

ITALIAN PATENT OFFICE

Document No.

102009901753148A1

Publication Date

20110123

Applicant

FONDAZIONE ISTITUTO ITALIANO DI TECNOLOGIA

Title

PROCEDIMENTO PER LA GENERAZIONE DI UN INSIEME DI CONFLITTI
PER LA DIAGNOSI DI SISTEMI BASATA SU MODELLO, E PROCEDIMENTO DI
DIAGNOSI CORRISPONDENTE

DESCRIZIONE dell'invenzione industriale dal titolo:

"Procedimento per la generazione di un insieme di conflitti per la diagnosi di sistemi basata su modello, e procedimento di diagnosi corrispondente"

di: FONDAZIONE ISTITUTO ITALIANO DI TECNOLOGIA,
nazionalità italiana, Via Morego 30 - 16163 GENOVA

Inventori designati: Amir FIJANY, Anthony BARRETT,
Farrokh VATAN

Depositata il: 23 luglio 2009

* * *

DESCRIZIONE

La presente invenzione riguarda in generale la diagnostica dei sistemi e, più specificamente, la generazione di un insieme di conflitti per la diagnosi di un sistema basata su modello, e un procedimento per la diagnosi di un sistema, basato sulla determinazione di un insieme di conflitti rappresentativi del comportamento reale del sistema.

In particolare, l'invenzione ha per oggetto un procedimento per la generazione di un insieme di conflitti del tipo definito nel preambolo della rivendicazione 1, ed un procedimento per la diagnosi di un sistema, secondo il preambolo della rivendicazione 6.

Il funzionamento di un sistema - termine gene-

rico col quale si indicheranno in questa descrizione e nelle rivendicazioni allegate impianti industriali, apparecchiature di produzione o di ricerca, macchine di diversi generi (ad esempio, velivoli o sonde spaziali) - è controllato tipicamente mediante sofisticati sistemi diagnostici in grado di rilevare ed isolare condizioni anomale di funzionamento appena esse si manifestano. Nelle missioni spaziali guidate da terra, in orbita terrestre o nello spazio profondo, grande attenzione è dedicata alla diagnosi del sistema costituito dal velivolo e dai suoi apparati di bordo, ed in particolare alla rivelazione in tempo reale dei guasti al sistema, al fine di rimediare alle anomalie che potrebbero compromettere la missione.

Il principio fondamentale della diagnosi basata su modelli è quello di confrontare il comportamento atteso o nominale di un sistema, fornito da un modello del sistema, con il comportamento reale desunto da misure sul sistema, ottenute tramite un insieme di sensori ad esso associati.

In generale, la diagnosi di un sistema basata su modello comprende tre fasi:

- Rivelazione dei guasti: dato uno specifico insieme di ingressi del sistema ed il suo modello,

è eseguita una simulazione del sistema per calcolare i valori attesi dei sensori. Ogni discrepanza o incongruenza tra il valore atteso dei sensori ed i loro valori reali rappresenta un guasto. Questa fase consiste essenzialmente nel determinare l'esistenza di incongruenze tra valori attesi ed osservati dei sensori;

- Generazione degli insiemi di conflitti: in questa fase, date le incongruenze tra i valori attesi ed i valori osservati dei sensori, è generato un gran numero di insiemi di conflitti, ciascuno dei quali implica che almeno un suo componente sia guasto per via delle incongruenze osservate;

- Diagnosi: in questa fase, dati gli insiemi di conflitti, il sistema è diagnosticato, ovvero è determinato il numero minimo di componenti guasti. Questa fase è eseguita risolvendo problemi di determinazione di un hitting set, i quali, dati gli insiemi di conflitti, determinano il numero minimo di componenti intersezione di tutti gli insiemi di conflitti. Questo insieme minimo rappresenta l'insieme di componenti guasti all'origine delle incongruenze osservate, e quindi rappresenta, in definitiva, la diagnosi del sistema.

La prima fase di rivelazione dei guasti è im-

mediata e richiede soltanto una simulazione del sistema. La terza fase è stata per lungo tempo una limitazione ad una diagnosi efficiente, ma recentemente è stato sviluppato uno strumento logico-matematico che ha permesso una rapida soluzione del problema di determinazione di un hitting set, anche per sistemi complessi. L'attuale ostacolo ad una rapida diagnosi di sistema è attualmente l'efficienza nella fase di generazione degli insiemi di conflitti.

Attualmente, vi sono due classi di metodologie ed approcci distinti per la derivazione di insiemi di conflitti.

Negli ultimi decenni la ricerca nel campo della diagnosi di sistemi basata su un modello descrittivo della funzione dei componenti del sistema e della sua connettività (topologia), è stata condotta essenzialmente secondo due differenti discipline: una, l'approccio di rivelazione e di isolamento dei guasti (Fault Detection and Isolation, FDI), sfrutta la conoscenza completa del sistema ed è basata sulle teorie dei controlli automatici e decisioni statistiche; l'altra, nota come approccio DX, non necessita della completa conoscenza del sistema ed è basata su tecniche di in-

telligenza artificiale applicate ad un insieme di assunzioni sui modi di funzionamento del sistema nel suo complesso.

L'approccio FDI impiega nella sua applicazione le *relazioni di ridondanza analitica* (Analytical Redundancy Relations, ARR), note anche come residuo o equazione di parità, che rappresentano ciascuna una differente relazione tra parametri misurati del sistema. Ogni ARR non soddisfatta rappresenta una discrepanza tra il comportamento atteso del sistema e quello reale, e permette di distinguere un funzionamento anomalo del sistema, dovuto alla presenza di qualche guasto, rispetto alla normale attività.

L'approccio DX si fonda invece sul concetto di *conflitto*, e più in generale di *insieme di conflitti* (conflict set), che è un insieme di componenti del sistema, la cui assunzione di corretto funzionamento non è consistente con il comportamento osservato del sistema.

Recentemente, un quadro unificato delle due teorie citate ne ha ricostruito la sostanziale equivalenza. Il rapporto tra i concetti di relazione di ridondanza analitica e di conflitto è stato riconosciuto nel fatto che il supporto di una ARR,

ovvero l'insieme di componenti coinvolte in tale ARR è un *possibile conflitto*, ovvero esiste un possibile scenario di misure sul sistema che produce tale insieme come un conflitto.

Entrambi gli approcci, adottati singolarmente per la conduzione della diagnosi di un sistema, presentano notevoli svantaggi computazionali, che li rendono inefficienti per molte applicazioni di interesse.

Per quanto riguarda l'approccio basato sulle relazioni di ridondanza analitica (ARR), gli algoritmi noti per la generazione di un insieme completo di ARR presentano una complessità di calcolo esponenziale, per cui la generazione e l'applicazione delle ARR risultano, nei casi reali, praticamente impossibili.

Inoltre, per molti sistemi pratici di interesse, l'insieme delle ARR può non essere ottenibile in forma analitica, e ciò ne impedisce il concreto utilizzo.

Nell'approccio DX, invece, l'algoritmo General Diagnosis Engine (GDE) più comunemente impiegato richiede l'esecuzione di molte verifiche di coerenza (*consistency checks*) tra valori attesi dal modello e valori osservati sul sistema, molte delle

quali potrebbero non rivelarsi strettamente necessarie al risultato della diagnosi, per cui anche la sua applicazione determina una complessità esponenziale del calcolo.

Gli approcci DX ed FDI

Nel seguito è fornita una discussione più approfondita degli approcci alla diagnosi di un sistema secondo le tecniche note DX ed FDI, che risulterà utile a comprendere gli sviluppi dell'invenzione.

Nella diagnosi basata su modelli, i modelli dei dispositivi costituenti un sistema complesso sono oggetto di confronto con le osservazioni del comportamento reale del sistema per rilevare eventuali discrepanze (incongruenze) e diagnosticarne le cause all'origine (guasti).

Un modello di sistema (System Model, SM) consiste di un modello comportamentale (Behavioral Model, BM) e di un modello di osservazioni (Observation Model, OM). Il modello comportamentale BM è una descrizione del sistema basata sui suoi componenti e consiste di un insieme di *relazioni primarie* (Primary Relations, PR). Ciascun componente è descritto dalla funzione che esso realizza, ovvero da una o più relazioni primarie PR e dai suoi in-

gressi ed uscite, per cui la descrizione basata sui componenti include anche la topologia del sistema. Il modello di osservazioni OM è l'insieme di relazioni che definiscono le osservazioni che sono effettuate sul sistema attraverso una pluralità di sensori ad esso associati.

In figura 1 è mostrato l'esempio di un sistema a più porte, consistente di tre moltiplicatori (M_1 , M_2 , M_3) e due sommatore (A_1 , A_2).

