben. Anderenfalls existiert $t_j([x_1],\dots,[x_n]) \times s_j([x_1],\dots,[x_n])$ nach Vorraussetzung. Damit existieren insbesondere auch $t_j([x_1],\dots,[x_n])$ und $s_j([x_1],\dots,[x_n])$, und es gilt $t_j([x_1],\dots,[x_n]) \neq s_j([x_1],\dots,[x_n])$. Also gibt es $[x_1],\dots,[x_n] \in \mathbb{P}^2$, sodass $t_j(X_1,\dots,X_n)\diamond s_j(X_1,\dots,X_n)$ für alle $j \in M$ gilt und die Existenzbedingungen erfüllt werden, und es folgt $t_1(X_1,\dots,X_n)\diamond s_1(X_1,\dots,X_n)\square\dots\square t_m(X_1,\dots,X_n)\diamond s_m(X_1,\dots,X_n) \in \mathrm{SAT}_{5^p}$.

Sei $t_1(X_1,\dots,X_n)\diamond s_1(X_1,\dots,X_n)\square\dots\square t_m(X_1,\dots,X_n)\diamond s_m(X_1,\dots,X_n) \in \mathrm{SAT}_{5^p}$. Dann gibt es $[x_1],\dots,[x_n] \in \mathbb{P}^2$, sodass eine von der Belegung der Variablen sowie der Klammerung und den logischen Verknüpfungen festgelegte Teilmenge N der Gleichungen und Ungleichungen gelten und die entsprechenden Existenzbedingungen erfüllt werden. Sei M definiert als die Menge der Indizes, für welche die zugehörige Gleichung bzw. Ungleichung in N enthalten ist. Wie oben genügt es wieder, eine Belegung $[x_1],\dots,[x_{n+m}] \in \mathbb{P}^2$ zu finden, sodass für alle $j \in M$ die Gleichungen $T_j([x_1],\dots,[x_{n+m}])$ gelten und die Existenzbedingungen erfüllt sind.
Sei $t_j(X_1,\dots,X_n)\diamond s_j(X_1,\dots,X_n)$ für ein beliebiges $j \in M$ so, dass $\diamond$ dem Gleichheitszeichen entspricht. Dann ändert die Reduktionsfunktion nichts, und $[x_1],\dots,[x_n] \in \mathbb{P}^2$ wie oben erfüllen alle geforderten Bedingungen. Da diese Gleichungen von $[x_{n+1}],\dots,[x_{n+m}]$ unabhängig sind, können diese von den

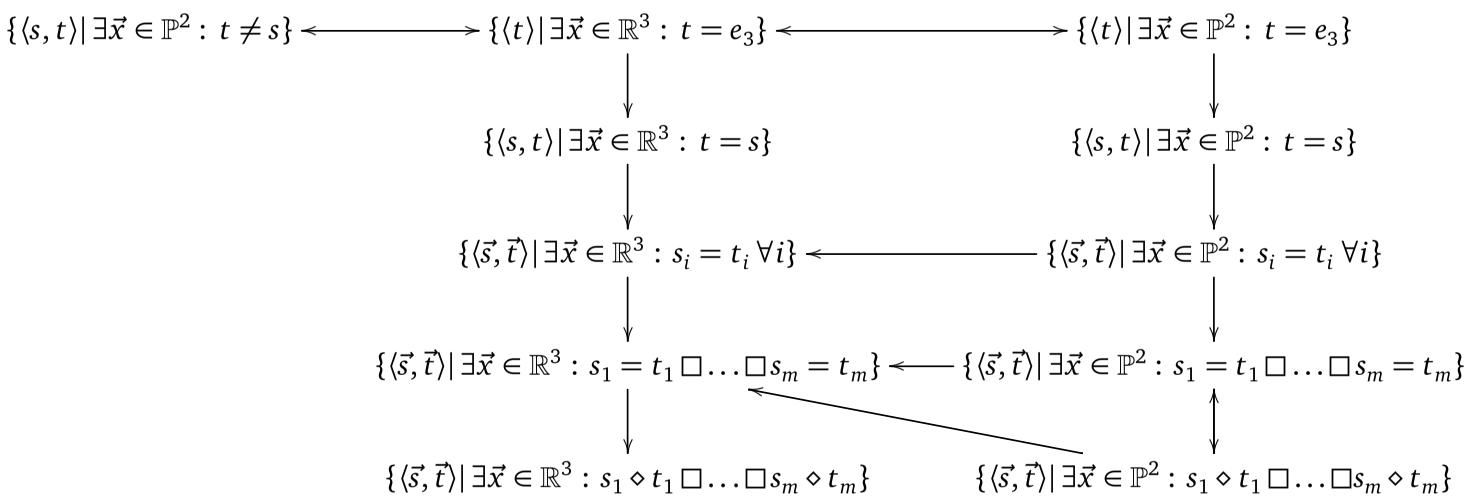
[1] Mit "Ungleichung" ist in der gesamten Arbeit $\neq$ gemeint, nicht, wie normalerweise üblich, $\leq$

entsprechenden Ungleichungen festgelegt werden, ohne dass dies die Erfüllbarkeit der Gleichungen beeinflusst.
Sei nun $t_j(X_1,\dots,X_n) \diamond s_j(X_1,\dots,X_n)$ für ein beliebiges $j \in M$ so, dass $\diamond$ dem Ungleichheitszeichen entspricht. Nach Voraussetzung gibt es $[x_1],\dots,[x_n] \in \mathbb{P}^2$, sodass $t_j([x_1],\dots,[x_n])$ und $s_j([x_1],\dots,[x_n])$ existieren, und $t_j([x_1],\dots,[x_n]) \neq s_j([x_1],\dots,[x_n])$ gilt. (Hierbei sind die $[x_1],\dots,[x_n]$ die gleichen Elemente in $\mathbb{P}^2$ wie oben, sodass dadurch die Gültigkeit der Gleichungen (d.h. $\diamond$ entspricht dem Gleichheitszeichen) mit $j \in M$ nicht beeinflusst wird.) Damit folgt, dass $t_j([x_1],\dots,[x_n]) \times s_j([x_1],\dots,[x_n])$ existiert, und es gibt ein $[x_{n+j}]$, sodass $t_j([x_1],\dots,[x_n]) \times s_j([x_1],\dots,[x_n]) = [x_{n+j}]$ gilt.
Für diejenigen j, welche nicht in M enthalten sind, oder solche, die in M liegen und die Gleichheit zweier Kreuzprodukt-Terme fordern, kann $[x_{n+j}] \in \mathbb{P}^2$ beliebig gewählt werden, da die Variablen X_{n+j} für diese j keinen Einfluss auf den Wahrheitswert der Auswertung von $T_1(X_1,\dots,X_{n+m}) \square \dots \square T_m(X_1,\dots,X_{n+m})$ (mit entsprechender Klammerung) haben.
Also folgt $f(t_1(X_1,\dots,X_n) \diamond s_1(X_1,\dots,X_n) \square \dots \square t_m(X_1,\dots,X_n) \diamond s_m(X_1,\dots,X_n)) \in \mathrm{SAT}_{4^p}$. □

2.4 Übersicht über die bisherigen Reduktionen

Zusammengefasst ergibt sich das nachfolgende Schaubild, in dem zur Verbesserung der Übersichtlichkeit t bzw. s statt $t(X_1,\dots,X_n)$ oder $t(x_1,\dots,x_n)$ bzw. $s(X_1,\dots,X_n)$ oder $s(x_1,\dots,x_n)$ geschrieben wird. Weiterhin wird $s_1,\dots,s_m$ und $t_1,\dots,t_m$ und auch deren entsprechende Klammerung und Kombination mit logischen $\vee$ und $\wedge$ durch $\vec{s},\vec{t}$ ersetzt. Die Symbole $\vec{t},\vec{s},t,s,t_i,s_i$ stehen immer für Kreuzprodukt-Terme, und $\vec{x}$ steht für $x_1,\dots,x_n$ aus $\mathbb{R}^3$ oder $[x_1],\dots,[x_n]$ aus $\mathbb{P}^2$. Die Bedingung, dass die Auswertung der Kreuzprodukt-Terme nicht null sein darf bzw. existieren muss, wird nicht ausdrücklich erwähnt. Pfeile zwischen den Erfüllbarkeitsproblemen stehen für eine gefundene Reduktionsfunktion. Befinden sich Probleme auf gleicher Höhe, sind aber nicht durch Pfeile miteinander verbunden, bedeutet dies nicht, dass sie polynomialzeitäquivalent sein müssen, hier ist noch unklar, in welcher Relation diese Erfüllbarkeitsprobleme zueinander stehen.

Bemerkung 2.10 Abweichend zu dem hier betrachteteten Fall des $\mathbb{R}^3$ mit Standardskalarprodukt und kanonischer positiv orientierter Orthonormalbasis kann man Kreuzprodukte auch über allgemeinen dreidimensionalen orientierten euklidischen Vektorräumen definieren. Dadurch gibt es zwei verschiedene Definitionen des Kreuzproduktes, die sich allerdings nur durch das Vorzeichen unterscheiden. Die obigen Ergebnisse lassen sich auf diesen allgemeinen Fall übertragen, dies soll jedoch hier nicht weiter betrachtet werden, unter anderem, da im projektiven Fall ohnehin keine Orientierung existiert, und es für die Reduktionen unerheblich ist, welches der beiden Kreuzprodukte vorliegt.


$\{\langle s,t\rangle \mid \exists \vec{x} \in \mathbb{P}^2 : t \neq s\}$
$\{\langle t\rangle \mid \exists \vec{x} \in \mathbb{R}^3 : t = e_3\}$
$\{\langle t\rangle \mid \exists \vec{x} \in \mathbb{P}^2 : t = e_3\}$
$\{\langle s,t\rangle \mid \exists \vec{x} \in \mathbb{R}^3 : t = s\}$
$\{\langle s,t\rangle \mid \exists \vec{x} \in \mathbb{P}^2 : t = s\}$
$\{\langle \vec{s},\vec{t}\rangle \mid \exists \vec{x} \in \mathbb{R}^3 : s_i = t_i\ \forall i\}$
$\{\langle \vec{s},\vec{t}\rangle \mid \exists \vec{x} \in \mathbb{P}^2 : s_i = t_i\ \forall i\}$
$\{\langle \vec{s},\vec{t}\rangle \mid \exists \vec{x} \in \mathbb{R}^3 : s_1 = t_1 \square \ldots \square s_m = t_m\}$
$\{\langle \vec{s},\vec{t}\rangle \mid \exists \vec{x} \in \mathbb{P}^2 : s_1 = t_1 \square \ldots \square s_m = t_m\}$
$\{\langle \vec{s},\vec{t}\rangle \mid \exists \vec{x} \in \mathbb{R}^3 : s_1 \diamond t_1 \square \ldots \square s_m \diamond t_m\}$
$\{\langle \vec{s},\vec{t}\rangle \mid \exists \vec{x} \in \mathbb{P}^2 : s_1 \diamond t_1 \square \ldots \square s_m \diamond t_m\}$

3 Einordnung der Erfüllbarkeitsprobleme in Komplexitätsklassen

Nachdem im vorherigen Kapitel die Beziehungen zwischen den verschiedenen Erfüllbarkeitsproblemen von Kreuzprodukt-Termen betrachtet wurden, stellt sich nun die Frage, in welcher Komplexitätsklasse sich diese Probleme befinden. Dazu werden zunächst das BSS-Modell und die Definition einiger Komplexitätsklassen wiederholt, siehe [1] und [2].

3.1 Einordnung der reellwertigen Erfüllbarkeitsprobleme

Eine BSS-Maschine, die über einem Ring R rechnet, erhält als Eingabe ein Tupel $x \in R^n$. Sie kann in jedem Schritt eine Addition, Subtraktion, Multiplikation oder, im Falle eines Körpers, Division durchführen, wobei sie exakt rechnet. Alternativ kann sie einen Test auf Gleichheit oder Ungleichheit durchführen, oder im Fall eines geordneten Rings $\leq, \geq, >$ oder $<$ testen, und in Abhängigkeit des Ergebnisses des Tests weitere Berechnungen durchführen. Zusätzlich zu ihrer Eingabe hat die BSS-Maschine Zugriff auf endlich viele weitere Konstanten $c \in R$, falls die entsprechende Komplexitätsklasse dies nicht ausschließt. Wie üblich wird die benötigte Zeit in der Länge der Eingabe gemessen, welche, anders als bei einer Turingmaschine, nicht von der Größe der eingegebenen Zahlen abhängt, sondern für gegebenes $x \in R^n$ als n definiert wird.

Definition 3.1. *Für ein Entscheidungsproblem $\mathscr{L}$ gilt*

$$\begin{aligned}
\mathscr{L} \in \mathscr{P}_{\mathbb{R}}^0 \quad &:\Leftrightarrow \quad \mathscr{L} \text{ ist von einer BSS-Maschine, die über } \mathbb{R} \text{ rechnet, aber keine Konstanten} \\
&\qquad \text{zur Verfügung hat, in polynomieller Zeit entscheidbar} \\
&\textit{sowie} \\
\mathscr{L} \in \mathscr{NP}_{\mathbb{R}}^0 \quad &:\Leftrightarrow \quad \mathscr{L} = \{x \in \mathbb{R}^* : \exists z \in \mathbb{R}^{p(|x|)} : \langle x, z\rangle \in \mathscr{L}'\} \\
&\qquad \text{für ein } \mathscr{L}' \in \mathscr{P}_{\mathbb{R}}^0. \\
&\textit{und} \\
BP\left(\mathscr{NP}_{\mathbb{R}}^0\right) \quad &:= \quad \{\mathscr{L} | \mathscr{L} \subseteq \{0,1\}^*, \mathscr{L} \in \mathscr{NP}_{\mathbb{R}}^0\}.
\end{aligned}$$

Das folgende Entscheidungsproblem wird später von Nutzen sein:

Definition 3.2. *Sei $R \supseteq \mathbb{Z}$ ein kommutativer Ring. Dann ist $FEAS_{R,R}$ definiert als*

$$\begin{aligned}
FEAS_{R,R} := \{\langle p_1, \ldots, p_k\rangle \quad | \quad & p_1, \ldots, p_k \in R[X_1, \ldots, X_n], \\
& \exists x_1, \ldots, x_n \in R : p_1(x_1, \ldots, x_n) = \ldots = p_k(x_1, \ldots, x_n) = 0\}.
\end{aligned}$$

Allgemeiner kann man $FEAS_{R_1,R_2}$ definieren. Hierbei ist R_1 der Ring, aus dem die Koeffizienten der Polynome stammen, und in R_2 wird nach einer gemeinsamen Nullstelle der Polynome gesucht.

