

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

**INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)**

(51) Internationale Patentklassifikation 5 : G06F 15/60		A1	(11) Internationale Veröffentlichungsnummer: WO 92/18944 (43) Internationales Veröffentlichungsdatum: 29. Oktober 1992 (29.10.92)
(21) Internationales Aktenzeichen: PCT/EP92/00789 (22) Internationales Anmeldedatum: 7. April 1992 (07.04.92) (30) Prioritätsdaten: 91 106 157.0 17. April 1991 (17.04.91) EP (34) Länder für die die regionale oder internationale Anmeldung eingereicht worden ist: AT usw. (71) Anmelder (für alle Bestimmungsstaaten ausser US): SIEMENS AKTIENGESellschaft [DE/DE]; Wittelsbacherplatz 2, D-8000 München 2 (DE). (72) Erfinder; und (75) Erfinder/Anmelder (nur für US) : FILKORN, Thomas [DE/DE]; Gabelsbergerstraße 79, D-8000 München 2 (DE).		(74) Anwalt: SIEMENS AG; Postfach 22 16 34, D-8000 München 22 (DE). (81) Bestimmungsstaaten: AT (europäisches Patent), BE (europäisches Patent), CH (europäisches Patent), DE (europäisches Patent), DK (europäisches Patent), ES (europäisches Patent), FR (europäisches Patent), GB (europäisches Patent), GR (europäisches Patent), IT (europäisches Patent), LU (europäisches Patent), MC (europäisches Patent), NL (europäisches Patent), SE (europäisches Patent), US. Veröffentlicht Mit internationalem Recherchenbericht. Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.	
(54) Title: PROCEDURE FOR VERIFYING DATA-PROCESSING SYSTEMS (54) Bezeichnung: VERFAHREN ZUR VERIFIKATION DATENVERARBEITENDER SYSTEME (57) Abstract The implementation and specification of synchronous sequential circuits and other data-processing systems can be modelled by finite automata. The verification, i.e. the comparison of the implementation and the specification, of such systems can then be reduced to the comparison of two finite automata. Based on a symbolic representation of finite automata using binary decision diagrams, a procedure has been developed for comparing finite automata. This procedure is capable of being run automatically on computing facilities, thus making automatic verification of such circuits possible, without any need for simulation. (57) Zusammenfassung Implementierung und Spezifikation synchroner, sequentieller Schaltungen und anderer datenverarbeitender Systeme können durch endliche Automaten modelliert werden. Die Verifikation, d.h. der Vergleich der Implementierung und der Spezifikation solcher Systeme kann dann auf den Vergleich zweier endlicher Automaten zurückgeführt werden. Basierend auf einer symbolischen Darstellung endlicher Automaten mit Hilfe binärer Entscheidungsdiagramme wurde eine Methode für den Vergleich endlicher Automaten entwickelt, welche auf Rechenanlagen automatisch ablauffähig ist und somit die automatische Verifikation solcher Schaltungen ohne Simulation ermöglicht.			

LEDIGLICH ZUR INFORMATION

Code, die zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AT	Österreich	FI	Finnland	MN	Mongolei
AU	Australien	FR	Frankreich	MR	Mauritanien
BB	Barbados	GA	Gabon	MW	Malawi
BE	Belgien	GB	Vereinigtes Königreich	NL	Niederlande
BF	Burkina Faso	GN	Guinea	NO	Norwegen
BG	Bulgarien	GR	Griechenland	PL	Polen
BJ	Benin	HU	Ungarn	RO	Rumänien
BR	Brasilien	IE	Irland	RU	Russische Föderation
CA	Kanada	IT	Italien	SD	Sudan
CF	Zentrale Afrikanische Republik	JP	Japan	SE	Schweden
CG	Kongo	KP	Demokratische Volksrepublik Korea	SN	Senegal
CH	Schweiz	KR	Republik Korea	SU	Soviet Union
CI	Côte d'Ivoire	LI	Liechtenstein	TD	Tschad
CM	Kamerun	LK	Sri Lanka	TG	Togo
CS	Tschechoslowakei	LU	Luxemburg	US	Vereinigte Staaten von Amerika
DE*	Deutschland	MC	Monaco		
DK	Dänemark	MG	Madagaskar		
ES	Spanien	ML	Mali		

5 Verfahren zur Verifikation datenverarbeitender Systeme

Fehler in der Entwurfsphase digitaler Schaltungen sind ein Hauptgrund für unerwartete Verzögerungen und zusätzliche Kosten. Um diese zu vermeiden, werden momentan verschiedene
10 Simulationsverfahren zur Verifikation eines logischen Schaltungsentwurfs eingesetzt. Unglücklicherweise wächst die Zahl der zur Verifikation einer Schaltung oder eines datenverarbeitenden Systems nötigen Simulationen exponentiell mit der Zahl der Eingänge kombinatorischer Schaltkreise und sogar
15 schneller für sequentielle Schaltkreise, da bei diesen alle möglichen Eingangssequenzen zu simulieren sind. Obwohl solche Methoden zur Simulation digitaler Schaltungen weit verbreitet sind und einen wichtigen Platz im Entwurfsprozeß solcher Schaltungen einnehmen, sind sie weit davon entfernt zur vollständigen Überprüfung und Verifikation von Schaltungen geeignet zu sein, weshalb die Richtigkeit einer Schaltung, d.h.
20 die Übereinstimmung zwischen ihrer tatsächlichen Implementierung und ihrer Entwurfsspezifikation nicht garantiert werden kann. Aus diesem Grunde sind formale Verifikationsmethoden jeder Art von Simulation vorzuziehen, da diese im Prinzip die
25 vollständige Richtigkeit einer Schaltung beweisen können.