Il modello comportamentale per questo sistema, che ne fornisce una descrizione di componenti e topologia, è dato da un insieme di Relazione Primarie PR e dai componenti loro associati, come definito nel seguito:

$$PR_1: x = a \ c; \quad M_1$$

$$PR_2: y = b \ d; \quad M_2$$

$$PR_3: z = c \ e; \quad M_3$$

$$PR_4: f = x + y; \quad A_1$$

$$PR_5: g = y + z; \quad A_2$$

L'approccio DX

Dal punto di vista dell'approccio DX ciascuna relazione primaria PR è modellizzata come insieme di regole per propagare valori da una variabile a un'altra.

Ad esempio, il componente moltiplicatore M_1 è

definito dalle seguenti tre regole, che assumono la condizione in cui M_1 funziona correttamente.

1) $x = a \cdot c$

2) if $(a \neq 0)$ then $c = x/a$

3) if $(c \neq 0)$ then $a = x/c$

Si noti che mentre la prima regola inferisce un'uscita dati gli ingressi, le altre due determinano in modo condizionale un ingresso data l'uscita e l'altro ingresso.

Di fatto, l'approccio DX permette a ciascuna variabile di assumere un insieme di possibili valori date diverse assunzioni, e la considerazione di ogni valore insieme all'utilizzo delle relative regole consente di calcolare i valori di altre variabili del sistema. Dal momento che tali calcoli si basano su assunzioni di partenza, un algoritmo DX contraddistingue ciascun valore assegnato ad una variabile con le assunzioni che contribuiscono al suo calcolo (valore contrassegnato).

Pertanto, le regole sopra citate si traducono di fatto nelle seguenti, in cui S_v è l'insieme di valori associabili alla variabile v , e $\langle n:N \rangle \in S_v$ indica che v è uguale ad n (ossia, la variabile v assume il valore n) quando è verificato l'insieme delle assunzioni N .

$$\begin{aligned}
\langle n:N \rangle \in S_a \wedge \langle m:M \rangle \in S_c &\Rightarrow \langle n \cdot m : N \cup M \cup \{M1\} \rangle \in S_x \\
\langle n:N \rangle \in S_a \wedge \langle m:M \rangle \in S_x \wedge n \neq 0 &\Rightarrow \langle m \div n : N \cup M \cup \{M1\} \rangle \in S_c \\
\langle n:N \rangle \in S_c \wedge \langle m:M \rangle \in S_x \wedge n \neq 0 &\Rightarrow \langle m \div n : N \cup M \cup \{M1\} \rangle \in S_a
\end{aligned}$$

Ad esempio, l'impostazione degli ingressi $a=2$ e $c=2$ determina l'aggiunta di $\langle 2:\{\} \rangle$ in S_a e di $\langle 2:\{\} \rangle$ in S_c , il che porta l'algoritmo DX ad inferire che $\langle 3:\{M1\} \rangle \in S_x$, ciò che innesca ulteriori inferenze aggiungendo un elemento all'insieme S_x .

Una discrepanza o incongruenza sorge durante la propagazione inferenziale dei valori tra le variabili del sistema, dagli ingressi alle uscite, quando due diversi valori sono assegnati alla stessa variabile.

Ad esempio, l'impostazione di tutti gli ingressi del sistema multi-porta di figura 1 a "2" determina per inferenza $\langle 8:\{M2,M3,A2\} \rangle \in S_g$.

Una successiva misurazione $g = 9$ determina una discrepanza poiché $\langle 9:\{\} \rangle$ è anch'esso un elemento di S_g dovuto alla misura, ma non è coerente con il modello del sistema. L'unione delle assunzioni che contribuiscono a questo risultato porta al riconoscimento di una discrepanza, che implica che M_2 , M_3 , o A_2 deve essere un dispositivo guasto.

Tipicamente, nel corso di una propagazione in-

ferenziale di valori entro un sistema non sono rintracciate discrepanze, ma quando occorrono guasti al sistema possono apparire molteplici discrepanze. Il processo di inferenza causale continua infatti a determinare nuove discrepanze fino al completamento della propagazione dei valori possibili contrassegnati delle variabili alle uscite del sistema, il che può richiedere molto tempo poiché il numero di valori attribuiti a ciascuna variabile può crescere esponenzialmente col numero di possibili assunzioni. Ciò porta un generico algoritmo DX a richiedere una quantità di tempo esponenziale per la propagazione dei valori nell'intero sistema.

Successivamente, il generico algoritmo DX rintraccia gli insiemi minimi di assunzioni intersezioni di tutte le discrepanze rivelate, che rappresentano le diagnosi delle cause all'origine delle misure contraddittorie.

Purtroppo, il calcolo dell'insieme minimo è per complessità equivalente ad un problema di calcolo dei primi implicanti, che è un problema NP-completo.

Per migliorare le prestazioni l'algoritmo DX GDE (General Diagnosis Engine) applica un approccio minimalista alla gestione degli insiemi, eli-

minando $\langle n:L_i \rangle$ da un insieme se $\langle n:L_j \rangle$ appartiene all'insieme e $L_i \subsetneq L_j$. Ciò è possibile poiché il secondo elemento rende $\langle n:L_i \rangle$ ridondante quando si determina un valore sulla base delle assunzioni di partenza.

L'insieme di discrepanze è inoltre minimizzato eliminando una discrepanza ridondante L_i quando esiste un'altra discrepanza L_j tale per cui $L_j \subsetneq L_i$. Tali test su sottoinsiemi riducono gli oneri computazionali della procedura inferenziale, ma fanno sì anche la procedura di test sia richiamata numerose volte nell'algoritmo, il che richiede comunque un tempo di calcolo elevato.

In definitiva, il modello diagnostico secondo l'approccio DX risulta in un sistema in cui ogni variabile può essere testata. L'obiettivo sarebbe tuttavia quello di testare il minor numero di variabili possibile. Effettivamente, un algoritmo DX è in grado di identificare un numero di possibili diagnosi di una discrepanza e di suggerire la misurazione di un determinato sottoinsieme di variabili per ridurre l'ambiguità della diagnosi.

Benché questo approccio sia in teoria conveniente, all'atto pratico ci si accorge che alcune variabili non possono essere misurate quando il si-

stema in questione è distante o irraggiungibile (si pensi a sonde in viaggio nello spazio profondo). L'approccio DX deve dunque essere applicato stabilendo a priori le variabili effettivamente misurabili, ossia i sensori associati al sistema che ne consentono l'osservazione. Sorge dunque il problema di identificare a priori le variabili più appropriate che si vuole rilevare, al fine di minimizzare le ambiguità di diagnosi.

L'approccio FDI

L'aspetto principale per cui l'approccio FDI differisce dall'approccio DX è l'assunzione iniziale che i sensori di osservazione del sistema sono stabiliti a priori.

L'ottimizzazione dei sensori e la tecnica diagnostica si basano sui concetti di relazione di ridondanza analitica (ARR) e matrice di firma dei guasti (FSM).

Nel seguito si introducono e si discutono brevemente i concetti di relazioni di ridondanza analitica (ARR) e matrice di firma dei guasti (Fault Signature Matrix, FSM), per chiarezza e semplicità assumendo il caso di un singolo guasto di un sistema.

L'insieme di variabili (V) di un sistema, ad

esempio il sistema di figura 1, può essere scomposto in un insieme di variabili incognite (X) e un insieme di variabili osservate (O), ovvero vale la relazione $V = X \cup O$.

Una *relazione di ridondanza analitica* (ARR) è un vincolo dedotto dal modello del sistema (SM). Le ARR possono essere derivate dal modello SM eliminando le variabili incognite dalle Relazioni Primarie. Pertanto una ARR contiene soltanto variabili osservate, e quindi può essere calcolata a partire da esse.

Il *supporto di una ARR* è il sottoinsieme di componenti coinvolti nella derivazione della ARR.

Per il sistema di figura 1, se i sensori sono disposti alle uscite f e g , e sono noti gli ingressi a, b, c, d, e , allora $O = \{a, b, c, d, e, f, g\}$ e $X = \{x, y, z\}$.

Le ARR risultanti sono date nella tabella 1 seguente:

Tabella 1 - ARR, componenti di supporto e sensori riferiti all'esempio di figura 1

ARR	Componenti di supporto	Sensori
ARR ₁ : $f = ac + bd$	M ₁ , M ₂ , A ₁	f

ARR ₂ : $g = bd + ce$	M ₂ , M ₃ , A ₂	g
ARR ₃ : $f - g = ac - ce$	M ₁ , M ₃ , A ₂ , A ₁	f, g

Le ARR sono quindi utilizzate per verificare la consistenza delle osservazioni sul sistema rispetto al modello SM. In altre parole, le ARR sono soddisfatte se il comportamento del sistema osservato soddisfa i vincoli del modello, ossia produce osservazioni attese dal modello.

Nell'assunzione di un singolo guasto, ovvero se una componente del supporto di una ARR è guasta, allora tale ARR non è soddisfatta.

Di fatto, con il concetto di insieme di supporto, questa affermazione costituisce il fondamento dell'approccio di diagnosi basata su modelli nell'ambito della metodologia FDI.

