

新

組み込みソフトへの 数理的アプローチ

～形式仕様記述をどのように使うか～

第6回

原因結果グラフ

—原因と結果の関係を木構造で表現する

藤倉 俊幸

はじめに

● 原因と結果の関係をグラフで表現する

前回(2009年5月号, pp169-175), AND-OR木を形式化する方法を説明した。今回はこの続きで, AND-OR木の一種である原因結果グラフ(cause-effect graph; CEG)の形式化を説明する。

原因結果グラフはテスト分野で以前から使われている実績のある手法である。実際に現場で使われているため, いろいろな流儀が生まれてきた。ここで説明するのもそんな派生の一つである。だから, 原因結果グラフをAND-OR木の一種と言い切ってよいかどうかはたぶん意見が分かれるだろう。単なる論理式を作る手段と言った方がよい場合もあるし, 論理式を意識していない場合もある。

原因結果グラフはテスト・ケースを設計するだけでなく, 仕様のあいまいさや矛盾を発見することもできる。この意味では, 形式仕様記述と言える。しかも, 述語論理などの難しい道具を使わずに命題論理だけで扱える優れものである。命題論理は, 形式化することが難しい文章を形式化せずにそのまま命題としてしまえば使える。ただし, 真偽が確定する文章を切り出して命題としなければならない。あるいは真偽を知りたいことを命題とする。そして, 切り出した命題間の関係をAND, OR, NOTで記述して, 全体としての整合性を確認する。原因結果グラフと命題論

理の合わせ技で, いわゆるセミフォーマルな手段として利用しようというのが今回のもくろみである。

● 真理表を使う方法もある

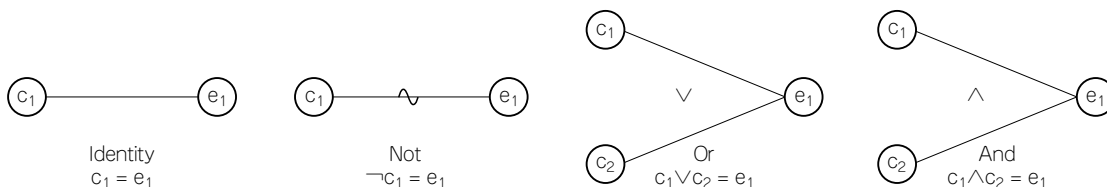
従来の原因結果グラフの利用の仕方は, 命題間の関係を記述しても最後の解釈のところに人手が掛かりすぎて, そこにあまいさが入る, 手間が掛かる, 間違ふ, 難しいなどの壁があったように思う。そのまま真理表を使えば見通しがよくなる部分がある。テストの分野では, 原因結果グラフから作る真理表のサブセットをデジジョン・テーブルと呼んでいる。これはマイヤーズ氏が1970年代に書いた本⁽¹⁾に解説されている。

マイヤーズ氏のアプローチを形式仕様記述と考えれば, VDMなどよりも早くから仕様を論理的に扱おうとしている。仕様書の形式化の手順などは非常に参考になる。そのためテスト設計だけでなく, ソフトウェア開発の上流部分でも利用価値の高いものだし, 上流工程において仕様分析とテスト設計を同時に行うという意味でも興味深い。

1 原因結果グラフ

● 原因結果グラフの表記法

原因結果グラフは, 原因と結果の間の論理的な関係をグラフで表現したものである。原因とは, 仕様書などに含まれる入力条件や入力データ, システムの動作を引き起こす



= は論理記号の \Leftrightarrow の意味で使っている。しかし, Identity以外は \Rightarrow と解釈した方がよい場合もある。形式化しようとする仕様に依存する

図1 原因結果グラフの基本記号