Bemerkung 3.3 Es gilt $FEAS_{R,R} \in \mathscr{NP}_R$, d.h. eine nichtdeterministische BSS-Maschine über R kann dieses Problem entscheiden: Bei gegebenen Polynomen rät sie eine gemeinsame Nullstelle und prüft durch Einsetzen, exaktes Rechnen über R und Vergleichen mit 0, ob es sich tatsächlich um eine Nullstelle aller Polynome handelt.
Weiter gilt, dass $FEAS_{R,R}$ $\mathscr{NP}_R$-vollständig und $FEAS_{\mathbb{Z},R}$ $BP\left(\mathscr{NP}_R\right)$-vollständig ist.

Mit der obigen Definition lassen sich die in dieser Arbeit untersuchten Erfüllbarkeitsprobleme in eine Komplexitätsklasse einordnen:

Theorem 3.4 Die Entscheidungsprobleme SAT_i liegen für alle $i \in \{1, \ldots, 5\}$ in $BP(\mathcal{NP}^0_{\mathbb{R}})$.

Beweis: Hierzu ist folgendes zu zeigen:

1. $\mathcal{L} \subseteq \{0,1\}^*$, d.h. Kreuzproduktgleichungen und -ungleichungen sowie beliebige Kombinationen verknüpft mit logischen „und“ und „oder“ lassen sich allein durch die Zahlen 0 und 1 kodieren.
2. $\mathcal{L} \in \mathcal{NP}^0_{\mathbb{R}}$, d.h. es gibt ein Entscheidungsproblem $\mathcal{L}'$, welches bei gegebenem Zeugen von einer BSS-Maschine, die außer den im gegebenen Zeugen vorhandenen Zahlen aus $\mathbb{R}$ keine Konstanten aus $\mathbb{R}\backslash\mathbb{Q}$ zur Verfügung hat, mit diesen aber exakt rechnet, in polynomieller Zeit entschieden werden kann.

Zu 1.: Durch konkrete Angabe einer möglichen Kodierung für SAT_5:
Zunächst legt man (willkürlich) die Kodierung aller möglichen Zeichen fest.

Zeichenfolge	Bedeutung
000	(
001	)
010	$\times$
011	$\wedge$
100	$\vee$
101	$=$
110	$\neq$
111	Variable folgt

Um eine Variable zu kodieren, wird also zuerst 111 angegeben, und dann der Index der Variablen in Binärdarstellung. Damit eindeutig ist, bei welchen Stellen es sich noch um den Index der Variablen handelt, und wann das nächste Zeichen beginnt (so könnte sonst 111101011110 für $X_1 \times X_2$, aber auch für X_{350} stehen), wird der Index der Variablen immer in 3er-Gruppen angegeben. Dazu muss die Zahl gegebenenfalls mit bis zu zwei Nullen beginnen, oder, bei einer Zahl echt größer als sieben, erneut mit 111 angegeben werden, dass es sich um den Index einer Variablen handelt. (Da auf eine Variable nie eine weitere Variable folgen kann, ohne dass diese durch eine Klammer, ein Kreuzproduktzeichen, ein Gleichheits- oder Ungleichheitszeichen oder ein logisches „und“ oder „oder“ getrennt sind, ist diese Kodierung eindeutig.)

Beispielsweise wird

$$((X_1 \times X_2) \times X_3 = X_1 \times X_4) \wedge (X_1 \neq X_3)$$

als

$$\underbrace{000}_{(}\,\underbrace{000}_{(}\,\underbrace{111\,001}_{X_1}\,\underbrace{010}_{\times}\,\underbrace{111\,010}_{X_2}\,\underbrace{001}_{)}\,\underbrace{010}_{\times}\,\underbrace{111\,011}_{X_3}\,\underbrace{101}_{=}\,\underbrace{111\,001}_{X_1}\,\underbrace{010}_{\times}\,\underbrace{111\,100}_{X_4}\,\underbrace{001}_{)}$$
$$\underbrace{011}_{\wedge}\,\underbrace{000}_{(}\,\underbrace{111\,001}_{X_1}\,\underbrace{110}_{\neq}\,\underbrace{111\,011}_{X_3}\,\underbrace{001}_{)}$$

kodiert. Der Term

$$(X_8 \times X_2) \times X_{11}$$

(als Teil eines größeren Kreuzproduktgleichungssystems) wird kodiert als

$$\underbrace{000}_{(}\ \underbrace{111\ 001\ 111\ 000}_{X_8}\ \underbrace{010}_{\times}\ \underbrace{111\ 010\ 001}_{X_2}\ \underbrace{010}_{)}\ \underbrace{010}_{\times}\ \underbrace{111\ 001\ 111\ 011}_{X_{11}},$$

wobei die Leerzeichen zwischen den 3er-Gruppen nur zur besseren Lesbarkeit eingefügt wurden.

Um auch SAT_1, SAT_2, SAT_3 und SAT_4 kodieren zu können, wird noch ein zusätzliches Trennzeichen, z.B. ein Komma, benötigt, sodass man eigentlich 9 verschiedene Zeichen kodieren muss. Dazu würden 3 Ziffern im Binärsystem nicht ausreichen. Da man aber bei diesen Versionen von SAT wenigstens für „=“ und „≠“ keine Kodierung benötigt, genügt es auch hier, die Kodierung in 3er-Gruppen einzuteilen.

Zu 2.: Damit eine BSS-Maschine bei gegebenem Kreuzprodukt-Term (bzw. Kreuzprodukt-Termen und ihren logischen Verknüpfungen) und zugehörigem Zeugen entscheiden kann, ob es sich tatsächlich um eine erfüllende Belegung handelt, muss sie in der Lage sein, die Rechenanweisungen der gegebenen Kreuzprodukt-Terme zu erkennen, durchzuführen und anschließend die Ergebnisse zu vergleichen.
Dazu liest sie die Eingabe und führt pro 3er-Gruppe Eingabecode maximal 8 Tests auf Gleichheit durch, um den Kreuzprodukt-Term (bzw. die Kreuzprodukt-Terme und ihre logischen Verknüpfungen) zu bestimmen. Je nach Ergebnis der Tests wird ein anderer Pfad im Berechnungsbaum durchlaufen, welcher die nun folgenden nötigen Berechnungen eindeutig festlegt.
Um ein Kreuzprodukt zu berechnen, werden wegen

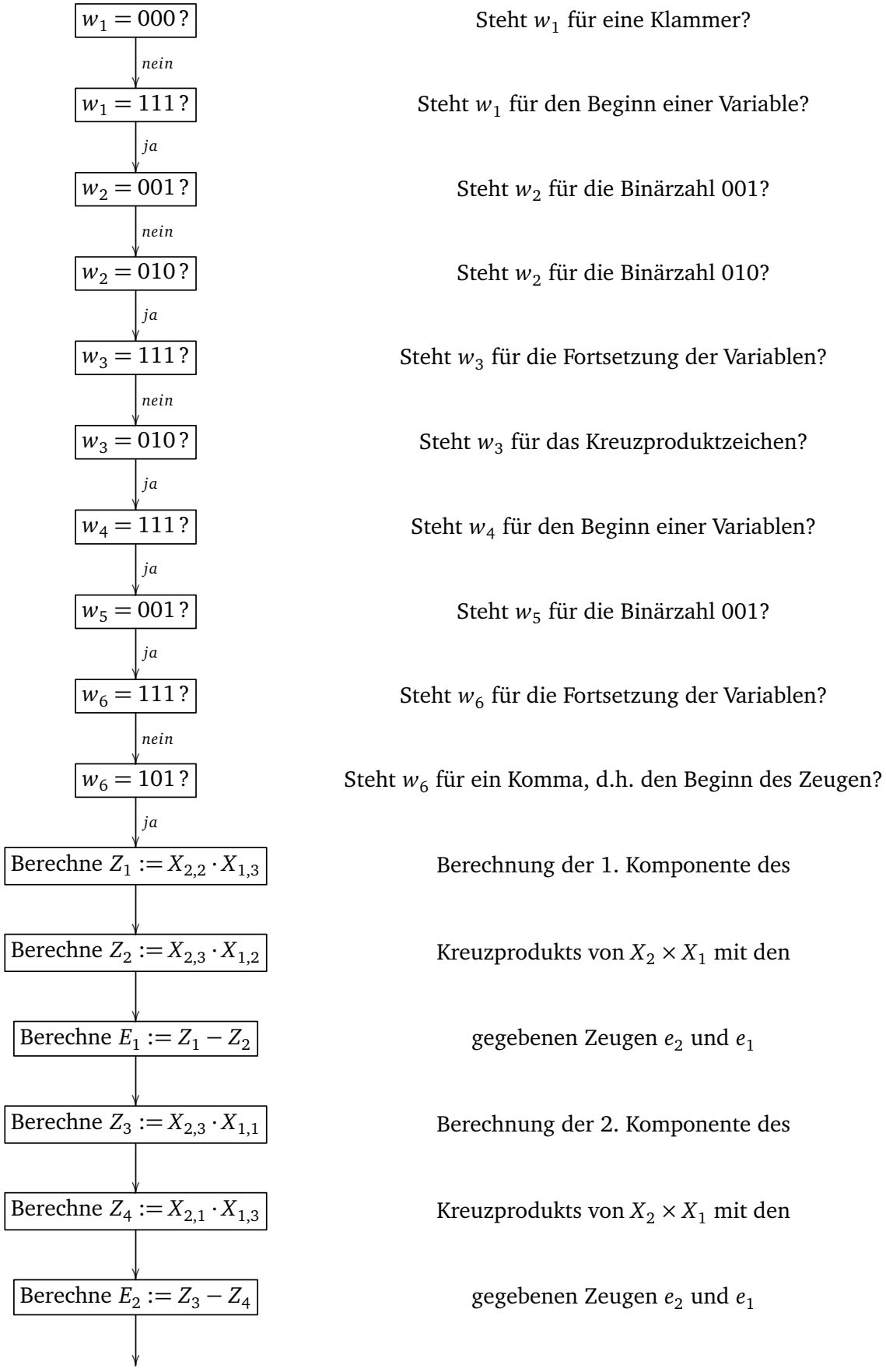
$$a \times b := \begin{pmatrix} a_2 \cdot b_3 - a_3 \cdot b_2 \\ a_3 \cdot b_1 - a_1 \cdot b_3 \\ a_1 \cdot b_2 - a_2 \cdot b_1 \end{pmatrix}$$

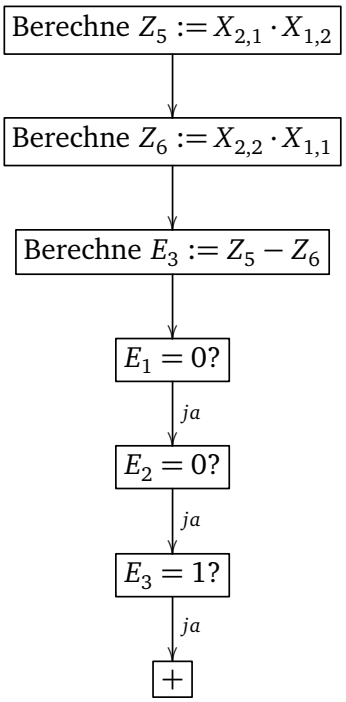
nur Multiplikation und Subtraktion benötigt, sodass dies von einer BSS-Maschine über $\mathbb{R}$ berechenbar ist, indem sie jeden Vektor $x \in \mathbb{R}^3$ als Tripel (x_1, x_2, x_3) mit $x_i \in \mathbb{R}$ auffasst.
Also kann eine BSS-Maschine die vorgegebenen Kreuzprodukte berechnen. Dies geschieht nur mit den im Zeugen gegebenen Zahlen, sodass keine Konstanten aus $\mathbb{R}\backslash\mathbb{Q}$ benötigt werden.
Anschließend kann sie (komponentenweise testen und) entscheiden, ob der berechnete Kreuzprodukt-Term mit e_3 übereinstimmt bzw. ob die berechneten Kreuzprodukt-Terme (alle oder teilweise, je nach logischen Verknüpfungen und Klammerung) gleich bzw. ungleich und nicht gleich 0 sind.
All dies benötigt nur polynomiell viel Zeit.

Insgesamt folgt also $SAT_i \in BP(\mathcal{NP}^0_{\mathbb{R}})$ für alle $i \in \{1, \ldots, 5\}$. □

Beispiel 3.5 Hier wird nun ein Beispiel eines möglichen Berechnungspfads im Berechnungsbaum einer BSS-Maschine, die SAT_1 mit exakter Rechnung über $\mathbb{R}$ in polynomieller Zeit entscheidet, über keine reellen Konstanten verfügt, der gegebene Zeuge allerdings Zahlen aus $\mathbb{R}\backslash\mathbb{Q}$ enthalten darf, angegeben:
Hier wird für die Kodierung des Zeichens „ ,“ die Sequenz 101 verwendet. Dies ist möglich, da (wie oben erwähnt) für SAT_1 keine Kodierung von „=“ notwendig ist. Auch muss der Zeuge nicht weiter kodiert werden, da für $\mathcal{L} \in BP(\mathcal{NP}^0_{\mathbb{R}})$ nur gefordert wird, dass $\mathcal{L} \subseteq \{0,1\}^*$ und $\mathcal{L} \in \mathcal{NP}^0_{\mathbb{R}}$ gilt. Letzteres fordert die Existenz eines Zeugen $z \in \mathbb{R}^{p(|x|)}$ und eines Entscheidungsproblems $\mathcal{L}' \in \mathcal{P}^0_{\mathbb{R}}$, sodass $\langle x, z\rangle \in \mathcal{L}'$ gilt, aber es ist nicht erforderlich (und wegen der Möglichkeit, dass $z \in \mathbb{R}\backslash\mathbb{Q}$ gilt, auch nicht möglich), dass $\mathcal{L}' \subseteq \{0,1\}^*$ gilt.
Im Berechnungspfad ist zur besseren Lesbarkeit die Eingabe in Tripel unterteilt, durchnummeriert und anschließend entsprechend der Nummerierung mit w_i bezeichnet worden.