Spezifikationen von kombinatorischen oder synchronen sequentiellen Schaltungen werden häufig in Form sog. Hardware-Beschreibungssprachen (hardware description languages, HDL) formuliert. In solchen Fällen bedeutet die formale Verifikation den Vergleich einer digitalen Schaltung, wie sie z.B. in Form einer Netzliste gegeben ist mit ihrer Spezifikation in Form einer Beschreibung mit den Methoden einer Hardware-Beschreibungssprache. Aus der Literatur (Erik Tidén, Richard Schmid,
35 "Verifying ASICs bei symbolic simulation", in EURO ASIC 90, 1990) sind formale Schaltkreisverifikationswerkzeuge bekannt,

-2-

1

deren Anwendbarkeit aber auf kombinatorische Schaltkreise beschränkt ist. Die formale Verifikation sequentieller Digital-schaltungen ist wesentlich schwieriger, und es sind nur
5 wenige Ansätze zu einer Lösung des Problems der Verifikation digitaler Schaltungen mit einer großen Zahl von Zuständen bekannt.

Die Erfindung betrifft ein Verfahren zur Verifikation datenverarbeitender Systeme, insbesondere digitaler Schaltungen, welche auf der symbolischen Darstellung boolescher Funktionen mit Hilfe binärer Entscheidungsdiagramme basiert. Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zur Verifikation datenverarbeitender Systeme, insbesondere digitaler Schaltungen
15 anzugeben, welches in der Lage ist, nicht nur kombinatorische, sondern auch sequentielle Systeme großer Komplexität zu verifizieren und damit die Probleme der zum Stand der Technik bekannten Verfahren zu überwinden. Diese Aufgabe wird mit Hilfe eines Verfahrens zur Verifikation datenverarbeitender Systeme, insbesondere digitaler Schaltungen, mit Merkmalen nach Anspruch 1
20 gelöst.

Dieses Verfahren basiert ebenfalls wie das aus dem Stand der Technik bekannte Verfahren auf dem Vergleich zweier unabhängig voneinander erstellter formaler Beschreibungen eines zu verifizierenden Systems, z.B. der mit Hilfe einer Hardware-Beschreibungssprache formulierten Systemspezifikation und der z.B. in Form einer Netzliste vorliegenden Schaltungsimplementierung.
Das erfindungsgemäße Verfahren bedient sich einer speziellen Darstellung boolescher Funktionen mit Hilfe binärer Entscheidungsdiagramme oder hierzu gleichwertiger Mittel. Diese spezielle und vorteilhafte Darstellung boolescher Funktionen ermöglicht die Durchführung des Vergleichs beider Systembeschreibungen mit Hilfe einer Fixpunktiteration, mit deren Hilfe nicht äquivalente
30 Zustände der beiden Systembeschreibungen aufgefunden werden. Dazu werden die beiden miteinander zu vergleichenden Systembeschreibungen als Mealy-Automaten modelliert. Mit Hilfe einer
35

1

-3-

Fixpunkt-Iteration wird die Menge der nicht-äquivalenten Zustände der beiden Mealy-Automaten in Form binärer Entscheidungsdiagramme oder hierzu äquivalenter Mittel dargestellt.

5

Zur Durchführung der Fixpunktiteration werden die Ausgangs- und Übergangsfunktionen der beiden Mealy-Automaten ebenfalls durch binäre Entscheidungsdiagramme oder hierzu äquivalente Mittel dargestellt.

10

Die erfindungsgemäße Form der Darstellung durch binäre Entscheidungsdiagramme bewirkt eine äußerst effiziente Speicherung der Datenstrukturen des Verfahrens und ermöglicht eine Beschränkung der zur Durchführung des Verfahrens notwendigen Operationen auf einfache Substitutionen und Boolesche Operationen auf binären Entscheidungsdiagrammen. Hierdurch wird das Verfahren für technisch interessierende Systeme überhaupt erst praktisch anwendbar.

15

Das erfindungsgemäße Verfahren kann auf datenverarbeitende Systeme verschiedener Art, wie z.B. auf digitale Schaltungen, Kommunikationsprotokolle, Computerprogramme und Mikroprogramme zu deren Verifikation angewendet werden. Jedes technische System, welches als Mealy-Automat modelliert werden kann, kann mit Hilfe des Verfahrens verifiziert werden.

20

Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen.

Figur 1 zeigt ein Ablaufdiagramm des Verfahrens.

25

Im folgenden wird die Erfindung anhand eines speziellen Ausführungsbeispiels näher beschrieben. Aus Gründen der besseren Verständlichkeit werden die wichtigsten grundlegenden hierzu benötigten Begriffe am Anfang erläutert. Im übrigen sind die hier verwendeten Begriffe und Bezeichnungsweisen dem Fachmann auf diesem Gebiet geläufig und können z.B. in den Veröffentlichungen von W. Brauer, "Automatentheorie", B.G. Teubner, 1964 oder Z. Kohavi, "Switching and Finite Automata Theory", McGraw-Hill Book Edition, 1978, entnommen werden.

30

35

-4-

1

Bei synchronen sequentiellen Digitalschaltungen werden alle Elemente mit internen Zuständen, wie z.B. Flip-Flops, Latches, Register und speichernde Elemente mit Hilfe eines globalen Clocksignals getriggert, sodaß alle Elemente ihren Zustand simultan bei einem Clocksignal-Übergang ändern. Der neue Zustand einer synchronen sequentiellen Digitalschaltung hängt dabei ausschließlich von ihrem momentanen Zustand und den Werten der Eingangssignale ab. Damit hängen auch die Ausgangssignale der Digitalschaltung nur von den Eingangssignalen und dem internen Zustand dieser Schaltung ab. Aus diesem Grunde kann das Verhalten einer synchronen sequentiellen Digitalschaltung durch das Modell des endlichen Automaten (finite state machine), genauer als Mealy-Automat modelliert werden (Z.Kohavi, 1978, W.Brauer, 1984). Sowohl die Spezifikation einer synchronen sequentiellen Digitalschaltung als auch ihre Implementierung kann daher als Mealy-Automat aufgefaßt werden. Dabei wird die Implementierung einer solchen Digitalschaltung häufig in Form einer sog. Netzliste vorliegen. Die Spezifikation kann vorteilhaft mit Hilfe einer Übergangstabelle oder einer geeigneten Hardware-Beschreibungssprache geschehen. Eine synchrone sequentielle Digitalschaltung zu verifizieren bedeutet, eine Implementierung dieser Schaltung mit ihrer Spezifikation zu vergleichen. Wegen der Modellierbarkeit beider Beschreibungen durch Mealy-Automaten läßt sich dieses Problem auf den Vergleich zweier unterschiedlich beschriebener Mealy-Automaten reduzieren. Die folgenden Definitionen endlicher deterministischer Mealy-Automaten und der Äquivalenz zwischen zwei Mealy-Automaten sind in der Automatentheorie (Z.Kohavi, 1978; W.Brauer, 1984) üblich. Der besseren Verständlichkeit halber werden diese Definitionen hier kurz zusammengestellt.

