(19) Deutsches Patent- und Markenamt

(10) **DE 11 2019 007 400 T5** 2022.03.10

(12) # Veröffentlichung

der internationalen Anmeldung mit der
(87) Veröffentlichungs-Nr.: **WO 2020/244028**
in der deutschen Übersetzung (Art. III § 8 Abs. 2 IntPatÜbkG)
(21) Deutsches Aktenzeichen: **11 2019 007 400.8**
(86) PCT-Aktenzeichen: **PCT/CN2019/096256**
(86) PCT-Anmeldetag: **17.07.2019**
(87) PCT-Veröffentlichungstag: **10.12.2020**
(43) Veröffentlichungstag der PCT Anmeldung in deutscher Übersetzung: **10.03.2022**

(51) Int Cl.: ***G06F 8/10*** (2018.01)
G06F 8/30 (2018.01)
G06F 8/75 (2018.01)
G06F 30/20 (2020.01)

(30) Unionspriorität:
201910480184.9 04.06.2019 CN

(71) Anmelder:
Nanjing University, Nanjing, Jiangsu, CN

(74) Vertreter:
Nowack, Linda, Dr.-Ing., 83026 Rosenheim, DE

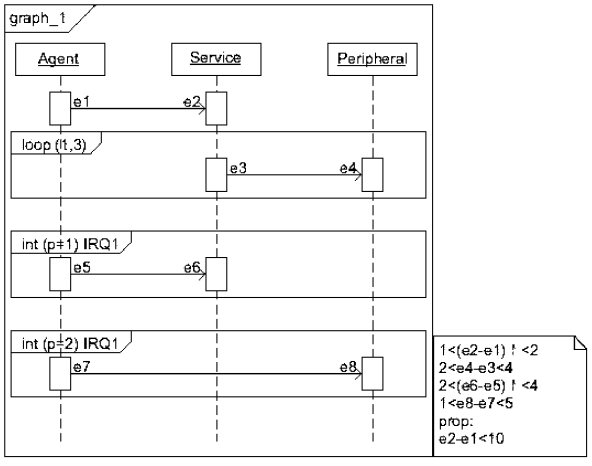
(72) Erfinder:
Pan, Minxue, District Nanjing, Jiangsu, CN; Chen, Shouyu, District Nanjing, Jiangsu, CN; Zhang, Tian, District Nanjing, Jiangsu, CN; Wang, Linzhang, District Nanjing, Jiangsu, CN; Li, Xuandong, District Nanjing, Jiangsu, CN

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Verfahren zur Verifizierung eines Interrupt-Antriebssystems basierend auf einem Interrupt-Sequenzdiagramm**

(57) Zusammenfassung: Die vorliegende Erfindung betrifft ein Verfahren zur Verifizierung eines Interrupt-Antriebssystems basierend auf einem Interrupt-Sequenzdiagramm, das die folgenden Schritte umfasst: Aufbau eines Modells des Interrupt-Antriebssystems basierend auf dem Interrupt-Sequenzdiagramm; Aufteilen Interaktionssegmente in dem Interrupt-Sequenzdiagramm in grundlegende Interaktionssegmente und zusammengesetzte Interaktionssegmente, die sequentiell in einen Automaten umgewandelt werden; Kombinieren von Automaten zu einem Hybrid-Automaten; Hinzufügen von Beschränkungen des Interrupt-Sequenzdiagramms zu dem konvertierten Automatenmodell; Hinzufügen der Verifizierungsattributinformation im Interrupt-Sequenzdiagramm als eine Beschränkung zu dem konvertierten Automatenmodell; Beschreiben des Automaten als Eingabeformat, das für das Automatenverifizierungswerkzeug akzeptabel ist; die Verifikation erfolgt mit einem Automatenverifizierungswerkzeug.



Beschreibung

TECHNISCHES GEBIET

[0001] Die vorliegende Erfindung gehört zum Gebiet der Softwaretechnik und der Überprüfung des Systemdesigns. Die vorliegende Erfindung betrifft ein Verfahren zur Verifizierung eines Interrupt-Antriebssystems basierend auf einem Interrupt-Sequenzdiagramm. Der Konstrukteur eines Interrupt-Antriebssystems kann mit diesem Verfahren eine einfache und intuitive Beschreibung des Interrupt-Antriebssystems ermöglichen und verifizieren.

STAND DER TECHNIK

[0002] Mit dem schnellen Fortschritt der Computertechnologie haben Computersysteme in alle Bereiche unseres Lebens Einzug gehalten, und Schienenverkehrssysteme, Finanzsysteme, medizinische Systeme und dergleichen sind alle hochgradig computerisiert. Interrupt-Antriebssysteme sind weit verbreitet in Interrupt-Antriebssystemen verwendet worden, in denen die Software- und Hardware-Ressourcen relativ begrenzt sind, wie z. B. in der Luft- und Raumfahrt, in der industriellen Prozesssteuerung und Ähnlichem. Diese Systeme sind jedoch häufig sicherheitskritische Systeme, deren Fehlfunktion oder Ausfall zu einem erheblichen wirtschaftlichen Schaden, massiven Zerstörungen oder sogar Unfällen führen kann, die tödlich für Menschen sind. Bei Interrupt-Antriebssystemen werden die meisten Aufgaben-Zeitpläne und Verarbeitungsprozesse von Interrupts initiiert. Eine Echtzeitsteuerung, eine automatische Fehlerbehandlung, eine Datenübertragung zwischen Geräten wird häufig auf eine interruptgesteuerte Weise durchgeführt, hauptsächlich weil der Interrupt-Overhead gering ist und sich an die relativ begrenzten Hardware-Ressourcen des Systems anpassen kann. Außerdem ist die Interrupt-Reaktion schnell, was die Echtzeitanforderungen vieler Systeme erfüllen kann. Die Gewährleistung der Zuverlässigkeit des Interrupt-Antriebssystems ist von großer Bedeutung.

[0003] Die Gewährleistung der Zuverlässigkeit des Interrupt-Antriebssystems ist jedoch sehr schwierig, was in erster Linie durch die Merkmale des Interrupts bedingt ist. In einem Interrupt-System kann das Auftreten eines Interrupts mit Unsicherheit und die Verschachtelung von Interrupts die Zeitsequenz des Betriebs des Systems besonders komplex machen, und potentielle Fehler im System können jedoch nur bei bestimmter Interrupt-Trigger-Zeitsequenz angezeigt werden. Probleme, die durch Interrupt in dem Interrupt-Antriebssystem verursacht werden, wie die Laufzeitverzögerung, der Datenkonkurrenzbetrieb und dergleichen, sind daher schwer zu verifizieren.

[0004] Das Interrupt-Sequenzdiagramm basiert auf einer Erweiterung des UML-Sequenzdiagramms, das eine Modellierung des Prozesses für die Verarbeitung von kombinationalen Interrupt-Segment für die Interrupt-Aufgabe bereitstellt, und entsprechende semantische und grammatikalische Anforderungen werden vorgeschlagen. Zusätzlich erweitert das Interrupt-Sequenzdiagramm auch die Darstellung von zeitlichen Beschränkungen, was die Darstellungsfähigkeit des Modells für die Anforderungen an die Echtzeitfähigkeit des Systems erhöht. Das auf der Grundlage des Interrupt-Sequenzdiagramms beschriebene Interrupt-Antriebssystem-Modell kann das Interaktionsverhalten in dem Interrupt-Antriebssystem in intuitiver Weise zeigen und die Echtzeitanforderungen des Systems in einer vereinfachten zeitlichen Beschränkung ausdrücken, und es stellt eine einfach verständliche und intuitive grafische Darstellung bereit, die es dem Interrupt-Antriebssystementwickler ermöglicht, leicht, einfach und schnell eine interruptgesteuerte interaktive Szene zu modellieren.

[0005] Im Zusammenhang mit der Modellverifikation wird typischerweise ein Modell eines Automatenmodells verwendet, um auf der Grundlage der Idee der Modellverifikation eine umfassende Überprüfung eines Softwaresystems durchzuführen. Tatsächlich sind Interrupt-Antriebssysteme, basierend auf der Darstellung eines Automatenmodells, für einen Interrupt-Antriebssystementwickler beim Modellieren des Systems nicht geeignet, und das Automatenmodell kann nicht in der Lage sein, das Interaktionsverhalten und die Echtzeitanforderungen des Systems intuitiv auszudrücken, wie ein Sequenzdiagramm. Für einige komplexe Szenarien von Systeminteraktionen ist der Zustandsraum des Systems groß, und die Konstruktion eines solchen Automatenmodells ist eine schwierige und sehr fehleranfällige Angelegenheit. In Kombination mit dem oben Gesagten ist es notwendig, das Interrupt-Sequenzdiagramm in ein Automatenmodell umzuwandeln, wobei das Attributverifikationsproblem des Interrupt-Antriebssystems durch das Verifizierungswerkzeug des Automatenmodells in ein Entscheidungsproblem der Erreichbarkeit des Automaten umgewandelt wird. Auf diese Weise können Entwickler leicht und schnell Interaktionsszenarien für Interrupt-System modellieren und verifizieren.

INHALT DER VORLIEGENDEN ERFINDUNG

[0006] Die vorliegende Erfindung beruht auf einem Interrupt-Sequenzdiagramm, wobei das Interrupt-Antriebssystem unter Verwendung eines Verifizierungswerkzeugs eines Automaten durch Umwandeln des Interrupt-Sequenzdiagramms in ein hierzu äquivalentes Automatenmodell verifiziert wird. Die vorliegende Erfindung stellt ein Verfahren zum Konvertieren eines Interrupt-Sequenzdiagramm-Modells in ein entsprechendes Automatenmodell bereit, das die Erzeugung von Fehlern beim direkten Konstruieren des Automatenmodells reduziert, die Kosten für das Modellkonstruieren reduziert und die Verifizierung des Interrupt-Antriebssystems kann direkt unter Verwendung des Verifizierungswerkzeugs des Automatenmodells ausgeführt werden.