Eingabe: Kodierung von $X_2 \times X_1$ mit Zeugen e_2, e_1.
Berechnungspfad bei dieser Eingabe (mit Erklärung):


$w_1 = 000\,?$
Steht w_1 für eine Klammer?
nein
$w_1 = 111\,?$
Steht w_1 für den Beginn einer Variable?
ja
$w_2 = 001\,?$
Steht w_2 für die Binärzahl 001?
nein
$w_2 = 010\,?$
Steht w_2 für die Binärzahl 010?
ja
$w_3 = 111\,?$
Steht w_3 für die Fortsetzung der Variablen?
nein
$w_3 = 010\,?$
Steht w_3 für das Kreuzproduktzeichen?
ja
$w_4 = 111\,?$
Steht w_4 für den Beginn einer Variablen?
ja
$w_5 = 001\,?$
Steht w_5 für die Binärzahl 001?
ja
$w_6 = 111\,?$
Steht w_6 für die Fortsetzung der Variablen?
nein
$w_6 = 101\,?$
Steht w_6 für ein Komma, d.h. den Beginn des Zeugen?
ja
Berechne $Z_1 := X_{2,2} \cdot X_{1,3}$
Berechnung der 1. Komponente des
Berechne $Z_2 := X_{2,3} \cdot X_{1,2}$
Kreuzprodukts von $X_2 \times X_1$ mit den
Berechne $E_1 := Z_1 - Z_2$
gegebenen Zeugen e_2 und e_1
Berechne $Z_3 := X_{2,3} \cdot X_{1,1}$
Berechnung der 2. Komponente des
Berechne $Z_4 := X_{2,1} \cdot X_{1,3}$
Kreuzprodukts von $X_2 \times X_1$ mit den
Berechne $E_2 := Z_3 - Z_4$
gegebenen Zeugen e_2 und e_1



Berechnung der 3. Komponente des Kreuzprodukts von $X_2 \times X_1$ mit den gegebenen Zeugen e_2 und e_1

Test auf Gleichheit

aller Komponenten des Ergebnisses

mit dem Wunschergebnis e_3

3.2 Einordnung der projektiven Erfüllbarkeitsprobleme

Nachdem festgestellt wurde, dass alle Erfüllbarkeitsprobleme über $\mathbb{R}^3$ in der Komplexitätsklasse $BP(\mathcal{NP}^0_{\mathbb{R}})$ liegen, wird dies nun auch für die entsprechenden projektiven Erfüllbarkeitsprobleme gezeigt.

Theorem 3.6 Auch SAT_{i^p} und $\mathrm{SAT}_{2^{p*}}$ liegen für alle $i \in \{1,\ldots,5\}$ in $BP(\mathcal{NP}^0_{\mathbb{R}})$.

Beweis: $\mathcal{L} \subseteq \{0,1\}^*$ folgt wie in Theorem 3.4.

Für $\mathcal{L} \in \mathcal{NP}^0_{\mathbb{R}}$ werden die Berechnungen der BSS-Maschine analog durchgeführt (als Zeugen werden Repräsentanten aus $\mathbb{R}^3\backslash\{0\}$ der Äquivalenzklassen in $\mathbb{P}^2$ gegeben, sodass alle Rechnungen über $\mathbb{R}^3\backslash\{0\}$ durchgeführt werden können), nur das Testen auf Gleichheit zweier Terme $[t(x_1,\ldots,x_n)]$, $[s(x_1,\ldots,x_n)] \in \mathbb{P}^2$ muss durch folgendes Verfahren ersetzt werden:

1) Teste nacheinander, ob mindestens eines der $s^i(x_1,\ldots,x_n)$ für $i \in \{1,2,3\}$ nicht 0 ist (wobei $s^i(x_1,\ldots,x_n)$ für die i-te Komponente von $s(x_1,\ldots,x_n)$ steht).
   Falls nein, verwerfe.
   Falls ja, fahre mit 2.i) fort, wobei i demjenigen $i \in \{1,2,3\}$ entspricht, für welches $s^i(x_1,\ldots,x_n) \neq 0$ festgestellt wurde. (Sobald ein solches i gefunden wurde, wird sofort zu Schritt 2.i) übergegangen.)

2.i) Berechne $\lambda_i := t^i(x_1,\ldots,x_n)/s^i(x_1,\ldots,x_n)$ und fahre mit Schritt 3.i) fort.

3.1) Teste, ob $\lambda_1 \cdot s^2(x_1,\ldots,x_n) = t^2(x_1,\ldots,x_n)$ und $\lambda_1 \cdot s^3(x_1,\ldots,x_n) = t^3(x_1,\ldots,x_n)$.
   Falls nein, verwerfe.
   Falls ja, akzeptiere.

3.2) Teste, ob $t^1(x_1,\ldots,x_n) = 0$ und $\lambda_2 \cdot s^3(x_1,\ldots,x_n) = t^3(x_1,\ldots,x_n)$.
   Falls nein, verwerfe.
   Falls ja, akzeptiere.

3.3) Teste, ob $t^1(x_1,\ldots,x_n)=0$ und $t^2(x_1,\ldots,x_n)=0$.
Falls nein, verwerfe.
Falls ja, akzeptiere.

Durch Anpassen des Akzeptierens bzw. Verwerfens kann analog auch auf Ungleichheit getestet werden. Auch dies benötigt nur polynomiell viel Zeit, denn es werden die polynomiell vielen Einlese- und Berechnungsschitte aus Theorem 3.4 unverändert durchgeführt, und nur (polynomiell viele) Tests auf Gleichheit durch das obige Verfahren ersetzt. Pro Test auf Gleichheit, der nur eine Zeiteinheit benötigt, werden nun 6 Multiplikationen, Divisionen bzw. Tests auf Gleichheit benötigt, sodass dies noch immer in polynomieller Zeit möglich ist. □

3.3 Untersuchen der Erfüllbarkeitsprobleme auf Vollständigkeit

Nun sollen die Erfüllbarkeitsprobleme auf Vollständigkeit bezüglich der Komplexitätsklasse $BP\left(\mathcal{NP}^0_{\mathbb{R}}\right)$ untersucht werden. Es wird sich herausstellen, dass wenigstens einige dieser Probleme $BP\left(\mathcal{NP}^0_{\mathbb{R}}\right)$-vollständig sind. Um dies zu zeigen, soll $FEAS_{\mathbb{Z},\mathbb{R}}$ auf SAT_{3^p} reduziert werden, wobei ein großer Teil der Reduktion von $FEAS_{\mathbb{Z},\mathbb{F}}$ auf $SAT_{L(\mathscr{H})}$ aus [4] im Fall $\mathbb{F}=\mathbb{R}$ benutzt werden wird.
Um diese Reduktionen durchführen zu können, werden einige Grundlagen aus der Verbandstheorie benötigt, die hier nun wiederholt werden sollen. Diese sind [4] entnommen, können aber beispielsweise auch in [6] nachgelesen werden.

3.3.1 Grundlagen der Verbandstheorie

Definition 3.7. *Sei $\mathbb{F}\subseteq\mathbb{C}$ ein unter komplexer Konjugation abgeschlossener Körper.*

a) Ein $\mathbb{F}$-unitärer Raum ist ein $\mathbb{F}$-Vektorraum $\mathscr{H}$, der mit einem unitären Skalarprodukt ausgestattet ist.

b) Orthogonalität auf $\mathscr{H}$ ist definiert durch $x\perp y$ genau dann wenn $\langle x,y\rangle=0$.

c) Eine Teilmenge U von $\mathscr{H}$ heißt abgeschlossen, wenn $U=U^{\perp\perp}$ gilt, wobei $U^\perp:=\{x\in\mathscr{H}\,|\,x\perp u\;\forall u\in U\}$.

d) Für $U,V\subseteq\mathscr{H}$ schreibt man $U\perp V$, falls $U\subseteq V^\perp$ (oder äquivalent dazu $V\subseteq U^\perp$) gilt.

e) Das System der quantenlogischen Eigenschaften von $\mathscr{H}$, die Quantenlogik von $\mathscr{H}$, besteht aus der Menge $L(\mathscr{H})$ aller abgeschlossenen Teilmengen von $\mathscr{H}$ ausgestattet mit den Konstanten $\mathbf{0}:=\{0\}\in L(\mathscr{H})$ und $\mathbf{1}:=\mathscr{H}\in L(\mathscr{H})$ sowie den folgenden Verknüpfungen:

- $\wedge: L(\mathscr{H})\times L(\mathscr{H})\to L(\mathscr{H}),\ (U,V)\mapsto U\cap V$
- $\vee: L(\mathscr{H})\times L(\mathscr{H})\to L(\mathscr{H}),\ (U,V)\mapsto (U\cup V)^{\perp\perp}$
- $\neg: L(\mathscr{H})\to L(\mathscr{H}),\ U\mapsto U^\perp$

f) $L_k(\mathscr{H})$ sei die Menge der k-dimensionalen Unterräume von $\mathscr{H}$.

Bemerkung 3.8 Jede im Sinne von Definition 3.7c) abgeschlossene Teilmenge U ist ein linearer Unterraum von $\mathscr{H}$. Ist $\mathscr{H}$ endlichdimensional, so gilt $U\vee V=U+V$, wobei $U+V:=\{u+v\,|\,u\in U,\,v\in V\}$.

Definition 3.9. *Ein Verband ist eine algebraische Struktur mit zwei Verknüpfungen $\wedge$ ("meet") und $\vee$ ("join"), die assoziativ, kommutativ und idempotent sind, den folgenden Absorptionsgesetzen*

$$A\wedge(A\vee B)=A=A\vee(A\wedge B)$$

genügen und für die

$$\mathbf{0} \wedge A = \mathbf{0} \qquad \textit{und} \qquad \mathbf{1} \wedge A = A$$

gilt.
(Alternativ definiert man eine partielle Ordnung mit $A \leq B \;:\Leftrightarrow\; A = A \wedge B$. Dann ist $A \vee B$ das Supremum und $A \wedge B$ das Infimum von A und B, und $\mathbf{0}$ bzw. $\mathbf{1}$ sind kleinstes bzw. größtes Element.)
Gibt es eine weitere Abbildung $\neg$ innerhalb des Verbands, welche die Eigenschaften

$$\neg A \vee A = \mathbf{1}, \qquad \neg A \wedge A = \mathbf{0}, \qquad \neg\neg A = A, \qquad A \leq B \text{ genau dann wenn } \neg B \leq \neg A$$

besitzt, so nennt man dies einen Orthoverband. Ein Orthoverband erfüllt die De Morgan'schen Regeln.
Gilt weiter das Modularitätsgesetz

$$A \geq C \qquad \Rightarrow \qquad A \wedge (B \vee C) = (A \wedge B) \vee C$$

so nennt man dies einen modularen Orthoverband (MOL).

Bemerkung 3.10 $L(\mathscr{H})$ ist ein Orthoverband. Ist $\mathscr{H}$ endlichdimensional, so ist $L(\mathscr{H})$ sogar ein modularer Orthoverband. Vgl. dazu [4].

Definition 3.11. *Seien L, L' Verbände. Eine Abbildung $\varphi : L \to L'$ heißt Homomorphismus, wenn*

$$\varphi(x \vee y) = \varphi(x) \vee \varphi(y) \textit{ und } \varphi(x \wedge y) = \varphi(x) \wedge \varphi(y)$$

gilt.
Sind L, L' sogar Orthoverbände, so muss zusätzlich $\varphi(\neg x) = \neg\varphi(x)$ gelten.

Definition 3.12. *Sei L ein Verband. Eine Teilmenge $\emptyset \neq L' \subseteq L$ nennt man Unterverband, falls sie bezüglich der Verknüpfungen $\vee$ und $\wedge$ abgeschlossen ist, d.h. falls für alle $x, y \in L'$ auch $x \vee y \in L'$ und $x \wedge y \in L'$ gilt.*

Fakt 3.13 Sei L ein modularer Verband mit $\mathbf{0}$ und $\mathbf{1}$. Für c) bis e) enthalte L eine endliche maximale Kette.

a) Seien $u, v \in L$. Das Intervall $[u, v] := \{x \,|\, u \leq x \leq v\}$ ist ein Unterverband und insbesondere ebenfalls modular.

b) Zwischen den Intervallen $[a \wedge b, a]$ und $[b, a \vee b]$ gibt es die zueinander inversen Verbandsisomorphismen $[a \wedge b, a] \ni x \mapsto b \vee x \in [b, a \vee b]$ und $[b, a \vee b] \ni y \mapsto a \wedge y \in [a \wedge b, a]$.

c) Alle maximalen Ketten C in L haben die gleiche Kardinalität. Die Dimension oder Höhe von L wird definiert als $\dim(L) := |C| - 1$. Insbesondere ist $\dim(u) := \dim([\mathbf{0}, u])$ für alle $u \in L$ wohldefiniert.

d) Für alle $U \in L(\mathscr{H})$ stimmt die Vektorraumdimension mit $\dim(U)$ überein.

e) Es gelten die folgenden Dimensionsformeln:

$$\dim(v) = \dim(u) + \dim([u, v]) \text{ falls } u \leq v \quad \text{und} \quad \dim(a) + \dim(b) = \dim(a \wedge b) + \dim(a \vee b).$$

Beweis:

a) Seien $a, b \in [u, v]$. Dann gilt nach Voraussetzung $u \leq a \leq v$ sowie $u \leq b \leq v$. Nach Definition der Ordnungsrelation gilt damit u.a.

$$\begin{array}{llllll} (I) & u = u \wedge a & (II) & u = b \wedge u & (III) & a = a \wedge v \\ (IV) & a = a \vee u & (V) & v = a \vee v & (VI) & v = b \vee v \end{array}$$

Mit diesen Gleichungen sowie Assoziativität und Kommutativität der Verknüpfungen folgt

$$\begin{aligned} u &\overset{(I)}{=} u \wedge a \overset{(II)}{=} (b \wedge u) \wedge a = u \wedge (a \wedge b) \\ &\Rightarrow \quad u \leq a \wedge b \end{aligned}$$

$$\begin{aligned} a \wedge b &\overset{(III)}{=} (a \wedge v) \wedge b = (a \wedge b) \wedge v \\ &\Rightarrow \quad a \wedge b \leq v \\ &\Rightarrow \quad a \wedge b \in [u, v] \end{aligned}$$

$$\begin{aligned} a \vee b &\overset{(IV)}{=} (a \vee u) \vee b = (a \vee b) \vee u \\ &\Rightarrow \quad u \leq a \vee b \end{aligned}$$

$$\begin{aligned} v &\overset{(V)}{=} v \vee a \overset{(VI)}{=} (v \vee b) \vee a = v \vee (a \vee b) \\ &\Rightarrow \quad a \vee b \leq v \\ &\Rightarrow \quad a \vee b \in [u, v] \end{aligned}$$

Seien nun $a, b, c \in [u, v]$ mit $a \leq c$.
Dann gilt auch $a, b, c \in L$, und da L modular ist, folgt $a \vee (b \wedge c) = (a \vee b) \wedge c$, sodass $[u, v]$ modular ist.

b) Seien $f : [a \wedge b, a] \to [b, a \vee b],\ x \mapsto b \vee x$ und $g : [b, a \vee b] \to [a \wedge b, a],\ y \mapsto a \wedge y$.
Für $y \in [b, a \vee b]$ gilt nach Voraussetzung (I) $b \leq y$ sowie (II) $y = y \wedge (a \vee b)$, für $x \in [a \wedge b, a]$ gilt analog (III) $x \leq a$ sowie (IV) $x = x \vee (a \wedge b)$. Mit Modularität, Assoziativität und Kommutativität folgt damit

$$\begin{aligned} f(g(y)) = f(a \wedge y) = b \vee (a \wedge y) &\overset{(I)}{=} (b \vee a) \wedge y \overset{(II)}{=} y \\ g(f(x)) = g(b \vee x) = a \wedge (b \vee x) &\overset{(III)}{=} (a \wedge b) \vee x \overset{(IV)}{=} x, \end{aligned}$$

d.h. f und g sind zueinander inverse Abbildungen.