Ein endlicher deterministischer Mealy-Automat ist durch die Angabe eines Alphabetes von Eingangsgrößen, einer endlichen Menge von Zuständen, eines Alphabetes von Ausgangsgrößen, einer Ausgangsfunktion, welche jedem Wert der Eingangsgrößen und der Zustände einen Wert der Ausgangsgrößen zuordnet,

35

-5-

1

einer Übergangsfunktion, welche jedem Eingangswert und Zustand einen Zustand zuordnet, sowie eines anfänglichen Zustandes gegeben.

5

Ein deterministischer Mealy-Automat definiert eine partielle Abbildung, welche jedem Wort aus Elementen des Alphabets von Eingangsgrößen ein Wort aus Elementen des Alphabets der Ausgangsgrößen zuordnet. Wird dem Automaten eine Folge von Eingangsgrößen eingegeben, so wird dieser Folge eine Folge von Ausgangsgrößen zugeordnet, wobei zunächst aus den Eingangsgrößen mit Hilfe der Übergangsfunktion neue Zustandsgrößen und daraufhin aus den Zustandsgrößen und den Eingangsgrößen mit Hilfe der Ausgangsfunktion die neuen Ausgangsgrößen berechnet werden.

15 Betrachtet man den Automaten von außen, so sind diese Zuordnungen das einzige was über sein Verhalten beobachtet werden kann und es ist deshalb natürlich, zwei deterministische Mealy Automaten als äquivalent anzusehen, wenn sie ein übereinstimmendes Eingangs- und Ausgangsalphabet haben und wenn ihre oben

20 beschriebenen Zuordnungen äquivalent sind. Die Abbildung wird dabei als partiell bezeichnet, weil im allgemeinen die Übergangsfunktion und die Ausgangsfunktion nur partiell definierte Funktionen sind. Indem diese Funktionen vervollständigt werden, was z.B. in Z.Kohavi, 1978 beschrieben ist, kann das Problem

25 des Vergleichs zweier unvollständig beschriebener Automaten auf einen Vergleich zweier vollständig beschriebener Automaten zurückgeführt werden. Im folgenden wird deshalb angenommen, daß die Ausgangs- und Übergangsfunktion vollständig definierte Funktionen sind, und es wird deshalb lediglich das Problem des

30 Vergleichs zweier vollständiger deterministischer Mealy-Automaten betrachtet.

Zwei Zustände zweier deterministischer Mealy-Automaten mit übereinstimmenden Eingangs- und Ausgangsalphabeten heißen

35 äquivalent genau dann, falls

a) die Werte ihrer Ausgangsfunktionen für diese beiden Zustände bei jeweils gleichen Eingangssignalen übereinstimmen und

-6-

1

b) für alle Werte der Eingangssignale, die sich aus ihren Übergangsfunktionen aus diesen Zuständen ergebenden Zustände bei jeweils gleichen Eingangssignalen äquivalent sind.

5

Zwei deterministische Mealy-Automaten mit gleichen Eingangs- und Ausgangsalphabeten heißen äquivalent dann und nur dann, wenn ihre Anfangszustände äquivalent sind.

- 10 Ein Standardverfahren zur Überprüfung der Äquivalenz zweier Mealy-Automaten wird in dem Aufsatz von Z.Kohavi 1978 beschrieben: Hierzu definiert man zu zwei Mealy-Automaten mit identischen Eingangs- und Ausgangsalphabeten den Produktautomaten, indem man als Eingangsalphabet des Produktautomaten das den
15 beiden ursprünglichen Mealy-Automaten zugrundeliegende gemeinsame Eingangsalphabet verwendet, die Menge der Zustände des Produktautomaten gleich dem kartesischen Produkt der Zustandsmenge der Ausgangsautomaten wählt, das Ausgangsalphabet des Produktautomaten aus den beiden booleschen Werten "wahr" bzw.
20 "falsch" bestehen läßt, der Ausgangsfunktion des Produktautomaten den Wert "wahr" zuweist, falls die Ausgangsfunktionen der ursprünglichen Automaten übereinstimmen, der Ausgangsfunktion des Produktautomaten den Wert "falsch" zuweist, falls die Ausgangsfunktionen der ursprünglichen Automaten nicht
25 übereinstimmen, und der Übergangsfunktion des Produktautomaten die aus den Werten der Übergangsfunktionen der ursprünglichen Automaten gebildeten Zweitupel zuweist. Mit Hilfe dieser Definition können die beiden Definitionen über die Äquivalenz zweier Zustände zweier deterministischer Mealy-Automaten sowie die Definition über die Äquivalenz von Mealy-
30 Automaten wie folgt formuliert werden:
Die Äquivalenzrelation zwischen Zuständen zweier deterministischer Mealy-Automaten ist die größte Relation auf dem kartesischen Produkt der beiden Zustandsräume zweier Mealy-Auto-
35 maten mit der folgenden Eigenschaft:
Ein Element des Produkt-Zustandsraums gehört zur Relation dann und nur dann, falls für alle Eingangswerte gilt:

1

-7-

Die Ausgangsfunktion des Produktautomaten nimmt für dieses Element des Produktzustandsraums den Wert "wahr" an und das Bild der Übergangsfunktion gehört ebenfalls zur Relation. Zwei deterministische mealy-Automaten heißen dann äquivalent dann und nur dann, falls sämtliche aus den Anfangszuständen dieser beiden Automaten gebildeten Zustände des Produktzustandsraums zu dieser Äquivalenzrelation gehören.