[0007] Um die oben genannten Ziele zu erreichen, verwendet die vorliegende Erfindung eine technische Lösung: ein Verfahren zur Verifizierung eines Interrupt-Antriebssystems basierend auf einem Interrupt-Sequenzdiagramm, welches die folgenden Schritte aufweist:

Schritt 1: Aufbau eines Modells des Interrupt-Antriebssystems basierend auf dem Interrupt-Sequenzdiagramm;
das Interrupt-Sequenzdiagramm wird durch Interaktionsobjekte, Interaktionssegmente, Beschränkungen, Interaktionssegmente und dergleichen Elemente als eine zweidimensionale Grafik erstellt. Die Querachse listet aufeinander folgend Interaktionsobjekte auf, die Längsachse ist eine Zeitachse, und die Zeit erstreckt sich entlang der vertikalen Linie nach unten, um eine chronologische Reihenfolge der Interaktionszeiten der Objekte zu beschreiben. Interaktionsobjekte sind durch Lebenslinien dargestellt, und Interaktionen zwischen Objekten sind durch Nachrichten beschrieben. Nachrichten sind ein Kommunikationsmechanismus zwischen Objekten, ein Signal wird von dem sendenden Objekt an ein anderes oder an mehrere andere empfangende Objekte gesendet, und der Nachrichtenübermittlungsprozess wird durch einen Pfeil beschrieben, und der Nachrichtenname wird auf der Linie mit dem Pfeil platziert, die Sende-und Empfangsereignisse einer Nachricht weisen beide eindeutige Ereignisnamen auf und werden am Anfang und am Ende der Pfeillinie platziert. Der komplexe Steuerungsablauf in dem Interrupt-Sequenzdiagramm ist durch das kombinierte Segment dargestellt, wobei die Funktionalität der verschiedenen kombinierten Segmente durch den Typ ihrer Interaktionsoperation bestimmt wird, loop zeigt eine Schleifenoperation, alt zeigt eine Verzweigungsoperation und opt zeigt eine optionale Operation an, und die Darstellungsmethode ist dieselbe wie im UML-Sequenzdiagramm, während int-Operation eine erweiterte Operation des Interrupt-Sequenzdiagramms im Verhältnis zum Sequenzdiagramm ist, die auch die Grenzen eines kombinierten Segments darstellt, das von einem Block dargestellt wird, und links oben im Block zeigt die Zeichenfolge int an, dass der Typ des kombinierten Segments der Interrupt-Operationstyp ist, p zeigt die Interrupt-Priorität an, id ist der Name des kombinationalen Interrupt-Segments, condition ist ein bedingter Ausdruck, der eine Bedingung angibt, dass ein Interrupt aufgetreten ist. Da das Auftreten und Verarbeiten von Interrupts eine zeitliche Ungewissheit besitzt, wird vorgesehen, dass es keine zeitliche teilweise geordnete Beziehung zwischen Interaktionsereignissen innerhalb eines kombinationalen Interrupt-Segments und Ereignissen außerhalb davon gibt, wobei für Interrupt-Priorität vorgesehen ist, dass die Ausführung von Interrupt-Segmenten mit hoher Priorität die Ausführung von Interrupts mit niedriger Priorität unterbrechen kann, jedoch kann die Ausführung eines Interrupt mit niedriger Priorität nicht die Ausführung eines Interrupt mit hoher Priorität unterbrechen, wobei für einen bedingten Ausdruck bedeutet das, wenn der bedingte Ausdruck wahr ist, dass die Interrupt-Aufgabe ausgelöst werden kann, und umgekehrt nicht ausgelöst werden kann.

Schritt 2: Aufteilen der Interaktionssegmente gemäß dem Interrupt-Sequenzdiagramm, das aus Schritt 1 resultiert, in grundlegende Interaktionen und zusammengesetzte Interaktionssegmente;

Schritt 3: Umwandeln der grundlegenden Interaktionssegmente und zusammengesetzten Interaktionssegmente in Automaten;

[0008] 1) Für ein grundlegendes Interaktionssegment wird die grundlegende Interaktionssequenz in einem Quaternion BIS = (O, M, E, V) ausgedrückt, wobei O den Satz der Interaktionsobjekte, M den Satz der Nachrichten, E den Satz der Ereignisse und V eine teilweise geordnete Beziehung zwischen Interaktionsereignissen darstellen, und daraus ergibt sich ein Satz T von Spuren der Interaktionsfolge, der dann gemäß dem folgenden Algorithmus umgesetzt wird.

Algorithmus 1 Grundlegende Interaktionssegmente werden in ein Automatenmodell transformiert
Eingabe: BIS=(O, M, E, V)

Ausgabe: Automatenmodell

1: Erzeugen eines initialen Zustandsknotens q0;

2: Für jeden Nicht-Endzustandsknoten q, der über keine Kante hinausgeht:

3: Erhalten eines Satzes L von Ereignissen aus dem Zustand q0 bis q;

4: Jedes Ereignis e gehört zum Satz E-L:

5: Wenn ein beliebiges Ereignis e' die Formel (e', e) E V und e' E L erfüllt:

6: Erzeugen eines neuen Zustandsknotens q' und eines neuen Übergangs (q, e, q');

7: Zu einem beliebigen Zustandsknoten q"(q":≠q'):

8: L': = alle Ereignissatze von Zustandsknoten q0 bis q';

9: L": = alle Ereignissatze von Zustandsknoten q0 bis q';

10: wenn L' = L":

11: Zusammenführen von Zustandsknoten q' und q" zu einem Knoten q';

12: Aktualisierung des Übergangs (q, e, q") zu (q, e, q');

13: Wenn der Zustandsknoten q keine neue Übergangsaktualisierung aufweist:

14: Markieren q als der Endzustandsknoten;

15: Ausgabe des Automatenmodells

[0009] Zuerst wird ein Anfangszustand q0 erzeugt, wobei der Satz L den Satz von Ereignissen darstellt, die im Übergang vom Zustand q0 zum Zustand q über eine Anzahl von Übergängen auftreten, und als nächstes werden Ereignisse in dem Satz E-L, welche keine Vorgängerereignisse oder Vorgängerereignisse in dem Satz L aufweisen, gefunden, wodurch neue Übergänge und Zustände erzeugt werden, und die jeweiligen Sätze werden dann für die Iteration aktualisiert, bis keine weitere Übergänge und Zustände erzeugt werden. In dem Prozess des Erzeugens des Automaten werden die gleichen Zustandsknoten in dem Satz L zusammengeführt, wodurch der einfachste Automat erzeugt wird.

[0010] 2) Für einen zusammengesetzten Interaktionssegment, Erzeugen eines entsprechenden Automaten von der internen Interaktionssequenz nach dem Transformationsverfahren des grundlegenden Interaktionssegments, wobei q0 der Anfangszustand und qn der Endzustand ist. Gleichzeitig ist es erforderlich, die Generierung des kompletten Automaten nach seinen verschiedenen Typen zu treffen, und die Methode ist wie folgt:

[0011] 21) Für ein zyklisches kombiniertes Segment mit einem Minimum a Zyklen und einem Maximum von b Zyklen (a ≤ b) werden zuerst zwei neue Positionsknoten q und qf erzeugt, und gleichzeitig wird die Steuervariable i erzeugt, und i ist an allen Knoten über die Zeit inkrementierbar, und die folgenden Übergängen $q\xrightarrow[i:=i+1]{i<b} q0$, $q\xrightarrow{i\geq b} qf$ fwerden dann erzeugt, wobei die Formel verwendet wird, um die Anzahl von Zyklen zu begrenzen, und die Zuweisungsoperation i : =i+1 wird verwendet, um die Anzahl von Zyklenausführungen aufzuzeichnen, die nach jeder Ausführung um 1 erhöht wird; $qn\xrightarrow{i\geq a} qf$, wobei die Formel i ≥ a angibt, dass der Eintritt in den Zustand qf nur zugelassen wird, nachdem die Anzahl der Zyklenausführungen a überschreitet, und anderenfalls in den Zustand q übergegangen wird, und schließlich werden die Positionsknoten q und qf als neuer Anfangszustand und Endzustand des aktuellen Automaten markiert.

[0012] 22) Für das auswählbare kombinierte Segment wird zunächst ein neuer Positionsknoten q erzeugt, um anzuzeigen, ob die Formel g erfüllt ist, und das Hinzufügen eines neuen Übergangs $q\xrightarrow{g} q0$, $q\xrightarrow{!g} qn$ bedeutet, dass das Interaktionsverhalten innerhalb des kombinierten Interaktionssegments nur ausgeführt wird, wenn die Formel g erfüllt ist, andernfalls fährt es direkt in den Endzustand qn fort, und abschließend wird q als neuer Anfangszustand des aktuellen Automaten markiert.

[0013] 23) Für das verzweigte kombinierte Segment wird zunächst ein neuer Positionsknoten erzeugt, um anzuzeigen, ob die Formel g erfüllt ist, und der Übergang durch das Hinzufügen des Zustands q zu einem Anfangszustand eines erzeugten Automaten repräsentiert die Ausführung eines Verhaltens innerhalb des Interaktionssegments, wenn die Formel g erfüllt ist, und ansonsten wird das Verhalten in einem anderen

Interaktionssegment ausgeführt, und abschließend wird q als neuer Anfangszustand des aktuellen Automaten markiert.

[0014] 24) Für das kombinationale Interrupt-Segment wird vorgesehen, dass es keine Zeitsequenz-Beziehung zwischen Interaktionsereignissen innerhalb des kombinationalen Interrupt-Segments und Interaktionsereignissen außerhalb des Interrupts gibt, und das kombinationalen Interrupt-Segment wird als unabhängiges Subsystem zur Verarbeitung betrachtet, und aus seinen internen Interaktionssegment wird ein entsprechender Automat auf die oben beschriebene Weise erzeugt.

