Verbindliche Telekooperation - Ein Modell für Electronic Commerce auf der Basis formaler Sprachen

Rüdiger Grimm, Peter Ochsenschläger

Institut für Telekooperationstechnik, GMD
64201 Darmstadt

Zusammenfassung

Dieser Artikel erarbeitet eine formale Bestimmung der Begriffe „elektronischer Vertrag“, seine „Ziele“, „Verpflichtungen“ und seine „verbindliche Phase“. Es wird in einem Theorem der „Sog ins Ziel“ durch einen geeignet gestalteten elektronischen Vertrag bewiesen. Die Begriffe beruhen auf der Theorie der formalen Sprachen bzw. der Automaten. Sie werden an einem einfachen Beispiel einer bilateralen Auftragskooperation demonstriert.

1 Zielsetzung des Modells

Menschliches Verhalten ist im allgemeinen nicht vollständig spezifizierbar. Das gilt auch schon für zielgerichtete Kooperationen in eingeschränkten Anwendungskontexten, wie zum Beispiel in verbindlichen Geschäftsvorgängen. Es ist das Ziel der Telekooperationstechnik, den spezifizierbaren Anteil solcher Kooperationen zu implementieren und auf diese Weise die Partner in ihrer Kooperation zu unterstützen.

Wir modellieren Geschäftsvorgänge als zielgerichtete Telekooperationen von Akteuren, die in Rollen agieren. Rollen sind spezifizierte Handlungsmuster mit ausgewiesenen Zielzuständen. Die Handlungsskripte enthalten nicht-deterministische Verzweigungspunkte, an denen steuernde und verantwortliche Personen nach semantischen Gesichtspunkten Entscheidungen im Rahmen vorgegebener Handlungsalternativen treffen. Unser Telekooperationsmodell ist in [Gri94, 72 ff] genauer ausgeführt.

Ein Beispiel für ein kooperatives Handlungsmuster und seine Ziele ist der Austausch von Ware und Geld. Der semantische Zweck der Kooperationsziele wird dabei nicht spezifiziert, in unserem Beispiel könnte das die Befriedigung durch Gewinn sein. Wie bei einem Spiel ist zwar für jede Telekooperation ein gemeinsames syntaktisches Ziel als ordentliche Beendigung der Kooperation spezifiziert, nicht aber die semantische Ausgestaltung des Ziels, wie zum Beispiel Sieg und Niederlage. Das Kooperations*ziel* ist allen gemeinsam, die *Zwecke* können verschieden sein und sogar im Konflikt zueinander stehen.

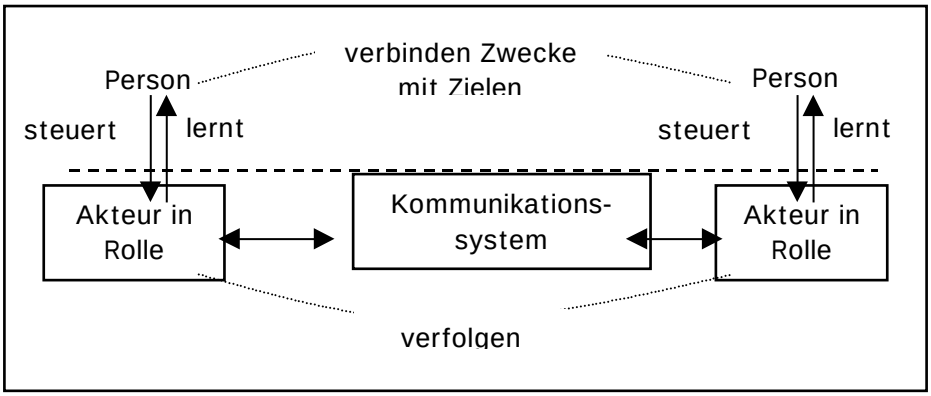

Abb.1: Autonome Personen handeln als Akteure nach spezifizierten Handlungsskripten, d.h. in Rollen. Der Bereich unter der gestrichelten Linie ist spezifiziert, und ggf. auch technisch implementiert.

Jeder Partner verfolgt sein eigenes spezifiziertes individuelles Ziel: der Käufer den Erhalt der Ware, der Verkäufer den Erhalt des Geldes. Unsere Telekooperationen sind grundsätzlich so gestaltet, dass entweder jeder Teilnehmer sein (syntaktisches) Ziel erreicht oder keiner. Diese Erfolgskopplung begründet das Kooperationsprinzip eines gemeinsamen Ziels. Es besagt nichts über den semantischen Zweck, den einer mit dem Erreichen seines Zieles verknüpfen mag.

2 Formale Sprachen, Automaten und Sprachhomomorphismen

Das Verhalten L eines diskreten Systems läßt sich durch die Menge seiner möglichen Aktionsfolgen formal beschreiben. Es gilt also $L \subseteq \Phi^*$, wobei Φ die Menge aller Aktionen des Systems ist und Φ^* die Menge aller endlichen Folgen von Elementen von Φ, einschließlich der mit ε bezeichneten leeren Folge, darstellt. Diese Terminologie stammt aus der Theorie der formalen Sprachen, wo man Φ das Alphabet, die Elemente von Φ Buchstaben, die Elemente von Φ^* Worte und Teilmengen von Φ^* formale Sprachen nennt. Worte lassen sich zusammensetzen: sind u und v Worte, dann ist uv ebenfalls ein Wort. Diese Operation wird *Konkatenation* genannt; es gilt insbesondere $\varepsilon u = u\varepsilon = u$. Ein Wort u heißt *Präfix* eines Wortes v, wenn es ein Wort x gibt, so dass $v = ux$. Die Menge aller Präfixe eines Wortes u bezeichnen wir mit pre(u); es gilt $\varepsilon \in$ pre(u) für jedes Wort u. Formale Sprachen, welche Systemverhalten beschreiben, besitzen die Eigenschaft, dass für jedes Wort $u \in L$ auch $\text{pre}(u) \subseteq L$ gilt; diese Eigenschaft heißt *Präfixstabilität*. Systemverhalten wird also durch präfixstabile formale Sprachen beschrieben.
Formale Sprachen können durch Automaten, bestehend aus Zuständen (Kreisen) und Zustandsübergängen (gerichteten Kanten), dargestellt werden. Die Kanten sind mit Buchstaben beschriftet, welche Aktionen repräsentieren. Aktionen werden automatengerecht ausgeführt, indem den Pfeilen folgend die Wege durchlaufen werden. Die zugehörigen Buchstaben bilden ein Wort. Ein Automat akzeptiert ein Wort, indem er, ausgehend von einem ausgezeichneten Anfangszustand, die zu den Buchstaben gehörigen Aktionen abarbeitet und dabei einen Endzustand erreicht. Jeder Automat definiert auf diese Weise eine formale Sprache. Handelt es sich um eine präfixstabile Sprache, dann sind alle Zustände Endzustände. Da wir in diesem Papier nur präfixstabile Sprachen betrachten, werden wir deshalb im folgenden Endzustände nicht mehr explizit erwähnen.