Una *matrice di firma dei guasti* (FSM) è derivabile dalle ARR. Essa è definita come una matrice binaria le cui righe sono le ARR generate per il sistema in esame e le cui colonne identificano i componenti del sistema. Un elemento FS_{ij} di questa matrice ha valore 1 se l'associato componente C_i del sistema è parte del supporto della relazione ARR_j , altrimenti $FS_{ij} = 0$. La i -esima colonna corrispondente al componente C_i è definita come vettore

di firma del guasto di C_i ed è denominata $FSV_i = [FSV_{i1}, \dots, FSV_{in}]^t$.

Con riferimento al sistema di figura 1, la FSM può essere derivata dalla tabella 1 ed è data nella seguente tabella 2.

Tabella 2 - Matrice di firma dei guasti per il sistema di figura 1

	A ₁	A ₂	M ₁	M ₂	M ₃
ARR ₁	1	0	1	1	0
ARR ₂	0	1	0	1	1
ARR ₃	1	1	1	0	1

Il caso di guasti multipli può essere trattato espandendo le colonne della matrice FSM. Il vettore FSV di firma di un guasto multiplo è ottenibile dai vettori FSV_k di firma dei singoli guasti occorsi simultaneamente eseguendo una operazione di OR logico tra elementi corrispondenti dei rispettivi vettori di firma FSV_k . Pertanto, in un sistema con n componenti, la considerazione di tutte le possibili combinazioni di guasti multipli porta a costruire una matrice FSM con 2^n colonne.

La diagnosi del sistema è quindi basata sulla valutazione delle ARR, a partire da un insieme di osservazioni del sistema.

Se una ARR_i è soddisfatta sulla base delle osservazioni, allora $ARR_i = 0$, altrimenti $ARR_i = 1$. Le ARR sono istanziate con i valori osservati fornendo una *firma osservata*. La firma della i -esima osservazione è definita come un vettore binario $OS_i = [OS_{i1}, \dots, OS_{in}]^t$, in cui $OS_{ij} = 0$ se ARR_j è soddisfatta dalle osservazioni, e $OS_{ij} = 1$ altrimenti.

La tabella 3 mostra la diagnosi del sistema di figura 1 sulla base di differenti firme di osservazione.

Tabella 3 - Diagnosi del sistema di figura 1 mediante ARR , per differenti firme di osservazione.

Diagnosi	Osservazioni				
ARR_1	0	0	1	1	1
ARR_2	0	1	0	1	1
ARR_3	0	1	1	0	1
Diagnosi di guasto singolo	nessuno	$A_2; M_3$	$A_1; M_1$	M_2	Nessuno
Diagnosi di guasto multiplo	nessuno	(A_2, M_3)	(A_1, M_1)	nessuno	Tutti gli insiemi di guasti doppi, esclusi (A_1, M_1) e (A_2, M_3)

La diagnosi è formulata sulla base dei guasti tenuti in conto nella matrice di firma dei guasti, ovvero una firma osservata $OS_i = [OS_{i1}, \dots, OS_{in}]^t$ è consistente con una firma di guasto $FS_i = [FS_{i1}, \dots,$

$FS_{in}]^t$ se $FS_{ij} = OS_{ij}$ per ogni j .

Ad esempio, per il sistema di figura 1 la firma di osservazione $[0,1,1]^t$ è equivalente alla firma di guasto dei componenti A_2 ed M_3 .

Si noti che ciò indica che, dipendentemente dai sensori del sistema, i guasti delle componenti A_2 ed M_3 non possono essere discriminati, così come nel caso di A_1 ed M_1 .

Il criterio di rivelazione ed isolamento (discriminazione dei guasti) può essere descritto in termini di FSM.

Tutti i guasti possono essere rivelati (rivelazione completa) se non vi è alcuna colonna interamente nulla (ossia, nessun vettore di firma dei guasti nullo) nella FSM. Ovvero, per un dato componente guasto C_i , almeno una ARR viene influenzata. L'isolamento dei guasti è invece assicurato richiedendo che non esistano due colonne della FSM identiche, dal momento che ciò implicherebbe che i due vettori di firma dei guasti siano identici e che quindi i relativi guasti non possano essere distinti.

Il maggiore inconveniente nell'applicazione delle ARR ad un procedimento di diagnosi è relativo alla derivazione efficiente dell'insieme completo e

non ridondante di ARR, che è una limitazione degli algoritmi attuali di esecuzione di diagnosi secondo un approccio FDI.

Un primo aspetto da considerare è innanzitutto il possibile numero di relazioni di ridondanza analitica.

Si consideri un sistema descritto da n relazioni primarie PR (tipicamente ciò significa che il sistema ha n componenti, ma in generale questo potrebbe implicare che il sistema ha al massimo n componenti) ed m sensori (osservazioni) in cui, nella maggior parte dei casi pratici, $n > m$.

Se si considerano le ARR come funzioni di tutte le possibili combinazioni di osservazioni, allora il numero totale di ARR sarebbe dell'ordine di $O(2^m)$. D'altro canto, se si considera che le ARR sono ottenute dalla combinazione di relazioni primarie attraverso l'eliminazione delle variabili incognite, ciò implica un limite superiore al numero di relazioni ARR dell'ordine di $O(2^n)$.

Il punto chiave, che gli inventori ritengono non abbia ricevuto sufficiente attenzione nelle tecniche attualmente applicate, è dato dal fatto che le relazioni ARR possono coinvolgere tutte le possibili combinazione di relazioni primarie PR e

di osservazioni.

Di fatto, un medesimo insieme di relazioni primarie può portare a differenti relazioni ARR, ovvero a differenti ARR con il medesimo insieme di componenti di supporto, ma differenti insiemi di osservazioni.

Si possono anche considerare casi in cui un medesimo insieme di osservazioni può portare a differenti relazioni ARR che differiscono nelle proprie componenti di supporto.

Adottando questo punto di vista si può dunque concludere che il limite superiore al numero totale di relazioni ARR è di fatto dell'ordine di $O(2^{n+m})$. Naturalmente, per ogni sistema di interesse pratico il numero di relazioni ARR è sempre finito a causa dei vincoli strutturali del sistema.

Un'ulteriore questione fondamentale nell'applicazione delle relazioni ARR sia per la diagnosi di sistemi che per la risoluzione del problema di ottimizzazione dei sensori, è relativa alla *completezza* dell'insieme di ARR. Più precisamente, gli inventori sono consapevoli che la questione del *minimo insieme completo* di ARR non ha finora ricevuto sufficiente attenzione.

In letteratura sono stati discussi i concetti

di *d-completezza* (completezza per la rivelazione dei guasti) e *i-completezza* (completezza per l'isolamento dei guasti). Tuttavia, questi due concetti possono essere applicati per l'analisi dell'applicabilità di un dato insieme di ARR per la diagnosi di un sistema, mentre non è affrontato direttamente il problema della derivazione di un insieme completo di relazioni ARR, ma è altrettanto ovvio che la completezza è un aspetto fondamentale sia nella diagnosi che nella ottimizzazione dei sensori, dal momento che in entrambi i problemi è richiesta la maggiore informazione possibile proveniente dalle relazioni ARR.

E' inoltre ovvio che qualsiasi applicazione di un insieme incompleto di relazioni ARR, sia per la diagnosi di un sistema che per l'ottimizzazione dei sensori ad esso associati potrebbe portare a risultati errati e/o subottimali.

Gli inventori, nel proprio articolo dal titolo "A new efficient method for system structural analysis and generating analytical redundancy relations", *Proc. IEEE Aerospace Conference*, Marzo 2009, hanno presentato un innovativo procedimento per la derivazione di un insieme completo di relazioni di ridondanza analitica, la cui complessità è

pari - nel caso peggiore - solo a $O(L^4)$, dove L è il numero di relazioni del sistema, che risolve alcuni limiti degli algoritmi di generazione di ARR fino ad allora noti, svantaggiosamente non-deterministici e di complessità esponenziale.

Un altro aspetto da considerare è che, benché la complessità di calcolo delle ARR sia specifica di ogni sistema, un comune inconveniente di questa tecnica è dato dal fatto che per la diagnosi del sistema è richiesta la valutazione di tutte le ARR, il che comporta significativi oneri di calcolo, anche quando non sono presenti guasti nel sistema. In altre parole, non è possibile determinare a priori un sottoinsieme di ARR che è sufficiente calcolare per rispondere alle necessità di diagnosi contingenti.

Altro aspetto meritevole di considerazione è l'effettiva procedibilità nel calcolo (valutazione) delle ARR. Poiché una ARR è per definizione ottenibile per combinazione di un insieme di relazioni primarie, tale combinazione può richiedere l'inversione delle funzioni rappresentative di una o più relazioni primarie, espresse in forma analitica. Di fatto, nei sistemi reali che si incontrano in applicazioni pratiche, le funzioni rappresentative

della relazioni primarie di alcuni componenti non lineari non possono essere invertite in forma analitica, ma solo in forma numerica, il che rappresenta un ulteriore forte inconveniente che accresce gli oneri computazionali della procedura e ne limita l'applicazione pratica.