Seien $x, x' \in [a \wedge b, a]$ und $y, y' \in [b, a \vee b]$. Dann folgt

$$f(x \vee x') = b \vee (x \vee x') = (b \vee b) \vee (x \vee x') = (b \vee x) \vee (b \vee x') = f(x) \vee f(x')$$

sowie

$$g(y \wedge y') = a \wedge (y \wedge y') = (a \wedge a) \wedge (y \wedge y') = (a \wedge y) \wedge (a \wedge y') = g(y) \wedge g(y').$$

Da f und g zueinander inverse Abbildungen, und damit insbesondere auch bijektiv sind, gibt es für $x, x' \in [a \wedge b, a]$ genau ein $y, y' \in [b, a \vee b]$ mit $x = g(y)$ (und $f(x) = y$) sowie $x' = g(y')$ (und $f(x') = y'$). Mit den obigen beiden Gleichungen folgt

$$f(x \wedge x') = f(g(y) \wedge g(y')) = f(g(y \wedge y')) = y \wedge y' = f(x) \wedge f(x').$$

Analog dazu folgt auch

$$g(y \vee y') = g(f(x) \vee f(x')) = g(f(x \vee x')) = x \vee x' = g(y) \vee g(y').$$

Damit sind f und g zueinander inverse Verbandsisomorphismen.

c) Sei L ein modularer Verband, dessen längste maximale Kette die Länge $n+1$ hat. Die Aussage wird durch Induktion über n gezeigt:
Sei $n = 1$. Dann gilt $L = \{\mathbf{0}, \mathbf{1}\}$, denn wäre $a \in L$ mit $\mathbf{0} \neq a \neq \mathbf{1}$, so würde $\mathbf{0} \leq a \leq \mathbf{1}$ gelten und $\mathbf{0}, a, \mathbf{1}$ wäre eine Kette der Länge 3. In $\{\mathbf{0}, \mathbf{1}\}$ gibt es nur die maximale Kette $\mathbf{0}, \mathbf{1}$, sodass die Länge aller maximalen Ketten in L gleich ist.
Sei nun $n > 1$ und seien C, C' maximale Ketten in L und $a \in C \backslash \{\mathbf{0}, \mathbf{1}\}$, $b \in C' \backslash \{\mathbf{0}, \mathbf{1}\}$. Seien weiter

$$I_1 = [\mathbf{0}, a], \quad I_2 = [a, \mathbf{1}], \quad I_1' = [\mathbf{0}, b], \quad I_2' = [b, \mathbf{1}],$$

d.h. die Ketten C und C' werden in je 2 Teile zerlegt, wobei das Element an der Trennstelle nun in beiden Kettenteilen vorkommt.
Da $\mathbf{1} \notin I_1, I_1'$ und $\mathbf{0} \notin I_2, I_2'$ haben alle maximalen Ketten in diesen Intervallen höchstens Länge n, und damit nach Induktionshypothese die gleiche Länge.
Wegen $\mathbf{0} \leq a \wedge b \leq a$, $\mathbf{0} \leq a \wedge b \leq b$, $a \leq a \vee b \leq \mathbf{1}$ und $b \leq a \vee b \leq \mathbf{1}$ folgt $a \wedge b \in I_1$, $a \wedge b \in I_1'$, $a \vee b \in I_2$ und $a \vee b \in I_2'$. Da alle maximalen Ketten in diesen Intervallen gleich lang sind, kann man o.B.d.A. annehmen, dass C und C' die Elemente $a \wedge b$ und $a \vee b$ enthalten.
Seien nun

$$\begin{aligned} J_1 &= [\mathbf{0}, a \wedge b], \quad J_2 = [a \wedge b, a], \quad J_3 = [a, a \vee b], \quad J_4 = [a \vee b, \mathbf{1}], \\ J_1' &= [\mathbf{0}, a \wedge b], \quad J_2' = [a \wedge b, b], \quad J_3' = [b, a \vee b], \quad J_4' = [a \vee b, \mathbf{1}]. \end{aligned}$$

Auch in diesen Intervallen sind nach Induktionshypothese alle maximalen Ketten gleich lang. Mit b) folgt die Isomorphie von J_2 und J_3' , sodass die Länge der maximalen Ketten in J_2 mit der Länge der maximalen Ketten in J_3' übereinstimmt. Analog folgt dies für J_3 und J_2'. Wegen $J_1 = J_1'$ und $J_4 = J_4'$ folgt insgesamt, dass C und C' gleich lang sind.
Damit haben alle maximalen Ketten in L die gleiche Kardinalität und die Dimension eines Intervalls ist wohldefiniert.

d) Sei $U \in L(\mathscr{H})$ und $\{v_1, \ldots, v_m\}$ eine Basis von U. Dann ist $U_0 = \{0\}, U_i = U_{i-1} + \mathbb{F} \cdot v_i$ für $i \in \{1, \ldots, m\}$ eine maximale Kette, sodass $\dim(U) = m$ gilt, und diese Definition der Dimension stimmt mit der Vektorraumdimension überein.

e) i) Sei $u \leq v$ und $C_1 = (c_{1,1}, \ldots, c_{1,n})$ eine maximale Kette in $[\mathbf{0}, u]$, $C_2 = (c_{2,1}, \ldots, c_{2,m})$ eine maximale Kette in $[u, v]$. Wegen $[\mathbf{0}, u] \cup [u, v] = [\mathbf{0}, v]$ folgt, dass $(c_{1,1}, \ldots, c_{1,n}, c_{2,2}, \ldots, c_{2,m})$ eine maximale Kette in $[\mathbf{0}, v]$ ist. Damit folgt

$$\dim(v) = (n + (m-1)) - 1 = (n-1) + (m-1) = \dim(u) + \dim([u, v]).$$

ii) Wegen $a \wedge b \leq a$ und $b \leq a \vee b$ folgt mit i)

$$\dim(a) = \dim(a \wedge b) + \dim([a \wedge b, a]) \quad \text{und} \quad \dim(a \vee b) = \dim(b) + \dim([b, a \vee b]).$$

Nach b) gilt $\dim([a \wedge b, a]) = \dim([b, a \vee b])$. Insgesamt folgt

$$\dim(a) + \dim(b) = \dim(a \wedge b) + \dim(a \vee b).$$

□

Definition 3.14.

a) *Ein (Orthoverbands- oder quantenlogischer) Term ist ein syntaktisch korrekter Ausdruck über Variablen $x_1, \ldots, x_n$ mit Operationen $\wedge, \vee, \neg$ und Konstanten $\mathbf{0}, \mathbf{1}$. Man schreibt manchmal $t(\overline{x})$, um die Abhängigkeit von $\overline{x} := (x_1, \ldots, x_n)$ zu betonen.*
Die syntaktische Länge von t, $|t|$, wird rekursiv definiert durch $|x| = 1$, $|\neg t| = |t| + 1$ und $|s \vee t| = |s \wedge t| = |s| + |t| + 1$.

b) *Für einen Orthoverband $(L, \wedge, \neg, \vee, \mathbf{0}, \mathbf{1})$ und $\overline{a} = (a_1, \ldots, a_n) \in L^n$ bezeichnet $t_L(a_1, \ldots, a_n) = t_L(\overline{a}) \in L$ den Wert von t in L, wenn man jedes x_i durch a_i ersetzt.*

c) *Ein von n Variablen abhängiger Term t ist stark erfüllbar in L, wenn es $\overline{a} \in L^n$ gibt, sodass $t_L(\overline{a}) = \mathbf{1}$, und schwach erfüllbar, wenn es $\overline{a} \in L^n$ gibt, sodass $t_L(\overline{a}) \neq \mathbf{0}$ gilt.*

d) *Die zu starker und schwacher Erfüllbarkeit in L gehörigen Entscheidungsprobleme werden definiert als*

$$\begin{aligned} SAT_L &:= \{\langle t(x_1, \ldots, x_n)\rangle \mid n \in \mathbb{N},\ t \text{ Term}, \exists\, \overline{a} \in L^n : t(\overline{a}) = \mathbf{1}\} \subseteq \{0,1\}^* \\ sat_L &:= \{\langle t(x_1, \ldots, x_n)\rangle \mid n \in \mathbb{N},\ t \text{ Term}, \exists\, \overline{a} \in L^n : t(\overline{a}) \neq \mathbf{0}\} \subseteq \{0,1\}^*. \end{aligned}$$

Definition 3.15. *Ein System $\overline{a} = (a_{ij} \mid 1 \leq i, j \leq d)$ von Elementen eines modularen Verbands L nennt man d-Rahmen, wenn die folgenden Bedingungen erfüllt sind, bei denen a_{ii} durch a_i abgekürzt wird:*

$$\begin{aligned} \mathbf{1} &= a_1 \vee \ldots \vee a_d \\ \mathbf{0} &= a_i \wedge \bigvee_{j \neq i} a_j && \text{für alle } i \in \{1, \ldots, d\} \\ \mathbf{0} &= a_i \wedge a_{ij} && \text{für alle } i, j \in \{1, \ldots, d\} \text{ mit } i \neq j \\ a_i \vee a_j &= a_i \vee a_{ij} && \text{für alle } i, j \in \{1, \ldots, d\} \text{ mit } i \neq j \\ a_{ij} &= a_{ji} && \text{für alle } i, j \in \{1, \ldots, d\} \text{ mit } i \neq j \\ a_{ik} &= (a_i \vee a_k) \wedge (a_{ij} \vee a_{jk}) && \text{für alle } i, j, k \in \{1, \ldots, d\} \text{ mit } i \neq j \neq k \neq i \end{aligned}$$

Fakt 3.16 Sei $\overline{a}$ ein d-Rahmen in einem modularen Verband L. Dann gilt

a) $\dim(a_i) = \dim(a_j) = \dim(a_{ij})$ für alle $i, j \in \{1, \ldots, d\}$.

b) $\dim\left(\bigvee_{i \in I} a_i\right) = |I| \cdot \dim(a_1)$ für $I \subseteq \{1, \ldots, d\}$.

c) $\dim(L) = d \cdot \dim(a_1)$.

d) Sei $\dim(\mathscr{H}) = d$. Dann ist $\overline{A} = (A_{ij} \mid 1 \leq i, j \leq d)$ genau dann ein d-Rahmen von $L(\mathscr{H})$, wenn es eine Basis $\{v_1, \ldots, v_d\}$ von $\mathscr{H}$ gibt, sodass $A_i = A_{ii} = \mathbb{F}v_i$ und $A_{ij} = \mathbb{F}(v_i - v_j)$ für $i \neq j$ gilt.

e) Insbesondere gibt es für jedes $L(\mathscr{H})$ mit $\dim(\mathscr{H}) = d$ einen d-Rahmen.