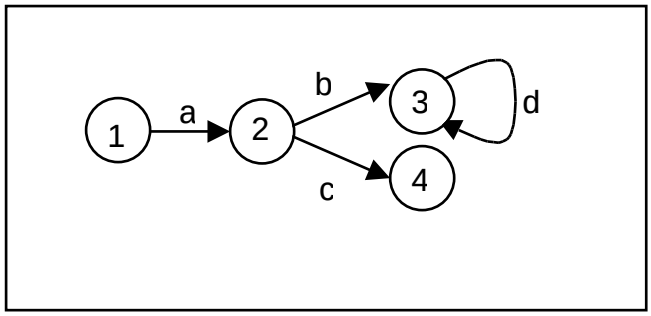

Abb. 2: Automat, der die Sprache aller Wörter {ε, a, ac, ab, abd, abdd, abddd, ...} akzeptiert. Zustand 1 ist der Anfangszustand.

Für den Zusammenhang zwischen Automaten und formalen Sprachen spielt die Menge der möglichen Fortsetzungen eines Wortes x L in der Sprache L eine wichtige Rolle. Sie wird formal durch den *Linksquotienten* $x^{-1}(L)=\{y \quad \Phi^* | xy \quad L\}$ zum Ausdruck gebracht [Eil74]. Zum Beispiel ist in der Sprache L={ε, a, ac, ab, abd, abdd, abddd, ...} der Abb. 1 die Menge der Fortsetzungen von *ab* ebenso wie von *abd* gleich der Menge $\{d^n | n\geq 0\}$; es gilt also $(ab)^{-1}(L)=(abd)^{-1}(L)=\{d^n | n\geq 0\}$. Das Wort *ac* kann in L nur mit dem leeren Wort fortgesetzt werden: $(ac)^{-1}(L)=\{\varepsilon\}$. Solche Worte nennt man *maximal* in L; max(L) bezeichnet die Menge aller maximalen Worte in einer Sprache L, also $\max(L)=\{y \quad L | y^{-1}(L)=\{\varepsilon\}\}$.
Im Automaten der Abb. 1 entsprechen die Zustände in eindeutiger Weise den unterschiedlichen Linksquotienten der akzeptierten Sprache L; beispielsweise entspricht $\{d^n | n\geq 0\}$ dem Zustand 3. Mittels dieser Identifikation von Linksquotienten und Zuständen kann zu jeder formalen Sprache ein akzeptierender Automat konstruiert werden [Eil74]; Automaten und formale Sprachen entsprechen sich also.
Abbildungen $f: \Phi^* \rightarrow \Phi'^*$, welche mit der Konkatenation verträglich sind, für die also f(u)f(v)=f(uv) und f(ε)=ε gilt, nennt man *Sprachomomorphismen*. Sprachhomomorphismen mit der Eigenschaft $f(\Phi) \quad \Phi' \quad \{\varepsilon\}$ nennt man *alphabetisch* (da sie einzelne Buchstaben auf einzelne Buchstaben oder auf das leere Wort abbilden). Mit alphabetischen Sprachhomomorphismen können Abstraktionen von Systemverhalten ausgedrückt werden, denn sie beschreiben das Ausblenden (f(a)=ε) und Identifizieren von Aktionen (f(a)=f(b)).
Besteht ein System aus mehreren Komponenten, die miteinander kommunizieren (verteiltes System), dann zerfällt das Alphabet seiner Aktionen in disjunkte Teilmengen. Im Falle von zwei Komponeneten wird also sein Verhalten durch eine päfixstabile Sprache $L \quad (\Phi \quad \Gamma)^*$ beschrieben, wobei $\Phi \cap \Gamma =$; die Aktionen der einen Komponente liegen in Φ und die der anderen in Γ. Aktionen sind eindeutig den sie ausführenden Komponenten zugeordnet. Mittels spezieller Homomorphismen (Projektionen genannt) $\pi_\Phi: (\Phi \quad \Gamma)^* \rightarrow \Phi^*$ und $\pi_\Gamma: (\Phi \quad \Gamma)^* \rightarrow \Gamma^*$ läßt sich das lokale Verhalten $F \quad \Phi^*$ bzw. $G \quad \Gamma^*$ der einzelnen Systemkomponenten aus dem globalen Systemverhalten L extrahieren: $F=\pi_\Phi(L)$ und $G=\pi_\Gamma(L)$. Die Projektionen π_Φ und π_Γ sind dabei durch $\pi_\Phi(x)=x$ für $x \quad \Phi$ und $\pi_\Phi(x)=\varepsilon$ für $x \quad \Gamma$ sowie $\pi_\Gamma(x)=x$ für $x \quad \Gamma$ und $\pi_\Gamma(x)=\varepsilon$ für $x \quad \Phi$ definiert. In [Och96] ist die Sprachoperation *Kooperationsprodukt* definiert, die es erlaubt, das globale Systemverhalten L mittels der lokalen Systemverhalten F und G darzustellen; in diese Operation fließen natürlich die Eigenschaften des benutzten Kommunikationssystems sowie das Kommunikationsverhalten der Komponenten mit ein.

3 Beispiel Auftragskooperation und vereinfachende Annahmen

In einer einfachen Auftragskooperation tauschen ein Käufer und ein Verkäufer nach bestimmten Regeln eines Geschäftsvertrags Ware (result) und Geld (money) aus. Sie verwenden dabei ein Kommunikationssystem, das dafür sorgt, dass das Senden einer Nachricht von der einen Seite den Empfang der Nachricht auf der anderen Seite zur Folge hat. Zunächst erlaubt der Geschäftsvertrag den Austausch allgemeiner Nachrichten wie Bitte um Angebote, Reklame, Grüße, Anfragen und Unterhaltungssendungen, die für beide Seiten unverbindlich sind. Darüberhinaus schreibt der Geschäftsvertrag den verbindlichen Austausch von Ware und Geld in einer Reihe fest vorgegebener Kommunikationsschritte vor. Wir wählen in diesem Beispiel die Variante „erst die Ware, dann das Geld“. Die zugehörigen Nachrichten sind Angebot (offer), Auftrag (order), Ware (result) und Geld (money).
Der Käufer verfolgt das Ziel, die Ware zu erhalten (*r_result*), der Verkäufer verfolgt das Ziel, das Geld zu erhalten (*r_money*). Um einen Kooperationsverlauf zu unterstützen, in dem entweder jeder Partner oder keiner sein Ziel erreicht, akzeptiert jeder der beiden Partner eine Verpflichtung, die den Partner im richtigen Moment ins Ziel führt. Der Verkäufer ist verpflichtet, die Aktionsfolge *s_offer r_order* auf seiner Seite mit dem Senden der Ware *s_result* fortzusetzen. Der Käufer ist verpflichtet, die Aktionsfolge *s_order r_result* auf seiner Seite mit dem Senden des Geldes *s_money* fortzusetzen.