Infine, come più sopra richiamato, successivamente alla valutazione delle ARR ed alla formazione del vettore delle osservazioni o firme osservate, quest'ultimo deve essere confrontato con i vettori dei guasti nella matrice FSM. Benché questa operazione sia piuttosto semplice, la complessità è accresciuta nel caso di diagnosi di guasti multipli.

Se si considera un sistema con n componenti e tutte le possibili combinazioni di guasti, allora si formerebbe una matrice FSM di 2^n colonne, il che comporta una crescita esponenziale nello spazio di memoria da allocare alla FSM nel sistema di elaborazione per l'esecuzione dell'algoritmo di diagnosi e nel tempo di calcolo impiegato da tale sistema per il confronto del vettore di osservazione con i vettori di guasti.

* * *

La presente invenzione si prefigge lo scopo di

fornire una soluzione soddisfacente ai problemi in precedenza esposti, evitando gli inconvenienti della tecnica nota.

Più in particolare, la presente invenzione si prefigge lo scopo di fornire un procedimento efficiente, in particolare dal punto di vista computazionale, e corretto per la diagnosi tempestiva di guasti critici ad un sistema, basata su un modello del sistema.

Secondo la presente invenzione tali scopi vengono raggiunti grazie ad un procedimento per la generazione di un insieme di conflitti per la diagnosi di un sistema basata su modelli, avente le caratteristiche richiamate nella rivendicazione 1, ed un procedimento di diagnosi avente le caratteristiche richiamate nella rivendicazione 6.

Modi particolari di realizzazione formano oggetto delle rivendicazioni dipendenti, il cui contenuto è da intendersi come parte integrale o integrante della presente descrizione.

Formano ulteriore oggetto dell'invenzione un sistema di diagnosi ed un programma per elaboratore per l'attuazione dei suddetti procedimenti, come rivendicato.

La presente invenzione si fonda sul principio

di combinare le caratteristiche vantaggiose degli approcci DX e FDI sopra descritti, ed in particolare dell'algoritmo DX GDE e dell'algoritmo FDI basato sulle ARR, evitando l'applicazione integrale di ognuno di essi, che farebbe incorrere nei rispettivi svantaggi sopra menzionati.

In particolare, il procedimento oggetto dell'invenzione trae vantaggio dall'approccio di diagnosi basato sulle ARR, che corrispondono ai potenziali conflitti alla base della tecnica di diagnosi DX, in quanto le ARR sono generate a priori una sola volta per un dato sistema. Ciò consente di eseguire una diagnosi più rapida, in confronto con la ripetuta esecuzione di algoritmi di ricerca degli insiemi di conflitti secondo l'approccio DX.

Più specificamente, le relazioni di ridondanza analitica sono ricavate secondo il procedimento descritto dagli inventori nel citato articolo "A new efficient method for system structural analysis and generating analytical redundancy relations", *Proc. IEEE Aerospace Conference*, Marzo 2009.

Ciascuna relazione intermedia, di seguito indicata brevemente R_j , impiegata per derivare l'insieme di relazioni di ridondanza analitica ARR, che per definizione comportano solo variabili note (os-

servazioni), è data da una quadrupla della forma seguente:

$$R_j = (N_j, C_j, S_j, T_j)$$

in cui N_j è il numero d'ordine assegnato alla relazione R_j , C_j è l'insieme delle componenti di supporto, S_j è l'insieme delle variabili coinvolte in R_j e T_j è l'insieme delle relazioni primarie utilizzate per derivare la relazione R_j .

Specificamente, ciascuna relazione primaria è rappresentata da una quadrupla di forma

$$R_j = (n_j, C_j, S_j, \{n_j\})$$

in cui n_j è il numero della relazione primaria, e dal momento che ciascuna relazione primaria non dipende dalle altre relazioni, l'ultima componente della quadrupla è $\{n_j\}$.

Operazione di base del procedimento di generazione di un insieme completo di ARR è la generazione di una nuova relazione a partire da due relazioni date, per eliminazione di una variabile comune.

Date due relazioni:

$$R_j = (N_j, C_j, S_j, T_j) \quad \text{e} \quad R_k = (N_k, C_k, S_k, T_k)$$

se sono soddisfatte entrambe le seguenti condizioni:

$$S_j \cap S_k \neq \{\} \quad \text{e} \quad T_j \cap T_k = \{\}$$

allora, per ciascuna variabile non osservata

$x \in S_j \cap S_k$ si genera la seguente relazione

$$R = (N, C_j \cup C_k, (S_j \cup S_k) - \{x\}, T_j \cup T_k),$$

in cui N è un nuovo numero.

Poiché è possibile che si ottengano le medesime relazioni (intermedie o ARR) attraverso differenti derivazioni, per evitare di mantenere diverse copie di una medesima relazione, due relazioni

$$R_j = (N_j, C_j, S_j, T_j) \text{ e } R_k = (N_k, C_k, S_k, T_k)$$

si definiscono *identiche* se

$$(S_j, T_j) = (S_k, T_k)$$

e nel processo di generazione delle ARR, se una nuova relazione intermedia o una ARR è identica ad una generata precedentemente, allora essa è cancellata dall'elenco.

Si noti che la generazione di ogni nuova relazione è eseguita in forma implicita attraverso operazioni su insiemi, senza necessità di determinare a priori alcuna espressione analitica e calcolare l'inversione delle funzioni rappresentative di una o più relazioni.

A partire dall'insieme completo di relazioni di ridondanza analitica in forma implicita è comunque possibile derivare la matrice FSM del sistema, senza necessità di conoscere esattamente le funzio-

ni analitiche di ciascuna relazione e di calcolarne l'inversione, ricorrendo alla derivazione della forma esplicita ed alla valutazione esclusivamente di un sottoinsieme limitato di relazioni ARR per l'effettiva diagnosi del sistema.

Ogni ARR necessaria alla diagnosi del sistema può essere calcolata numericamente considerando l'insieme di relazioni primarie coinvolte nella sua derivazione, nonché il suo percorso di derivazione, ossia l'ordine di combinazione delle suddette relazioni primarie. Occorre evidenziare che la valutazione del sottoinsieme di ARR richiede esclusivamente l'inversione numerica della relativa funzione e non la determinazione della forma analitica della sua inversa.

In tal modo è possibile sfruttare le due caratteristiche vantaggiose dell'approccio di diagnosi basato sulla valutazione delle ARR, ossia la derivazione in una sola occasione delle relazioni di ridondanza analitica che stabiliscono le relazioni tra i valori osservati dei sensori ed i componenti del sistema, nonché la possibilità di derivazione della matrice di firma dei guasti per una analisi a priori delle proprietà di rivelazione ed isolamento dei guasti del sistema e la determinazione degli

insiemi di ambiguità nella diagnosi.

Per ovviare all'onere computazionale proprio di una diagnosi basata su ARR secondo la tecnica nota FDI, che richiederebbe la valutazione di tutte le ARR, tanto più impegnativa quanto più le relative espressioni analitiche non sono disponibili e devono essere calcolate numericamente, poiché la derivazione delle ARR deve essere convenientemente effettuata in tempo reale ogniqualvolta è eseguito l'algoritmo di diagnosi, l'invenzione si basa sul principio di ridurre il numero di ARR da valutare quale chiave per migliorare l'efficienza del procedimento di diagnosi.

Come discusso nell'articolo di M-O.Cordier et al. "Conflicts vs. analytical redundancy relations: a comparative analysis of the model based diagnosis approach from the artificial intelligence and automatic control perspectives", *IEEE Transactions on Systems, Man and Cybernetics, Part B: Cybernetics*, vol. 34, n. 5, pagg. 2163-2177, Ottobre 2004, le ARR possono essere raggruppate in ARR di rivelazione (D-ARR) e ARR di isolamento (I-ARR). Le D-ARR riguardano un solo sensore o variabile di osservazione del sistema (quindi il loro numero complessivo è pari a quello dei sensori), mentre le I-ARR

dipendono ciascuna da più sensori (variabili di osservazione del sistema). Il meccanismo di generazione delle ARR individua direttamente da quali e quanti sensori dipendono, quindi ne permette automaticamente la classificazione.

Nell'esempio del sistema multi-porta di figura 1, ARR_1 ed ARR_2 sono D-ARR, mentre ARR_3 è una I-ARR.

Secondo l'invenzione, solo le D-ARR determinano i valori attesi dei sensori.

Queste ARR rappresentano di fatto la simulazione del sistema, ovvero le relazioni per il calcolo dei valori attesi dei sensori utilizzando il modello di sistema, per un dato insieme di valori delle variabili di ingresso. Si noti che ciascuna D-ARR coinvolge solo un sensore, e quindi il numero di D-ARR corrisponde al numero complessivo prestabilito dei sensori del sistema. Inoltre, esse non necessitano di una inversione della relativa funzione.