Beweis:

a) Da $a \leq a \vee b$ für alle $a, b \in L$ gilt, folgt aus der 2. definierenden Eigenschaft eines d-Rahmens $\mathbf{0} = a_i \wedge \bigvee_{j \neq i} a_j \geq a_i \wedge a_k$ für $k \neq i$, sodass $\mathbf{0} = a_i \wedge a_k$ und damit $0 = \dim(\mathbf{0}) = \dim(a_i \wedge a_k)$ für $i \neq k$ gilt.
Mit 3.13e) und der 3. und 4. definierenden Eigenschaft eines d-Rahmens folgt für $i, j \in \{1, \ldots, d\}$ mit $i \neq j$

$$\begin{aligned} \dim(a_i) + \dim(a_j) &= \dim(a_i \vee a_j) + \dim(a_i \wedge a_j) \\ &= \dim(a_i \vee a_j) \\ &= \dim(a_i \vee a_{ij}) \\ &= \dim(a_i \vee a_{ij}) + \dim(a_i \wedge a_{ij}) \\ &= \dim(a_i) + \dim(a_{ij}) \end{aligned}$$

sodass

$$\dim(a_j) = \dim(a_{ij}).$$

Weiter folgt

$$\dim(a_i \vee a_{ij}) = \dim(a_i \vee a_j) = \dim(a_j \vee a_i) = \dim(a_j \vee a_{ji})$$

und

$$\dim(a_j \vee a_{ji}) = \dim(a_j \vee a_{ji}) + \dim(a_j \wedge a_{ji}) = \dim(a_j) + \dim(a_{ji})$$

sowie durch Umbenennung der Indizes

$$\dim(a_i \vee a_{ij}) = \dim(a_i) + \dim(a_{ij}) = \dim(a_i) + \dim(a_{ji}),$$

sodass

$$\dim(a_i) + \dim(a_{ji}) = \dim(a_i \vee a_{ij}) = \dim(a_j \vee a_{ji}) = \dim(a_j) + \dim(a_{ji})$$

und damit

$$\dim(a_i) = \dim(a_j).$$

b) Analog zur 1. Beobachtung in a) folgt $\mathbf{0} = a_i \wedge \bigvee_{j\in I, j\neq i} a_j$ und $0 = \dim\left(a_i \wedge \bigvee_{j\in I, j\neq i} a_j\right)$ für $I \subseteq \{1,\dots,d\}$. Sei nun $I = \{i_1,\dots,i_k\} \subseteq \{1,\dots,d\}$. Damit gilt

$$\begin{aligned}
\dim\left(\bigvee_{i\in I} a_i\right) &= \dim\left(a_{i_1} \vee \ldots \vee a_{i_k}\right) \\
&= \dim\left(a_{i_1} \vee \ldots \vee a_{i_k}\right) + \dim\left(a_{i_1} \wedge \left(a_{i_2} \vee \ldots \vee a_{i_k}\right)\right) \\
&= \dim\left(a_{i_1}\right) + \dim\left(a_{i_2} \vee \ldots \vee a_{i_k}\right) \\
&= \ldots \\
&= \dim\left(a_{i_1}\right) + \ldots + \dim\left(a_{i_k}\right) \\
&= k \cdot \dim\left(a_1\right) \\
&= |I| \cdot \dim\left(a_1\right)
\end{aligned}$$

c) Da $L = [\mathbf{0}, \mathbf{1}]$ gilt, folgt mit der 1. definierenden Eigenschaft eines d-Rahmens sowie a) und b)

$$\begin{aligned}
\dim(L) &= \dim([\mathbf{0}, \mathbf{1}]) \\
&= \dim(\mathbf{1}) \\
&= \dim(a_1 \vee \ldots \vee a_d) \\
&= d \cdot \dim(a_1).
\end{aligned}$$

d) ” $\Rightarrow$ ”
Sei $\overline{A} = (A_{ij} \mid 1 \leq i, j \leq d)$ ein d-Rahmen von $L(\mathscr{H})$ und $\dim(\mathscr{H}) = d$. Mit a) bis c) folgt $\dim(A_i) = 1$ für alle $i \in \{1,\dots,d\}$ sowie $\mathscr{H} = A_1 \oplus \ldots \oplus A_d$. Also kann man eine Basis $\{v_1,\dots,v_d\}$ von $\mathscr{H}$ wählen, sodass $A_i = \mathbb{F}v_i$ gilt.
Wegen $\dim(A_i) = \dim(A_{ij})$ ist auch A_{ij} und damit insbesondere A_{1j} eindimensional. Also gibt es ein $w_{1j} \in \mathbb{F}^d$, sodass $A_{1j} = \mathbb{F}w_{1j}$ gilt. Aus $A_i \vee A_j = A_i \vee A_{ij}$ folgt $A_{1j} \leq A_1 \vee A_j$, sodass $\mathbb{F}w_{1j} \subseteq \mathbb{F}v_1 + \mathbb{F}v_j$ gilt. Damit gibt es $r_j, s_j \in \mathbb{F}$ mit $w_{1j} = r_j v_1 + s_j v_j$. Mit $A_{1j} \vee A_1 = A_j \vee A_1 \neq A_1$ folgt $s_j \neq 0$. Also existiert s_j^{-1}, und man kann v_j durch $-s_j^{-1} r_j v_j$ ersetzen, sodass

$w_{1j} = r_j v_1 + s_j \cdot (-s_j^{-1} r_j) v_j = r_j v_1 - r_j v_j$, und damit gilt $A_{1j} = \mathbb{F}(v_1 - v_j)$.
Damit folgt dann wie gewünscht für die noch nicht betrachteten A_{ik} mit $1 \neq i \neq k$

$$\begin{aligned} A_{ik} &= (A_i \vee A_k) \wedge (A_{i1} \vee A_{1k}) \\ &= (A_i \vee A_k) \wedge (A_{1i} \vee A_{1k}) \\ &= (\mathbb{F}v_i \cup \mathbb{F}v_k) \cap (\mathbb{F}(v_1 - v_i) \cup \mathbb{F}(v_1 - v_k)) \\ &= \{x v_i + y v_k \mid x, y \in \mathbb{F}\} \cap \{z(v_1 - v_i) + w(v_1 - v_k) \mid z, w \in \mathbb{F}\} \\ &= \{x v_i - x v_k \mid x \in \mathbb{F}\} \\ &= \mathbb{F}(v_i - v_k). \end{aligned}$$

"$\Leftarrow$"
Sei $\dim(\mathscr{H}) = d$ und $\{v_1, \ldots, v_d\}$ eine Basis von $\mathscr{H}$, sodass $A_i = \mathbb{F}v_i$ und $A_{ij} = \mathbb{F}(v_i - v_j)$ für $i \neq j$ gilt. Dann folgt

- $$\begin{aligned} A_1 \vee \ldots \vee A_d &= \mathbb{F}v_1 \vee \ldots \vee \mathbb{F}v_d \\ &= \{x_1 v_1 + \ldots + x_d v_d \mid x_1, \ldots x_d \in \mathbb{F}\} \\ &= \mathscr{H} \\ &= \mathbf{1} \end{aligned}$$

- $$\begin{aligned} A_i \wedge \bigvee_{j \neq i} A_j &= \mathbb{F}v_i \wedge \bigvee_{j \neq i} \mathbb{F}v_j \\ &= \{x_i v_i \mid x_i \in \mathbb{F}\} \cap \left\{ \sum_{j \neq i} x_j v_j \mid x_j \in \mathbb{F} \right\} \\ &= \mathbf{0} \end{aligned}$$

- $$\begin{aligned} A_i \wedge A_{ij} &= \mathbb{F}v_i \wedge \mathbb{F}(v_i - v_j) \\ &= \{x v_i \mid x \in \mathbb{F}\} \cap \{y(v_i - v_j) \mid y \in \mathbb{F}\} \\ &= \mathbf{0} \end{aligned}$$

- $$\begin{aligned} A_i \vee A_{ij} &= \mathbb{F}v_i \vee \mathbb{F}(v_i - v_j) \\ &= \{x v_i \mid x \in \mathbb{F}\} \cup \{y(v_i - v_j) \mid y \in \mathbb{F}\} \\ &= \{x v_i + y v_j \mid x, y \in \mathbb{F}\} \\ &= \{x v_i \mid x \in \mathbb{F}\} \cup \{y v_j \mid y \in \mathbb{F}\} \\ &= \mathbb{F}v_i \vee \mathbb{F}v_j \\ &= A_i \vee A_j \end{aligned}$$

- $$\begin{aligned} A_{ij} &= \mathbb{F}(v_i - v_j) \\ &= \{x(v_i - v_j) \mid x \in \mathbb{F}\} \\ &= \{x(v_j - v_i) \mid x \in \mathbb{F}\} \\ &= \mathbb{F}(v_j - v_i) \\ &= A_{ji} \end{aligned}$$

- $(A_i \vee A_k) \wedge (A_{ij} \vee A_{jk}) = (\mathbb{F}v_i \vee \mathbb{F}v_k) \wedge (\mathbb{F}(v_i - v_j) \vee \mathbb{F}(v_j - v_k))$
$= \big(\{xv_i \mid x \in \mathbb{F}\} \cup \{yv_k \mid y \in \mathbb{F}\}\big) \cap$
$\big(\{z(v_i - v_j) \mid z \in \mathbb{F}\} \cup \{w(v_j - v_k) \mid w \in \mathbb{F}\}\big)$
$= \{xv_i + yv_k \mid x, y \in \mathbb{F}\} \cap \{zv_i + (w - z)v_j - wv_k \mid w, z \in \mathbb{F}\}$
$= \{x(v_i - v_k) \mid x \in \mathbb{F}\}$
$= \mathbb{F}(v_i - v_k)$
$= A_{ik}$

  sodass $\overline{A} = (A_{ij} \mid 1 \leq i, j \leq d)$ ein d-Rahmen von $L(\mathscr{H})$ ist.

e) Folgt aus d) und der Tatsache, dass für $L(\mathscr{H})$ eine Basis $\{v_1, \ldots, v_d\}$ existiert.

□

3.3.2 Weitere Hilfsmittel zum Beweis von Theorem 3.21

Die Verknüpfungen $\ominus$, $\oplus$ und $\otimes$, welche im folgenden Theorem definiert werden, erscheinen vorerst willkürlich. Sie sind jedoch motiviert durch Arbeiten von Descartes und Anderen, welcher die Subtraktion und Multiplikation von skalaren Größen geometrisch definierte. Vgl. dazu [4].

Fakt 3.17 Sei $\dim(\mathscr{H}) = 3$, $\overline{A}$ ein 3-Rahmen in $L(\mathscr{H})$ und $\{v_1, v_2, v_3\}$ die zugehörige Basis. Dann gibt es einen Isomorphismus $\Theta_{\overline{A}}$ zwischen $(\mathbb{F}, +, -, 0, \cdot, 1)$ und $(\mathscr{R}_{\overline{A}}, \oplus_{\overline{A}}, \ominus_{\overline{A}}, A_1, \otimes_{\overline{A}}, A_{12})$, wobei
$\mathscr{R}_{\overline{A}} := \{X \in L(\mathscr{H}) \mid X \cap A_2 = \mathbf{0},\ X + A_2 = A_1 + A_2\}$ und die Verknüpfungen folgendermaßen definiert sind:

$$\begin{aligned} P \ominus_{\overline{A}} Q &:= ([(Q_{13} + A_2) \cap (P + A_{23})] + A_3) \cap (A_1 + A_2) \\ \text{wobei} \quad Q_{13} &:= (Q + A_{23}) \cap (A_1 + A_3) \\ P \otimes_{\overline{A}} Q &:= (Q_{13} + P_{32}) \cap (A_1 + A_2) \\ \text{wobei} \quad P_{32} &:= (P + A_{13}) \cap (A_2 + A_3) \text{ und } Q_{13} \text{ wie oben} \\ P \oplus_{\overline{A}} Q &:= P \ominus_{\overline{A}} (A_1 \ominus_{\overline{A}} Q). \end{aligned}$$

Beweis: Sei $\Theta_{\overline{A}} : \mathbb{F} \to \mathscr{R}_{\overline{A}}$, $r \mapsto \mathbb{F}(v_1 - rv_2)$. Da v_1 und v_2 Basisvektoren, also insbesondere linear unabhängig sind, ist klar, dass $\Theta_{\overline{A}}$ injektiv ist.

Sei nun $X \in \mathscr{R}_{\overline{A}}$. Da $\dim(X + A_2) = \dim(A_1 + A_2) = 2$ gilt, folgt $1 \leq \dim(X) \leq 2$, und wegen $X \cap A_2 = \mathbf{0}$ folgt $\dim(X) = 1$. Damit lässt sich X schreiben als $X = \mathbb{F}(x_1v_1 + x_2v_2)$ für $x_1, x_2 \in \mathbb{F}$. Wäre $x_1 = 0$, so würde im Widerspruch zu den definierenden Eigenschaften eines 3-Rahmens $A_1 \subseteq A_2$ gelten. Also ist $x_1 \neq 0$, und es gilt $X = \mathbb{F}(x_1v_1 + x_2v_2) = \mathbb{F}(x_1v_1 + x_1x_1^{-1}x_2v_2) = \mathbb{F}(v_1 + x_1^{-1}x_2v_2) = \mathbb{F}(v_1 - (-x_1^{-1}x_2)v_2) = \Theta_{\overline{A}}(-x_1^{-1}x_2)$. Damit ist $\Theta_{\overline{A}}$ surjektiv.

Weiter gilt $\Theta_{\overline{A}}(0) = \mathbb{F}v_1 = A_1$ und $\Theta_{\overline{A}}(1) = \mathbb{F}(v_1 - v_2) = A_{12}$.

Seien $P = \mathbb{F}(v_1 - pv_2)$, $Q = \mathbb{F}(v_1 - qv_2) \in \mathscr{R}_{\overline{A}}$. Dann gilt

$$\begin{aligned} Q_{13} &= (Q + A_{23}) \cap (A_1 + A_3) \\ &= (\mathbb{F}(v_1 - qv_2) + \mathbb{F}(v_2 - v_3)) \cap (\mathbb{F}v_1 + \mathbb{F}v_3) \\ &= \{xv_1 - (xq + y)v_2 - yv_3 \mid x, y \in \mathbb{F}\} \cap \{zv_1 + wv_3 \mid z, w \in \mathbb{F}\} \\ &= \{xv_1 - xqv_3 \mid x \in \mathbb{F}\} \\ &= \mathbb{F}(v_1 - qv_3), \end{aligned}$$

sodass

$$\begin{aligned}
P \ominus_{\overline{A}} Q &= ([(Q_{13}+A_2)\cap(P+A_{23})]+A_3)\cap(A_1+A_2)\\
&= ([(\mathbb{F}(v_1-qv_3)+\mathbb{F}v_2)\cap(\mathbb{F}(v_1-pv_2)+\mathbb{F}(v_2-v_3))]+\mathbb{F}v_3)\cap(\mathbb{F}v_1+\mathbb{F}v_2)\\
&= ([\{xv_1+yv_2-xqv_3\,|\,x,y\in\mathbb{F}\}\cap\{zv_1-(zp+w)v_2-wv_3\,|\,z,w\in\mathbb{F}\}]+\mathbb{F}v_3)\cap(\mathbb{F}v_1+\mathbb{F}v_2)\\
&= (\{xv_1-x(p-q)v_2-xqv_3\,|\,x\in\mathbb{F}\}+\mathbb{F}v_3)\cap(\mathbb{F}v_1+\mathbb{F}v_2)\\
&= \{xv_1-x(p-q)v_2-(xq-y)v_3\,|\,x,y\in\mathbb{F}\}\cap\{zv_1-wv_2\,|\,z,w\in\mathbb{F}\}\\
&= \{xv_1-x(p-q)v_2\,|\,x\in\mathbb{F}\}\\
&= \mathbb{F}(v_1-(p-q)v_2)
\end{aligned}$$

folgt, und damit

$$\Theta_{\overline{A}}(p-q) = \Theta_{\overline{A}}(p)\ominus_{\overline{A}}\Theta_{\overline{A}}(q)$$