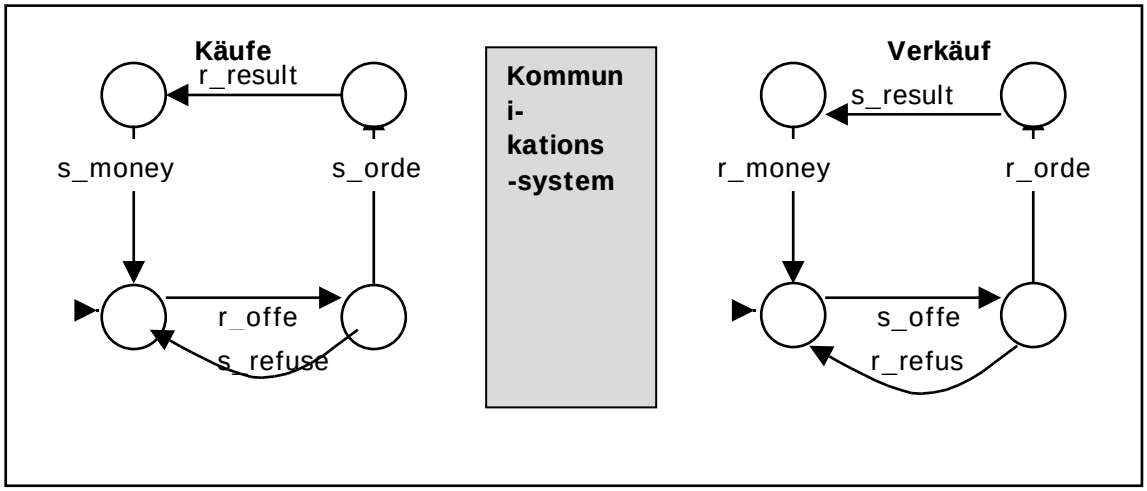

Abb. 3: Verbindliche Phase im elektronischen Vertrag der einfachen Auftragskooperation. Anfangszustände sind durch leere Pfeilspitzen markiert.
Man beachte den nicht-deterministischen Verzweigungspunkt hinter r_offer *beim Käufer.*
Das Kommunikationssystem kann ebenfalls als Automat modelliert werden. Es funktioniert hier so, dass jede Nachricht, die ein Partner abschickt, beim anderen Partner abgeliefert wird.

In dem Zusammenspiel zwischen Verpflichtungen und Zielen ergibt sich der ideale Kooperationsdurchgang durch das globale Wort *s_offer r_offer s_order r_order s_result r_result s_money r_money*, in dem beide Partner ihr Ziel erreichen. Hingegen sind auch andere Kooperationsdurchgänge erlaubt, in denen der Käufer Angebote ablehnt oder ignoriert. Diese sind im Sinne der Geschäftsbedingungen geregelte Abbrüche. Im weiteren Verlauf modellieren wir für unsere Auftragskooperation der Einfachheit halber nur die explizite Zurückweisung eines Angebotes als geregelten Abbruch und verzichten auf das unbeantwortete Ignorieren eines Angebots als zweite Möglichkeit eines geregelten Abbruchs.

Kooperationsschritte, die für beide Seiten unverbindlich sind, wie Bitte um Angebote, Reklame, Grüße usw., können durch den Geschäftsvertrag auch erlaubt sein, werden aber in der weiteren Verfolgung unseres Beispiels der Einfachheit halber nicht berücksichtigt. Das heißt, in unserem Beispiel sind alle Kooperationsschritte für mindestens einen der Partner verbindlich und gehören daher zur “verbindlichen Phase” des Geschäftsvertrags.
Zur Vereinfachung der weiteren Betrachtungen setzen wir hier voraus, dass das Kommunikationssystem sicher ist, d.h. dass das Senden einer Nachricht garantiert ihren Empfang auf der anderen Seite zur Folge hat, sowie dass der Empfang einer Nachricht garantiert auf ihr Absenden von der anderen Seite zurückgeht. Wir setzen weiter voraus, dass alle Aktionen unabstreitbar beweisbar sind. Es gibt technische Mechanismenen für diese Voraussetzungen, zum Beispiel die digitale Signatur (Unabstreitbarkeit des Ursprungs) und Quittungsverfahren (Unabstreitbarkeit des Empfangs), die hier nicht weiter diskutiert werden. Durch diese vereinfachenden Voraussetzungen werden globale Aktionsfolgen *s_offer r_offer s_order r_order s_result r_result ...* gewissermaßen reduzierbar auf *offer order result ...*, welche auf beiden Seiten in gleicher Weise sichtbar und unabstreitbar beweisbar sind.
Ausblick: Dieses Kommunikationsmodell wird verfeinert durch die Zwischenschaltung eines Kommunikationssystems, das die Sicherheitseigenschaften explizit realisiert. Ein solches explizites Verhalten des Kommunikationssystems muss bei der Beweisbarkeit von Aktionen auf der anderen Seite mit Hilfe sogenannter "Bewegungsausdrücke" einbezogen werden. Eine solche Verfeinerung dient dem Studium von Sicherheitseigenschaften eines Kommunikations-systems. Es wird aber nichts an den hier dargestellten Prinzipien verbindlicher Telekooperation ändern.

4 Elektronischer Vertrag

Ein *elektronischer Vertrag EC* zwischen zwei (idealen) Kooperationspartnern F Φ^* und G Γ^* mit $\Phi \cap \Gamma =$ wird definiert als eine präfixstabile Sprache EC $(\Phi \Gamma)^*$ mit der Eigenschaft π_Φ(EC) F und π_Γ(EC) G.
Ein elektronischer Vertrag ist also die Festlegung einer Menge globaler Aktionsfolgen mit Aktionen aus Φ und Γ, deren Projektionen auf die eine oder andere Seite Aktionsfolgen von F bzw. G darstellen. Das bedeutet: *F und G können sich gemäß EC verhalten*. Bei der Betrachtung von F und G wird man sich oft nur auf das Vertragsverhalten in EC beschränken, daher könnte man auch schärfer die Gleichheit fordern: π_Φ(EC)=F und π_Γ(EC)=G. Die etwas allgemeinere Formulierung der Inklusion erlaubt aber die Beschreibung allgemeinerer Partner F und G, die sich auch außerhalb eines Vertrags verhalten können, beispielsweise um mehrere Verträge abzuarbeiten.
Wir haben hier einen elektronischen Vertrag mit einem globalen Ansatz beschrieben, der das gesamte Verhalten aller Seiten einbezieht. Diese globale Sicht ist zur Spezifikation eines idealen Geschäftsablaufs, sozusagen zur Vertragsgestaltung, ausreichend.
Oft ist aber auch der umgekehrte, konstruktive Ansatz erforderlich. Dabei werden erst die lokalen Komponenten beschrieben, die dann zu einem stimmigen Ganzen, hier zu einer Beschreibung einer vertragskonformen Telekooperation zusammengesetzt werden. Das wird besonders bei der Implementierung der einzelnen Systemkomponenten, die eine vertragsgetreue Telekooperation unterstützen sollen, notwendig werden. Die konstruktive Beschreibung einer Telekooperation aufgrund ihrer Partnerkomponenten und eines vermittelnden Kommunikationssystems verwendet das formale Ausdrucksmittel des in [Och96] eingeführten *Kooperationsprodukts*. Wir werden dies in einer gesonderten Arbeit ausführen. Für die hier folgenden Überlegungen, die sich allein auf die ideale Vertragsformulierung beziehen, ist die globale Sichtweise vollkommen ausreichend.