[0015] Schritt 4: Zusammenfassen der in Schritt 3 erhaltenen mehreren Automaten zu einem Automaten;

[0016] 1) Zusammenführen aller anderen Interaktionssegmente als des kombinationalen Interrupt-Segments zu einem Automaten, und da alle Interaktionssegmente eine gewisse Beziehung aufweisen, werden ihre jeweiligen Automaten gemäß ihrer Beziehung zusammengeführt. Unter der Annahme, dass für zwei Automaten A und B die Auftrittszeit aller Ereignisse, die Automaten A entsprechen, allen Ereignissen in Automaten B vorausgeht, und die Arbeitsschritte zum Zusammenführen sind wie folgt:

11) Kombinieren des Endzustands qa des Automaten A mit dem Anfangszustand lb des Automaten B und Neumarkieren des Zustands mit q;

12) Ändern eines beliebigen Übergangs (1, e, qa) in Automaten A in (1, e, q) , wobei 1 der Zustand im Automaten A ist und e ein Ereignis im Automaten A ist;

13) Ändern eines beliebigen Übergangs (lb, e', l') im Automaten B in (q, e', l') , wobei l' der Zustand im Automaten B ist und e' ein Ereignis im Automaten B ist;

[0017] 2) Kombinieren eines Automatenmodells, das dem kombinationalen Interrupt-Segment entspricht, in den Automaten, der in 1) erzeugt wurde. Für ein nicht unterbrochenes Interaktionssegment wird es als ein Interaktionssegment mit einer Priorität 0 angesehen, und irgendein anderer Interrupt kann seine Ausführung der Aufgabe unterbrechen, und die Arbeitsschritte zum Zusammenführen sind wie folgt:

21) Verbinden von hochprioren Automaten mit niedrigprioren Automaten nach dem Prinzip, dass hochpriore Aufgaben niederpriore Aufgaben unterbrechen. Unter der Annahme, dass die Priorität des Automaten A als 1 vorgesehen ist und die Priorität des Automaten B als 2 vorgesehen ist, kann der Zustand des Automaten B hinter jedem Zustand des Automaten A auftreten. Q ist ein beliebiger Zustandsknoten des Automaten A, und 10 ist der Anfangszustandsknoten des Automaten B, und In ist der Endzustandsknoten des Automaten B, und Hinzufügen des folgenden neuen $\text{Übergang}\, q \xrightarrow[\text{gMacher=mark;}]{\text{macher=gMacher;}} 10$, $In \xrightarrow[\text{gMacher=macher;}]{\text{gMacher=mark;}} q$, wobei mark eine einzige Paarmarke beim

[0018] Aufzeichnen des Eintritts in das aktuelle Interrupt und Verlassen des Interrupts ist, und gMacher eine globale Variable ist, die eine Marke anzeigt, dass der aktuelle Interrupt eintritt, während macher eine Paarmarke zum Aufzeichnen bevor der Interrupt eintrifft ist. der Übergang von q → 10 zeigt an, dass die Paarmarke vom Eintritt beim Eintritt in einen Automaten mit hoher Priorität durch macher gespeichert wurde, und dass die Paarmarke des aktuellen Übergangs durch gMacher aufgezeichnet wurde, und die Formel des Übergangs In → q stellt dar, dass der Zustand q durch den Übergang erreicht werden kann, wenn die Paarmarken identisch sind, wobei gMacher die Paarmarke vor Eintritt des Interrupts erneut aufzeichnet, damit es beim Austritt des vorherigen Interrupts für paarweisen Übergang verwendet wird. dieselbe Operation wird für alle Zustände im Automaten A durchgeführt, um einen kombinierten Automaten C zu erhalten;

[0019] 22) gemäß Schritt 21) werden alle Automaten so verbunden, dass hohe Priorität niedrige Priorität unterbricht, um den kombinierten Automaten C zu erhalten.

[0020] Schritt 5: Extrahieren von Beschränkungen im Interrupt-Sequenzdiagramm, wobei die Beschränkungen zu dem konvertierten Automatenmodell hinzugefügt werden;

[0021] 1) Für jede normale Zeitbeschränkung, Erzeugen einer Taktvariable c, die bei jedem Zustandsknoten über die Zeit erhöht werden kann. Die Zeitbeschränkung $e_y - e_x < a$ angibt, dass ein Ereignis e_y in a Zeiteinheiten nach dem Auftreten des Ereignissee_x abgeschlossen werden muss. Für alle Ereignissequenzen, Setzen des Taktes c auf 0, wenn das Ereignis $e_x$auftritt, Die Übergangsformel $c< a$ wird zum Zeitpunkt des Auf-

tretens des Ereignisses e_y hinzugefügt, was angibt, dass der Übergang vom Automaten zum nächsten Zustand erfolgt, wenn die Bedingung erfüllt ist.

[0022] 2) Für jede der Projektionszeitbeschränkungen wird eine Taktvariable c ebenfalls erzeugt; es wird angenommen, dass die Projektionszeitbeschränkung $(e_y - e_x) \uparrow < a$ anzeigt, dass ein Ereignis e_y innerhalb von a Zeiteinheiten nach dem Auftreten des Ereignissese$_x$ (die Laufzeit der Interrupt-Aufgabe wird entfernt) beendet werden muss. Dabei kann die Taktvariable c an allen Zustandsknoten bei Ereignis e_y und e_x des Automaten mit der Zeit erhöht werden, während die Taktvariable an Zustandsknoten anderer Automaten unverändert bleiben. Für alle Ereignissequenzen, Setzen des Taktes c auf 0 ebenfalls, wenn das Ereignis $e_x$auftritt, wobei, wenn ein Interrupt auftritt, die Taktung ausgesetzt wird, da die Änderungsrate der Taktvariable c an den anderen Zustandsknoten 0 ist, wobei die Taktung erneut beginnt, wenn die Interrupt-Aufgabe endet und zu der aktuellen Aufgabenausführungssequenz zurückkehrt, und das Hinzufügen von Übergangsformel $c< a$ bei Auftreten eines Ereignisses e_y zeigt an, dass der Übergang vom Automaten zum nächsten Zustand erst dann erfolgt, wenn die Bedingung erfüllt ist.

[0023] Schritt 6: Extrahieren von Verifizierungsattribute-Informationen im Interrupt-Sequenzdiagramm, wobei die Verifizierungsattribute als Beschränkungen dem konvertierten Automatenmodell hinzugefügt werden; hinsichtlich der Aufgaben-Zeitüberschreitungsattribute und der Datenkonsistenionsattribute werden Ausdrücke, die ihre Attribute beschreiben, invertiert, die als Zeitbeschränkungsausdruck gemäß der Methode von Schritt 5 zu dem Automaten hinzugefügt werden.

[0024] Schritt 7: Beschreiben des Automaten als Eingabeformat, das für das Automatenverifizierungswerkzeug akzeptabel ist; die gemäß Schritt 6 erhaltenen Informationen des Automaten werden in ein für das Verifizierungswerkzeug akzeptables Dateiformat konvertiert.

Technische Effekte der Erfindung sind:

1) Es wird ein Übergangsalgorithmus für das Interrupt-Sequenzdiagramm-Modell in ein Automatenmodell bereitgestellt, und das intuitiv visuelle und leicht verständliche Interrupt-Sequenzdiagramm-Modell kann automatisch in ein entsprechendes Automatenmodell umgesetzt werden, was die Modellierungskosten und die Wahrscheinlichkeit von Modellfehlern reduziert, und das Hinzufügen eines Beschränkungsausdrucks als eine Taktvariable zu dem Automaten stellt effektiv die Echtzeitanforderungen des Interrupt-Antriebssystems dar;

2) Durch das Kombinieren des Automaten, der aus dem kombinationalen Interrupt-Segment erhalten wird, und des Automaten, der aus den Interaktionssegmenten außerhalb des kombinationalen Interrupt--Segments erhalten werden, wird eine große Anzahl an ineffizienten Übergängen effektiv verringert;

Das Umwandeln eines Attributverifizierungsproblems des Interrupt-Antriebssystems in ein Entscheidungsproblem der Erreichbarkeit des Automaten unter Verwendung des Verifizierungswerkzeugs des Automatenmodells erfolgt indirektes Verifizieren des Interrupt-Sequenzdiagramm-Modells, um den Entwickler und Designer zu unterstützen;

Die vorliegende Erfindung modelliert das Interrupt-Antriebsmodell unter Verwendung eines Interrupt-Sequenzdiagramms, und gleichzeitig wird ein Verfahren zum Konvertieren eines Interrupt-Sequenzdiagramm-Modells in ein entsprechendes Automatenmodell bereitgestellt, und das Interrupt-Sequenzdiagramm-Modell indirekt unter Verwendung eines Verifizierungswerkzeugs des Automatenmodells verifiziert wird, um die Modellbildung und Verifikation des Interrupt-Antriebssystems durch den Entwickler zu erleichtern.

Figurenliste

Fig. 1 ist eine Darstellung eines Interrupt-Sequenzdiagramm-Modells in einem Ausführungsbeispiel der vorliegenden Erfindung.

Fig. 2 ist ein Automatenmodell, das durch grundlegende Interaktionssegmente in einem Ausführungsbeispiel der vorliegenden Erfindung erzeugt wird.

Fig. 3 ist ein Automatenmodell, das durch zyklische kombinierte Interaktionssegmente in einem Ausführungsbeispiel der vorliegenden Erfindung erzeugt wird.

Fig. 4 ist ein Automatenmodell, das durch kombinierte Interrupt-Interaktionssegmente in einem Ausführungsbeispiel der vorliegenden Erfindung erzeugt wird.

Fig. 5 ist ein Automatenmodell, das durch alle Interaktionssegmente mit Ausnahme eines Interrupts in einem Ausführungsbeispiel der vorliegenden Erfindung erzeugt wird.

Fig. 6 ist ein Automatenmodell nach der Vereinigung aller Interaktionssegmente in einem Ausführungsbeispiel der vorliegenden Erfindung.

Fig. 7 ist ein Automatenmodell, in dem übliche Zeitbeschränkungen in einem Ausführungsbeispiel der vorliegenden Erfindung als Taktvariable hinzugefügt sind.

Fig. 8 ist ein Automatenmodell, in dem Projektionszeitbeschränkungen in einem Ausführungsbeispiel der vorliegenden Erfindung als Taktvariable hinzugefügt sind.