gilt. Weiter folgt

$$\begin{aligned}
\Theta_{\overline{A}}(p)\oplus_{\overline{A}}\Theta_{\overline{A}}(q) &\overset{Def.}{=} \Theta_{\overline{A}}(p)\ominus_{\overline{A}}(\Theta_{\overline{A}}(0)\ominus_{\overline{A}}\Theta_{\overline{A}}(q))\\
&= \Theta_{\overline{A}}(p)\ominus_{\overline{A}}\Theta_{\overline{A}}(0-q)\\
&= \Theta_{\overline{A}}(p)\ominus_{\overline{A}}\Theta_{\overline{A}}(-q)\\
&= \Theta_{\overline{A}}(p-(-q))\\
&= \Theta_{\overline{A}}(p+q)
\end{aligned}$$

und es gilt

$$\begin{aligned}
P_{32} &= (P+A_{13})\cap(A_2+A_3)\\
&= (\mathbb{F}(v_1-pv_2)+\mathbb{F}(v_1-v_3))\cap(\mathbb{F}v_2+\mathbb{F}v_3)\\
&= \{(x+y)v_1-xpv_2-yv_3\,|\,x,y\in\mathbb{F}\}\cap\{zv_2+wv_3\,|\,z,w\in\mathbb{F}\}\\
&= \mathbb{F}(pv_2-v_3),
\end{aligned}$$

sodass

$$\begin{aligned}
P\otimes_{\overline{A}} Q &= (Q_{13}+P_{32})\cap(A_1+A_2)\\
&= (\mathbb{F}(v_1-qv_3)+\mathbb{F}(pv_2-v_3))\cap(\mathbb{F}v_1+\mathbb{F}v_2)\\
&= \{xv_1+ypv_2-(xq+y)v_3\,|\,x,y\in\mathbb{F}\}\cap\{zv_1+wv_2\,|\,z,w\in\mathbb{F}\}\\
&= \{xv_1-xqpv_2\,|\,x\in\mathbb{F}\}\\
&= \mathbb{F}(v_1-(pq)v_2)
\end{aligned}$$

und damit

$$\Theta_{\overline{A}}(p\cdot q) = \Theta_{\overline{A}}(p)\otimes_{\overline{A}}\Theta_{\overline{A}}(q)$$

folgt. □

Korollar 3.18 Sei $\mathbb{F}=\mathbb{R}$ und $\mathscr{H}=\mathbb{R}^3$, sowie $\overline{A}$ ein 3-Rahmen. Dann gilt für beliebige P,Q aus $\mathscr{R}_{\overline{A}}$ wie oben und jede der Verknüpfungsarten $\ominus_{\overline{A}}$, $\oplus_{\overline{A}}$, $\otimes_{\overline{A}}$, dass alle Zwischenschritte der Berechnung entweder aus dem Schnitt zweier nicht miteinander übereinstimmenden Ebenen oder dem Spann zweier voneinander linear unabhängigen Vektoren besteht.

Beweis: Folgt durch erneutes Betrachten der Rechnungen im Beweis des Fakts 3.17. □

Bemerkung 3.19 Der vorherige Fakt 3.17 gilt allgemeiner für $\dim(\mathscr{H}) = d \geq 3$, einen d-Rahmen in $L(\mathscr{H})$ mit zugehöriger Basis $\{v_1, \ldots, v_d\}$, sowie für beliebige Indexkombinationen $i, j, k \in \{1, \ldots, d\}$ mit $i \neq j \neq k \neq i$.

Lemma 3.20 Für jedes $c \in \mathbb{N}$ gibt es einen Term t_c über $(1, +, \cdot)$ mit Länge $|t_c| \leq \mathcal{O}(\log c)$, dessen Auswertung in jedem Ring, der $\mathbb{N}$ enthält, c entspricht. Die Berechnung eines solchen Terms aus c ist möglich und benötigt (gemessen in der binären Länge von c) nur polynomiell viel Zeit.

Beweis: Behauptung: $|t_c| \leq 2 + 7\log_2(c)$. Dies wird mit Induktion gezeigt.
Für $c = 1$ gilt $t_1 = 1$, sodass $|t_1| = 1 \leq 2 + 7\log_2(1)$. Im Fall $c = 2$ gilt $t_2 = 1 + 1$, und damit $|t_2| = 3 \leq 2 + 7\log_2(2)$, und für $c = 3$ gilt $t_3 = 1 + 1 + 1$, sodass $|t_3| = 5 \leq 2 + 7\log_2(3)$ gilt.
Die Termlänge ändert sich in den obigen Fällen nicht, wenn die Terme in polnischer Notation dargestellt werden. In polnischer Notation werden jedoch keine Klammern benötigt, sodass die Terme $t_{2c} := (1 + 1) \cdot t_c$ und $t_{2c+1} := (1 + 1) \cdot t_{2c} + 1$ höchstens Länge $|t_c| + 7$ besitzen. Damit folgt

$$\begin{aligned} |t_{2c}| &\leq 7 + |t_c| \\ &\leq 7 + 2 + 7\log_2(c) \\ &= 2 + 7 \cdot \left(\log_2(2) + \log_2(c)\right) \\ &= 2 + 7\log_2(2c) \end{aligned}$$

sowie

$$\begin{aligned} |t_{2c+1}| &\leq 7 + |t_c| \\ &\leq 7 + 2 + 7\log_2(c) \\ &= 2 + 7\log_2(2c) \\ &\leq 2 + 7\log_2(2c + 1). \end{aligned}$$

□

3.3.3 Vollständigkeit einiger der betrachteten Erfüllbarkeitsprobleme

Theorem 3.21 SAT_{3^p} ist $BP\left(\mathscr{NP}^0_{\mathbb{R}}\right)$-vollständig.

Beweis: Der folgende Beweis nutzt große Teile der Reduktion von $\mathrm{FEAS}_{\mathbb{Z},\mathbb{F}}$ auf $\mathrm{SAT}_{L(\mathscr{H})}$ aus [4] im Spezialfall $\mathbb{F} = \mathbb{R}$ und $d = 3$, d.h. $\mathscr{H} = \mathbb{R}^3$, $\wedge$ entspricht dem Schnitt, $\vee$ entspricht dem Spann, und zeigt $\mathrm{FEAS}_{\mathbb{Z},\mathbb{R}} \leq_P \mathrm{SAT}_{3^p}$.
Die Grundidee des 2. Teils des Beweises sind die Beziehungen $\mathbb{R}a \vee \mathbb{R}b = (a \times b)^\perp$ und $a^\perp \wedge b^\perp = \mathbb{R}(a \times b)$ für linear unabhängige $a, b \in \mathbb{R}^3$, welche aus [3] entnommen wurden.

Sei $\langle p_1, \ldots, p_k \rangle$, d.h. die Kodierung von k Polynomen in n Variablen mit Koeffizienten aus $\mathbb{Z}$, deren gemeinsame Nullstelle in $\mathbb{R}$ gesucht ist, gegeben. Dann soll die Turingmaschine diese Polynome folgendermaßen in Kreuzprodukt-Terme umformulieren:

i) Ersetze alle Koeffizienten der Polynome durch einen Ausdruck über $1, +, -, \cdot$. Dies ist möglich, da diese nach Voraussetzung natürliche Zahlen sind.

ii) Ersetze in den umgeformten Termen die Konstanten 0 und 1 durch A_1 bzw. A_{12}, sowie alle Verknüpfungen $+, -, \cdot$ durch $\oplus_{\bar{A}}, \ominus_{\bar{A}}, \otimes_{\bar{A}}$.

iii) Ergänze die so erhaltenen Verbandsterme $t_j\left(X_1,\ldots,X_n,\overline{A}\right)$ zu Verbandsgleichungen $t_j\left(X_1,\ldots,X_n,\overline{A}\right)=A_1$.

iv) Füge für jede Variable X_i die Bedingungen $X_i \wedge A_2 = \mathbf{0}$ und $X_i \vee A_2 = A_1 \vee A_2$

v) sowie für $\overline{A}$ die definierenden Eigenschaften eines 3-Rahmens hinzu.

vi) Ersetze nun die definierenden Eigenschaften des 3-Rahmens

$$
\begin{array}{lrcll}
(I) & \mathbf{1} & = & A_1 \vee A_2 \vee A_3 & \\
(II) & \mathbf{0} & = & A_i \wedge \bigvee_{j\neq i} A_j & \text{für alle } i \in \{1,2,3\} \\
(III) & \mathbf{0} & = & A_i \wedge A_{ij} & \text{für alle } i,j \in \{1,2,3\} \text{ mit } i \neq j \\
(IV) & A_i \vee A_j & = & A_i \vee A_{ij} & \text{für alle } i,j \in \{1,2,3\} \text{ mit } i \neq j \\
(V) & A_{ij} & = & A_{ji} & \text{für alle } i,j \in \{1,2,3\} \text{ mit } i \neq j \\
(VI) & A_{ik} & = & (A_i \vee A_k) \wedge (A_{ij} \vee A_{jk}) & \text{für alle } i,j,k \in \{1,2,3\} \text{ mit } i \neq j \neq k \neq i
\end{array}
$$

durch

$$
\begin{array}{lrcl}
 & A_1 \times A_2 & = & C_3 \\
(I') & A_2 \times A_3 & = & C_1 \\
 & A_1 \times A_3 & = & C_2
\end{array}
$$

$$
\begin{array}{lrcl}
 & C_1 \times C_2 & = & C_4 \\
(II') & C_1 \times C_3 & = & C_5 \\
 & C_2 \times C_3 & = & C_6
\end{array}
$$

$$
(III') \quad A_i \times A_j = A_i \times A_{ij} \qquad \text{für alle } i,j \in \{1,2,3\} \text{ mit } i \neq j
$$

$$
\begin{array}{lrcll}
(IV') & A_{ij} & = & A_{ji} & \text{für alle } i,j \in \{1,2,3\} \text{ mit } i \neq j \\
(V') & D_{ik} & = & A_i \times A_k & \text{für alle } i,k \in \{1,2,3\} \text{ mit } i \neq k \\
(VI') & D_{ijjk} & = & A_{ij} \times A_{jk} & \text{für alle } i,j,k \in \{1,2,3\} \text{ mit } i \neq j \neq k \neq i \\
(VII') & A_{ik} & = & D_{ik} \times D_{ijjk} & \text{für alle } i,j,k \in \{1,2,3\} \text{ mit } i \neq j \neq k \neq i
\end{array}
$$

vii) und die Bedingungen für die Variablen aus Unterpunkt iv) durch

$$
X_i \times A_2 = A_1 \times A_2 \qquad \text{für alle } i \in \{1,\ldots,n\}.
$$

viii) Ersetze in den Verbandsgleichungen aus iii) alle Verknüpfungen $\vee$ und $\wedge$ durch ein Kreuzprodukt. Dabei wird die Klammerung der Terme nicht verändert.

Alle diese Schritte sind von einer Turingmaschine in polynomieller Zeit (gemessen in der binären Länge aller Polynome p_j) berechenbar.
Zunächst erscheinen die in den Unterpunkten iv) und v) hinzugefügten Gleichungen überflüssig, da sie in den Schritten vi) und vii) sofort wieder ersetzt werden. Ein entscheidender Teil des folgenden Beweises der Erfüllbarkeitsäquivalenz nutzt jedoch diese Zwischenschritte aus.

" $\Rightarrow$ "
Sei $(p_1(X_1,\ldots,X_n),\ldots,p_k(X_1,\ldots,X_n)) \in \mathrm{FEAS}_{\mathbb{Z},\mathbb{R}}$, d.h. es gibt $x_1,\ldots,x_n \in \mathbb{R}$, sodass $p_1(x_1,\ldots,x_n) = \ldots = p_k(x_1,\ldots,x_n) = 0$ gilt.
Nach Fakt 3.16e) gibt es einen 3-Rahmen $\overline{a} = (a_1,a_2,a_3,a_{12},a_{13},a_{23},a_{21},a_{31},a_{32})$ in $L\left(\mathbb{R}^3\right)$, sodass v) erfüllbar ist. Mit struktureller Induktion und Fakt 3.17 folgt

$$t_j(\Theta_{\overline{a}}(x_1),\ldots,\Theta_{\overline{a}}(x_n)) = \Theta_{\overline{a}}(p_j(x_1,\ldots,x_n)),$$

sodass eine gemeinsame Nullstelle $x_1,\ldots,x_n \in \mathbb{R}$ zu einer Belegung $x_1',\ldots,x_n' \in L\left(\mathbb{R}^3\right)$ mit $x_i' := \Theta_{\overline{a}}(x_i)$ führt, und wegen $\Theta_{\overline{a}}(0) = a_1$ ist dies (zusammen mit $\overline{a}$) eine erfüllende Belegung für die Gleichungen, die in den Unterpunkten i) bis v) konstruiert werden.
Zur Vereinheitlichung der Notation sei der obige 3-Rahmen nun mit $\overline{a}' = (a_1',a_2',a_3',a_{12}',a_{13}',a_{23}',a_{21}',a_{31}',a_{32}')$ bezeichnet, da es sich um Elemente aus $L\left(\mathbb{R}^3\right)$ handelt. Alle Elemente aus $\mathbb{R}$ seien ohne weitere Markierung, Elemente aus $\mathbb{R}^3$ mit einem * gekennzeichnet.
Sei also $\overline{a}'$ zusammen mit $x_1',\ldots,x_n'$ eine erfüllende Belegung für die in i) bis v) konstruierten Gleichungen. Nach 3.13d) und 3.16a), c) gilt

$$3 = \dim\left(\mathbb{R}^3\right) = 3\cdot\dim(a_i') = 3\cdot\dim(a_{ij}') \qquad \text{für alle } i,j\in\{1,2,3\},\ i\neq j,$$

sodass

$$\dim(a_i') = \dim(a_{ij}') = 1 \qquad \text{für alle } i,j\in\{1,2,3\},\ i\neq j$$

gilt, d.h. a_i' und a_{ij}' sind für alle $i,j\in\{1,2,3\}$ und $i\neq j$ eindimensionale Unterräume. Da alle x_i' mit $i\in\{1,\ldots,n\}$ die Gleichungen aus iv) erfüllen, folgt

$$x_i' \subseteq a_1'\vee a_2',$$

und mit

$$x_i'\wedge a_2' = \mathbf{0}$$

folgt

$$\dim(x_i') = 1,$$

sodass auch x_i' für alle $i\in\{1,\ldots,n\}$ eindimensionale Unterräume sind. Damit gibt es für alle $i,j\in\{1,2,3\}$ mit $i\neq j$ Elemente a_i^*, a_{ij}^* und $x_1^*,\ldots,x_n^*$ aus $\mathbb{R}^3$, sodass $a_i' = \mathbb{R}a_i^*$, $a_{ij}' = \mathbb{R}a_{ij}^*$ und $x_1' = \mathbb{R}x_1^*,\ldots,x_n' = \mathbb{R}x_n^*$ gilt.