5 Verbindlichkeit

5.1 Begriffsbestimmung

Verbindlichkeit ist die Verbindung zwischen einem Versprechen (Sprache) und seiner Erfüllung (Handlung). Mit dem Versprechen wird eine Verpflichtung eingegangen, die sozusagen als Spannungszustand erzeugt wird und solange erhalten bleibt, bis sie erfüllt und dadurch aufgelöst wird.
Da in offenen Kooperationsumgebungen wie z.B. auf einem offenen Markt autonomer Agenten Verpflichtungen nicht einfach durch zentral gesteuerte Automatismen erfüllt werden können, werden verbindliche Kooperationen mit Hilfe von *Verträgen* beschrieben. Verträge enthalten für jeden Partner seine *Ziele*, die er erreichen *will*, und seine (bedingten und unbedingten) *Pflichten*, die er ausführen *muss*. Durch eine geeignete Strukturierung von Zielen und Verpflichtungen (von Wollen und Müssen) ziehen sich die Geschäftspartner bei vertragskonformem Verhalten gegenseitig derart ins Ziel, dass am Ende beide Partner ihre Ziele erreichen. Dieser "Sog ins Ziel" ist für Kooperationsverträge charakteristisch.
Ein Durchsetzungsprinzip von Verpflichtungen in offenen Umgebungen beruht auf einer effektiven Gerichtsbarkeit, welche die unabstreitbare Beweisbarkeit von Verpflichtungen erfordert. Vertragskonforme Kooperationsprotokolle befolgen daher ein stetiges *Gleichgewicht zwischen Verpflichtungen und ihren Beweisen*.
Das Gleichgewichtsmodell ist ausführlich in [Gri94, 133 ff.] dargestellt.

5.2 Grundidee der Formalisierung

Die Grundidee der Formalisierung von Verbindlichkeit besteht in der Definition verbindlicher Phasen V in Verträgen EC $(\Phi\ \Gamma)^*$. *Verbindliche Phasen* V $(\Phi\ \Gamma)^*$ *innerhalb von EC* sind präfixstabile Sprachen, die dadurch gekennzeichnet sind, dass sie nur aus *endlich vielen Wörtern* bestehen (*Endlichkeit*), die, soweit sie nicht maximal in V sind, *innerhalb von V das gleiche Fortsetzungsverhalten wie innerhalb von EC* besitzen (*Abschluss*). Diese beiden Bedingungen einer verbindlichen Phase bedeuten, dass man, wenn man einmal in eine verbindlichen Phase eingetreten ist, innerhalb dieser zu einem Ende kommt.
Individuelle *Ziele* sind Mengen ausgezeichneter *Teilworte* innerhalb der verbindlichen Phase. Bei einem Vertrag, der das *Kooperationsprinzip* gemeinsamer Ziele unterstützt, sind die individuellen Ziele derart angelegt, dass jedes maximale Wort der verbindlichen Phase entweder die Ziele beider Partner oder kein Ziel erreicht (*Erfolgskopplung*). Die maximalen Wörter in V, die Ziele erreichen, repräsentieren die Kooperationsdurchgänge, die zum Erfolg führen (der Käufer hat die Ware und der Verkäufer das Geld). Die maximalen Wörter in V, die keine Ziele erreichen, repräsentieren die geregelten Abbrüche (der Käufer behält sein Geld, und der Verkäufer behält seine Ware, zum Beispiel weil man sich nicht über den Preis einig wurde).
Individuelle *Verpflichtungen* sind Paare aus Worten und ihren buchstabenweisen Forsetzungen in der verbindlichen Phase. Die Worte repräsentieren dabei Bedingungen, die Versprechen enthalten. Die buchstabenweise Fortsetzungen repräsentieren die Erfüllungen der Versprechen. Indem ein Wort einer individuellen Verpflichtung ausgeführt wird, wird die darin enthaltene bedingte Verpflichtung zu einer unbedingten Verpflichtung, und das Restwort (ein Buchstabe) *muss* nun ausgeführt werden, und dadurch wird die Verpflichtung erfüllt.
Bei einem Vertrag, der das Kooperationsprinzip gemeinsamer Ziele unterstützt, erfüllen die verbindlichen Phasen die Fortschrittsbedingung, dass sie *vollständig durch Verpflichtungen abgedeckt sind*.

Das Haupttheorem dieser Arbeit wird feststellen, dass *Endlichkeit*, *Abschluss*, *Erfolgskopplung* und *Abdeckungsbedingung* einer verbindlichen Phase für den *Sog ins Ziel* sorgen: Bei Eintritt in eine verbindliche Phase werden immer Verpflichtungen in endlich vielen Schritten ganz abgearbeitet. Dabei kommen aufgrund der Erfolgskopplung der verbindlichen Phase alle beteiligten Kooperationspartner entweder zu einem geregelten Abbruch der Kooperation, oder sie erreichen alle ihre individuellen Ziele.

5.3 Formale Definition einer „verbindlichen Phase“

Es sei EC $(\Phi \Gamma)^*$ ein elektronischer Vertrag. Eine präfixstabile Sprache V $(\Phi \Gamma)^*$ ist eine *verbindliche Phase in EC*, wenn gilt

(5.1) *Endlichkeit:* V ist endlich und $V \cap (\Phi \Gamma) \neq$

(5.2) *Abschluss:* x EC mit x=yz und z V\(max(V) {ε}) gilt:
$x^{-1}(EC) \cap (\Phi \Gamma) = z^{-1}(V) \cap (\Phi \Gamma)$

In der “Abschluss“-Bedingung (2) ist *y* der (möglicherweise leere) unverbindliche Anteil und *z* der verbindliche Anteil von *x*. Die Bedingung (2) besagt nun, dass unabhängig von der Vorgeschichte *y* eines verbindlichen Anteils *z* eines Geschäftsvorgangs *x* innerhalb einer verbindlichen Phase immer gilt: was danach überhaupt noch gemacht werden kann ($x^{-1}(EC)$), muss innerhalb von V stattfinden: $z^{-1}(V)$. Das gilt rekursiv auch für jeden weiteren Schritt (Buchstaben), soweit noch kein maximales Wort erreicht ist. Bildlich gesprochen: Worte aus EC, die in V hineinragen, bleiben fortan und enden auch in V.
max(V) sind alle geregelten Beendigungen einer verbindlichen Phase. Zur Erinnerung: V besteht definitionsgemäß nur aus endlich vielen Wörtern, und deshalb gibt es für die Länge *aller* Wörter in V eine gemeinsame obere endliche Schranke: man weiß also immer schon vorab, wie viele Aktionsschritte einem nach Eintritt in V höchstens noch bevorstehen.

> In der einfachen Auftragskooperation haben wir nur die Wörter der verbindlichen Phase dargestellt, indem wir allgemeine Nachrichten wie Bitte um Angebote *please_send_offer*, Grüße, Reklamesendungen, Unterhaltungssendungen usw., die im Rahmen einer Verkaufskommunikation möglich sind, fortgelassen haben. Wörter, die zum Geschäftsvertrag gehören, aber nur in ihren Endstücken in der verbindlichen Phase liegen, wären zum Beispiel alle Wörter *please_send_offer s_offer r_offer ...*, da *please_send_offer* noch für beide Seiten unverbindlich ist.
>
> max(V) besteht hier nur aus den beiden *Wörtern* *s_offer r_offer s_order r_order s_result r_result s_money r_money* und *s_offer r_offer s_refuse r_refuse*.
> Man beachte, dass durch die zyklische Spezifikation von Käufer und Verkäufer in Abb. 3 die verbindliche Phase beliebig oft hintereinander durchlaufen werden kann.