10 Die bekannten Verfahren (O.Coudert, Ch. Berthet, J.Ch. Madre, "Verification of sequential machines using boolean functional vectors", in IMEC-IFIP International Workshop on Applied Formal Methods For Correct VLSI Design, 1989; S.Devadas, Hi-Keung Tony Ma, R. Newton, "On the verification of sequential machines at differing levels of abstraction", IEEE-Transactions on Computer-Aided Design, 7(6): 713-722, 1988; K.J.Supovit, S.J. Friedman, "A new method for verifying sequential circuits, in 23rd ACM/IEEE Design Automation Conference, 1986) zur Überprüfung der Äquivalenz zweier synchroner sequentieller Schaltungen (Mealy-Automaten) gehen von einem Anfangszustand des Produktautomaten aus, und suchen nach einem Übergang bei dem die Ausgangsfunktion des Produktautomaten den Wert falsch annimmt, wodurch ein Unterschied im Ausgangsverhalten der beiden ursprünglichen Maschinen signalisiert wird. Falls kein solcher Übergang gefunden wird, nachdem der gesamte erreichbare Zustandsraum der Produktmaschine abgearbeitet worden ist, ist die Äquivalenz der ursprünglichen Mealy-Automaten und damit der zu vergleichenden synchronen sequentiellen Schaltungen bewiesen.

30

Die explizite Konstruktion des Zustandsdiagramms (K.H.Supovit, S.J.Friedman 1986) des Produktautomaten ist ein sehr speicher-
verzehrender Vorgang und kommt daher nur zur Verifikation mit Automaten mit nur sehr wenigen Zuständen, wie sie z.B. zu
35 Kontrollschaltungen gehören, in Betracht. Andere Verfahren (O.Coudert, et al, 1989) untersuchen den Produktautomaten ohne sein Zustandsdiagramm explizit zu konstruieren. Die Untersu-

-8-

1 chung des Produktautomaten beginnt mit einem Anfangszustand des
Produktautomaten und bei jedem neuen Zustand wird überprüft, ob
kein Übergang den Ausgang falsch erzeugt, wodurch ein unter-
5 schiedliches Verhalten der ursprünglichen Automaten angezeigt
würde. Bei einer derartigen Untersuchung des Produktautomaten
bieten sich grundsätzlich zwei verschiedene Strategien zur
Buchführung über alle erzeugten Zustände an:
Die erste Strategie kann als depth-first Strategie bezeichnet
10 werden (S.Devadas, et, 1988). Diese Strategie hat den Nachteil,
daß ihre Komplexität linear mit der Zahl der erreichbaren Zu-
stände wächst. Aus diesem Grunde können mit Hilfe dieser Strate-
gie nur Automaten mit einer sehr kleinen Zahl von Zuständen
(z.B. 2764 in dem Beispiel in dem Aufsatz von S.Devadas, et al,
15 1988) verglichen werden. Die zweite mögliche Strategie kann
als breadth-first Strategie bezeichnet werden (O.Coudert, et
al, 1989). Bei dieser Strategie werden in einem Schritt mehrere
Zustände anstelle nur eines Zustandes, wie bei der depth-first
Strategie behandelt, so daß diese Strategie von einer effi-
20 zienten Darstellung von Mengen mit Hilfe binärer Entscheidungs-
diagramme profitieren kann (R.E.Bryant, "Graph-based algorithm-
mus for boolean function manipulation", IEEE Transactions Com-
puter, C-35 (12): 1035-1044, 1986). Die Vorzüge dieses Ver-
fahrens sind mit Hilfe von Beispielen demonstriert worden, bei
25 denen Automaten mit bis zu 22 Mill. Zuständen verifiziert
worden sind. Trotzdem wächst die Komplexität einer breadth-
first Untersuchung linear mit der Länge des längsten Zyklus
im erreichbaren Teil der Produktmaschine, und deshalb kann eine
recht große Klasse interessanter Automaten, wie z.B. Zähler,
30 nicht mit Hilfe eines solchen Verfahrens verglichen werden.
Ein anderes Problem des Verfahrens von Coudert et al besteht
darin, daß zu der Durchführung dieses Verfahrens zwischen ver-
schiedenen Darstellungen gewechselt werden muß und daß der
Wechsel zwischen diesen Darstellungen Operationen mit exponen-
35 tieller Komplexität erfordert.

1

-9-

Um die Probleme, welche mit der Abarbeitung des erreichbaren Zustandsraumes eines Produktautomaten und der adäquaten Darstellung von Mealyautomaten einhergehen, zu überwinden, wird ein
5 anderes Verfahren verwendet. Aus der Definition der Äquivalenz zweier Zustände bzw. der Äquivalenz zweier Mealyautomaten geht hervor, daß für den Fall, daß zwei nicht äquivalente Zustände existieren es eine endliche Eingangssequenz geben muß, für welche sich die zugehörigen Ausgangssequenzen der beiden Mealyautomaten unterscheiden. Es wird daher angenommen, daß in
10 den meisten praktisch interessierenden Fällen eine recht kurze Eingangssequenz existiert, welche diese Eigenschaft hat, da, wenn zwei Zustände nicht äquivalent sind, dies nach einer kurzen Zeit bei Verwendung einer geeigneten Eingangssequenz am
15 Ausgang beobachtbar sein sollte. Anstelle also den gesamten erreichbaren Zustandsraum zu erzeugen und die Äquivalenz aller Zustände zu überprüfen, wie dies bei den Verfahren aus der Literatur geschieht, wird bei dem erfindungsgemäßen Verfahren die gesamte Relation der nicht äquivalenten Zustände, d.h. das
20 Komplement der Menge der äquivalenten Zustände auf dem Produktraum der Zustände berechnet. Die Berechnung wird mittels einer Fixpunkt-Iteration durchgeführt, in der nur einfache Operationen auf binären Entscheidungsdiagrammen benötigt werden.

