

# MENDELS ZONE

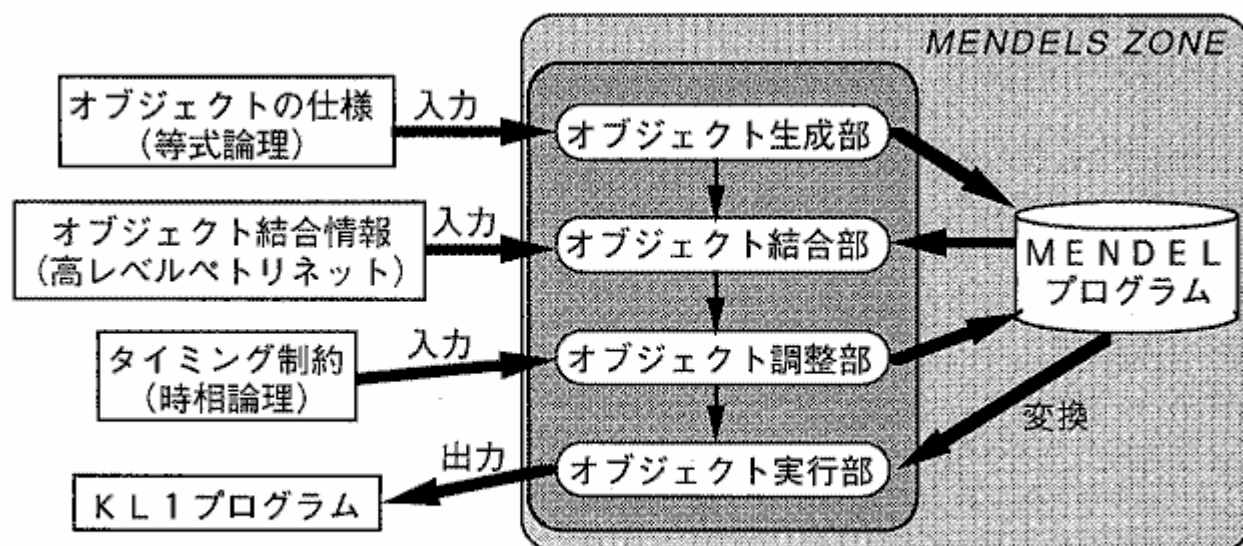
## 並列プログラム開発支援システム

### 概 要

MENDELS ZONE は並列プログラムの開発を支援するシステムである。MENDEL オブジェクトの仕様と、オブジェクト間のタイミングに関する制約を入力すると、定理の自動証明法によってそれらの正しさが検証され、正しい KL1 プログラムが自動生成される。

### 特 徴

- オブジェクト生成: 等式論理によって記述されたオブジェクトの仕様が、項書換え技法によって並列に自動検証される。正しさの確認された仕様からは、オブジェクトのプログラム (MENDEL プログラム) が自動生成される。
- オブジェクト結合: 高レベルペトリネットによって表現されたオブジェクトを、ユーザが結合する。
- オブジェクト調整: タイミングに関する制約を時相論理によって記述する。ペトリネットで表されたオブジェクトがその仕様を満たさない場合は、定理証明手法により仕様を満たすように自動的に調整される。



MENDELS ZONE の構成

## 概 要

今後、分散処理システムや並列システムの形態によるアプリケーションの増加が予想されるが、並列プログラムのデバッグやテストには多大な労力を要する。そのため、高信頼性の保証されたプログラムを生成するための手段の確立が必要となる。MENDELS ZONE は、この手段の確立を目指した並列プログラム開発支援システムであり、種々の形式的手法によって正しい並列プログラムの生成を支援する。

## 本 論

### アプローチ

MENDEL は、ペトリネットをベースとした KL1 の拡張言語であり、KL1 に変換され Multi-PSI 上で実行される。そのプログラムは、互いに同期を取りながら並列に動作する複数の“オブジェクト”から構成される。MENDELS ZONE は、MENDEL の知的プログラミング開発支援システムであり、数学的枠組に基づいた形式的手法の実装を特徴とする。