6 Ziele

Der Erfolg einer Kooperation wird mit dem Erreichen von Zielen durch die Kooperationspartner verknüpft. Dafür definieren wir *individuelle Ziele* Z_F von F bzw. Z_G von G als Teilmengen von $(\Phi \Gamma)^* \backslash \{\varepsilon\}$. Wir können dann die “Erfolgskopplung” so formulieren, dass die maximalen Pfade von V entweder Ziele beider Partner vollständig erreichen, oder gar keine Ziele, nicht einmal Teilziele eines der Partner. Wir verlangen von einer zielgerichteten Kooperation grundsätzlich, dass kein Partner das leere Wort als individuelles Ziel hat, damit jeder Partner immer auf eine Aktion zusteuern kann. Formal definieren wir:

"Individuelle Ziele" von F und G sind Teilmengen $Z_F, Z_G \quad (\Phi \quad \Gamma)^* \setminus \{\varepsilon\}$

Enthält ein Ziel mehr als ein Wort, so repräsentieren diese alternative Ziele ("oder"). Oft wird ein Ziel nur ein einzelnes Wort enthalten. Enthält ein Zielwort mehr als einen Buchstaben, so repräsentieren diese mehrere Aktionen, die alle in der vorgegebenen Reihenfolge erreicht werden müssen ("und" mit festgelegter Reihenfolge). Teilziele sind echte *subwords* von Zielen. Sollte ein Partner kein "eigenes" Ziel haben (wie zum Beispiel bei einer Auskunftspflicht), so kann man statt des verbotenen leeren Wortes sein Ziel mit dem des Partners identifizieren, denn wir verlangen ja von den individuellen Zielen der Partner keinen leeren Durchschnitt.

In der einfachen Auftragskooperation hat jeder Kooperationspartner ein einbuchstabiges Wort als Ziel: $Z_{Käufer}=\{r\_result\}$ und $Z_{Verkäufer}=\{r\_money\}$.

Das *Erreichen* von Zielen wird mit Hilfe der Projektionen $\pi_{\Phi Z} : (\Phi \quad \Gamma)^* \rightarrow \Phi Z^*$ und $\pi_{\Gamma Z} : (\Phi \quad \Gamma)^* \rightarrow \Gamma Z^*$ definiert, wobei $\Phi Z \quad \Phi \quad \Gamma$ bzw. $\Gamma Z \quad \Phi \quad \Gamma$ die Menge der Buchstaben aller Worte aus Z_F bzw. Z_G ist: Ein Wort u V *erreicht* das Ziel Z_F bzw. Z_G falls $\pi_{\Phi Z}(u) \quad Z_F$ bzw. $\pi_{\Gamma Z}(u) \quad Z_G$, d.h. wenn es ein ganzes Wort (vollständiges Ziel) von Z_F bzw. Z_G als *subword* enthält.
Ein *individueller Zielpfad* von F ist ein solches maximales Wort von V, das Z_F erreicht, analog für G. Die Menge V_{ZF} bzw. V_{ZG} der individuellen Zielpfade von F bzw. G ist definiert durch

"Individuelle Zielpfade" $V_{ZF} := \pi_{\Phi Z}^{-1}(Z_F) \cap \max(V)$ bzw. $V_{ZG} := \pi_{\Gamma Z}^{-1}(Z_G) \cap \max(V)$

Ein *gemeinsamer Zielpfad* ist dadurch gekennzeichnet, dass er *sowohl* das Ziel Z_F, *als auch* das Ziel Z_G (vollständig) erreicht:

"Gemeinsame Zielpfade" $V_Z := V_{ZF} \cap V_{ZG} \qquad (= \pi_{\Phi Z}^{-1}(Z_F) \cap \pi_{\Gamma Z}^{-1}(Z_G) \cap \max(V))$

Streng komplementär dazu ist ein *geregelter Abbruch* dadurch gekennzeichnet, dass er keinen einzigen Buchstaben eines Zieles enthält, d.h. kein Teilziel von F oder G erreicht:

"Geregelte Abbrüche" $V_A = \pi_{\Phi Z}^{-1}(\varepsilon) \cap \pi_{\Gamma Z}^{-1}(\varepsilon) \cap \max(V)$

Es gilt nun

$V_A \cap V_Z =$,denn wenn x V_Z, dann ist $\pi_{\Phi Z}(x) \quad Z_F$ (und $\pi_{\Gamma Z}(x) \quad Z_G$), und da $\varepsilon \quad Z_F$ (bzw. $\varepsilon \quad Z_G$), ist $\pi_{\Phi Z}(x) \neq \varepsilon$ (sowie $\pi_{\Gamma Z}(x) \neq \varepsilon$), also x V_A.

Weiterhin gilt natürlich $V_A \quad V_Z \quad \max(V)$, und im allgemeinen ist diese Inklusion auch echt. Das heißt, im allgemeinen gibt es maximale Pfade, bei denen ein Partner sein Ziel erreicht, ohne dass der andere sein Ziel ebenfalls erreicht. Für die Erfolgskopplung wird nun die Gleichheit verlangt, das heißt, dass auch umgekehrt ein maximaler Pfad entweder in V_A liegt (dann erreicht er überhaupt kein Ziel, nicht einmal ein Teilziel) oder in V_Z (dann erreicht er Ziele aller Partner vollständig):

(6.1) *Erfolgskopplung:* $\quad V_A \quad V_Z = \max(V)$

In der einfachen Auftragskooperation enthält max(V) nur die beiden Wörter *s_offer r_offer s_order r_order s_result r_result s_money r_money* und *s_offer r_offer s_refuse r_refuse*. Das erste Wort erreicht sowohl das individuelle Ziel des Käufers {*r_result*}, als auch das individuelle Ziel des Verkäufers {*r_money*}, und deshalb gehört es zu $V_Z=V_{ZF}\cap V_{ZG}$. Das zweite Wort erreicht weder das eine noch das andere Ziel und gehört deshalb zu V_A. In diesem Beispiel gilt also die Erfolgskopplung.

Für erfolgsgekoppelte verbindliche Phasen gelten die beiden folgenden Sachverhalte:

(6.2) V_A V_Z =max(V) $V_Z=V_{ZF}=V_{ZG}$ (die Umkehrung gilt i.a. nicht)
(6.3) V_A V_Z =max(V) $\Leftrightarrow$ $V_A = \max(V) \setminus \pi_{\Phi Z}^{-1}(Z_F) = \max(V) \setminus \pi_{\Phi Z}^{-1}(Z_G)$

Beweis für (6.2): Es gelte V_A V_Z =max(V) und es sei x V_{ZF} . Wegen ε Z_F gilt $\pi_{\Phi Z}(x)\neq\varepsilon$, also x V_A. Da aber V_A V_Z=max(V), muss x V_Z, und da nach Definition $V_Z=V_{ZF}\cap V_{ZG}$, liegt damit auch x V_{ZG}, also liegt V_{ZF} V_{ZG} . Die umgekehrte Inklusion ergibt sich analog.
Für Ziele der Länge 1 gilt in (6.2) sogar die Äquivalenz. Für Ziele größerer Länge hingegen, die echte Teilziele enthalten, gilt die Umkehrung von (6.2) im allgemeinen nicht, da die Übereinstimmung der maximalen Pfade, die indiduelle Ziele ganz erreichen, nicht ausschließt, dass es Pfade gibt, die zwar Teilziele, aber nicht vollständige Ziele erreichen.
(6.3) beweist man direkt mit Hilfe einfacher mengentheoretischer Überlegungen.
Eine Kooperation mit Erfolgskopplung hat nun diese erwünschten Eigenschaften: Erstens können maximale Worte von V Ziele erreichen. Zweitens gibt es kein maximales Wort, in dem ein Partner ein Teilziel erreicht, ohne dass sowohl er als auch sein Partner sein Ziel ganz erreicht; und wird kein Ziel erreicht, dann ist die Kooperation geregelt abgebrochen.