25 Zur Durchführung dieser Iteration betrachtet man als Ausgangspunkt die Menge aller Zustandspaare, d.h. die Menge aller Zustände des Produktautomaten der zu überprüfenden Mealy-Automaten, welche unterschiedliche Ausgangswerte für mindestens ein Eingangsmuster haben. Diese Ausgangsmenge wird nun schrittweise um diejenigen Zustandspaare erweitert, für welche gilt,
30 daß von ihnen aus unter Anwendung der Übergangsfunktionen der zu verifizierenden Mealyautomaten bzw. der Übergangsfunktion des Produktautomaten die Zustandspaare der Ursprungsmenge in endlich vielen Schritten unter Annahme geeigneter Eingangsmuster erreicht werden können. Diese Iteration endet, falls
35 die dabei erzeugte Menge von Zustandspaaren sich nicht mehr ändert, falls also ein Fixpunkt erreicht wird. Es ist klar aus der Definition der Äquivalenz von Mealyautomaten, daß diese Fixpunktmenge die Menge aller nicht äquivalenten Zustände ist.

-10-

1

Es handelt sich also um alle nicht äquivalenten Zustandspaare der zu vergleichenden Mealyautomaten. Diese sind nun äquivalent, falls ihre Anfangszustände äquivalent sind. Es bleibt also lediglich zu prüfen, ob die Anfangszustände der zu vergleichenden Mealyautomaten bzw. die aus diesen Zuständen gebildeten Zustandspaare Elemente der erzeugten Fixpunktmenge sind oder nicht. Dieses Verfahren hat den Vorteil, daß in allen praktisch untersuchten Fällen die Fixpunktmenge bereits nach sehr wenigen Schritten konstruiert ist. Daneben hat dieses Verfahren den Vorteil, daß alle zur Konstruktion der Fixpunktmenge nötigen Operationen sehr effizient mit Hilfe binärer Entscheidungsdiagramme realisiert werden können. Diese werden in dem Aufsatz von Bryant 1986 detailliert beschrieben (R.E. Bryant, "Graph based algorithmus for boolean function manipulation", IEEE Trans. Computer, C-35 (12): 1035-1044, 1986).

Bei synchronen sequentiellen Digitalschaltungen sind die Zustände und Eingangs- bzw. Ausgangssignale der diese Schaltkreise modellierenden Mealyautomaten boolesche Vektoren und die Ausgangs- und Übergangsfunktionen sind als vektorwertige boolesche Funktionen definiert, deren Argumente boolesche Vektoren sind. Zur Darstellung solcher booleschen Funktionen und der Operationen auf ihnen wurden von Bryant (R.E. Bryant 1986) die binären Entscheidungsdiagramme (BODS) eingeführt. Binäre Entscheidungsdiagramme haben vorteilhafte Eigenschaften nur für bestimmte Klassen boolescher Funktionen, da die Größe eines binären Entscheidungsdiagramms, welches eine boolesche Funktion darstellt, schlimmstenfalls eine exponentiell wachsende Funktion der Zahl der Argumente dieser booleschen Funktion ist. Andererseits haben empirische Untersuchungen ergeben, daß boolesche Funktionen, welche durch kombinatorische oder sequentielle Digitalschaltungen realisiert werden, kompakte Darstellungen durch binäre Entscheidungsdiagramme haben und daß binäre Entscheidungsdiagramme vorteilhaft zur Darstellung sequentieller Digitalschaltungen eingesetzt werden können.

In dem oben beschriebenen Fixpunktiterationsverfahren zur Erzeugung der Relation der nicht äquivalenten Zustände zweier

1

-11-

Mealyautomaten wird eine Methode zur Darstellung der Mengen, welche im Laufe des Fixpunktiterationsverfahrens erzeugt werden benötigt. Diese Mengen sind Relationen über dem kartesischen Produkt der Zustandsräume beider Mealyautomaten, d.h. Teilmengen eines binären Einheitswürfels entsprechender Dimensionen. Jede Teilmenge U eines k -dimensionalen binären Würfels kann durch ihre charakteristische Funktion beschrieben werden, welche jedem Punkt des binären Würfels, welcher zugleich Element der Menge U ist, den Wert 1 zuordnet und allen anderen Elementen des Würfels den Wert 0. Dabei entspricht die charakteristische Funktion einer Durchschnittsmenge zweier Mengen der UND-Verknüpfung beider charakteristischen Funktionen dieser Mengen, die charakteristische Funktion einer Vereinigungsmenge der ODER-Verknüpfung und die charakteristische Funktion einer Differenzbildung der UND-Verknüpfung der charakteristischen Funktionen der Ausgangsmenge mit der charakteristischen Funktion des Komplements der subtrahierten Menge. In dem Aufsatz von J.R.Burch, et al, "Sequential circuit verification using symbolic model checking", in ACM/IEEE Design Automation Conference, 1990, wird anstelle der Übergangsfunktion die entsprechende Übergangsrelation zur Modellierung einer synchronen sequentiellen Digitalschaltung verwendet. Diese Übergangsrelation wird mit Hilfe eines binären Entscheidungsdiagramms der charakteristischen Funktion dieser Übergangsrelation dargestellt. Empirische Untersuchungen haben gezeigt, daß die Darstellung synchroner sequentieller Digitalschaltungen und kombinatorischer Digitalschaltungen mit Hilfe funktionaler Vektoren binärer Entscheidungsdiagramme Vorteile gegenüber einer Darstellung in Form von charakteristischen Funktionen hat, da sie offenbar in der Lage ist, Schaltkreise höherer Komplexität darzustellen.