Fig. 9 ist ein aus **Fig. 1** konvertiertes Automatenmodell.

AUSFÜHRLICHE BESCHREIBUNG

[0025] Der detaillierte Prozess der Modellumwandlung und Modellvalidierung wird im Folgenden unter Verwendung des vorliegenden Verfahrens in Verbindung mit einem einfachen Interrupt-Sequenzdiagramm-Modell erläutert.

[0026] Verfahren zur Verifizierung eines Interrupt-Antriebssystems basierend auf einem Interrupt-Sequenzdiagramm des vorliegenden Ausführungsbeispiels, 1) zuerst wird ein Beispiel eines Interrupt-Sequenzdiagramm-Modells erläutert. Die Modellsituation ist in **Fig. 1** dargestellt:

11) Es gibt drei Interaktionsobjekte in dem System: Proxy-Objekt (Agent), Interruptsdienst-Objekte (Service) und Fremdgeräte-Objekte (Peripheral).

12) Es gibt drei kombinierte Interaktionssegmente in dem System, d.h. ein zyklisches kombiniertes Segment, zwei kombinationale Interrupt-Segmente IRQ1 und IRQ2, mit Prioritäten, die jeweils 1 und 2 sind. IRQ1 ist die Interaktion des Proxy-Objekts mit dem Interruptsdienst-Objekt, und IRQ2 ist die Interaktion des Proxy-Objekts mit dem Fremdgeräte-Objekt.

13) Eine Anzahl von Beschränkungen und Verifizierungsattributen, einschließlich normalen Zeitbeschränkungen und Projektionszeitbeschränkungen.

2) Aufteilen der Interaktionssegmente in grundlegende Interaktionssegmente und kombinierte Interaktionssegmente gemäß Schritt 2, und nach **Fig. 1** können wir ein grundlegendes Interaktionssegment und drei kombinierte Interaktionssegmente (ein zyklisches kombiniertes Interaktionssegment und zwei kombinierte Interrupt-Interaktionssegmente) erhalten;

3) Umwandeln aller resultierenden Interaktionssegmente in ein entsprechendes Automatenmodell;

31) Für die Gruppe der grundlegenden Interaktionssegmente in **Fig. 1** sind ihre Quaternion wie folgt dargestellt: einen Satz von Interaktionsobjekten O = {Agent, Service, Peripheral}, einen Satz von Nachrichten M = {e12, e34}, einen Satz von Ereignissen E = {e1, e2, e3, e4}, eine zeitsequentielle Beziehung eines Interaktionsereignisses V = {e1 < e2, e2<e3, e3<e4}, und der Satz der Spuren der grundlegenden Interaktionssegmente wird als T = {e1 → e2 → e3 → e4} erhalten, und zunächst wird aus einer ersten Zeile des Algorithmus eine Ausgangsposition 0 des Automaten erzeugt, und der zu diesem Zeitpunkt erzeugte Automat hat nur einen Nicht-Endzustand 0 und hat keinen Übergang, und nach dem Eintritt in den Zyklus der zweiten Zeile ist es einer leere Satz, d. h. der Satz der Ereignisse, die vom Anfangszustand 0 nach mehreren Übergängen zur Position q aufgetreten sind. Dann wird es in Zeile 4 erfolgen - = {1, 2, 3, 4}, und dann werden alle Ereignisse, die keine Vorgängerereignisse haben und die nicht in dem Satz von bereits aufgetretenen Ereignissen aufgetreten sind, in Zeile 5 gefunden, und entsprechende Positionen und Übergänge werden dann in Zeile 6 erzeugt. Zu diesem Zeitpunkt ist {0, 1} der Zustandssatz der Automaten, und {(0, 1, 1)} ist der Übergangssatz. Über die fortlaufenden Iterationen, wenn keine neuen Zustandsknoten und Übergänge zu dem Automaten hinzugefügt werden, wird der letzte Zustandsknoten als Endknoten gekennzeichnet, und der sich ergebende Automat ist in **Fig. 2** gezeigt.

32) Für jedes zirkuläre kombinierte Segment innerhalb des zusammengesetzten kombinierten Segments, wird der Automat in der Form von grundlegenden Interaktionssegmenten in dessen Inneren erzeugt, danach wird ein neuer Zustandsknoten q und qn erzeugt, und das Hinzufügen des i≥3 i≥1 i<3 neuen Übergangs, $q \xrightarrow{i\geq 3} qn$, $q2 \xrightarrow{i\geq 1} qn$, $q2 \xrightarrow{i<3} q$ erfolgt, und q und qn sind dann als neue Anfangszustand und Endzustand vorgesehen, und der resultierende Automat ist in **Fig. 3** gezeigt.

33) Für ein kombinationales Interrupt-Segment hat das Interrupt-Interaktionssegment keine zeitliche Beziehung zu Interaktionssegmenten außerhalb des Interrupts, somit betrachten wir das kombinationale Interrupt-Segment als ein einzelnes Subsystem, wobei der resultierende Automat wie in **Fig. 4** gezeigt ist.

4) Alle resultierende Automaten werden zu einem Automaten zusammengefasst.

41) Zunächst werden alle Automaten außer den Automaten, die durch das Interrupt-Interaktionssegment erzeugt wurden, gemäß der Zeitsequenz-Beziehung zu einem Automaten zusammengefasst, und der Endzustand des vorhergehenden Automaten in der Zeitbeziehung wird mit dem Anfangszustand des nachfolgenden Automaten in der Zeitbeziehung kombiniert, und die Zustandsvariablen in relevanten Übergängen werden modifiziert, um einen neuen Automaten zu erhalten, wie in **Fig. 5** gezeigt.

42) Interaktionssegmente, die durch den in Schritt 41) erhaltenen Automaten beschrieben wird, werden als Interaktionssegmente mit der Priorität 0 angesehen. Da ein hochpriorer Automat an einem beliebigen Zustandsknoten einen niedrigprioren Automaten unterbrechen kann, ist es notwendig, den hochprioren Automaten mit dem niedrigprioren Automaten zu verbinden, und alle Zustandsknoten mit niedriger Priorität werden zu den Übergängen von Automaten mit hoher Priorität hinzugefügt und aus diesen entfernt. Wenn man den Zustandsknoten q1 als Beispiel nimmt und angenommen wird, dass das Interrupt IRQ1 im Zustand q1 stattfindet, müssen wir zwei neue Übergänge

$q1 \xrightarrow[\substack{macher=gMacher;\\ gMacher=1}]{} q8;$ $q10 \xrightarrow[gMacher=macher;]{gMacher=1;} q1$ hinzufügen (q8 und q10 sind der Anfangszustand und Endzustand des Interrupts IRQ1) , wobei gMacher verwendet wird, um die eindeutige Paarmarke seiner eingehenden und ausgehenden Kante aufzuzeichnen, macher wird zum Aufzeichnen von Paarmarke vor Eintritt in den Automaten hoher Priorität verwendet. Die oben beschriebenen Operationen werden an allen anderen Zustandsknoten ausgeführt, und gleiches gilt für IRQ2 entsprechend, und es ist zu beachten, dass IRQ2 nicht nur die grundlegenden Interaktionssegmente unterbrechen kann, sondern auch IRQ1 unterbrechen kann. Das resultierende Automatenmodell ist in **Fig. 6** dargestellt, in der die Formel des Übergangs und die Zuweisung wie folgt sind: 1: macher: =gMacher; gMacher: =0

2: macher: =gMacher; gMacher: =1

3: macher: =gMacher; gMacher: =2

4: macher: =gMacher; gMacher: =3

5: macher: =gMacher; gMacher: =4

6: macher: =gMacher; gMacher: =5

7: macher: =gMacher; gMacher: =6

8: macher: =gMacher; gMacher: =7

9: gMacher=0; gMacher: =macher

10: gMacher=1; gMacher: =macher

11: gMacher=2; gMacher: =macher

12: gMacher=3; gMacher: =macher

13: gMacher=4; gMacher: =macher

14: gMacher=5; gMacher: =macher

15: gMacher=6; gMacher: =macher

16: gMacher=7; gMacher: =macher

17: macher: =gMacher; gMacher: =0

18: macher: =gMacher; gMacher: =1

19: macher: =gMacher; gMacher: =2

20: macher: =gMacher; gMacher: =3

21: macher: =gMacher; gMacher: =4

22: macher: =gMacher; gMacher: =5

23: macher: =gMacher; gMacher: =6

24: macher: =gMacher; gMacher: =7

25: gMacher=0; gMacher: =macher

26: gMacher=1; gMacher: =macher

27: gMacher=2; gMacher: =macher

28: gMacher=3; gMacher: =macher

29: gMacher=4; gMacher: =macher

30: gMacher=5; gMacher: =macher

31: gMacher=6; gMacher: =macher

32: gMacher=7; gMacher: =macher

33: macher: =gMacher; gMacher: =0

34: macher: =gMacher; gMacher: =1

35: macher: =gMacher; gMacher: =2

36: gMacher=0; gMacher: =macher

37: gMacher=1; gMacher: =macher

38: gMacher=2; gMacher: =macher。

[0027] 5) Extrahieren von Beschränkungen im Interrupt-Sequenzdiagramm, wobei die Beschränkungen zu dem konvertierten Automatenmodell hinzugefügt werden;

[0028] 51) Für den normalen Zeitbeschränkungsausdruck stellen wir die Taktvariablen c43, d.h. 2< e4-e3<4 als ein Beispiel ein, wobei die Rate der Änderung des Takts an allen Zustandsknoten eins ist, und wir finden den Übergang auf dem Automatenmodell, bei dem Ereignis e3 stattgefunden hat, und initialisieren c43 auf 0, und das Hinzufügen von Formel 2< c43<4 beim Übergang, bei dem Ereignis e4 stattgefunden hat, anzeigt, dass der nächste Zustandsknoten durch den Übergang nur erreicht werden kann, wenn die Taktvariablen erfüllt werden, wobei das Teil des Automatenmodells in **Fig. 7** dargestellt ist.