従来より、信頼性の高いプログラム開発における形式的手法の有効性が知られているが、実用化にあたっては次のような問題があった。

1. 単一の形式的手法によるシステム全体の記述は困難である。
2. 仕様の記述量が増えると、形式的記述の理解性が低下する。
3. 大規模なシステムの記述に不向きである。
4. 仕様の検証やプログラムの生成に多くの時間を要する。

MENDELS ZONE では、オブジェクトの機能を等式論理に基づく代数仕様で、オブジェクトの動作タイミング仕様を時相論理で記述することにより、(1) の問題を解決している。また(2)に対しては、形式的手法で記述された仕様の理解性を高め、かつ記述量を減らすために、ペトリネットなどの図形仕様が併用されている。そして、その理解性とモジュラリティの高さから、オブジェクトの部品化再利用が可能となり、これにより大規模なシステム開発が可能となる。仕様の検証やプログラムの生成には、等式論理、時相論理の定理証明系を利用している。これらの定理証明系は、並列実行により処理時間が短縮されており、(4) の問題の改善が図られている。

以上のアプローチに従い、MENDELS ZONE は形式的手法を実装した。その結果、仕様の正しさの検証や仕様からプログラムへの自動変換が可能になり、信頼性の高いプログラムが生成される。

システムの概要

MENDELS ZONE 上の開発は、オブジェクトを生成する“代数仕様フェーズ”とオブジェクトを結合する“ペトリネットフェーズ”に分けられる。

図1に代数仕様フェーズの画面イメージを示す。

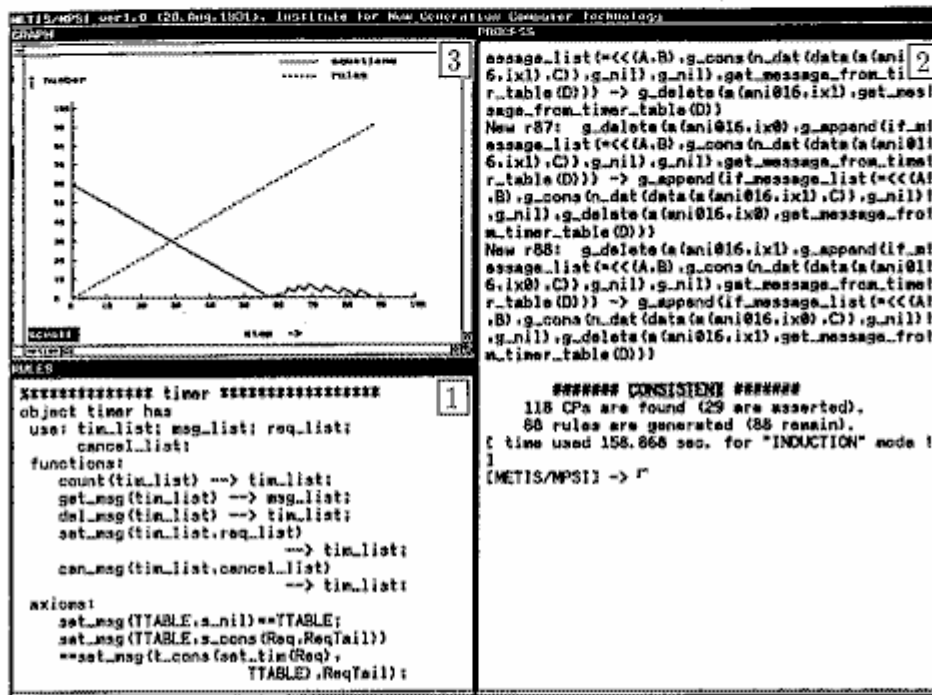


図1

ユーザは、オブジェクトの機能(メソッド)を代数的仕様記述で与える<sup>1</sup>。正しい仕様を記述するために、MENDELS ZONE は、仕様の文法チェック、項書換えとしての直接実行、潜在帰納法による検証などの支援を行なう。ユーザは、<sup>2</sup>より仕様の満たすべき検証項目を入力すると、MENDELS ZONE は仕様がその検証項目を満たしているかどうかを自動検証し、<sup>3</sup>で検証手続きの進行状況が確認できる。正しさが確認されたら、MENDEL オブジェクトへ自動変換を行なう。