Auf der Basis der Darstellung von Mealyautomaten und Relationen mit Hilfe von booleschen Funktionen und damit durch binäre Entscheidungsdiagramme wird nun die Realisierung des Fixpunktverfahrens zur Berechnung der Relation der nicht äquivalenten

-12-

1 Zustände zweier Mealyautomaten beschrieben. Der erste Schritt
zur Vorbereitung der Fixpunktiteration besteht in der Berech-
nung der Ausgangsrelation M_0 , zu welcher alle Zustandspaare,
5 welche aus zwei Zuständen der beiden Mealyautomaten gebildet
sind, gehören, für welche gilt, daß mindestens ein Eingangs-
signal existiert, für welches die Ausgangsfunktionen der beiden
Mealyautomaten für die beiden Zustände verschiedene Werte
annehmen. Sind die Ausgangsfunktionen der beiden Mealyautomaten
10 als Vektoren binärer Entscheidungsdiagramme gegeben, kann die
charakteristische Funktion der Ausgangsrelation einfach berech-
net werden.

Dazu werden aus den Vektoren von binären Entscheidungsdiagram-
15 men für die Ausgangsfunktionen für jeden einzelnen Ausgang die
zugehörigen binären Entscheidungsdiagramme "EXOR" verknüpft.
Für jeden Ausgang wird also ein binäres Entscheidungsdiagramm
berechnet, welches für genau die Zustandspaare und Eingangssignale
den Wert "wahr" liefert für die dieser Ausgang in beiden Mealy-
20 automaten einen unterschiedlichen Wert liefert. Auf jedes die-
ser binären Entscheidungsdiagramme wird anschließend ein Exi-
stenzoperator bezüglich der Eingänge angewandt. Ein so berech-
netes binäres Entscheidungsdiagramm gibt genau für die Paare
von Zuständen den Wert "wahr", für welche mindestens ein Eingabe-
25 signal existiert, so daß das ursprüngliche binäre Entscheidungs-
diagramm den Wert "wahr" liefert, also der Ausgang einen unter-
schiedlichen Wert liefert. Der Existenzoperator auf einem binären
Entscheidungsdiagramm bezüglich einer Menge von Eingängen kann
sukzessive durch den Existenzoperator bezüglich eines einzelnen
30 Eingangs berechnet werden. Dazu wird auf das ursprüngliche binäre
Entscheidungsdiagramm der Existenzoperator bezüglich des ersten
Eingangs berechnet. Auf das entstandene binäre Entscheidungsdi-
agramm wird der Existenzoperator bezüglich des zweiten Eingangs
berechnet. Dieses Verfahren wird bis zum letzten Eingang fort-
35 gesetzt. Zur Berechnung eines Existenzoperators bezüglich eines
Eingangs wird in dem binären Entscheidungsdiagramm der Eingang
durch "wahr" bzw. "falsch" substituiert und die beiden ent-

1

-13-

stehenden binären Entscheidungsdiagramme werden "ODER" verknüpft. Der Existenzoperator ist also auf einfache Substitution und "ODER"-Verknüpfung zurückführbar. Nach Anwendung des Existenzoperators werden die für die einzelnen Ausgänge entstandenen binären Entscheidungsdiagramme noch alle "ODER" verknüpft und das Ergebnis ist ein binäres Entscheidungsdiagramm, welches die charakteristische Funktion für M_0 darstellt. Eine explizite Berechnung der Zwischenergebnisse ist nicht unbedingt erforderlich, sondern die gesamte oben beschriebene Berechnung von M_0 aus den Vektoren von binären Entscheidungsdiagrammen für die Ausgangsfunktionen kann auch zu einem einzigen Schritt verschmolzen werden.

Die Ausgangsrelation M_0 ist der Ausgangspunkt der Fixpunktiteration, welche aus der Ausgangsrelation weitere Relationen berechnet.

Während des Ablaufs des Iterationsverfahrens wird die charakteristische Funktion der zwischendurch auftretenden Relationen $M(i)$ aus den vorhergehenden charakteristischen Funktionen durch folgende Schritte berechnet:

In dem binären Entscheidungsdiagramm der charakteristischen Funktion für $M(i)$ werden die Zustände durch die binären Entscheidungsdiagramme ihrer Zustandsübergangsfunktionen ersetzt. Dies entspricht der Substitution von Variablen in binären Entscheidungsdiagrammen durch binäre Entscheidungsdiagramme. Das berechnete binäre Entscheidungsdiagramm gibt für jedes Paar von Zuständen und jedes Eingabesignal genau dann den Wert "wahr", wenn die Nachfolgezustände der betrachteten Zustände unter der Wirkung der Übergangsfunktion der Mealy-Automaten die Eigenschaft haben, daß die charakteristische Funktion der Relation $M(i)$ dieses Iterationsschrittes den Wert "wahr" besitzt.

Auf das berechnete binäre Entscheidungsdiagramm wird der Existenzoperator bezüglich der Eingangssignale angewandt und das Ergebnis mit dem binären Entscheidungsdiagramm der charakteri-

-14-

- 1 stischen Funktion der Relation $M(i)$ "ODER" verknüpft. die
Relation $M(i)$ wird also um genau die Paare von Zuständen
erweitert, für welche mindestens ein Eingangssignal existiert,
5 so daß die Nachfolgezustände in der Relation $M(i)$ enthalten
sind. Zur Durchführung des Iterationsschrittes sind also
lediglich Einsetzung, d.h. Substitution und f. "ODER"-Verknü-
pfung auf binären Entscheidungsdiagrammen erforderlich, da
der Existenzoperator wie vorherbeschrieben auf Substitution
10 und "ODER"-Verknüpfung zurückgeführt werden kann. Eine expli-
zite Berechnung der Zwischenergebnisse ist nicht unbedingt
erforderlich, sondern die gesamte oben beschriebene Berech-
nung kann zu einer einzigen Operation verschmolzen werden.
- 15 Im Effekt sind diese Operationen gleichwertig zu einer Vereini-
gung von Teilmengen des Produktzustandsraumes, bei der die
Menge $M(i)$, welche die Relation dieses Iterationsschrittes
repräsentiert, mit der Menge der Vorgänger-Zustandspaare unter
der Wirkung der Übergangsfunktionen der zu vergleichenden Mea-
20 ly Automaten vereinigt wird, um die Menge $M(i+1)$ zu erhalten,
welche die Relation des nachfolgenden Iterationsschrittes
repräsentiert.

