4M－7　階層化マトリクス型状態遷移図を用いた、組込型ソフトウェアの動的仕様記述方法の提案

小野綾子†　村田智洋†
†（株）日立製作所　システム開発研究所

１．はじめに

近年、コンピュータシステムの利用の拡大に伴い、高信頼、無停止システムへの要求が強まっている。ハードウェアの信頼性は２重化等で実現されるが、難しいのはシステム組込型の制御ソフトウェアにおいて、複雑なシステム状態の制御を正しく設計することである。

これに対して、階層化マトリクス型状態遷移図を用いた、システム状態遷移制御仕様記述方法を提案した。本論文では、階層化マトリクス型状態遷移図を用いた仕様記述方法とその作成手順について述べる。

２．システム状態遷移仕様記述の問題点

システム状態遷移を制御するソフトウェアは、システム外部、および内部からの刺激に常に対応し、イベントドリブンに動作する、リアクティブシステムの一つである。

このリアクティブシステムの高信頼設計のためには、設計の上流で、制御ソフトウェアが把握すべきシステム状態を全て洗いだし、それらの間の状態遷移を構造化して整理することが必要である。

一般にシステム状態は、並列動作する複数の要素（状態機械と見なせる）の組合せで表される。従ってシステム状態遷移は、それらの要素状態遷移を合成したものになる。

従来のシステム状態遷移記述方法で合成状態遷移を記述するには、図１に示すように、要素状態遷移の状態値の直積で合成状態値を記述し、それらの間の遷移をアークで表すフラットな記述と成る。しかし、フラットな状態遷移図の記述では、状態数が増えると状態遷移記述が組合せ的に複雑になり、仕様の理解が困難になる。

state chart（図２）[1]では、並列動作する要素の状態遷移をそのまま並べて記述する。一般に並行に動作する要素の状態遷移間には何らかの相互制約（インタラクション）があるが、state chart ではそれらをイベントのブロードキャストとしてインプリミットにしか表現できない。このため、それらの制約のもとでの要素状態の組合せとして、どのような状態遷移が存在するかを陽に表現できない。

さらに、state chartの記述では、状態のグルーピングの記述ができるが、論理階層に基づいて状態機械を抽象化し、マルチレイヤ化した状態機械の仕様を表現するのが難しい。

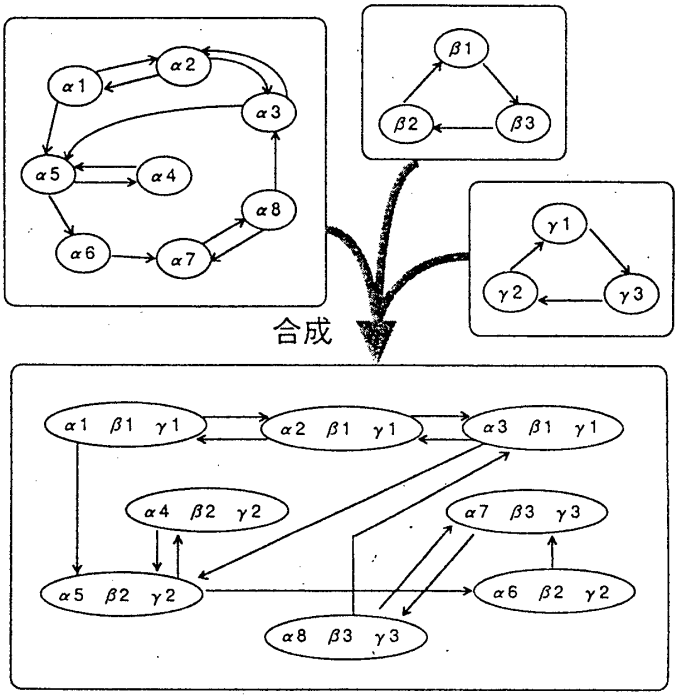

図1　従来方法による合成状態遷移の記述例

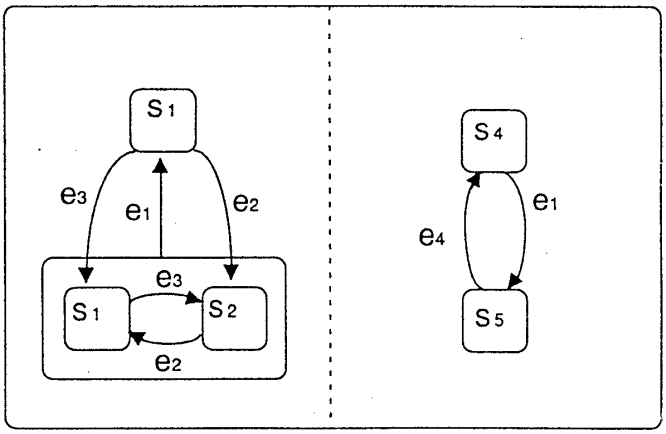

図２　ステートチャート

Description Method for Behavioral Specifications of Embedded Software usig Hierarchical State Diagram Matrix
Ayako ONO, Tomohiro MURATA, Systems Development Laboratry, HITACHI, Ltd.
1099 Ohzenji Asao, Kawasaki, 215 JAPAN