Pertanto, un primo passo del procedimento oggetto dell'invenzione per la generazione di un insieme di conflitti e la diagnosi di un sistema comprende una operazione di rivelazione dei guasti, in cui dato un insieme di ingressi è eseguita una simulazione sulla base del modello del sistema per

definire i valori attesi dei sensori. Ciò corrisponde alla valutazione delle D-ARR. Se il valore atteso dei sensori corrisponde a quello misurato, ovvero le D-ARR sono soddisfatte, allora non vi sono guasti al sistema.

Se i valori attesi dei sensori sono differenti da quelli misurati, ciò rappresenta una discrepanza, secondo la definizione dell'approccio DX.

E' quindi eseguito un successivo passo di generazione di conflitti a partire dalla conoscenza dei sensori che rappresentano le discrepanze rivelate, ossia quei sensori i cui valori attesi sono differenti da quelli misurati.

Secondo l'invenzione, dall'insieme di I-ARR quelle che non comportano alcun sensore che presenti una discrepanza sono necessariamente soddisfatte, dal momento che esse rappresentano relazioni tra gli ingressi del sistema e le misure risultanti corrette, attese dal modello. Al contrario, le I-ARR che comportano uno o più sensori che presentano discrepanze sono considerate come potenziali conflitti.

Le I-ARR che comportano uno o più sensori che presentano discrepanze (sottoinsieme di tutte le I-ARR possibili) sono quindi calcolate e valutate e-

seguendo una verifica di consistenza (*consistency check*).

La verifica di consistenza determina se ciascuna I-ARR in esame, ossia facente parte di quelle che dipendono da più sensori che coinvolgono componenti guasti, è soddisfatta oppure no. Questo controllo non viene eseguito calcolando esplicitamente la I-ARR (che è generata solo in forma implicita, dato che una forma esplicita o analitica potrebbe non esistere), ma calcolando la coerenza dei risultati delle relazioni primarie che sono coinvolte nella I-ARR medesima: se queste sono coerenti, la relativa I-ARR è soddisfatta, altrimenti no.

Una I-ARR soddisfatta è esclusa delle successive operazioni. Il supporto di ciascuna I-ARR che viene riconosciuta come non soddisfatta rappresenta definitivamente un conflitto.

A questo punto, avendo determinato le ARR non soddisfatte si può formare un vettore di osservazione ed eseguire la diagnosi del sistema mediante la matrice FSM, secondo un approccio FDI.

Come si comprenderà, questo approccio innovativo misto permette di raggiungere una maggiore efficienza rispetto alla singola tecnica GDE o alla singola tecnica di diagnosi basata su ARR, poiché

limita il calcolo alla valutazione di un sottoinsieme delle ARR.

Infine, poiché per sistemi complessi la diagnosi di guasti multipli mediante una matrice FSM espansa determinerebbe oneri crescenti esponenzialmente in termini di tempo di calcolo e spazio di memoria, è preferibile l'esecuzione di una diagnosi minima attraverso la risoluzione del relativo problema di determinazione dell'"hitting set" o insieme minimo intersezione di tutti gli insiemi dei potenziali conflitti così determinati, ossia dell'insieme minimo di componenti di cui almeno uno è contenuto in ciascuno degli insiemi di potenziali componenti guasti, definiti dalle ARR non soddisfatte. Benché il problema di determinazione dell'"hitting set" sia un problema NP-completo è possibile risolverlo efficientemente in casi pratici, ad esempio applicando l'algoritmo di branch-and-bound descritto da A. Fijany e F. Vatan in "New high performance algorithmic solution for diagnosis problem", *Proc. IEEE Aerospace conference*, Marzo 2005, e nel brevetto statunitense US 7 249 003 dal titolo "System for solving diagnosis and hitting set problems, degli stessi autori.

Ulteriori caratteristiche e vantaggi dell'in-

venzione verranno più dettagliatamente esposti nella descrizione particolareggiata seguente, data a titolo di esempio non limitativo, con riferimento ai disegni allegati, nei quali:

la figura 1 rappresenta uno schema circuitale di un sistema multi-porta analizzato nella parte introduttiva di questa descrizione; e

le figure 2a e 2b rappresentano rispettivi schemi circuitali di circuiti combinatori a cui è applicato il procedimento oggetto dell'invenzione.

Un sistema di elaborazione per la diagnosi di un sistema secondo il procedimento oggetto dell'invenzione comprende una stazione di lavoro computerizzata (workstation) di tipo noto (non raffigurata), ovvero un sistema di elaborazione di tipo distribuito, avente un sottosistema elaboratore e dispositivi periferici di ingresso/uscita, locali o remoti, predisposti per eseguire un programma di elaborazione e calcolo o gruppi/moduli di programma memorizzati su disco o accessibili in rete, che realizzano il procedimento (algoritmo) oggetto dell'invenzione. Tali soluzioni qui richiamate sono considerate ben note nella tecnica e non saranno ulteriormente descritte in questa sede perché di per sé non rilevanti ai fini dell'attuazione e del-

la comprensione della presente invenzione.

Per meglio comprendere lo sviluppo del procedimento misto oggetto dell'invenzione basato sulla derivazione di relazioni di ridondanza analitica implicite e l'estrapolazione da esse di un insieme di conflitti per la diagnosi di un sistema, è utile fornire una sintetica introduzione all'approccio DX secondo la tecnica nota, per poterne estendere la portata in un quadro di notazioni comuni al presente procedimento.

Secondo l'approccio DX, le variabili di un sistema sono rappresentate da un vettore di variabili e ciascuna relazione primaria PR è rappresentata da un insieme di regole per la propagazione dei valori da una variabile all'altra.

Ciascuna regola include cinque componenti, espresse nel seguito, in cui le variabili sono indicate dal vettore Vars[].

- out indice in Vars[]
- in[] vettori di indici in Vars[]
- Fn() funzione sugli ingressi
- Tst() test sugli ingressi
- A assunzione

In un tradizionale approccio DX ciascun elemento di Vars[] contiene un insieme di zero o più

espressioni nella forma `<valore:{assunzioni}>`, che denotano che una variabile può assumere un particolare valore in funzione di quale insieme di assunzioni valga. Ad esempio, con riferimento al sistema multi-porta di figura 1, la prima regola, espressione del moltiplicatore M_1 , avrebbe le seguenti cinque componenti, in cui gli indici 1, 3, 6 nel vettore `Vars[]` indicano le variabili "a", "c" e "x", rispettivamente.

```
- out      = 6
- in[]     = [1,3]
- Fn()     = moltiplica() - moltiplica semplicemente gli ingressi
- Tst()    = vero() - ritorna semplicemente vero
- A        =  $M_1$ 
```

Data questa rappresentazione delle variabili e delle regole, la propagazione dei valori nel sistema segue l'algoritmo in tabella 4, che rappresenta la routine `Propagate()` in cui `Vars[V]` assume un valore C ogniqualvolta risulta vero l'insieme di assunzioni S non contraddittorio.

Per determinare se un insieme di assunzioni è contraddittorio oppure no è eseguito il confronto con gli elementi di un insieme NGDS, contenente

tutti gli insiemi contraddittori di assunzioni noti.

Tabella 4 - Routine di propagazione dei valori tra variabili di un sistema, secondo un insieme di regole predeterminate

```
Propagate(V, <C:S>, Rules, Vars, NGDS)
Let Agenda2  $\leftarrow \emptyset$ 
For each R  $\in$  Rules, where V = R.in[X] for some X do
  For each P, where  $P[X] = \langle C:S \rangle \wedge P[] = \langle c:s \rangle \in \text{Vars}[R.in[]]$  do
    If  $R.Tst(P) \wedge N \not\subset \cup(s) \cup \{R.A\}$  for any  $N \in NGDS$  then
      Add [R.out,  $\langle R.Fn(P) \cup (s) \cup \{R.A\} \rangle$ ] to Agenda2
Return Agenda2
```

La routine di propagazione Propagate() riceve le proprie variabili di ingresso ed un insieme di regole (Rules) ed esegue iterazioni su ciascuna regola che abbia Vars[V] come ingresso. Poiché ciascuna regola presenta molteplici variabili di ingresso, e ciascuna variabile può avere molteplici valori in funzione delle assunzioni, ciascuna regola può propagare numerosi valori, in funzione dei propri ingressi. Questo calcolo, per ogni regola, è eseguito dal ciclo interno della routine che assicura che l'ingresso per V sia <C:S>.

Ciascuna iterazione del ciclo interno esegue due test per determinare se la regola deve applicarsi al proprio insieme di ingressi. Gli ingressi

tenuti in considerazione nel calcolo devono superare la funzione di test `Tst()` delle regole e le assunzioni non devono contraddirsi tra loro. Le contraddizioni sono testate raccogliendo l'unione delle assunzioni e determinando se l'insieme risultante contiene un insieme contraddittorio appartenente a NGDS.