- Das Iterationsverfahren bricht ab, wenn ein Iterationsschritt
25 zu keiner Veränderung der Relation führt. Um dies festzustel-
len, ist ein einfacher Vergleich zweier aufeinander folgender
binärer Entscheidungsdiagramme, welche die charakteristischen
Funktionen der Relationen darstellen, erforderlich.

- 30 Die zu vergleichenden Mealy-Automaten sind dann äquivalent,
wenn ihre Anfangszustände nicht zur Relation M der nichtäquiva-
lenten Zustände gehören.

- Die Kombination der Darstellung von Mealyautomaten mit Hilfe
35 von Vektoren von Funktionen, d.h. binärer Entscheidungs-
diagramme, und der Darstellung von Mengen durch ihre charak-
teristischen Funktionen kann mit Hilfe der obigen Substitutionen

1

-15-

einfach und elegant ausgeführt werden. Das Verfahren von Coudert et al (O.Coudert 1989) benötigt eine explizite Überführung der beiden Darstellungen ineinander, obwohl damit Operationen von exponentieller Komplexität verbunden sind. Das Iterationsverfahren kommt zum Stillstand, falls die erzeugten Mengen bzw. Relationen zwischen zwei Iterationschritten identisch sind. Diese Identität wird durch Auswertung der binären Entscheidungsdiagramme der charakteristischen Funktionen, welche diese Mengen repräsentieren durchgeführt.

Damit ist die Realisierung des gesamten Fixpunktverfahrens auf der Grundlage binärer Entscheidungsdiagramme beschrieben. Die einzigen Operationen auf binären Entscheidungsdiagrammen, welche innerhalb der Fixpunktiteration benötigt werden, sind die booleschen Funktionen "ODER" bzw. "ungleich" und die Ersetzung (Substitution) von Variablen boolescher Funktionen bzw. von Entscheidungsdiagrammen.

20

25

30

35

-16-

1

Patentansprüche

1. Verfahren zur Verifikation datenverarbeitender Systeme,
5 bei dem
a) zwei unabhängig voneinander erstellte Beschreibungen eines
zu verifizierenden Systems als Mealy-Automaten oder dazu
gleichwertig repräsentiert und miteinander verglichen werden;
b) der Vergleich mit Hilfe eines Fixpunktiterationsverfahrens
10 durchgeführt wird, welches die Menge M aller nicht äquivalenten
Zustandspaare aus Zuständen der beiden Mealy-Automaten erzeugt;
c) Äquivalenzrelationen zwischen Zuständen, Ausgangs- und Über-
gangsfunktionen von Mealy-Automaten durch binäre Entscheidungs-
diagramme oder hierzu äquivalente Mittel dargestellt werden;
15 d) in jedem Schritt der Fixpunktiteration lediglich boolesche
Operationen und Substitutionen auf binäre Entscheidungsdiagramme
angewendet werden.
2. Verfahren nach Anspruch 1, bei dem die datenverarbeitenden
20 Systeme digitale Schaltungen sind.
3. Verfahren nach Anspruch 2, bei dem die zu verifizierende
Digitalschaltung in Form zweier Netzlisten beschrieben ist.
- 25 4. Verfahren nach Anspruch 2, bei dem die zu verifizierende
Digitalschaltung in Form einer Netzliste und mit Hilfe einer
Hardware-Beschreibungssprache beschrieben ist.
5. Verfahren nach Anspruch 1, bei dem die datenverarbeitenden
30 Systeme Kommunikationsprotokolle sind.
6. Verfahren nach Anspruch 1, bei dem die datenverarbeitenden
Systeme Computerprogramme sind.
- 35 7. Verfahren nach Anspruch 1, bei dem die datenverarbeitenden
Systeme Mikroprogramme sind.

1

-17-

8. Verfahren nach einem der vorhergehenden Ansprüche,
bei dem

- zunächst die Menge MO aller Zustandspaare erzeugt wird,
welche für mindestens einen Satz von Eingangswerten minde-
stens einen verschiedenen Ausgangswert erzeugen;

- die Menge MO erweitert wird um die Menge aller Zustands-
paare, welche in endlich vielen Schritten der beiden Mealy-
Automaten auf ein Zustandspaar führen, das der Menge MO ange-
hört.