３．マトリクス型状態遷移図を用いた動的仕様記述による問題解決

上記問題点を図３の階層化マトリクス型状態遷移図HSDM（Hierarchical State Daigram Matrix）の記述方法を導入することにより解決した。

（１）マトリクスにより構造化された記述

マトリクスの縦横軸に２つの状態遷移の要素状態を割当て、縦横軸の交わりの領域（ドメイン）内に残りの１つの状態遷移の要素状態を表す。状態値の配置位置によって、その状態値が並行動作する３つの状態遷移のどんな状態値の組合せで定義されているのか明らかにできる。縦ドメイン内の表示にN^2チャート[2]の記述を用い、横ドメイン間の遷移をバスにまとめる。これにより、見やすい遷移の表示ができる。４個以上のコンポーネントの合成は、まず３個の要素状態遷移を合成し、合成したものを新たなの要素状態として、階層的に合成を繰り返すことにより実現する。

（２）インタラクションの表現

並行動作する状態遷移を合成する際のインタラクションとは、以下の３点である。

（ａ）状態制約：ある要素状態がこの状態値ならば、他の要素状態のこの状態値は取りえない。

（ｂ）遷移制約：ある要素状態のこの状態値ならば他の要素状態のこの状態遷移は起こらない。

（ｃ）遷移のアトミック化：ある要素状態の遷移と、他の要素状態の遷移の起こる順序は関係なく、どちらか一方の遷移だけが起こったときに取る中間状態は無視することができる。

以上のインタラクションを考慮して合成して仕様上の不要な状態遷移を除くことができる。

（３）状態の抽象化、階層化

合成したHSDMを新たなコンポーネントの状態遷移とみなして、１階層上位の状態遷移を合成する際に、状態値数が組合せ的に増加するのを防ぐために、各コンポーネントに対応するHSDM上のいくつかの状態値をまとめて、一つの状態値とするのが抽象化である。

４．階層化マトリクス型状態遷移図を用いた組込型ソフトウェアの動的仕様記述方法

仕様記述手順は、以下の６ステップからなる。

Step1：HSDMの合成の仕様を示すHSDMの階層ネットワーク構造を定義する

Step2：各ノードの状態遷移仕様を定義する

Step3：合成のための制約を定義する

Step4：HSDMを生成する

Step5：HSDM上の状態遷移を抽象化する

Step2～5を繰り返す

Step6：定義した状態遷移を実行形式に変換する

５．磁気ディスク制御装置の組込型ソフトウェア設計への適用例

本方法を、磁気ディスク制御装置の組込型ソフトウェアの構成制御機能の設計に適用した。

階層的に構造化されたHSDMで、並行動作するコンポーネント間の状態遷移の相互関係をビジュアルに表現することができた。このため、仕様ミス等の検出が容易になり、信頼性の向上にも効果が見られた。

６．おわりに

HSDMによる組込型ソフトウェアの動的仕様記述方法と、その作成手順を提案した。これを磁気ディスク制御装置に適用し、効果を確認した。

現在、各コンポーネントの状態遷移仕様をオブジェクト的に定義し、自動合成するための支援ツールを開発中である。

７．参考文献

［１］D.Harel:Statecharts:a Visual Formalism for Complex Systems,Science of Computer Programming 8 231-274, North-Holland(1987)

［２］R.J.Late:The N^2 Chart,TRW Software Series,TRW-SS-77-04,November 1977,TRW Defense and Space Systems Group,Redondo Beach,Calif.

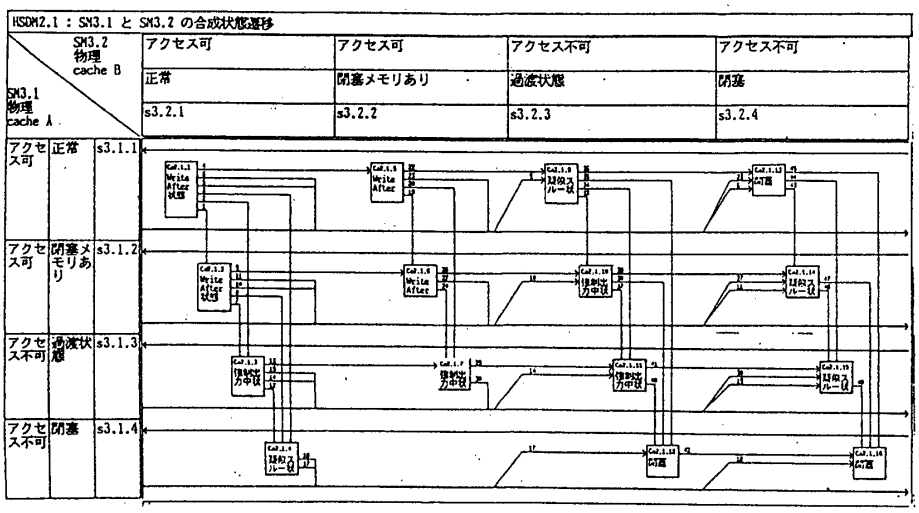

図3　HSDM記述例