図2にペトリネットフェーズの画面イメージを示す。自動変換で生成されたオブジェクトは、<sup>4</sup>の部品ライブラリに登録される。オブジェクトの結合は高レベルペトリネットで表現することができ、その記述は<sup>5</sup>のペトリネットエディタでマウス操作のみで行なえる。

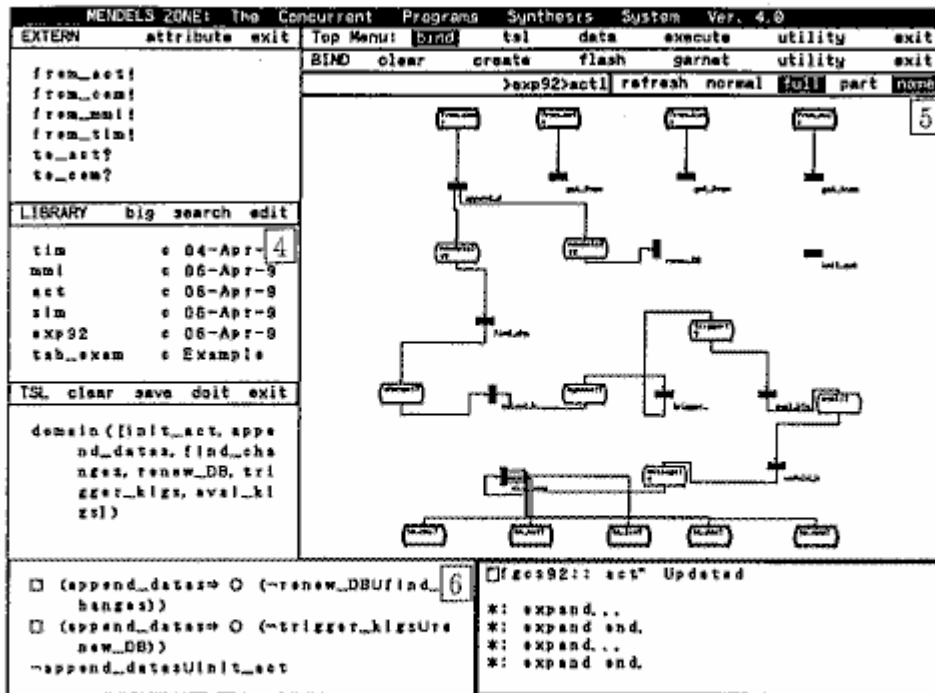


図 2

多くの場合、オブジェクト内のメソッド間、あるいはオブジェクト間には、その起動順序に何らかの制約を必要とする。このとき、ユーザは [6] にその順序制約を時相論理で記述する。MENDELS ZONE は、定理証明手続きタプロー法を用いて、その制約を満たすようにペトリネットの自動調整を行なう。ここでいう調整とは、プログラム制御用のアービターの生成を意味する。完成した MENDEL プログラムは、KL1 プログラムにコンパイルされる。生成された KL1 プログラムの実行は、MENDELS ZONE でグラフィカルにモニタできる。

### 成果

並列システム開発での MENDELS ZONE の有用性を評価するため、発電所制御エキスパートシステムの開発を行なった。このシステムは、先に直接 KL1 で開発されており、今回はそれと同機能のシステムを MENDELS ZONE 上で開発した。これにより、MENDELS ZONE によって実システムが充分構築できることが確認された。また両者を比較すると、MENDELS ZONE による開発ではコーディングに時間がかかるもののデバッグ時間はかなり短縮された。このことは、形式的手法による検証機能の有用性を示している。

### デモ概要

デモでは、MENDELS ZONE の機能を、発電所制御エキスパートシステムの開発例を用いて説明する。あわせて、この開発事例を基にした MENDELS ZONE の評価を示す。