[0029] 52) Für den Ausdruck der Projektionszeitbeschränkung nehmen wir 1<(e2-e1) ↑<2 als Beispiel, um die Taktvariable c21 zu setzen, und die Änderungsrate der Taktvariable in allen Zustandsknoten des Automaten, in denen sich Ereignisse e2 und e1 befinden, gleich 1 ist, und die Änderungsrate an den Zustandsknoten des anderen Automaten ist 0. Auch beim Übergang, bei dem Ereignis e1 stattgefunden hat, wird c21 auf 0 initialisiert, und das Hinzufügen von Formel 1<e2-e1<2 beim Übergang, bei dem Ereignis e2 stattgefunden hat, anzeigt, dass der nächste Zustandsknoten durch den Übergang nur erreicht werden kann, wenn die Taktvariablen erfüllt werden, und als Beispiel nehmen wir in diesem Teil IRQ1, der die Nachrichtenübertragung zwischen den Ereignissen e2 und e1 unterbricht, und das Automatenmodell ist in **Fig. 8** dargestellt.

[0030] 6) Extrahieren von Verifizierungsattributeninformationen e2-e1<10 aus dem Interrupt-Sequenzdiagramm, und wir invertieren den Ausdruck, um e2-e1≥ 10 zu erhalten, dann wird es dem Automatenmodell gemäß normalen Zeitbeschränkungen hinzugefügt, und das resultierende vollständige Automatenmodell wird in **Fig. 9** gezeigt, in der die Formel des Übergangs und die Zuweisung wie folgt sind:

1: macher: =gMacher; gMacher: =0

2: macher: =gMacher; gMacher: =1

3: macher: =gMacher; gMacher: =2

4: macher: =gMacher; gMacher: =3

5: macher: =gMacher; gMacher: =4

6: macher: =gMacher; gMacher: =5

7: macher: =gMacher; gMacher: =6

8: macher: =gMacher; gMacher: =7

9: gMacher=0; gMacher: =macher

10: gMacher=1; gMacher: =macher

11: gMacher=2; gMacher: =macher

12: gMacher=3; gMacher: =macher

13: gMacher=4; gMacher: =macher

14: gMacher=5; gMacher: =macher

15: gMacher=6; gMacher: =macher

16: gMacher=7; gMacher: =macher

17: macher: =gMacher; gMacher: =0

18: macher: =gMacher; gMacher: =1

19: macher: =gMacher; gMacher: =2

20: macher: =gMacher; gMacher: =3

21: macher: =gMacher; gMacher: =4

22: macher: =gMacher; gMacher: =5

23: macher: =gMacher; gMacher: =6

24: macher: =gMacher; gMacher: =7

25: gMacher=0; gMacher: =macher

26: gMacher=1; gMacher: =macher

27: gMacher=2; gMacher: =macher

28: gMacher=3; gMacher: =macher

29: gMacher=4; gMacher: =macher

30: gMacher=5; gMacher: =macher

31: gMacher=6; gMacher: =macher

32: gMacher=7; gMacher: =macher

33: macher: =gMacher; gMacher: =0

34: macher: =gMacher; gMacher: =1

35: macher: =gMacher; gMacher: =2

36: gMacher=0; gMacher: =macher

37: gMacher=1; gMacher: =macher

38: gMacher=2; gMacher: =macher。

[0031] 7) Der Automat wird als Eingabeformat beschrieben, das für das Automatenverifizierungswerkzeug akzeptabel ist, und in dem Automatenverifizierungswerkzeug verifiziert.

[0032] Oben sind nur die bevorzugten Ausführungsformen der Erfindung beschrieben. Es soll bemerkt werden, dass für die normalen Techniker in dem Fachgebiet, einige Verbesserungen und Modifikationen gemacht werden können, die als Schutzumfang der Erfindung angesehen werden sollen, ohne von den Lehren der Erfindung abzuweichen.

Patentansprüche

1. Verfahren zur Verifizierung eines Interrupt-Antriebssystems basierend auf einem Interrupt-Sequenzdiagramm, **dadurch gekennzeichnet**, dass die folgenden Schritte enthalten sind:
Schritt 1. Aufbau eines Modells des Interrupt-Antriebssystems basierend auf dem Interrupt-Sequenzdiagramm; das Interrupt-Sequenzdiagramm umfasst Interaktionsobjekte, Interaktionssegmente, Beschränkun-

gen, Verifizierungsattribute; da das Auftreten und Verarbeiten von Interrupts eine zeitliche Ungewissheit besitzt, wird vorgesehen, dass es keine zeitliche teilweise geordnete Beziehung zwischen Interaktionsereignissen innerhalb eines kombinationalen Interrupt-Segments und Ereignissen außerhalb davon gibt, wobei für Interrupt-Priorität vorgesehen ist, dass die Ausführung von Interrupt-Segmenten mit hoher Priorität die Ausführung von Interrupts mit niedriger Priorität unterbrechen kann, jedoch kann die Ausführung des Interrupts mit niedriger Priorität nicht die Ausführung des Interrupts mit hoher Priorität unterbrechen, wobei für einen bedingten Ausdruck dass der bedingte Ausdruck wahr ist bedeutet die Interrupt-Aufgabe kann ausgelöst werden, und umgekehrt kann nicht ausgelöst werden;
Schritt 2. Aufteilen der Interaktionssegmente gemäß dem Interrupt-Sequenzdiagramm, das aus Schritt 1 resultiert, in grundlegende Interaktionen und zusammengesetzte Interaktionssegmente;
Schritt 3. Sequentielles Umwandeln der grundlegenden Interaktionssegmente und zusammengesetzten Interaktionssegmente in jeweilige Automatenmodelle;
Schritt 4. Kombinieren der Vielzahl von Automatenmodellen, die in Schritt 3 erhalten wurden, zu einem Automatenmodell, das ein Automatenmodell ist, in das ein Interrupt-Antriebsmodell umgewandelt wurde;
Schritt 5. Extrahieren von Beschränkungen im Interrupt-Sequenzdiagramm, wobei die Beschränkungen zu dem konvertierten Automatenmodell hinzugefügt werden;
Schritt 6. Extrahieren von Verifizierungsattribute-Informationen im Interrupt-Sequenzdiagramm, wobei die Verifizierungsattribute als Beschränkungen dem konvertierten Automatenmodell hinzugefügt werden;
Schritt 7. Beschreiben des Automaten als Eingabeformat, das für das Automatenverifizierungswerkzeug akzeptabel ist;
Schritt 8. Die Verifikation erfolgt mit einem Verifizierungswerkzeug des Automaten.

2. Verfahren zur Verifizierung eines Interrupt-Antriebssystems basierend auf einem Interrupt-Sequenzdiagramm nach Anspruch 1, **dadurch gekennzeichnet**, dass das Interrupt-Sequenzdiagramm im Schritt 1 ein zweidimensionales Diagramm ist; die Querachse listet aufeinander folgend Interaktionsobjekte auf, die Längsachse ist eine Zeitachse, und die Zeit erstreckt sich entlang der vertikalen Linie nach unten, um eine chronologische Reihenfolge der Interaktionszeiten der Objekte zu beschreiben; Interaktionsobjekte sind durch Lebenslinien dargestellt, und Interaktionen zwischen Objekten sind durch Nachrichten beschrieben; Nachrichten sind ein Kommunikationsmechanismus zwischen Objekten, und ein Signal wird von dem sendenden Objekt an ein anderes oder an mehrere andere empfangende Objekte gesendet, und der Nachrichtenübermittlungsprozess wird durch einen Pfeil beschrieben, und der Nachrichtenname wird auf der Linie mit dem Pfeil platziert, und die Sende- und Empfangsereignisse einer Nachricht weisen beide eindeutige Ereignisnamen auf, die an den Anfangs- und Endpunkten der Pfeillinie angeordnet sind; der komplexe Steuerungsablauf in dem Interrupt-Sequenzdiagramm ist durch das kombinierte Segment dargestellt, wobei die Funktionalität der verschiedenen kombinierten Segmente durch den Typ ihrer Interaktionsoperation bestimmt wird, loop zeigt eine Schleifenoperation, alt zeigt eine Verzweigungsoperation und opt zeigt eine optionale Operation an, und die Darstellungsweise ist dieselbe wie im UML-Sequenzdiagramm, während int-Operation eine erweiterte Operation des Interrupt-Sequenzdiagramms im Verhältnis zum Sequenzdiagramm ist, die auch die Grenzen eines kombinierten Segments darstellt, das von einem Block dargestellt wird, und links oben im Block zeigt die Zeichenfolge int an, dass der Typ des kombinierten Segments der Interrupt-Operationstyp ist, und p zeigt die Interrupt-Priorität an, id ist der Name des kombinationalen Interrupt-Segments, und condition ist ein bedingter Ausdruck, der eine Bedingung angibt, dass ein Interrupt aufgetreten ist.