7 Verpflichtungen

Eine Verpflichtung von F Φ^* ist eine bedingte Aussage: "wenn in F die-und-die Aktionen stattgefunden haben, dann muss F mit der-und-der Aktion fortfahren". Der erste Teil stellt die Voraussetzung einer bedingten Verpflichtung dar und repräsentiert das Versprechen, der zweite Teil repräsentiert seine Erfüllung.
Die Menge der Verpflichtungen von F ist eine Menge O_F $\pi_\Phi(V) \times$ (Φ) mit den folgenden Eigenschaften (7.1)-(7.2), wobei x $\pi_\Phi(V)$ ein Versprechen und M Φ die ge"oder"ten Erfüllungspflichten darstellen ((Φ) bezeichnet die Potenzmenge von Φ). Begründet dieselbe Voraussetzung mehrere Pflichten (“und“), so werden sie in mehreren Verpflichtungs-ausdrücken (x_1,M_1), (x_2,M_2), ... niedergelegt, wobei die folgenden Voraussetzungen x_2, ... jeweils um eine erfüllte Verpflichtung der vorherigen Verpflichtung erweitert werden. Analog werden Verpflichtungen O_G für G definiert. Formal:
Die *Menge der Verpflichtungen* von F ist eine Menge O_F $\pi_\Phi(V) \times$ (Φ) mit den Eigenschaften

(7.1) (x,M) O_F und y $\pi_\Phi^{-1}(x)\cap V$ gilt: $y^{-1}(V)\cap M = y^{-1}(V)\cap\Phi \neq$.
Das bedeutet: alles, was überhaupt nach einem Versprechen *x* passieren kann, liegt (ggf. nach Zwischenschritten der anderen Seite) ganz in M ("="), und es gibt auch etwas in M zu tun ("≠ ").

(7.2) (x,M) O_F und m M y $\pi_\Phi^{-1}(x)$ mit ym V.
Das bedeutet: jede Erfüllung *m* beruht auf einem Versprechen *x*, die gemeinsam zu einem gültigen Wort *ym* der verbindlichen Phase gehören; *y* enthält dabei möglicherweise Zwischenschritte der anderen Seite.

Aus (7.1) und (7.2) folgt übrigens, wie sich leicht beweisen lässt, die Eindeutigkeit der Verpflichtung M aufgrund eines Versprechens x: (x,M) O_F und (x,M') O_F M=M'.
Wir sagen: *F ist nach einer Aktionsfolge y∈V in der Verpflichtung M,* wenn es ein (x,M) O_F mit $\pi_\Phi(y)=x$ gibt. Wegen (7.1) gibt es dann ein m M mit ym V; d. h. *F erfüllt seine Verpflichtung M mit der Aktionsfolge ym∈V.*

In der einfachen Auftragskooperation sei Φ das Aphabet des Käufers und Γ das Alphabet des Verkäufers. Käufer und Verkäufer haben jeweils eine Verpflichtung. Für den Verkäufer gilt: *Wenn* der Verkäufer ein Angebot macht *und wenn* er den zugehörigen Auftrag erhält, x_1 = *s_offer r_order* π_Γ(V), *dann muss* er die zugehörige Ware liefern, M_1={*s_result*} (Γ), d.h.

(x_1,M_1) = (*s_offer r_order*,{*s_result*}) $O_{Verkäufer}$ π_Γ(V)× (Γ)

ist die einzige Verpflichtung des Verkäufers.
Für den Käufer gilt: *Wenn* der Käufer einen Auftrag erteilt *und wenn* er die zugehörige Ware erhält, x_2 = *s_order r_result* π_Φ(V), *dann muss* er sie bezahlen, M_2={*s_money*} (Φ), d.h.

(x_2,M_2) = (*r_offer s_order r_result*, {*s_money*}) $O_{Käufer}$ π_Φ (V)× (Φ)

ist die einzige Verpflichtung des Käufers.

8 Abdeckung der verbindlichen Phase durch Verpflichtungen

Damit innerhalb einer verbindlichen Phase Verpflichtungen nicht ignoriert werden können, muss die Fortschrittsbedingung erfüllt sein, dass die Verpflichtungen O_F und O_G der Partner F und G die verbindliche Phase V *vollständig abdecken*.
Wir definieren die Abdeckungsbedingung zunächst vorläufig. Die Verpflichtungen O_F und O_G der Partner F und G decken die verbindliche Phase V ab, wenn gilt:

(8.1) Nach jeder Aktionsfolge v V \ (pre(V_A) max(V)) ist F oder G in einer Verpflichtung. Das heißt formal ausgeschrieben: v V \ (pre(V_A) max(V)) gilt: ((x,M) O_F mit $\pi_\Phi(v)=x$) ((x,M) O_G mit $\pi_\Gamma(v)=x$)

Das bedeutet, dass in V *hinter* der "Abzweigung von geregelten Abbrüchen", aber *vor* dem Ende (V\(pre(V_A) max(V))) immer einer der beiden Partner eine unbedingte Verpflichtung hat, weil die Voraussetzung seines Verpflichtungsausdrucks *x* erfüllt ist; *v* enthält dabei möglicherweise Zwischenschritte der anderen Seite. Deshalb erfolgt nach der Verpflichtungs-bedingung (7.1) als nächster Schritt auf jeden Fall die Erfüllung m M einer Verpflichtung.

In der einfachen Auftragskooperation liegt die letzte "Abzweigung zu einem geregelten Abbruch" vor dem Senden eines Auftrags vom Käufer an den Verkäufer (*s_order*: das impliziert *r_order* beim Verkäufer). Danach ist zuerst der Verkäufer verpflichtet, die Ware zu liefern (*s_result*: das impliziert *r_result* beim Käufer), und daraufhin ist der Käufer verpflichtet, das Geld zu senden (*s_money*: das impliziert *r_money* beim Verkäufer). Das einzige Wort in V_Z={*s_offer r_offer s_order r_order s_result r_result s_money r_money*} ist bis auf die Annahme, dass eine Sendeaktion eine entsprechende Empfangsaktion impliziert, ab *s_order* durch die beiden

Verpflichtungen von Käufer und Verkäufer abgedeckt, die sich wechselseitig durch die verbindliche Phase ziehen.