Ogniquale volta si applica una regola viene calcolato un valore contrassegnato da assegnare ad una variabile di uscita e le assegnazioni di tali valori sono raccolte nell'insieme `agenda2` di relazioni non soddisfatte (insieme di conflitti) e infine ritornati all'algoritmo chiamante.

L'algoritmo DX

L'algoritmo maggiormente applicato nella letteratura DX, che utilizza la routine di propagazione sopra richiamata, è certamente l'algoritmo GDE.

L'approccio generale usato nella tecnica DX è quello di assumere un insieme di osservazioni e propagarle attraverso un modello del sistema, ricercando le inconsistenze tra le assunzioni e le osservazioni. Date queste inconsistenze, l'algoritmo DX ricerca l'insieme delle assunzioni non rispettate che tiene conto nel modo più appropriato delle osservazioni.

Ad esempio, la seguente tabella 5 contiene un algoritmo mGDE, variante semplificata dell'algoritmo GDE, che usa la procedura Propagate() per la propagazione dei valori.

Tabella 5 - Algoritmo DX di propagazione dei valori

```

mGDE(Agenda, Rules)
Let NGDS  $\leftarrow \emptyset$ , Vars  $\leftarrow [\emptyset, \emptyset, \dots]$ 
While Agenda is not empty do
    Extract [V, <C:S>] from Agenda
    If there is no <C:S'>  $\in$  Vars[V], where  $S' \subset S$ 
        Remove all <C:S'>  $\in$  Vars[V], where  $S \subset S'$ 
        Add <C:S> to Vars[V]
    For each <D:L>  $\in$  Vars[V] where  $D \neq C$  do
        Add  $S \cup L$  to NGDS removing redundancies,
        Remove all <X:Y> from Vars where  $Y \supseteq S \cup L$ 
        Remove all [W, <X:Y>] from Agenda where  $Y \supseteq S \cup L$ 
    Add Propagate(V, <C:S>, Rules, Vars, NGDS) to Agenda
Return HittingSets(NGDS)

```

Questo algoritmo assume semplicemente un'agenda iniziale di assegnazioni di valori contrassegnati e li elabora per determinare insiemi di assunzioni reciprocamente inconsistenti.

Ciascuna iterazione, che avviene attraverso il ciclo WHILE più esterno, elabora una singola assegnazione di un valore contrassegnato. Se tale assegnazione non è ridondante rispetto ai valori contrassegnati già associati alla relativa variabile, allora essa è aggiunta all'insieme di valori con-

trassegnati della variabile. Quando un'aggiunta rende altri valori contrassegnati ridondanti, questi sono allora rimossi dall'insieme della variabile. Formalmente, un valore contrassegnato $\langle C:S \rangle$ rende $\langle C:T \rangle$ ridondante ogniquale volta le assunzioni S implicano le assunzioni T , o in altri termini, $S \subseteq T$.

Una volta che un valore contrassegnato è assegnato ad una variabile il ciclo FOR più interno gestisce gli insiemi di assunzioni inconsistenti. Innanzitutto, una variabile non può avere due valori allo stesso tempo, quindi questa condizione è indicata come una inconsistenza. Le inconsistenze sono aggiunte all'insieme NGDS una volta rimosse le ridondanze, dove un insieme è considerato ridondante se esso è un superinsieme di un altro. Queste inconsistenze contribuiscono anche a rimuovere elementi dall'agenda e dal vettore Vars[] quando le loro etichette sono riconosciute come inconsistenti.

Infine, il risultato ultimo ritornato dalla routine mGDE è l'hitting set delle inconsistenze, ovvero l'insieme che contiene almeno un elemento da ciascuno degli insiemi di inconsistenze.

L'insieme di diagnosi è dato dall'insieme dei

minimi hitting set di NGDS.

L'algoritmo basato sulle ARR implicite, oggetto dell'invenzione

Si consideri una ARR come una equazione analitica da verificare ed un insieme di assunzioni che si rivelano mutuamente inconsistenti quando l'equazione non è verificata.

Invece dell'equazione da verificare, si caratterizza esclusivamente l'insieme di sensori che intervengono nella verifica dell'equazione. Pertanto, una ARR per un sistema diagnosticabile adottando il procedimento secondo l'invenzione presenta due componenti:

- sensors un insieme di variabili rilevate o rilevabili; e
- assume un insieme di assunzioni

Utilizzando questa caratterizzazione delle ARR l'algoritmo di diagnosi include un modello DX del dispositivo per verificare ciascuna ARR e la procedura (l'algoritmo) di diagnosi per mezzo delle ARR somiglia a quello riportato in tabella 4, in cui gli ingressi denotano valori imposti al sistema e le uscite denotano i valori rilevati. Ciò differisce sostanzialmente dalla procedura mGDE sopra richiamata, che si basa solo sull'agenda di parame-

tri, con assegnazioni di valori contrassegnati per entrambi gli ingressi e le uscite.

Come mostrato in tabella 6 seguente, l'algoritmo esegue inizialmente un ciclo WHILE per simulare un sistema a partire dagli ingressi imposti e calcolare le uscite attese.

Tabella 6 - Procedura di diagnosi basata sulle ARR implicite

```

mARR(Inputs, Outputs, Rules, ARRS)
Let NGDS  $\leftarrow \emptyset$ , Vars  $\leftarrow [\emptyset, \emptyset, \dots]$ , and Agenda  $\leftarrow$  Inputs
While Agenda is not empty do
    Extract [V, <C:S>] from Agenda & add <C: $\emptyset\emptyset\emptyset$ ) to Agenda
    BADS  $\leftarrow \{V \mid [V, \langle C:\emptyset \rangle] \in \text{Outputs} \wedge \text{Vars}[V] \neq \{\langle C:\emptyset \rangle\}\}$ 
    For each A  $\in$  ARRS
        If BADS  $\cap$  A.sensors  $\neq \emptyset$ 
            Let Vars  $\leftarrow [\emptyset, \emptyset, \dots]$ 
            Let RS  $\leftarrow \{R \mid R \in \text{Rules} \wedge R.A \in A.\text{assume}\}$ 
            Let Agenda  $\leftarrow$  Inputs  $\cup$  Outputs
            While Agenda is not empty do
                Extract [V, <C:X>] from Agenda & add <C: $\emptyset\emptyset\emptyset\leftarrow$  {<C: $\emptyset\emptyset\emptyset\neq$ D
                    Add A.assume to NGDS and empty Agenda
                Else
                    Append Propagate(V, <C: $\emptyset\emptyset$ ) to Agenda
            Return HittingSets(NGDS)

```

Le uscite calcolate sono quindi confrontate con le uscite rilevate per determinare l'insieme BADS di valori rilevati che risultano inconsistenti

con i valori attesi calcolati.

Questo insieme è quindi utilizzato per determinare quali ARR devono essere verificate ulteriormente, al fine di calcolare la pluralità di insiemi di assunzioni inconsistenti (conflitti). Pertanto, il successivo ciclo FOR esegue una iterazione su per ciascuna ARR e verifica se i sensori che contribuiscono a tale ARR intersecano l'insieme BADS.

La verifica di una ARR comporta di considerare se gli ingressi ed i valori rilevati siano consistenti con le regole implicate dalle assunzioni della ARR medesima. Pertanto, il ciclo WHILE più interno ha notevoli somiglianze con l'algoritmo mGDE. La differenza primaria è data tuttavia dal fatto che i valori non sono contrassegnati. Ne deriva che il test delle ARR fallisce ogniqualvolta due valori differenti sono assegnati alla medesima variabile. Per questo motivo le etichette sono completamente superflue ed una variabile non possiede mai più di un valore ad essa associato.

Per questo motivo, la chiamata della procedura Propagate() da parte della routine mARR non ritorna mai più di un valore da aggiungere all'insieme Agenda di relazioni non soddisfatte o conflitti.

Conclusioni

Una verifica delle prestazioni del procedimento oggetto dell'invenzione è stata condotta confrontando l'esito di un procedimento di diagnosi basato su un tradizionale approccio DX con l'esito di un procedimento di diagnosi basato sull'algoritmo proposto dagli inventori, tramite la verifica su circuiti composti da sommatore e moltiplicatori come il circuito multi-porta di esempio, rappresentato in figura 1.

Per verificare la correttezza degli approcci sono stati provocati guasti in ciascun elemento del sistema ed entrambi gli algoritmi sono stati eseguiti per ottenere un insieme di risultati di diagnosi, i quali sono poi stati confrontati tra loro per verificare se restituivano i medesimi insiemi di diagnosi.