3. Verfahren zur Verifizierung eines Interrupt-Antriebssystems basierend auf einem Interrupt-Sequenzdiagramm nach Anspruch 1, **dadurch gekennzeichnet**, dass das Verfahren zur Transformation sowohl der grundlegenden Interaktionssegmente als auch der zusammengesetzten Interaktionssegmente in ein entsprechendes Automatenmodell in Schritt 3 ist:
1) Für ein grundlegendes Interaktionssegment wird die grundlegende Interaktionssequenz in einem Quaternion BIS = (O, M, E, V) ausgedrückt, wobei O einen Satz der Interaktionsobjekte, M einen Satz der Nachrichten, E einen Satz der Ereignisse und V eine teilweise geordnete Beziehung zwischen Interaktionsereignissen darstellen, und daraus ergibt sich ein Satz T von Spuren der Interaktionsfolge, der dann gemäß dem folgenden Algorithmus umgesetzt wird:
zuerst wird ein Anfangszustand q0 erzeugt, wobei der Satz L den Satz von Ereignissen darstellt, die im Übergang vom Zustand q0 zum Zustand q über eine Anzahl von Übergängen auftreten, und als nächstes werden Ereignisse in dem Satz E-L, welche keine Vorgängerereignisse oder Vorgängerereignisse in dem Satz L aufweisen, gefunden, wodurch neue Übergänge und Zustände erzeugt werden, und die jeweiligen Sätze werden dann für Iteration aktualisiert, bis keine weitere Übergänge und Zustände erzeugt werden; wobei in dem Prozess des Erzeugens des Automaten die gleichen Zustandsknoten in dem Satz L zusammengeführt werden, wodurch der einfachste Automat erzeugt wird;

2) Für einen zusammengesetzten Interaktionssegment, Erzeugen eines entsprechenden Automaten von der internen Interaktionssequenz nach dem Transformationsverfahren des grundlegenden Interaktionssegments, wobei q0 der Anfangszustand und qn der Endzustand ist; gleichzeitig ist es erforderlich, die Generierung des kompletten Automaten nach seinen verschiedenen Typen zu treffen, und die Methode ist wie folgt:

21) Für ein zyklisch kombiniertes Segment beträgt die Anzahl der Zyklen mindestens a und höchstens b, und zuerst werden zwei neue Positionsknoten q und qf erzeugt, während die Steuervariable i erzeugt wird, und i bleibt in jedem Zustandsknoten unverändert, und die folgenden Übergängen werden dann erzeugt $q\xrightarrow[i:=i+1]{i<b}q0$, $q\xrightarrow{i\geq b}qf$, wobei die Formel verwendet wird, um die Anzahl von Zyklen zu begrenzen, und die Zuweisungsoperation i:=i+1 wird verwendet, um die Anzahl von Zyklenausführungen aufzuzeichnen, die nach jeder Ausführung um 1 erhöht wird; $qn\xrightarrow{i\geq a}qf$, $qn\xrightarrow{i<b}q$, wobei die Formel i ≥ a angibt, dass der Eintritt in den Zustand qf nur zugelassen wird, nachdem die Anzahl der Zyklenausführungen a überschreitet, und anderenfalls in den Zustand q übergegangen wird, und schließlich werden die Positionsknoten q und qf als neuer Anfangszustand und Endzustand des aktuellen Automaten markiert;

22) Für das auswählbare kombinierte Segment wird zunächst ein neuer Positionsknoten q erzeugt, um anzuzeigen, ob die Formel g erfüllt ist, und das Hinzufügen eines neuen Übergangs $q\xrightarrow{g}q0$, $q\xrightarrow{!g}qn$ bedeutet, dass das Interaktionsverhalten innerhalb des kombinierten Interaktionssegments nur ausgeführt wird, wenn die Formel g erfüllt ist, andernfalls fährt es direkt in den Endzustand qn fort, und abschließend wird q als neuer Anfangszustand des aktuellen Automaten markiert;

23) Für das verzweigte kombinierte Segment wird zunächst ein neuer Positionsknoten erzeugt, um anzuzeigen, ob die Formel g erfüllt ist, und der Übergang durch das Hinzufügen des Zustands q zu einem Anfangszustand eines erzeugten Automaten repräsentiert die Ausführung eines Verhaltens innerhalb des Interaktionssegments, wenn die Formel g erfüllt ist, und ansonsten wird das Verhalten in einem anderen Interaktionssegment ausgeführt, und abschließend wird q als neuer Anfangszustand des aktuellen Automaten markiert;

24) Für das kombinationale Interrupt-Segment wird vorgesehen, dass es keine zeitliche Beziehung zwischen Interaktionsereignissen innerhalb des kombinationalen Interrupt-Segments und Interaktionsereignissen außerhalb des Segments gibt, und das kombinationale Interrupt-Segment wird als unabhängiges Subsystem behandelt, und aus seinen internen Interaktionssegment wird ein entsprechender Automat auf die oben beschriebene Weise erzeugt.

4. Verfahren zur Verifizierung eines Interrupt-Antriebssystems basierend auf einem Interrupt-Sequenzdiagramm nach Anspruch 1, **dadurch gekennzeichnet**, dass in Schritt 4 die in Schritt 3 generierten mehreren Automaten zu einem Automaten zusammengefasst werden, und die Methode ist wie folgt:

1) Zusammenführen aller anderen Interaktionssegmente als des kombinationalen Interrupt-Segments zu einem Automaten, und da alle Interaktionssegmente eine gewisse Beziehung aufweisen, werden ihre jeweiligen Automaten gemäß ihrer Beziehung zusammengeführt; für zwei Automaten A und B geht die Auftrittszeit aller Ereignisse, die Automaten A entsprechen, allen Ereignissen in Automaten B voraus, und die Arbeitsschritte zum Zusammenführen sind wie folgt:

11) Kombinieren des Endzustands qa des Automaten A mit dem Anfangszustand lb des Automaten B und Neumarkieren des Zustands mit q;

12) Ändern eines beliebigen Übergangs (1, e, qa) in Automaten A in (1, e, q) , wobei 1 der Zustand im Automaten A ist und e ein Ereignis im Automaten A ist;

13) Ändern eines beliebigen Übergangs (lb, e', l') im Automaten B in (q, e', l'), wobei 1' der Zustand im Automaten B ist und e' ein Ereignis im Automaten B ist;

2) Kombinieren eines Automatenmodells, das dem kombinationalen Interrupt-Segment entspricht, in den Automaten, der in 1) erzeugt wurde; für ein nicht-interruptes Interaktionssegment wird es als ein Interaktionssegment mit einer Priorität 0 angesehen, und irgendein anderer Interrupt kann seine Ausführung der Aufgabe unterbrechen, und die Arbeitsschritte zum Zusammenführen sind wie folgt:

21) Verbinden von hochprioren Automaten mit niedrigprioren Automaten nach dem Prinzip, dass hochpriore Aufgaben niederpriore Aufgaben unterbrechen; unter der Annahme, dass die Priorität des Automaten A als 1 vorgesehen ist und die Priorität des Automaten B als 2 vorgesehen ist, kann der Zustand des Automaten B hinter jedem Zustand des Automaten A auftreten; Q ist ein beliebiger Zustandsknoten des Automaten A, und 10 ist der Anfangszustandsknoten des Automaten B, und ln ist der Endzustandsknoten des Automaten B, und Hinzufügen des folgenden neuen $\text{Übergang}\,sq\xrightarrow[\substack{\text{macher=gMacher;}\\\text{gMacher=mark;}}]{}10$, $\text{ln}\xrightarrow[\text{gMacher=macher;}]{\text{gMacher=mark;}}q$, wobei mark eine einzige Paarmarke beim Aufzeichnen des Eintritts in das aktuelle Interrupt und Verlassen

des Interrupts ist, und gMacher eine globale Variable ist, die eine Marke anzeigt, dass der aktuelle Interrupt eintritt, während macher eine Paarmarke zum Aufzeichnen bevor der Interrupt eintrifft ist; der Übergang von q → 10 zeigt an, dass die Paarmarke vom Eintritt beim Eintritt in einen Automaten mit hoher Priorität durch macher gespeichert wurde, und dass die Paarmarke des aktuellen Übergangs durch gMacher aufgezeichnet wurde, und die Formel des Übergangs ln → q stellt dar, dass der Zustand q durch den Übergang erreicht werden kann, wenn die Paarmarken identisch sind, wobei gMacher die Paarmarke vor Eintritt des Interrupts erneut aufzeichnet, damit es beim Austritt des vorherigen Interrupts paarweise verwendet wird; dieselbe Operation wird für alle Zustandsknoten im Automaten A durchgeführt, um einen kombinierten Automaten C zu erhalten;
22) gemäß Schritt 21) werden alle Automaten so verbunden, dass hohe Priorität niedrige Priorität unterbricht, um den kombinierten Automaten C zu erhalten.

5. Verfahren zur Verifizierung eines Interrupt-Antriebssystems basierend auf einem Interrupt-Sequenzdiagramm nach Anspruch 1, **dadurch gekennzeichnet**, dass in Schritt 5 die Einschränkungsbedingung zu dem in Schritt 4 erhaltenen Automaten hinzugefügt wird, und die Methode ist wie folgt:
1) Für jede normale Zeitbeschränkung, Erzeugen einer Taktvariable c, die bei jedem Zustandsknoten über die Zeit erhöht werden kann; Angenommen, dass die Zeitbeschränkung e_y - e_x < a ist, die angibt, dass ein Ereignis e_y in a Zeiteinheiten nach dem Auftreten des Ereignisses e_x abgeschlossen werden muss; für alle Ereignissequenzen, Setzen des Taktes c auf 0, wenn das Ereignis $e_x$auftritt, und das Hinzufügen von Übergangsformel c< a bei Auftreten eines Ereignisses e_y zeigt an, dass der Übergang erfolgen wird, bis der Automat den nächsten Zustand erreicht, wenn die Bedingung erfüllt ist;
2) Für jede der Projektionszeitbeschränkungen wird eine Taktvariable c erzeugt; die Projektionszeitbeschränkung ist (e_y — e_x) ↑< a, die angibt, dass ein Ereignis e_y in a Zeiteinheiten nach dem Auftreten des Ereignisses e_x abgeschlossen werden muss, und die „a Zeiteinheiten“ umfassen die Laufzeit der Interrupt--Aufgabe nicht; dabei wird die Taktvariable c an allen Zustandsknoten bei Ereignis e_y und e_x des Automaten mit der Zeit erhöht, während die Taktvariable an Zustandsknoten anderer Automaten unverändert bleiben; gleiches gilt für alle Ereignissequenzen, dass Takt c zum Zeitpunkt des Auftretens des Ereignisses e_x auf 0 gesetzt wird, wobei, wenn ein Interrupt auftritt, die Taktung ausgesetzt wird, da die Änderungsrate der Taktvariable c an den anderen Zustandsknoten 0 ist, wobei die Taktung erneut beginnt, wenn die Interrupt-Aufgabe endet und zu der aktuellen Aufgabenausführungssequenz zurückkehrt, und wenn das Ereignis e_y eintritt, zeigt das Hinzufügen von Übergangsformel c< a an, dass der Übergang vom Automaten zum nächsten Zustand erst dann erfolgt, wenn die Bedingung erfüllt ist.