Das Beispiel offenbart eine Lücke in der formalen Abdeckungsbedingung einer verbindlichen Phase. Der Übergang vom Senden zum Empfangen einer Nachricht, bei der das Kommunikationssystem explizit in Erscheinung tritt, ist nämlich nicht formal durch unsere Abdeckungsbedingung erfasst. Es hilft nichts: an dieser Stelle muss das Kommunikationssystem explizit in die formale Beschreibung aufgenommen werden. Das geschieht an zwei Stellen.
Erstens lockern wir die Abdeckungsbedingung auf, indem wir diejenigen Aktionen aus der Abdeckung herausnehmen, die in der Initiative des Kommunikationssystems liegen. Das sind typischerweise die Empfangsaktionen als Folge von Sendeaktionen. Zweitens werden wir die Abdeckung durch eine *Verpflichtung des Kommunikationssystems*, jede entgegengenommene Nachricht sicher abzuliefern, erweitern. Das heißt, dass das Kommunikationssystem verpflichtet wird, Worte mit einer Sendeaktion am Ende durch die zugehörige Empfangssaktion fortzusetzen. In unserem Beispiel setzt das Kommunikationsystem Worte mit dem Wortende *s_offer* durch die Aktion *r_offer* fort, sowie Worte mit dem Wortende *s_order* durch *r_order* usw. Auf diesem Wege würde die Fortsetzung eines Wortes von der Sende- zur Empfangsaktion durch eine Verpflichtung des Kommunkationssystems abgedeckt.
An dieser Stelle tritt erstmals das Kommunikationssystem semantisch in Erscheinung. Wir sprechen zum ersten Mal von einer “Verpflichtung des Kommunikationssystems”, und wir heben zum ersten Mal Aktionen hervor, die “in der Initiative des Kommunikationssystems” liegen. Wir können das hier nur andeuten. Um das vollständig auszuführen, und insbesondere um die Unabhängigkeit dieser Verpflichtungen von speziellen Nachrichteninhalten ausdrücken zu können, muss der formale Begriff eines Kooperationsproduktes [Och96] eingeführt und auf den elektronischen Vertrag angewendet werden. Das wird in einer gesonderten Arbeit geschehen.
Formal wird das so aussehen: Wir zerlegen die Alphabete Φ und Γ der beiden Vertragsparteien F Φ^* und G Γ^* in jeweils zwei disjunkte Bestandteile $\Phi=\Phi \quad \Phi^0$ und $\Gamma=\Gamma \quad \Gamma^0$, wobei Φ und Γ in der Initiative von F bzw. G liegen (typischerweise Sendeaktionen von F oder G), während Φ^0 und Γ^0 beide in der Initiative des Kommunikationssystems liegen (typischerweise Empfangsaktionen von F oder G). Für die Verpflichtungen von F und G gilt dann $O_F \quad \pi_\Phi(V)\times \quad (\Phi)$ sowie $O_G \quad \pi_\Gamma(V)\times \quad (\Gamma)$.

In unserem Beispiel der einfachen Auftragskooperation sind
$\Phi = \{s\_refuse, s\_order, s\_money\}$, $\Phi^0 = \{r\_offer, r\_result\}$,
$\Gamma = \{s\_offer, s\_result\}$, $\Gamma^0 = \{r\_refuse, r\_order, r\_money\}$.

Wir verlangen als zusätzliche Voraussetzung, dass das Kommunikationssystem alle Aktionen, die in seiner Initiative liegen, auch zuverlässig ausführt. In Anlehnung an die in Abschnitt 7 eingeführten Sprechweise sagen wir:

(8.2) *Das Kommunikationssystem ist nach einer Aktionsfolge $y\in V$ in der Verpflichtung $\Phi^0 \quad \Gamma^0$*, wenn $y^{-1}(V)\cap(\Phi^0 \quad \Gamma^0)\neq$. Damit existiert ein r $\Phi^0 \quad \Gamma^0$ mit yr V; d. h. *das Kommunikationssystem erfüllt seine Verpflichtung $\Phi^0 \quad \Gamma^0$ mit der Aktionsfolge $yr\in V$.*

Damit lautet die allgemeine Abdeckungsbedingung wie folgt. Die Verpflichtungen O_F und O_G der Partner F $(\Phi \quad \Phi^0)^*$ und G $(\Gamma \quad \Gamma^0)^*$ *decken die verbindliche Phase V vollständig ab*, wenn gilt:

(8.3) Verallgemeinerte *Abdeckung* (Vereinigung von (8.1) und (8.2)):
Nach jeder Aktionsfolge v V \ (pre(V_A) max(V)) ist *F, G oder das Kommunikationssystem* in einer Verpflichtung.

9 Der "Sog ins Ziel"

Das Haupttheorem dieser Arbeit besagt, dass in einer verbindlichen Phase, in der die Erfolgskopplung und Fortschrittsbedingung gelten, das Kooperationsprinzip gilt, dass entweder keiner oder jeder der beteiligten Partner sein Ziel erreicht. Sie unterliegen in der verbindlichen Phase einem "Sog ins Ziel".

Theorem des Kooperationsprinzips:
Gelten für eine verbindliche Phase V eines elektronischen Vertrags EC (die ja durch *Endlichkeit* (5.1) und *Abschluss* (5.2) gekennzeichnet ist) zusätzlich die *Erfolgskopplung* (6.1) sowie die *Abdeckungsbedingung* (8.3 mit 7.1-2) und werden alle Verpflichtungen erfüllt, dann gilt auch das Kooperationsprinzip: entweder bricht die Kooperation nach endlich vielen Schritten ab, ohne dass irgendein Partner sein Ziel erreicht hat, oder die Kooperation endet nach endlich vielen Schritten erfolgreich damit, dass *jeder* Partner sein Ziel ganz erreicht hat.

Beweis:
Es sei $x \in V$. Wenn es in $max(V)$ liegt, dann gehört es entweder zu V_A oder zu V_Z, und wegen der Erfolgskopplung (6.1) ist dann für x die Aussage bereits erfüllt.
Ist $x \in V \backslash max(V)$, dann gehört es entweder zu $pre(V_A)$ oder nicht. Wenn es zu $pre(V_A)$ gehört, dann ist in x nach Definition von V_A noch kein Ziel erreicht. Alle folgenden Fortsetzungsüberlegungen für x sind wegen der Endlichkeit der Wörter in V (5.1) nach endlich vielen Wiederholungen beendet. Jede einbuchstabige Fortsetzung von x gehört wegen der Abgeschlossenheit von V (5.2) wiederum zu V, und daher gehört sie wiederum entweder zu $pre(V_A)$ oder nicht. Wenn die Fortsetzungen jedesmal in $pre(V_A)$ verbleiben, bis ein Wort in V_A erreicht ist, ist nach Definition von V_A nach wie vor kein Ziel erreicht und die Aussage des Theorems erfüllt. Wenn aber für eine einbuchstabige Fortsetzung $a \in x^{-1}(EC)$ das Wort $x'=xa$ nicht mehr in $pre(V_A)$ liegt, dann gilt $x' \in V \backslash pre(V_A)$.
Ist x' außerdem in $max(V)$, dann liegt es auch in V_Z. Wegen der Erfolgskopplung sind dann in x' alle Ziele erreicht und damit die Aussage des Theorems erfüllt. Andernfalls gilt $x' \in V \backslash (pre(V_A) \cup max(V))$, und damit gilt für x' die Abdeckungsbedingung 8.3. Wiederum sind wegen der Endlichkeit der Wörter in V (5.1) alle folgenden Fortsetzungsüberlegungen für x' nach endlich vielen Wiederholungen beendet. Und wegen der Abgeschlossenheit von V (5.2) verbleiben alle Fortsetzungen in V.
x' liege also in V hinter der Abzweigung geregelter Abbrüche ($V \backslash pre(V_A)$), aber vor dem Ende von V ($V \backslash max(V)$), und daher gilt die Abdeckungsbedingung (8.3). Es ist also F, G oder das Kommunikationssystem in einer Verpflichtung. Wird eine dieser Verpflichtungen erfüllt, dann existiert ein $m \in \Phi \cup \Gamma$ mit $x'm \in V$. Entweder ist das Wort dann zu Ende, d.h. es gilt $x'm \in V_Z$, dann hat es nach der Erfolgskopplung (6.1) alle Ziele erreicht, oder es ist noch nicht zu Ende. Falls es noch nicht zu Ende ist, liegt es wiederum in $V \backslash (pre(V_A) \cup max(V))$, und dasselbe Argument wird rekursiv wiederholt. Wegen der Endlichkeit (5.1) und Abgeschlossenheit (5.2) von V endet das Wort nach endlich vielen Fortsetzungen in V_Z. Nach der Erfolgskopplung (6.1) werden die Ziele beider Partner vollständig erreicht, und damit ist die Aussage des Theorems erfüllt.
Ende des Beweises.