A titolo esemplificativo, sono stati sottoposti a test due strutture circuitali rappresentate nelle figura 2a e 2b, che mostrano due schemi di circuiti combinatori includenti sommatore e moltiplicatori, dove gli ingressi sono raffigurati in alto e le uscite in basso. Specificamente, il primo esempio è una estensione del circuito multi-porta di figura 1, mentre il secondo rappresenta un circuito dalla connettività più complessa.

Per ottenere informazioni sulle prestazioni relative tra l'algoritmo di tecnica nota e l'algoritmo oggetto dell'invenzione, essi sono stati eseguiti su entrambi i circuiti per diagnosticare un guasto imposto ad una delle porte.

In tutti i casi, gli algoritmi di diagnosi hanno calcolato il medesimo insieme NGDS e hanno fornito in uscita i medesimi insiemi di diagnosi, in cui una delle diagnosi riconosciute era effettivamente la porta guasta.

Poiché gli insiemi NGDS erano identici, la miglior misura relativa della quantità di calcolo eseguita da ciascun algoritmo è rappresentata dal numero totale di assegnazioni di valori contrassegnati, forniti in uscita dalla routine Propagate().

La tabella 7 riporta, a scopo di confronto, alcuni risultati statistici per ciascuno dei tre sistemi descritti nelle figure 1, 2a e 2b.

Tabella 7 - Risultati del confronto tra procedimenti di diagnosi

	#ARR	mGDE	mARR
Circuito Fig. 1	3	45,8	9,3
Circuito Fig. 2a	39	1390,5	408,9
Circuito Fig. 2b	94	1807,7	1244,2

Nella prima colonna è riportato il numero di ARR richieste per diagnosticare il circuito. Nel caso in cui una qualsiasi di queste ARR sia rimossa, la procedura mGDE non fornisce la stessa diagnosi della procedura mARR, il che dimostra che l'intero insieme di ARR è necessario, ed è conveniente che si determinato col minor onere computazionale possibile.

La seconda colonna rappresenta il numero totale medio di calcoli effettuati dalla procedura Propagate() richiamata dalla routine mGDE, mentre la terza colonna rappresenta il numero totale medio di calcoli effettuati della procedura Propagate() richiamata dalla routine mARR.

Questi valori sono stati determinati iterando l'algoritmo per tutti i test con nessun guasto e con un guasto, sommando il numero di assegnazioni contrassegnate risultanti, e dividendo tale numero per il numero di iterazioni eseguite. Si nota chiaramente che la routine mARR oggetto dell'invenzione offre prestazioni decisamente migliori della routine mGDE.

Vantaggiosamente, dunque, il metodo oggetto dell'invenzione rende possibile la diagnosi efficiente di un sistema sfruttando, in una combinazio-

ne innovativa, i punti forti dei metodi di diagnosi basati sulle ARR e sulla tecnica DX, ma nel contempo evitandone gli inconvenienti, ottenendo prestazioni superiori ai procedimenti di diagnosi interamente basati sulla valutazione delle ARR o, in alternativa, sull'approccio DX.

La metodologia proposta rende possibile la più efficiente ed accurata derivazione degli insiemi di conflitti per la diagnosi di un sistema. Analogamente all'approccio FDI, essa impiega le ARR, ma in forma implicita e non in forma esplicita ed analitica, per cui può essere praticamente applicata ad ogni sistema. In modo analogo all'approccio DX, essa impiega le verifiche di consistenza per valutare alcune assunzioni sul sistema, ma diversamente da tale approccio essa sfrutta la conoscenza completa del sistema, fornita dalle ARR implicite, e riduce pertanto drasticamente il numero di verifiche di consistenza, a beneficio dell'efficienza.

La derivazione rapida e corretta di un insieme di conflitti è alla base per una efficiente e rapida diagnosi di un sistema, che consenta di attuare una strategia di recupero ed evitare la perdita del sistema ed ulteriori possibili danni.

Naturalmente, fermo restando il principio

dell'invenzione, le forme di attuazione ed i particolari di realizzazione potranno essere ampiamente variati rispetto a quanto è stato descritto ed illustrato a puro titolo di esempio non limitativo, senza per questo allontanarsi dall'ambito di protezione dell'invenzione definita dalle rivendicazioni allegate.

1. Procedimento attuabile per mezzo di un elaboratore per la generazione di un insieme di conflitti per la diagnosi di un sistema descrivibile da un modello basato sulla configurazione di componenti del sistema, comprendente un insieme di relazioni primarie tra ingressi ed uscite di ciascuna componente, indicative della relativa funzione operativa, ed al quale è associata una pluralità di sensori per l'osservazione di variabili indicative di condizioni di funzionamento,

in cui detto insieme di conflitti comprende un sottoinsieme di componenti del sistema la cui assunzione di corretto funzionamento non è consistente con il comportamento osservato del sistema,

il procedimento essendo caratterizzato dal fatto che comprende le operazioni di:

- generare, in via preliminare, un insieme completo di relazioni di ridondanza analitica (ARR) in forma implicita per il sistema, in cui ogni relazione è rappresentativa delle relazioni logiche tra un sottoinsieme di variabili osservabili del sistema ed un corrispondente sottoinsieme di componenti di supporto del sistema, e

per ogni istanza di diagnosi

- eseguire una simulazione del sistema sulla base del modello, dato un prestabilito insieme di valori agli ingressi del sistema, calcolando i valori attesi di un primo sottoinsieme di relazioni di ridondanza analitica (D-ARR) comprendente le relazioni che includono rispettivamente una sola variabile di osservazione del sistema,

- confrontare i valori attesi ed i valori osservati delle variabili di osservazione del sistema ed identificare le variabili di osservazioni discrepanti ovvero le relazioni di ridondanza di detto primo sottoinsieme che non sono soddisfatte, indicative di un guasto in almeno un componente del sistema; e

nel caso di rivelazione di discrepanze,

- verificare la consistenza di ciascuna relazione di un secondo sottoinsieme di relazioni di ridondanza analitica (I-ARR) comprendente relazioni che includono rispettivamente una pluralità di variabili di osservazione del sistema, almeno una delle quali presenta discrepanze tra i valori attesi ed i valori osservati; e

- identificare l'insieme dei supporti delle relazioni di ridondanza di detto secondo sottoinsieme che non sono soddisfatte come insieme di con-

flitti del sistema, atti a consentire la rivelazione e la discriminazione dei guasti al sistema.

2. Procedimento secondo la rivendicazione 1, caratterizzato dal fatto che comprende la selezione di un insieme completo di relazioni di ridondanza analitica (ARR_k) del sistema tra un insieme di relazioni intermedie stabilite tra variabili osservabili e non osservabili del sistema,

in cui ogni relazione intermedia (R_j) è generata per combinazione di due relazioni predeterminate

$$R_j = (N_j, C_j, S_j, T_j) \quad \text{e} \quad R_k = (N_k, C_k, S_k, T_k)$$

N_j, N_k essendo i numeri d'ordine assegnati rispettivamente alle relazioni R_j, R_k , ciascuna delle quali è espressa in forma implicita come tupla (i) di un sottoinsieme S_j di variabili del sistema, (ii) dell'insieme C_j delle componenti di supporto a tale relazione, e (iii) dell'insieme T_j delle relazioni primarie utilizzate per derivare detta relazione intermedia,

secondo la regola:

$$R = (N, C_j \cup C_k, (S_j \cup S_k) - \{x\}, T_j \cup T_k),$$

dove $(S_j \cup S_k) - \{x\}$ indica una operazione di differenza simmetrica tra i sottoinsiemi di

variabili S_j, S_k per ciascuna variabile non osservabile $x \in S_j \cap S_k$,

quando sono soddisfatte entrambe le condizioni:

$$S_j \cap S_k \neq \{\} \quad \text{e} \quad T_j \cap T_k = \{\}$$

3. Procedimento secondo la rivendicazione 2, caratterizzato dal fatto che detto insieme di relazioni intermedie non include relazioni intermedie identiche, secondo la relazione di identità:

$$(S_j, T_j) = (S_k, T_k).$$

4. Procedimento secondo la rivendicazione 1, 2 o 3, in cui la verifica della consistenza di ciascuna relazione di detto secondo sottoinsieme di relazioni di ridondanza analitica (I-ARR) è eseguita verificando la coerenza dei risultati delle relazioni primarie coinvolte nella relazione, espressa in forma implicita.

5. Procedimento secondo una qualsiasi delle rivendicazioni precedenti, comprendente l'operazione di derivare, a partire dall'insieme completo di relazioni di ridondanza analitica generato in forma implicita, la matrice di firma dei guasti per una condizione teorica di guasto singolo, per analizzare le proprietà di rivelazione ed isolamento di

guasti del sistema e determinarne gli insiemi di ambiguità.