- Aus (I) folgt, dass $\{a_1^*,a_2^*,a_3^*\}$ linear unabhängig sind. Damit folgt

  $$a_1^*\times a_2^*\neq 0,\quad a_2^*\times a_3^*\neq 0,\quad a_1^*\times a_3^*\neq 0,$$

  sodass die Gleichungen in (I') über $\mathbb{P}^2$ von der Belegung a_i^* mit $i\in\{1,2,3\}$, a_{ij}^* mit $i,j\in\{1,2,3\}$, $i\neq j$ und $c_3^* := a_1^*\times a_2^*$, $c_1^* := a_2^*\times a_3^*$, $c_2^* := a_1^*\times a_3^*$ erfüllt werden.

- Sei $0 = \lambda\left(a_1^*\times a_2^*\right) + \mu\left(a_2^*\times a_3^*\right) + \nu\left(a_1^*\times a_3^*\right)$. Durch Bilden des Skalarprodukts mit a_3^* folgt

  $$\begin{aligned} 0 &= \langle a_3^*, \lambda\left(a_1^*\times a_2^*\right) + \mu\left(a_2^*\times a_3^*\right) + \nu\left(a_1^*\times a_3^*\right)\rangle \\ &= \lambda\langle a_3^*, a_1^*\times a_2^*\rangle + \mu\underbrace{\langle a_3^*, a_2^*\times a_3^*\rangle}_{=0} + \nu\underbrace{\langle a_3^*, a_1^*\times a_3^*\rangle}_{=0} \\ &= \lambda\cdot\underbrace{\det\left(a_1^*,a_2^*,a_3^*\right)}_{\neq 0}, \end{aligned}$$

sodass $\lambda = 0$ gilt. Analog zeigt man $\mu = \nu = 0$. Insgesamt folgt, dass $\{a_1^* \times a_2^*, a_2^* \times a_3^*, a_1^* \times a_3^*\}$ linear unabhängig ist, sodass

$$\left(a_1^* \times a_2^*\right) \times \left(a_2^* \times a_3^*\right) \neq 0, \quad \left(a_1^* \times a_2^*\right) \times \left(a_1^* \times a_3^*\right) \neq 0, \quad \left(a_2^* \times a_3^*\right) \times \left(a_1^* \times a_3^*\right) \neq 0$$

gilt und a_i^* mit $i \in \{1,2,3\}$, a_{ij}^* mit $i,j \in \{1,2,3\}$, $i \neq j$ sowie den oben definierten c_1^*, c_2^*, c_3^* und $c_4^* := c_1^* \times c_2^*$, $c_5^* := c_1^* \times c_3^*$, $c_6^* := c_2^* \times c_3^*$ eine erfüllende Belegung für die Gleichungen aus (II') über $\mathbb{P}^2$ ist.

- Mit (IV) folgt $\text{span}\{a_i^*, a_j^*\} = \text{span}\{a_i^*, a_{ij}^*\}$. Damit gibt es $\lambda, \mu \in \mathbb{R}$, sodass $a_{ij}^* = \lambda \cdot a_i^* + \mu \cdot a_j^*$ gilt. Es folgt

$$\begin{aligned} a_i^* \times a_{ij}^* &= a_i^* \times \left(\lambda \cdot a_i^* + \mu \cdot a_j^*\right) \\ &= \lambda \cdot \underbrace{\left(a_i^* \times a_i^*\right)}_{=0} + \mu \cdot \left(a_i^* \times a_j^*\right) \\ &= \mu \cdot \left(a_i^* \times a_j^*\right), \end{aligned}$$

  und wegen der linearen Unabhängigkeit von $\{a_i^*, a_{ij}^*\}$ sind diese Kreuzprodukte nicht 0, sodass die obige Wahl der a_i^* und a_{ij}^* eine erfüllende Belegung der Gleichungen aus (III') über $\mathbb{P}^2$ ist.

- Die Gleichungen aus (IV') entsprechen genau den Gleichungen aus (V), sodass die obige Belegung der Variablen auch diese Gleichungen über $\mathbb{P}^2$ erfüllt.

- Die Gleichungen aus (V') sind eine Wiederholung der Gleichungen aus (I'), wobei in (V') zur Vereinfachung der Schreibweise des restlichen Beweises eine andere Indexbezeichnung gewählt wurde.

- Angenommen, $\{a_{ij}^*, a_{jk}^*\}$ wäre linear abhängig für $i \neq j \neq k \neq i$. Wegen (IV) gilt $a_{ij}^* \subseteq \text{span}\{a_i^*, a_j^*\}$, $a_{jk}^* \subseteq \text{span}\{a_j^*, a_k^*\}$. Damit würde $a_{ij}^*, a_{jk}^* \in \text{span}\{a_i^*, a_j^*\} \cap \text{span}\{a_j^*, a_k^*\}$ folgen. Da $\{a_1^*, a_2^*, a_3^*\}$ linear unabhängig ist, gilt $\text{span}\{a_i^*, a_j^*\} \cap \text{span}\{a_j^*, a_k^*\} = \text{span}\{a_j\}$, sodass dann $\{a_j^*, a_{ij}^*\}$ linear abhängig wäre. Dies widerspricht (III).
  Also ist $\{a_{ij}^*, a_{jk}^*\}$ linear unabhängig, $a_{ij}^* \times a_{jk}^* \neq 0$ und die Gleichungen aus (VI') werden von der gewählten Belegung und $d_{ijjk}^* := a_{ij}^* \times a_{jk}^*$ über $\mathbb{P}^2$ erfüllt.

- Angenommen, $\{a_i^* \times a_k^*, a_{ij}^* \times a_{jk}^*\}$ wäre linear abhängig, d.h. $\mathbb{R}\left(a_i^* \times a_k^*\right) = \mathbb{R}\left(a_{ij}^* \times a_{jk}^*\right)$. Dann würde

$$\begin{aligned} a'_{ij} &= \mathbb{R} a_{ij}^* \\ &\subseteq \left(\mathbb{R}\left(a_{ij}^* \times a_{jk}^*\right)\right)^\perp \\ &= \left(\mathbb{R}\left(a_i^* \times a_k^*\right)\right)^\perp \\ &= a'_i \vee a'_k \end{aligned}$$

  folgen, sodass

$$\begin{aligned} a'_i \vee a'_j &\overset{(IV)}{=} a'_i \vee a'_{ij} \\ &\subseteq a'_i \vee \left(a'_i \vee a'_k\right) \\ &= \left(a'_i \vee a'_i\right) \vee a'_k \\ &= a'_i \vee a'_k \end{aligned}$$

und damit

$$\begin{aligned}\mathbb{R}^3 &= a_i' \vee a_j' \vee a_k' \\ &\subseteq a_i' \vee a_k' \vee a_k' \\ &= a_i \vee a_k'\end{aligned}$$

gelten würde, was ein offensichtlicher Widerspruch zu (I) und (II) ist.
Also ist $\{a_i^* \times a_k^*, a_{ij}^* \times a_{jk}^*\}$ linear unabhängig, sodass $d_{ik}^* \times d_{ijjk}^* \neq 0$ gilt.
Weiter folgt

$$\begin{aligned}a_i^* \times a_k^* &\in \left(\operatorname{span}\{a_i^*, a_k^*\}\right)^\perp \\ &\subseteq \left(\operatorname{span}\{a_i^*, a_k^*\} \cap \operatorname{span}\{a_{ij}^*, a_{jk}^*\}\right)^\perp \\ &= \left(\left(a_i' \vee a_k'\right) \wedge \left(a_{ij}' \vee a_{jk}'\right)\right)^\perp \\ &\overset{(VI)}{=} \left(a_{ik}'\right)^\perp.\end{aligned}$$

Analog ist

$$a_{ij}^* \times a_{jk}^* \in \left(a_{ik}'\right)^\perp,$$

sodass

$$\operatorname{span}\{a_i^* \times a_k^*, a_{ij}^* \times a_{jk}^*\} \subseteq \left(a_{ik}'\right)^\perp$$

gilt. Mit

$$\dim\left(\left(a_{ik}'\right)^\perp\right) = 2 = \dim\left(\operatorname{span}\{a_i^* \times a_k^*, a_{ij}^* \times a_{jk}^*\}\right)$$

gilt sogar Gleichheit, sodass mit der linearen Unabhängigkeit von $\{a_i^* \times a_k^*, a_{ij}^* \times a_{jk}^*\}$

$$\begin{aligned}\mathbb{R}\, a_{ik}^* &= a_{ik}' \\ &= \left(\operatorname{span}\{a_i^* \times a_k^*, a_{ij}^* \times a_{jk}^*\}\right)^\perp \\ &= \mathbb{R}\left(\left(a_i^* \times a_k^*\right) \times \left(a_{ij}^* \times a_{jk}^*\right)\right) \\ &= \mathbb{R}\left(d_{ik}^* \times d_{ijjk}^*\right)\end{aligned}$$

folgt. Also erfüllt die gewählte Belegung die Gleichungen aus (VII') über $\mathbb{P}^2$.

- Aus den Gleichungen in iv) folgt, dass $\{x_i^*, a_2^*\}$ linear unabhängig ist, und es gilt

$$\operatorname{span}\{x_i^*, a_2^*\} = \operatorname{span}\{a_1^*, a_2^*\}.$$

Also gibt es $\lambda, \mu \in \mathbb{R}$, sodass $x_i^* = \lambda \cdot a_1^* + \mu \cdot a_2^*$ gilt. Damit folgt

$$\begin{aligned}0 &\neq x_i^* \times a_2^* \\ &= \left(\lambda \cdot a_1^* + \mu \cdot a_2^*\right) \times a_2^* \\ &= \lambda \cdot \left(a_1^* \times a_2^*\right) + \mu \cdot \underbrace{\left(a_2^* \times a_2^*\right)}_{=0} \\ &= \lambda \cdot \left(a_1^* \times a_2^*\right),\end{aligned}$$

sodass diese Belegung auch für die Gleichungen aus vii) über $\mathbb{P}^2$ eine erfüllende Belegung ist.

- Nach Korollar 3.18 gilt für die Terme aus ii), dass in jedem Zwischenschritt entweder der Spann zweier eindimensionaler Unterräume oder der Schnitt zweier zweidimensionaler Unterräume, die jeweils nicht miteinander übereinstimmen, gebildet wird. Durch Ergänzen der Terme zu Gleichungen in iii) wird dies nicht verändert, sodass dies für die gewählte erfüllende Belegung $\overline{a}', x_1', \ldots, x_n'$ gilt.
  Im ersten Fall kann also das Kreuzprodukt der Vektoren aus $\mathbb{R}^3$, welche die eindimensionalen Unterräume repräsentieren, gebildet werden, und dies ergibt einen auf dem Spann der Unterräume senkrecht stehenden Vektor, also einen Repräsentanten des Senkrechtraums des Spanns.
  Da alle zur erfüllenden Belegung gehörenden Unterräume eindimensional sind, kann der zweite Fall nur dann eintreten, wenn die nun zu schneidenden zweidimensionalen Unterräume jeweils durch den vorherigen Aufspann zweier eindimensionaler Unterräume entstanden sind. Damit wird nun also das Kreuzprodukt zweier Vektoren gebildet, die jeweils im Senkrechtraum des entsprechenden zweidimensionalen Teilraums liegen. Nachdem diese Unterräume nicht übereinstimmen, sind die entsprechenden Vektoren linear unabhängig, sodass das gebildete Kreuzprodukt nicht verschwindet. Analog dazu, dass die gewählte Belegung eine erfüllende Belegung für die Gleichungen in (VII') ist, zeigt man, dass der durch dieses Kreuzprodukt entstandene Vektor im Schnitt beider Unterräume liegt und somit wieder ein möglicher Repräsentant des entstandenen eindimensionalen Unterraums ist.
  Damit folgt iterativ, dass die obige Belegung auch alle Kreuzproduktgleichungen aus viii) erfüllt.

Insgesamt gibt es also eine über $\mathbb{P}^2$ erfüllende Belegung für alle in vi) bis viii) erstellten Gleichungen, d.h. $f(p_1(X_1,\ldots,X_n),\ldots,p_k(X_1,\ldots,X_n)) \in \mathrm{SAT}_{3^p}$.

"$\Leftarrow$"
Sei nun $f(p_1(X_1,\ldots,X_n),\ldots,p_k(X_1,\ldots,X_n)) \in \mathrm{SAT}_{3^p}$, d.h. es gibt eine erfüllende Belegung für alle Gleichungen, die in vi) bis viii) konstruiert wurden, wenn man diese projektiv betrachtet. Sei $x_1^*,\ldots,x_n^*,a_i^*,a_{ij}^*,c_1^*,\ldots,c_6^*$ sowie d_{ik}^* und d_{ijjk}^* für alle $i,j,k \in \{1,2,3\}$ mit $i \neq j \neq k \neq i$ aus $\mathbb{R}^3\backslash\{0\}$ ein Teil einer solchen erfüllenden Belegung, und $x_1' := \mathbb{R}x_1^*,\ldots,x_n' := \mathbb{R}x_n^*, a_i' := \mathbb{R}a_i^*, a_{ij}' := \mathbb{R}a_{ij}^*$, $c_1' := \mathbb{R}c_1^*,\ldots,c_6' := \mathbb{R}c_6^*$ sowie $d_{ik}' := \mathbb{R}d_{ik}^*$ und $d_{ijjk}' := \mathbb{R}d_{ijjk}^*$ für alle $i,j,k \in \{1,2,3\}$ mit $i \neq j \neq k \neq i$.