Im Beispiel der einfachen Auftragskooperation verpflichtet das Wort *s_offer r_offer s_order r_order* den Verkäufer wegen seiner Verpflichtung (*s_offer r_order, {s_result}*) zum nächsten Schritt *s_result*. Das Kommunikationssystem sorgt als nächsten Schritt für *r_result* auf Seiten des Käufers. Damit hat der Käufer sein Ziel erreicht. Inzwischen ist nun aber das Wort *s_offer r_offer s_order r_order s_result r_result* erreicht, und das verpflichtet den Käufer wegen seiner Verpflichtung (*s_order r_result, {s_money}*) zum nächsten Schritt *s_money*. Das Kommunikationssystem sorgt als nächsten Schritt für *r_money* auf Seiten des Verkäufers. Damit hat auch der Verkäufer sein Ziel erreicht.
Vor der Abzweigung *s_order* zum "Erfolgspfad" könnte noch das Wort aus V_A= {*s_offer r_offer s_refuse r_refuse* } erreicht werden, welches einen geregelten Abbruch darstellt, bei dem weder Käufer noch Verkäufer sein Ziel erreicht. Falls der elektronische Vertrag dem Käufer erlauben würde, ein Angebot unbeantwortet zu ignorieren, läge auch dieser zweite mögliche geregelte Abbruch *s_offer offer_ignored* V_A vor der Abzweigung *s_order*.

Bei den Bedingungen (7.1) und (7.2) ist nicht die allgemeinste Form gewählt worden; es wurde vielmehr darauf geachtet, dass die Grundidee deutlich wird. Wenn im Beispiel die strikte Sequentialisierung „erst die Ware, dann das Geld" aufgelockert wird zu „Ware und Geld in beliebiger Reihenfolge", dann ist die gewählte Formalisierung nicht mehr anwendbar. Für derartige Kooperationen mit mehr Nebenläufigkeit müssen die Bedingungen (7.1) und (7.2) in einer Weise aufgelockert werden, dass nicht nur Zwischenschritte der jeweils anderen Seite, sondern auch solche, die in der Initiative des Kommunikationssystems liegen, zugelassen werden. Diese Verallgemeinerung erfolgt in einer Nachfolgearbeit.

10 Das Gleichgewicht aus Beweisen und Verpflichtungen

Alle bisherigen Aussagen beruhen auf einer globalen Sichtweise. Die Partner ihrerseits haben aber nur eine eingeschränkte Sicht auf die Kooperation: Sie sehen ihre eigenen Aktionen direkt, aber die Aktionen ihres Partners sehen sie nur vermittelt über das Kommunikationssystem. Um Verpflichtungen ihrer Partner einfordern zu können, müssen sie daher die Erfüllung aller Voraussetzungen beweisen können, die ihre Partner nun in den Zustand einer unbedingten Verpflichtung versetzt haben. Um umgekehrt die falsche Behauptung abwehren zu können, sie hätten ihre Verpflichtung nicht erfüllt, brauchen sie selbst Beweise über die Erfüllung ihrer Verpflichtungen.
Deshalb muss man erstens den Begriff des Beweises definieren und schließlich die Gleichgewichtsregel formulieren, nach der jede Veränderung eines Verpflichtungszustandes durch einen Beweis für den begünstigten Partner kompensiert werden muss.
Das soll allgemein in nachfolgenden Arbeiten geschehen.
Mit der vereinfachenden Voraussetzung des vorliegenden Artikels, dass jede Aktion global auf allen Seiten in gleicher Weise sichtbar und beweisbar ist, ist jede globale Sichtweise gleichzeitig auch eine lokale Sichtweise und die Gleichgewichtsbedingung daher automatisch erfüllt.

11 Ausblick

In diesem Beitrag haben wir die Begriffe für eine zielorientierte Telekooperation, ihre verbindliche Phase und deren Abdeckung durch Verpflichtungen formuliert. Damit konnten wir *Prinzipien für ein ideales Vertragskprotokoll* aufstellen und formal beweisen, dass sie den

„Sog ins Ziel“ gewährleisten. Die formale Beschreibung erlaubt es, anhand einer Anforderungsspezifikation eines konkreten Geschäftsprotokolls zu beweisen oder zu widerlegen, dass es diese prinzipiellen Eigenschaften besitzt. Das Ziel ist mit diesem Beitrag erreicht.

Im nächsten Schritt werden wir uns der Realisierung der einzelnen Komponenten zuwenden und Konformitätsbedingungen dafür formulieren, dass sie in ihrem telekooperativen Zusammenspiel einen prinzipiengetreuen elektronischen Vertrag erfüllen können. Wir wollen damit für konkrete Geschäftsprotokolle die formale Zusicherung ermöglichen, dass *spezifikationsgetreue Implementierungen bei vertragskonformem Verhalten einen Sog ins Ziel garantieren*. Die Zusicherung bezieht sich auf die formalen Spezifikationen eines konkreten prinzipiengetreuen Geschäftsprotokolls sowie der Komponenten seiner Realisierung als Telekooperation.

Ein noch weitergehendes Ziel unserer Arbeit streben wir in einem dritten Schritt an. Da man über ein offenes und unsicheres Netz mit entfernten Geschäftspartnern verbindlich telekooperieren will, ohne zu wissen, ob diese sich überhaupt vertragskonform verhalten können oder wollen, brauchen wir *globale Zusicherungen, die allein auf der Korrektheit der eigenen lokalen Komponenten beruhen*. Zu diesem Zweck werden wir den in [Gri94] eingeführten Begriff des Gleichgewichts von Verpflichtungen und ihren Beweisen formalisieren. Man kann dann einem lokalen Partner formal zusichern, dass das Kooperationsprinzip gemeinsamer Ziele (notfalls mit einem Beweis einer offenen Verpflichtung des entfernten Partner) global immer eingehalten wird, auch wenn man sich auf das korrekte Verhalten des entfernten Partners nicht verlassen kann.

Außerdem lassen sich die Definitionen, Bedingungen und Aussagen auf mehr als zweiseitige Kooperationen, auf mehr als einen Vertrag und auf mehr Nebenläufigkeit in den Verpflichtungen verallgemeinern. Eine besondere Aufgabe besteht darin, realistische Telekooperationen mit den hier erarbeiteten Hilfsmitteln zu spezifizieren und dadurch ihre globale Sicherheit zu gewährleisten.

Die oben skizzierten Schritte, sowie ihre Verallgemeinerungen und Anwendungen auf konkrete Geschäftsabläufe werden in nachfolgenden Arbeiten ausgeführt.

12 Literatur

[Eil74] Eilenberg, Samuel: Automata, Languages and Machines, Vol. A . Academic Press, New York, 1974, 451 S.

[Gri94] Grimm, Rüdiger: Sicherheit für offene Kommunikation – Verbindliche Telekooperation. B.I. Wissenschaftsverlag, Mannheim, 1994, 274 S.

[Och96] Ochsenschläger, Peter: Kooperationsprodukte formaler Sprachen und schlichte Homomorphismen. Arbeitspapiere der GMD 1029. Sankt Augustin, November 1996, 52 S.