6. Verfahren zur Verifizierung eines Interrupt-Antriebssystems basierend auf einem Interrupt-Sequenzdiagramm nach Anspruch 1, **dadurch gekennzeichnet**, dass in Schritt 6 das Verifizierungsattribut zu dem in Schritt 4 erhaltenen Automaten hinzugefügt wird, und die Methode ist wie folgt: hinsichtlich der Aufgaben-Zeitüberschreitungsattribute und der Datenkonsistenionsattribute werden Ausdrücke, die ihre Attribute beschreiben, invertiert, die als Zeitbeschränkungsausdruck gemäß der Methode von Schritt 5 zu dem Automaten hinzugefügt werden.

7. Verfahren zur Verifizierung eines Interrupt-Antriebssystems basierend auf einem Interrupt-Sequenzdiagramm nach Anspruch 1, **dadurch gekennzeichnet**, dass in einem Schritt 7 der Automat als ein akzeptables Eingabeformat für das Automatenverifizierungswerkzeug beschrieben wird, und die Methode ist wie folgt: die gemäß Schritt 6 erhaltenen Informationen des Automaten werden in ein für das Verifizierungswerkzeug akzeptables Dateiformat konvertiert.

8. Verfahren zur Verifizierung eines Interrupt-Antriebssystems basierend auf einem Interrupt-Sequenzdiagramm nach Anspruch 1, **dadurch gekennzeichnet**, dass zunächst ein Verfahren zur Erzeugung entsprechender Automaten für unterschiedliche Interaktionssegmente in einem Interrupt-Sequenzdiagramm bereitgestellt wird, das auf Szenarien zur Verifizierung eines Interrupt-Antriebssystems anwendbar ist.

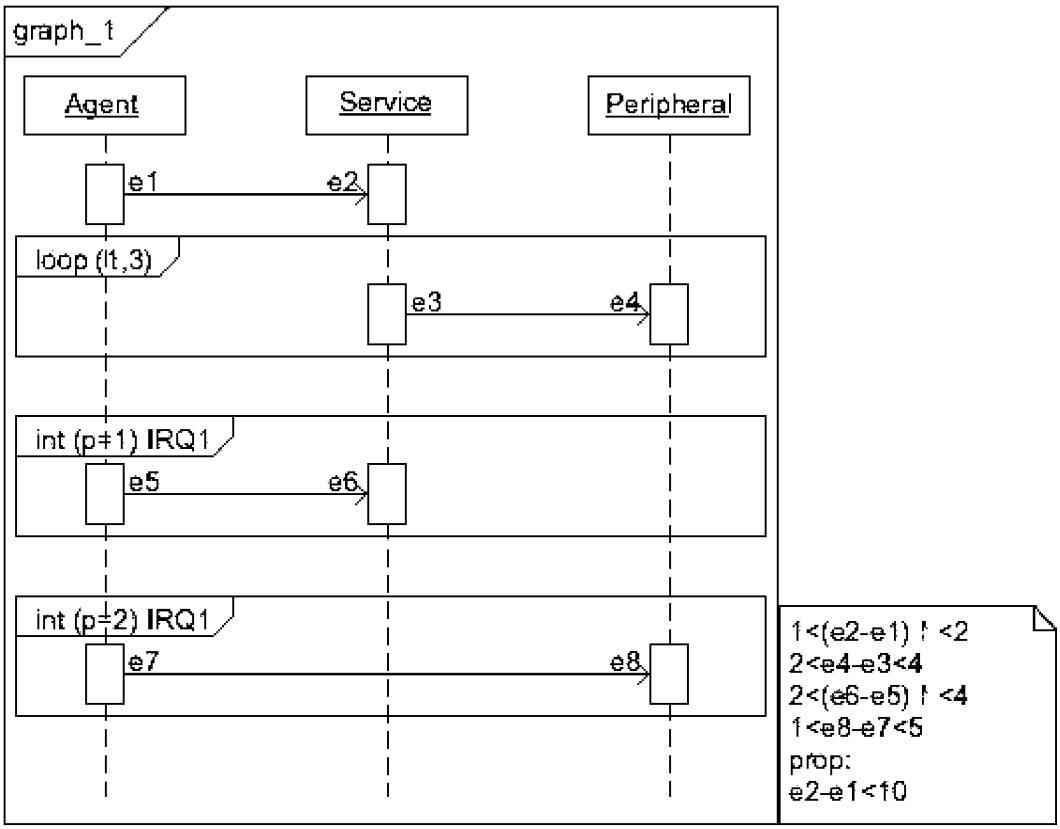
9. Verfahren zur Verifizierung eines Interrupt-Antriebssystems basierend auf einem Interrupt-Sequenzdiagramm nach Anspruch 2, **dadurch gekennzeichnet**, dass der Interrupt-Sequenzdiagramm insgesamt analysiert wird, und Automaten, die durch verschiedene Interaktionssegmente erzeugt wurden, werden als ein vollständiger Automat gemäß der Vereinigungsstrategie des Schritts 4 vereinigt, und Beschränkungen und Verifizierungsattribute werden dem Automaten hinzugefügt.

10. Verfahren zur Verifizierung eines Interrupt-Antriebssystems basierend auf einem Interrupt-Sequenzdiagramm nach Anspruch 1, **dadurch gekennzeichnet**, dass das Interrupt-Sequenzdiagramm-Modell in ein entsprechendes Automatenmodell umgewandelt wird und das Interrupt-Sequenzdiagramm-Modell indi-

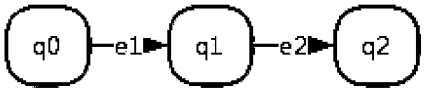
rekt unter Verwendung eines Verifizierungswerkzeugs des Automatenmodells verifiziert wird, um die Modellbildung und Verifikation durch den Entwickler zu erleichtern.