- Aus (I') folgt, dass $\{a_1^*, a_2^*\}$, $\{a_1^*, a_3^*\}$ und $\{a_2^*, a_3^*\}$ linear unabhängig sind. Angenommen, $\{a_1^*, a_2^*, a_3^*\}$ wäre linear abhängig. Dann gibt es $\lambda,\mu \in \mathbb{R}\backslash\{0\}$, sodass $a_3^* = \lambda \cdot a_1^* + \mu \cdot a_2^*$ gilt, und es folgt

$$\begin{aligned} a_1^* \times a_3^* &= a_1^* \times \left(\lambda \cdot a_1^* + \mu \cdot a_2^*\right) \\ &= \lambda \cdot \underbrace{\left(a_1^* \times a_1^*\right)}_{=0} + \mu \cdot \left(a_1^* \times a_2^*\right) \\ &= \mu \cdot \left(a_1^* \times a_2^*\right), \end{aligned}$$

  d.h. $\{a_1^* \times a_3^*, a_1^* \times a_2^*\}$ ist linear abhängig, sodass $[c_2^*] = [c_3^*]$ gilt, im Widerspruch (II'). Also ist $\{a_1^*, a_2^*, a_3^*\}$ linear unabhängig, und es gilt

$$\mathbb{R}^3 = a_1' \vee a_2' \vee a_3'$$

  sowie

$$\mathbf{0} = a_i' \wedge \bigvee_{j \neq i} a_j' \qquad \text{für alle } i,j \in \{1,2,3\}.$$

  Damit ist a_1', a_2', a_3' eine erfüllende Belegung für (I) und (II).

- Aus (III') folgt, dass $\{a_i^*, a_{ij}^*\}$ linear unabhängig ist. Also gilt

$$\begin{aligned} a_i' \wedge a_{ij}' &= \mathbb{R}a_i^* \wedge \mathbb{R}a_{ij}^* \\ &= \mathbf{0}. \end{aligned}$$

  Weiter folgt aus (III')

$$\begin{aligned} a_i' \vee a_j' &= \mathbb{R}a_i^* \vee \mathbb{R}a_j^* \\ &= \left(\mathbb{R}\left(a_i^* \times a_j^*\right)\right)^\perp \\ &= \left(\mathbb{R}\left(a_i^* \times a_{ij}^*\right)\right)^\perp \\ &= \mathbb{R}a_i^* \vee \mathbb{R}a_{ij}^* \\ &= a_i' \vee a_{ij}', \end{aligned}$$

  sodass a_i', a_{ij}' $(i, j \in \{1,2,3\}, i \neq j)$ auch die Gleichungen aus (III) und (IV) erfüllen.

- Da nach (IV') $a_{ij}^* = a_{ji}^*$ gilt, folgt trivialerweise $a_{ij}' = \mathbb{R}a_{ij}^* = \mathbb{R}a_{ji}^* = a_{ji}'$, sodass auch die Gleichungen aus (V) erfüllt werden.

- Aus (V'), (VI') und (VII') folgt

$$\begin{aligned} a_{ik}' &= \mathbb{R}a_{ik}^* \\ &= \mathbb{R}\left(d_{ik}^* \times d_{ijjk}^*\right) \\ &= \left(\mathbb{R}d_{ik}^* \vee \mathbb{R}d_{ijjk}^*\right)^\perp \\ &= \left(\mathbb{R}d_{ik}^*\right)^\perp \wedge \left(\mathbb{R}d_{ijjk}^*\right)^\perp \\ &= \left(\mathbb{R}\left(a_i^* \times a_k^*\right)\right)^\perp \wedge \left(\mathbb{R}\left(a_{ij}^* \times a_{jk}^*\right)\right)^\perp \\ &= \left(\mathbb{R}a_i^* \vee \mathbb{R}a_k^*\right) \wedge \left(\mathbb{R}a_{ij}^* \vee \mathbb{R}a_{jk}^*\right) \\ &= \left(a_i' \vee a_k'\right) \wedge \left(a_{ij}' \vee a_{jk}'\right). \end{aligned}$$

  Also ist die gewählte Belegung auch eine erfüllende Belegung für die Gleichungen aus (VI).

- Nach vii) gilt $[x_i^* \times a_2^*] = [a_1^* \times a_2^*]$. Es folgt

$$\begin{aligned} x_i' \vee a_2' &= \mathbb{R}x_i^* \vee \mathbb{R}a_2^* \\ &= \left(\mathbb{R}\left(x_i^* \times a_2^*\right)\right)^\perp \\ &= \left(\mathbb{R}\left(a_1^* \times a_2^*\right)\right)^\perp \\ &= \mathbb{R}a_1^* \vee \mathbb{R}a_2^* \\ &= a_1' \vee a_2'. \end{aligned}$$

  Weiter ist $\{x_i^*, a_2^*\}$ linear unabhängig, sodass

$$\begin{aligned} x_i' \wedge a_2' &= \mathbb{R}x_i^* \wedge \mathbb{R}a_2^* \\ &= \mathbf{0} \end{aligned}$$

  gilt. Damit sind auch die Gleichungen aus iv) von der gewählen Belegung erfüllt.

- Nach Korollar 3.18 wechseln sich die Verknüpfungen $\vee$ und $\wedge$ in den Termgleichungen, aus denen die Kreuzproduktgleichungen gebildet wurden, (gemäß der Reihenfolge, in der sie ausgeführt werden) ab. Hierbei wird die Verknüpfung $\wedge$ nur auf zwei Teilterme angewendet, die als $t_1 \vee t_2$ geschrieben werden können, wobei t_1, t_2 entweder wieder Terme oder aber Variablen sind.
  Da die Klammerung bei der Berechnung der Kreuzproduktgleichungen aus den Verbandsgleichungen nicht verändert wurde, kann man die Kreuzproduktzeichen in zwei Klassen einteilen; solche, welche die Verknüpfung $\vee$ ersetzt haben, und solche, welche die Verknüpfung $\wedge$ ersetzt haben, und diese wechseln sich weiterhin gemäß der Reihenfolge, in der sie ausgeführt werden, ab. Zur Vereinfachung der Schreibweise werden diese nun mit $\times_\vee$ bzw. $\times_\wedge$ bezeichnet.
  Im ersten Fall sind die Vektoren, deren Kreuzprodukt gebildet werden soll, linear unabhängig, da sonst die gesamte Kreuzproduktgleichung im Widerspruch dazu, dass es sich um eine erfüllende Belegung handelt, null wird. Also sind die eindimensionalen Unterräume, die sie repräsentieren, verschieden, und deren Spann ist zweidimensional. Weiter steht dieser senkrecht auf dem eindimensionalen Unterraum, welcher durch den Vektor, der durch Bilden des Kreuzproduktes entstanden ist, repräsentiert wird.
  Im zweiten Fall wird das Kreuzprodukt zweier Vektoren gebildet, die wiederum jeweils durch das Bilden eines Kreuzproduktes entstanden sind, wobei es sich bei diesen um $\times_\vee$-Kreuzprodukte handelt. Sie repräsentieren also jeweils einen eindimensionalen Unterraum, der senkrecht auf dem zweidimensionalen Unterraum steht, deren Schnitt nun gebildet werden soll. Da das Kreuzprodukt nicht null wird, sind die Vektoren linear unabhängig, und somit stimmen diese zweidimensionalen Unterräume nicht überein. Damit ist der Schnitt der Unterräume wieder eindimensional, und analog dazu, dass die gewählte Belegung eine erfüllende Belegung für die Gleichungen in (VI) ist, folgt, dass das Kreuzprodukt der beiden Vektoren in diesem Unterraum liegt, also ein Repräsentant für diesen eindimensionalen Unterraum ist.
  Damit folgt iterativ, dass $\overline{a}', x_1', \ldots, x_n'$ eine erfüllende Belegung für die Verbandsgleichungen aus iii) ist.

Insgesamt gilt also, dass $\overline{a}'$ ein 3-Rahmen und $\overline{a}', x_1', \ldots, x_n'$ eine erfüllende Belegung für alle Verbandsgleichungen $t_1(X_1, \ldots, X_n, \overline{A}) = A_1, \ldots, t_k(X_1, \ldots, X_n, \overline{A}) = A_1$ ist, wobei $x_1', \ldots, x_n'$ wegen der Bedingungen aus iv) Elemente aus $\mathscr{R}_{\overline{A}}$ sind.
Mit Fakt 3.17 und struktureller Induktion folgt dann für alle $j \in \{1, \ldots, k\}$

$$\Theta_{\overline{a}'}^{-1}(t_j(x_1', \ldots, x_n') = \Theta_{\overline{a}'}^{-1}(t_j(\Theta_{\overline{a}'}(x_1), \ldots, \Theta_{\overline{a}'}(x_n)) = \Theta_{\overline{a}'}^{-1}(\Theta_{\overline{a}'}(p_j(x_1, \ldots, x_n))) = p_j(x_1, \ldots, x_n),$$

sodass

$$0 = \Theta_{\overline{a}'}^{-1}(a_1') = \Theta_{\overline{a}'}^{-1}(t_j(x_1', \ldots, x_n')) = p_j(x_1, \ldots, x_n)$$

gilt, d.h. die Polynome $p_1(X_1, \ldots, X_n), \ldots, p_k(X_1, \ldots, X_n)$ besitzen eine gemeinsame Nullstelle.
Damit gilt $(p_1(X_1, \ldots, X_n), \ldots, p_k(X_1, \ldots, X_n)) \in \mathrm{FEAS}_{\mathbb{Z},\mathbb{R}}$.

□

Korollar 3.22 Damit sind auch SAT_{4^p} und SAT_{5^p} sowie SAT_3, SAT_4 und SAT_5 $BP\left(\mathscr{NP}_{\mathbb{R}}^0\right)$-vollständig.

Beweis: Die Aussage folgt aus den Propositionen 2.2 und 2.3 sowie Theorem 2.7. □

Korollar 3.23 Es gibt einen Kreuzprodukt-Term, der über $\mathbb{R}^3$, aber nicht über $\mathbb{Q}^3$ erfüllbar ist.

Beweis: Das Polynom $p(X) := X^2 - 2$, dessen Koeffizienten in $\mathbb{Z}$ liegen, besitzt die Nullstellen $\sqrt{2}$ und $-\sqrt{2}$ aus $\mathbb{R}\backslash\mathbb{Q}$. Mit der Reduktionsfunktion aus Theorem 3.21 kann man dieses Polynom in einen Kreuzprodukt-Term umformen, der in $\mathbb{R}^3$, aber nicht in $\mathbb{Q}^3$ erfüllbar ist. □

Ausblick

Im Rahmen dieser Arbeit wurde die Komplexität von Kreuzprodukt-Term über $\mathbb{R}^3$ bzw. $\mathbb{P}^2$ untersucht, wobei gezeigt wurde, dass SAT_{3^P} und somit auch SAT_{4^P}, SAT_{5^P}, SAT_3, SAT_4 und SAT_5 $BP\left(\mathcal{NP}^0_{\mathbb{R}}\right)$-vollständig sind. Es bleibt zu untersuchen, ob auch SAT_{1^P}, SAT_{2^P}, $SAT_{2^{P*}}$, SAT_1 und SAT_2 vollständig bezüglich dieser Komplexitätsklasse sind.
Es ist bekannt, dass sich Kreuzprodukte nur in $\mathbb{R}^3$ und $\mathbb{R}^7$ definieren lassen, wobei dies in $\mathbb{R}^3$ eindeutig ist, während es in $\mathbb{R}^7$ verschiedene Möglichkeiten für eine sinnvolle Definition gibt. Vgl. [5].
Definiert man nun die Erfüllbarkeitsprobleme von Kreuzprodukt-Termen über $\mathbb{R}^7$ und $\mathbb{P}^6$ analog zu den Erfüllbarkeitsproblemen über $\mathbb{R}^3$ und $\mathbb{P}^2$ (wobei ein „Kreuzprodukt“ über $\mathbb{P}^6$ analog zu dem „Kreuzprodukt“ über $\mathbb{P}^2$ durch die Äquivalenzklasse des Kreuzproduktes zweier Repräsentanten der Punkte aus $\mathbb{P}^6$, deren „Kreuzprodukt“ gebildet werden soll, definiert wird), so wäre zu untersuchen, ob sich die gefundenen Reduktionen aus Kapitel 2 übertragen lassen.
Desweiteren stellt sich die Frage, ob es Beziehungen zwischen den Erfüllbarkeitsproblemen über $\mathbb{R}^7$ und $\mathbb{R}^3$ sowie $\mathbb{P}^6$ und $\mathbb{P}^2$ (oder $\mathbb{R}^3$ und $\mathbb{P}^6$ bzw. $\mathbb{R}^7$ und $\mathbb{P}^2$) gibt, d.h. ob auch hier Reduktionen zwischen Erfüllbarkeitsproblemen über verschiedenen Räumen möglich sind, und falls ja, um welche der verschiedenen Erfüllbarkeitsprobleme es sich hierbei handelt.
Weiter kann untersucht werden, ob auch diese Erfüllbarkeitsprobleme in $BP\left(\mathcal{NP}^0_{\mathbb{R}}\right)$ liegen, und ob auch hier einige oder eventuell alle der Erfüllbarkeitsprobleme vollständig bezüglich dieser Komplexitätsklasse sind.

Quellenangaben

[1] Leonore Blum, Felipe Cucker, Mike Shub und Steve Smale, *Complexity and Real Computation*, Springer Verlag New York, 1998.

[2] Leonore Blum, Mike Shub und Steve Smale, *On a Theory of Computation and Complexity over the Real Numbers: NP-Completeness, Recursive Functions and Universal Machines*, Bulletin (New Series) of the American Mathematical Society, Volume 21, Number 1, July 1989.

[3] Hans Havlicek und Karl Svozil, *Density conditions for quantum propositions*, Journal of Mathematical Physics 37, 5337-5341, 1996.

[4] Christian Herrmann und Martin Ziegler, *Computational Complexity of Quantum Satisfiability*, Proceeding LICS '11 Proceedings of the 2011 IEEE 26th Annual Symposium on Logic in Computer Science, Seite 175-184, IEEE Computer Society Washington, DC, USA, 2011

[5] Zurab Silagadze, *Multi-dimensional vector product*, J. Phys. A: Math. Gen. **35** 4949, 2002.

[6] Karl Svozil, *Quantum Logic*, Springer, 1998

Danksagung

Danken möchte ich meinem Betreuer Prof. Dr. Martin Ziegler für seine exzellente Betreuung sowie meinen Eltern, meinen beiden Schwestern und meinem Mann für die finanzielle und emotionale Unterstützung während meiner Diplomarbeit und meines gesamten Studiums.