10

15

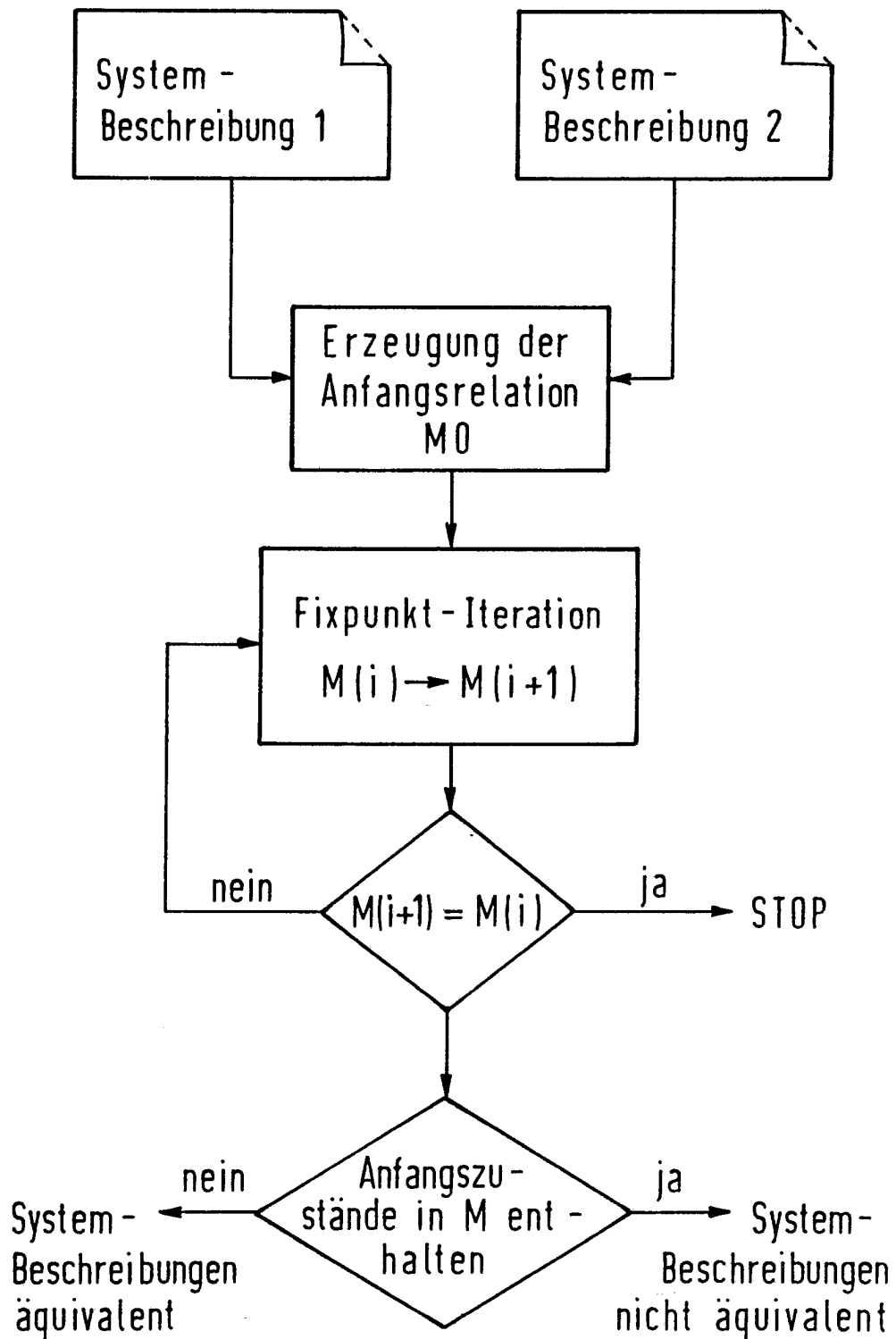
20

25

30

35

1/1



INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP92/00789

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.⁵ : G06F 15/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl.⁵ : G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	PROCEEDINGS OF THE IMEC-IFIP INTERNATIONAL WORKSHOP ON APPLIED FORMAL METHODS FOR CORRECT VLSI DESIGN 13-16 November 1989 HOUTHALEN BELGIUM pages 111-128; COUDERT ET AL: 'VERIFICATION OF SEQUENTIEL MACHINES USING BOOLEAN FUNCTIONAL VECTORS' cited in the application see the whole document	1-8
A	IEEE INTERNATIONAL CONFERENCE ON COMPUTER-AIDED DESIGN 11-15 November 1990 SANTA CLARA US pages 126-129; COUDET: 'A UNIFIED FRAMEWORK FOR THE FORMAL VERIFICATION OF SEQUENTIAL CIRCUITS' see the whole document -----	1-8

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

24 August 1992 (24.08.92)

Date of mailing of the international search report

9 September 1992 (09.09.92)

Name and mailing address of the ISA/

European Patent Office

Facsimile No.

Authorized officer

Telephone No.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 92/00789

I. KLASSIFIKATION DES ANMELDUNGSGEGENSTANDS (bei mehreren Klassifikationssymbolen sind alle anzugeben) ⁶		
Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC Int.Kl. 5 G06F15/60		
II. RECHERCHIERTE SACHGEBIETE		
Recherchierter Mindestprüfstoff ⁷		
Klassifikationssystem	Klassifikationssymbole	
Int.Kl. 5	G06F	
Recherchierte nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Sachgebiete fallen ⁸		
III. EINSCHLAGIGE VERÖFFENTLICHUNGEN ⁹		
Art. ⁹	Kennzeichnung der Veröffentlichung ¹¹ , soweit erforderlich unter Angabe der maßgeblichen Teile ¹²	Betr. Anspruch Nr. ¹³
A	PROCEEDINGS OF THE IMEC-IFIP INTERNATIONAL WORKSHOP ON APPLIED FORMAL METHODS FOR CORRECT VLSI DESIGN 13-16 NOVEMBER 1989 HOUTHALEN BELGIUM Seiten 111 - 128; COUDERT ET AL: 'VERIFICATION OF SEQUENTIAL MACHINES USING BOOLEAN FUNCTIONAL VECTORS' in der Anmeldung erwähnt siehe das ganze Dokument ---	1-8
A	IEEE INTERNATIONAL CONFERENCE ON COMPUTER-AIDED DESIGN 11-15 NOVEMBER 1990 SANTA CLARA US Seiten 126 - 129; COUDERT: 'A UNIFIED FRAMEWORK FOR THE FORMAL VERIFICATION OF SEQUENTIAL CIRCUITS' siehe das ganze Dokument ---	1-8
¹⁰ Besondere Kategorien von angegebenen Veröffentlichungen ¹⁰ : "A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist "E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist "L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt) "O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht "P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist "T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist "X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden "Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann nahelegend ist "&" Veröffentlichung, die Mitglied derselben Patentfamilie ist		
IV. BESCHEINIGUNG		
Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts	
24. AUGUST 1992	09. 09. 92	
Internationale Recherchenbehörde EUROPAISCHES PATENTAMT	Unterschrift des bevollmächtigten Bediensteten GUNGALE A.	