Es folgen 5 Seiten Zeichnungen

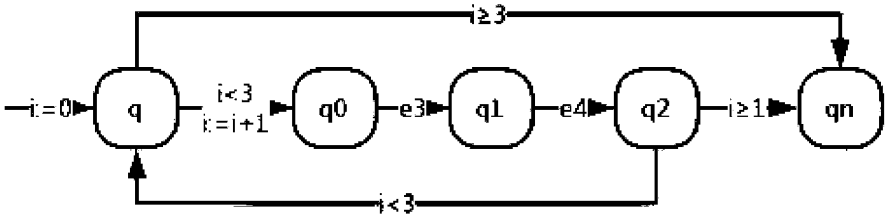
Anhängende Zeichnungen



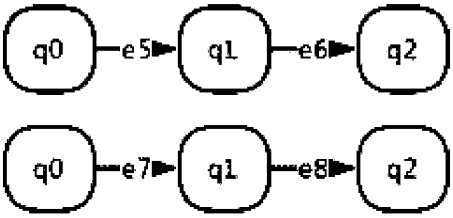
Figur 1



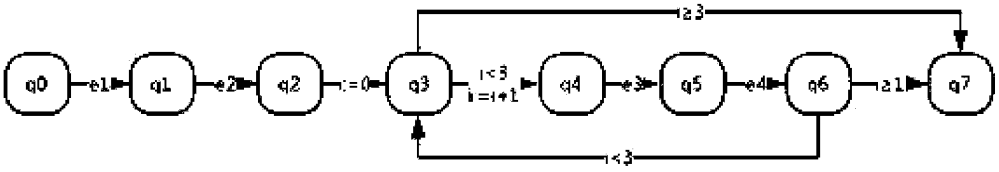
Figur 2



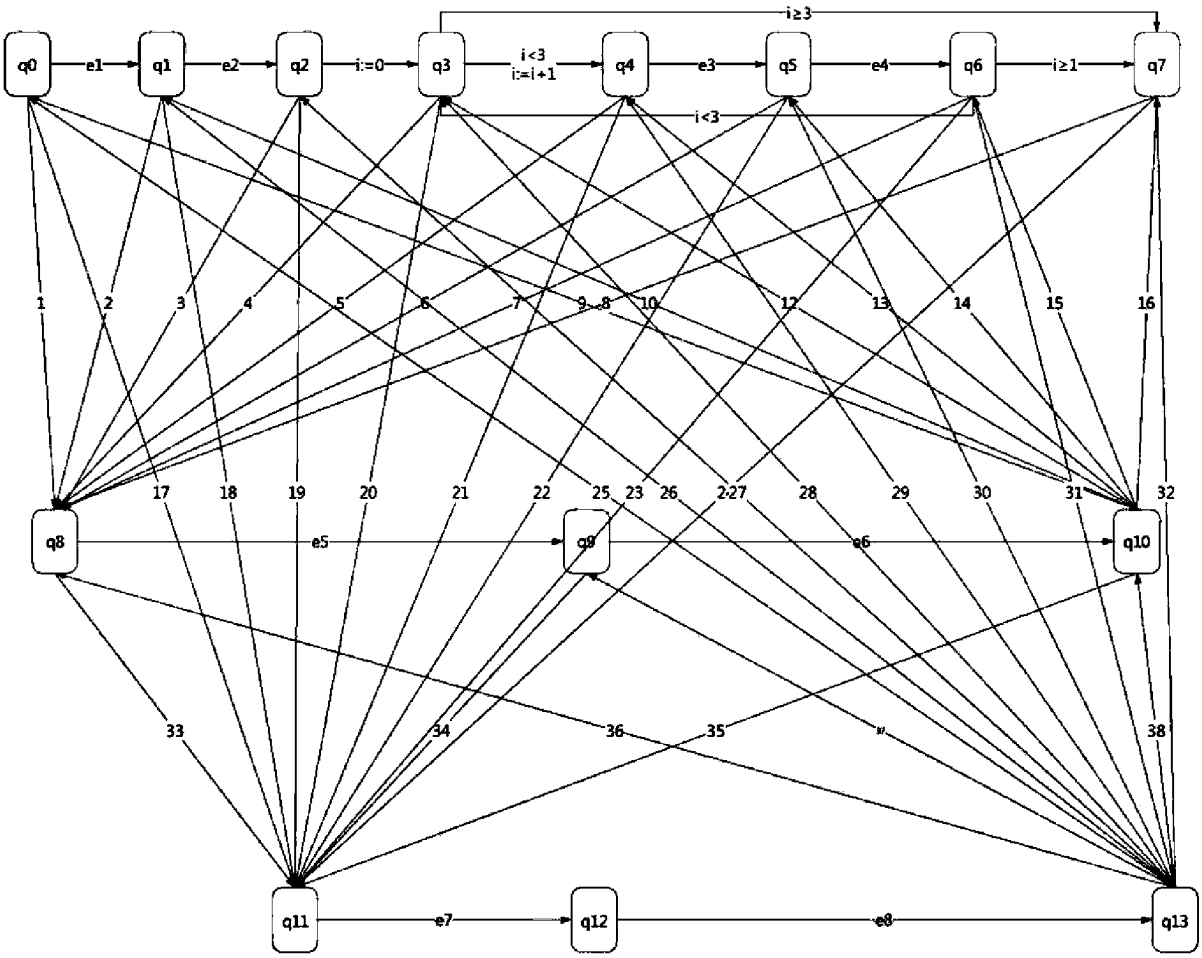
Figur 3



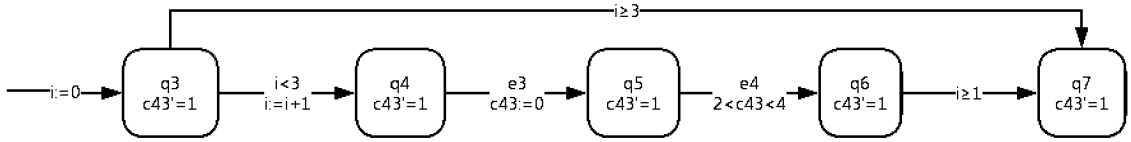
Figur 4



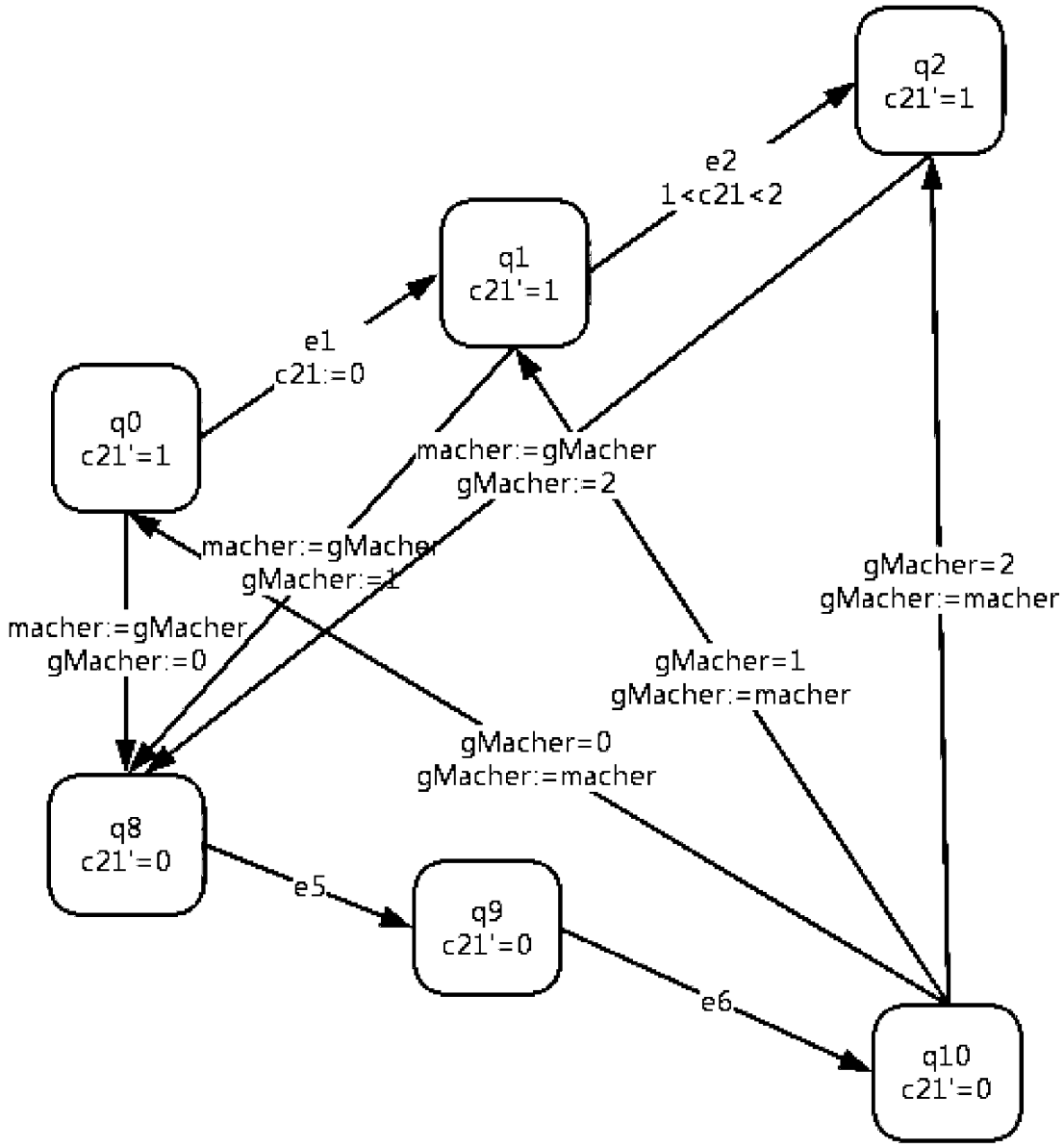
Figur 5



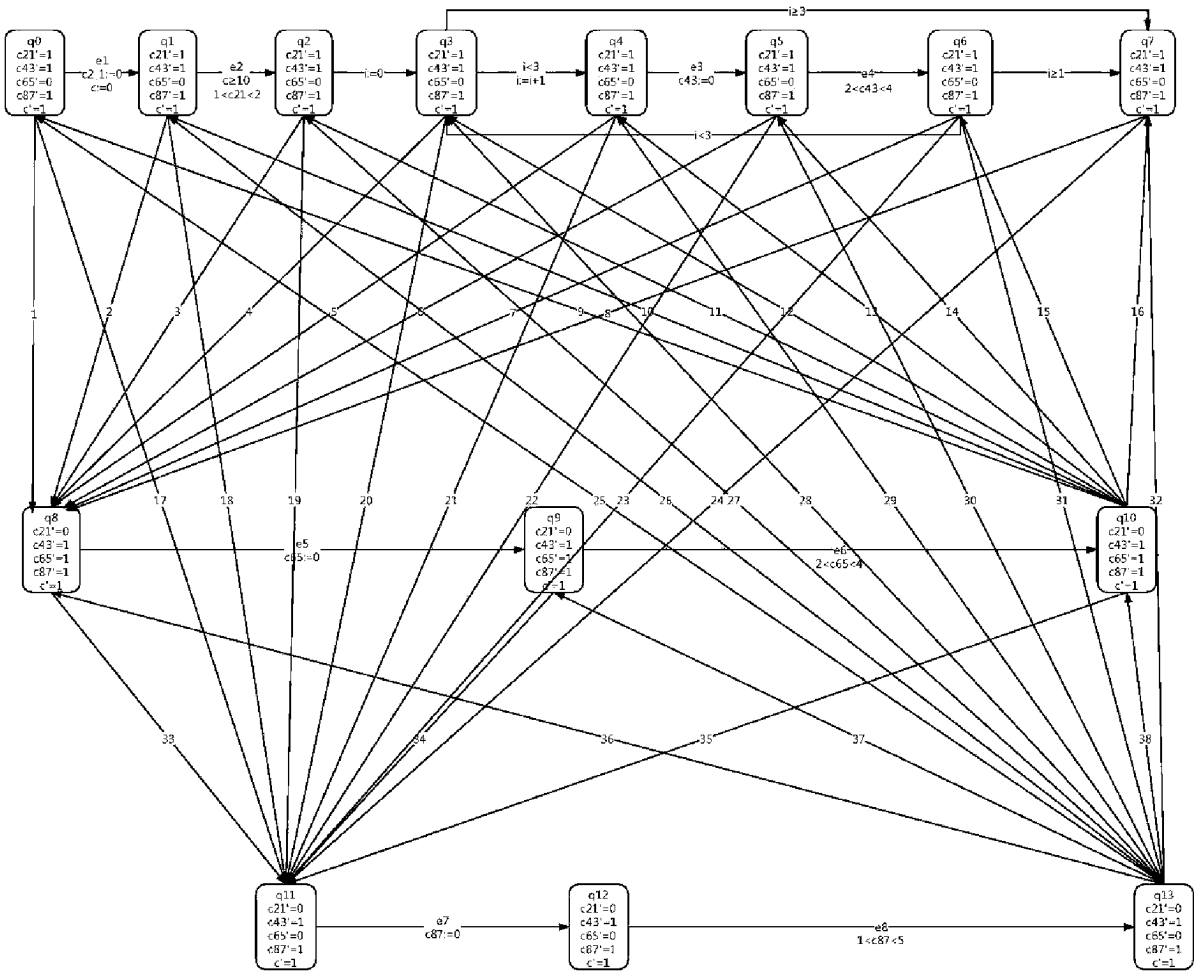
Figur 6



Figur 7


q2
c21'=1
e2
1<c21<2
q1
c21'=1
e1
c21:=0
q0
c21'=1
macher:=gMacher
gMacher:=2
macher:=gMacher
gMacher:=1
gMacher=2
gMacher:=macher
macher:=gMacher
gMacher:=0
gMacher=1
gMacher:=macher
gMacher=0
gMacher:=macher
q8
c21'=0
e5
q9
c21'=0
e6
q10
c21'=0

Figur 8



Figur 9