6. Procedimento per la diagnosi di un sistema al quale è associata una pluralità di sensori per l'osservazione di variabili indicative di condizioni di funzionamento, basata su un modello del sistema rappresentativo della configurazione di componenti del sistema, includente un insieme di relazioni primarie tra ingressi ed uscite di ciascuna componente, indicative della relativa funzione operativa, comprendente:

- la simulazione del sistema sulla base del modello;

- la rivelazione di guasti al sistema per confronto tra i valori attesi dalla simulazione ed i valori osservati delle variabili di osservazione del sistema;

- la generazione di almeno un insieme di conflitti comprendente un sottoinsieme di componenti del sistema la cui assunzione di corretto funzionamento non è consistente con il comportamento osservato del sistema; e

- la determinazione del minimo numero di componenti coinvolti nella generazione di discrepanze tra il comportamento atteso del sistema e quello

reale, intersezione di tutti gli insiemi di conflitti generati;

caratterizzato dal fatto che la generazione degli insiemi di conflitti è effettuata attraverso un procedimento secondo una qualsiasi delle rivendicazioni 1 a 5.

7. Sistema di diagnosi, comprendente un complesso di elaborazione predisposto per attuare un procedimento per la generazione di un insieme di conflitti e la diagnosi di un sistema descrivibile da un modello, secondo una qualsiasi delle rivendicazioni 1 a 6.

8. Programma di elaboratore o gruppo di programmi eseguibile/i da un complesso di elaborazione, comprendente/i uno o più moduli di codice per l'attuazione di un procedimento per la generazione di un insieme di conflitti e la diagnosi di un sistema descrivibile da un modello, secondo una qualsiasi delle rivendicazioni 1 a 6.

CLAIMS

I0136863

1. A computer-implemented method for generating a set of conflicts to diagnose a system describable by a model based on the arrangement of system components, said model including a set of primary relations (PRs) between inputs and outputs of each component, representing its operating function, and with which system a plurality of sensors is associated for the observation of variables indicative of operation conditions,

where said conflicts set includes a subset of system components for which the assumption of correct operation is not consistent with the observed system behaviour,

the method being characterized in that it includes the steps of:

- generating, as a preliminary step, a complete set of Analytical Redundancy Relations (ARRs) for the system in implicit form, in which each relation represents the logical relations between a subset of observable variables of the system and a corresponding subset of support components of the system, and

for each diagnosis instance

- performing a system simulation based on

the model, given a predetermined set of values as system inputs, computing the expected values for a first subset of Analytical Redundancy Relations (D-ARRs) including the relations involving only one system observation variable,

- comparing the expected and observed values of the system observation variables and identify the inconsistent observation variables, i.e. the unsatisfied redundancy relations of said first subset, indicating a fault in at least one system component; and

when discrepancies are detected,

- checking the consistency of each relation belonging to a second subset of Analytical Redundancy Relations (I-ARR), comprising relations involving a plurality of system observation variables, at least one of which exhibits discrepancies between expected and observed values; and

- identifying the support set of the unsatisfied Redundancy Relations of said second subset as set of system conflicts, adapted to detect and isolate the system faults.

2. Method according to Claim 1, characterized in that it includes the selection of a complete set of Analytical Redundancy Relations (ARR_s) for the sys-

tem among a set of intermediate relations existing between observable and non-observable system variables,

wherein each intermediate relation (R_i) is generated by combining two predetermined relations

$$R_j = (N_j, C_j, S_j, T_j) \text{ and } R_k = (N_k, C_k, S_k, T_k)$$

N_j, N_k being the ordinal numbers assigned to the relations R_j, R_k , each being expressed in implicit form as tuple (I) of a subset S_j of system variables, (II) of the set C_j of the support components of said relation, and (III) of the set T_j of the primary relations used to derive said intermediate relation,

according to the rule:

$$R = (N, C_j \cup C_k, (S_j \cup S_k) - \{x\}, T_j \cup T_k),$$

where $(S_j \cup S_k) - \{x\}$ indicates a symmetric difference operation between the subsets of variables S_j, S_k for each non-observable variable $x \in S_j \cap S_k$,

when both the conditions:

$$S_j \cap S_k \neq \{\} \quad \text{and} \quad T_j \cap T_k = \{\}$$

are satisfied.

3. Method according to Claim 2, characterized by the fact that said set of intermediate relations does not include identical intermediate relations,

according to the identity relation:

$$(S_j, T_j) = (S_k, T_k).$$

4. Method according to Claims 1, 2 or 3, wherein the consistency check of each relation of said second subset of analytical redundancy relations (I-ARR) is performed by checking the consistency of the results of the primary relations involved in the relation, expressed in implicit form.

5. Method according to any of the previous claims, comprising the operation of deriving the fault signature matrix for a single-fault theoretical condition, starting from the complete set of analytical redundancy relations generated in implicit form, to analyze the fault detection and isolation properties of the system and determine its ambiguity sets.

6. Method for the diagnosis of a system including a plurality of sensors observation variables representing operation conditions, said diagnosis being based on a system model describing the configuration of the system components and including a set of primary relations between inputs and outputs of each component, representing the corresponding operational function, said method including:

- the system simulation based on said

model;

- the detection of system faults by comparison between the values expected from the simulation and the observed values of the system observation variables;

- the generation of at least one conflicts set including a subset of system components for which the assumption of correct operation is not consistent with the observed system behaviour; and

- the determination of the minimum number of components involved in the generation of conflicts between the expected system behaviour and the observed one, i.e. the intersection of all the generated conflicts;

characterized in that the generation of the conflicts set is carried out by a method according to any of the claims 1 to 5.

7. Diagnostic system, including a processing assembly programmed to execute a method for generating a conflicts set and to diagnose a system describable by a model, according to any of claims 1 to 6.

8. Computer program or set of programs, executable by a processor, including one or more code modules to implement a method for generating a con-

flicts set and the diagnosis of a system describable by a model, according to any of claims 1 to 6.

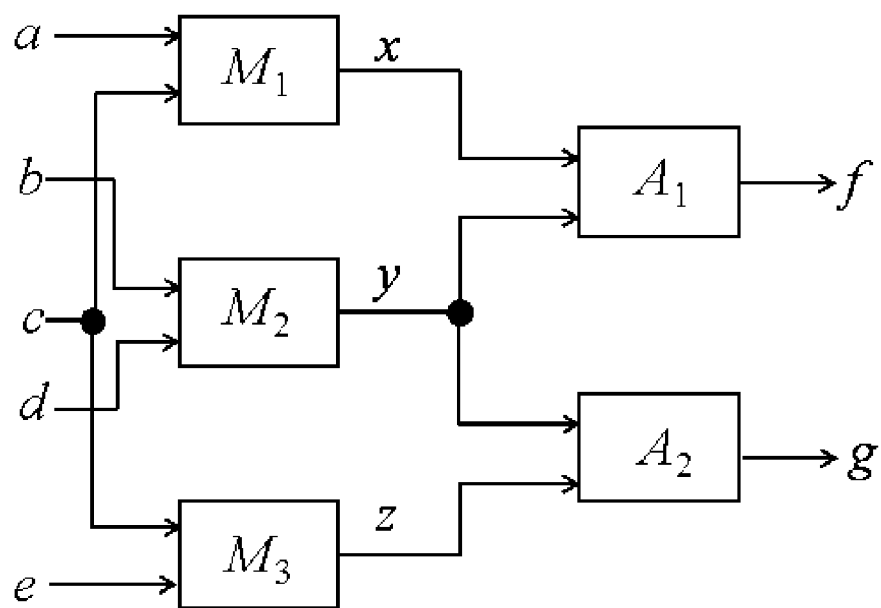


Fig. 1

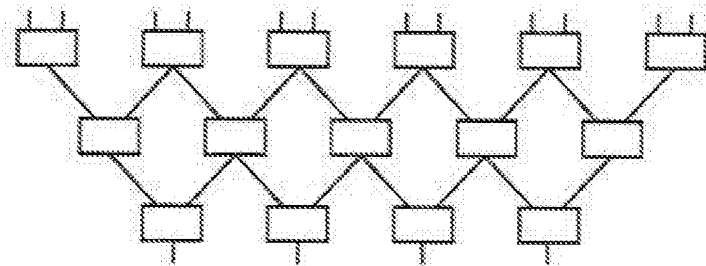


Fig. 2a

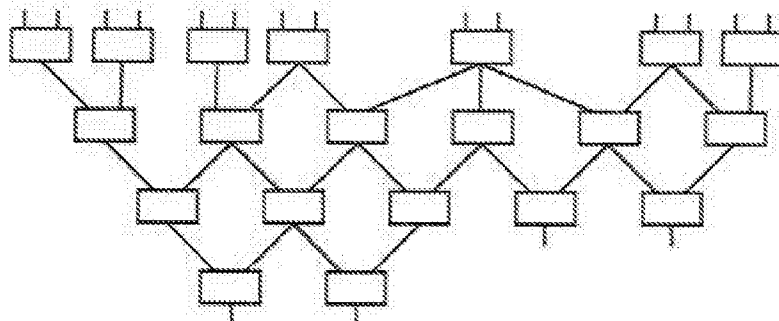


Fig. 2b