4X-5

代数的仕様の作成・検証・実現支援システムにおける公理解析部の生成

森田　光秋[+]　東野　輝夫[++]　谷口　健一[+]

+ 大阪大学　基礎工学部　++ 大阪大学　情報処理教育センター

1．はじめに

プログラムの仕様を形式的に記述する一つの方法として、代数的仕様記述法がある。代数的仕様記述の意味は、合同関係を用いて簡明に定義される。代数的手法を用いて、プログラムを設計・開発する場合、まず与えられた自然語による要求仕様を分析・整理し、基本的な概念・機能を抽出し、抽象度の高い代数的仕様を作成し、順次、より具体的な（抽象度の低い）仕様に変換し、最終的に計算機で実行可能なプログラムのレベルまで段階的に変換（詳細化）するという手法が用いられる。また、別に指定された性質を満たすかの検証（正当性の検証）や、記述の段階的な詳細化の過程において、下位のレベルの記述が上位のレベルの記述の正しい詳細化になっているかの形式的な検証ができれば望ましい。

2．支援システム

筆者らの研究グループでは、仕様記述言語として、我々のグループで設計した代数的言語ＡＳＬ／＊[1] を採用している。ＡＳＬ／＊における記述（テキスト）ｔは、一つの文脈自由文法Ｇと条件付公理の集合ＡＸからなり（以下、ｔ＝＜Ｇ，ＡＸ＞で表す）、Ｇによって表現式集合E_Gを定め、ＡＸによってE_G上の合同関係を指定する。ＡＳＬ／＊では、表現式集合を定める文法Ｇを書き手が指定できること、及び、公理のスタイルに制約を置いていないことから、各抽象化レベルで比較的自由に記述が行える。

ＡＳＬ／＊によって仕様を記述し、計算機上で実行可能なプログラムに変換していく場合、次のような機能を持った支援システムがあれば、有効である。

(1) 仕様作成支援機能
仕様を簡便に書くために導入した省略記法やマクロ記法の処理、各公理中の表現式が文脈自由文法から生成されるかどうかのチェック及び内部表現への変換、文法や公理をデータベース化して置く機能等

(2) 詳細化支援機能
書き手が段階的に仕様を詳細化していく（例えばより具体的なデータ構造を用いて抽象的なデータ構造や演算を実現する）のを支援する機能

(3) 検証支援機能
与えられた記述の上で別に指定された性質が成り立つかどうかの検証や詳細化が正しいかどうかの検証を支援する機能

(4) 実行機能
項書き換え系、抽象的順序機械モデル、関数型言語など、実際の計算機上で実行可能な、ＡＳＬ／＊の部分言語に対するインタプリタやコンパイラ

筆者らの研究グループでは、従来ＡＳＬ／＊の部分言語ＡＳＬ／Ｖ（prefix表現のみを許し、公理の右辺に表れる変数は左辺にも表れなければならない）に対する検証支援系を作成し、いくつかの検証作業を進めてきたが[2]、公理のスタイルに制約があることや、述語論理は扱えないなどの不便な点があった。また、直接実行可能な言語として、関数型言語ＡＳＬ／Ｆ[3] に対するコンパイラを作成しているが、検証支援系とＯＳが異なるため、同一計算機上で利用できない。このため、今回上述の(1)～(4)のような機能を持つ統合的な支援システムを作成することにした（図１）。

以下、ＡＳＬ／＊の構文ならびに、(1) の仕様作成支援機能の概略について述べる。

Albebraic Specification Language ASL/M and Its Parser

Mitsuaki MORITA, Teruo HIGASHINO, Kenichi TANIGUCHI

Osaka University

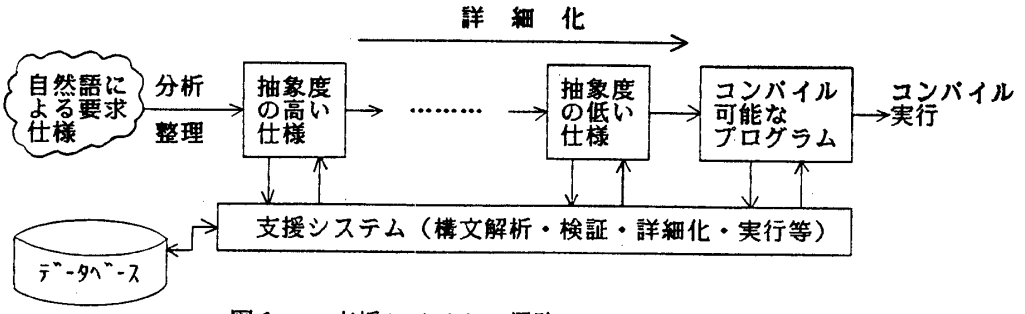

図1　　支援システムの概略

3．マクロ記法・省略記法

ＡＳＬ／＊の文法や条件付き公理の具体的な構文を定めたのが言語ＡＳＬ／１である。しかし、ＡＳＬ／１は文法や公理の構文を定めただけであるので、多くの仕様で共通して用いられる基本演算や、似通った文などを毎回書かなければならないなど実用的でない部分がある。そこで、マクロ記法や省略記法を備えた言語ＡＳＬ／Ｍを定義する。ＡＳＬ／Ｍテキストの意味は“そのテキストがどのようなＡＳＬ／１テキストを表すか”で定義する。ＡＳＬ／Ｍのマクロ記法・省略記法の主なものとしては以下のようなものがある。

・テキスト中の範囲を指定して検索や参照を可能にする機能。
・あらかじめ用意された別のテキスト中の指定された範囲を引用（コピー）する機能。
・テキストの引用をパラメータ付きで行う機能。
・指定した範囲において文字列の置換を行う機能。
・似通った文字列の置換を繰り返しを用いて行う機能。
・重複している記述の省略や、文脈から判断可能な省略を補う機能。

これらの機能を、適当な基本操作（例えば挿入、置換、範囲の指定等）を定義し、それらの複合演算として、形式的に定義する（例えば代数的方法で）ことを検討している。

4．仕様作成支援機能の概略

この支援部では、入力であるＡＳＬ／Ｍテキストに対して、まず省略表現を補い、マクロ表現されている部分を展開する。テキストは、この時点でＡＳＬ／１テキストに相当する。次に各条件付き公理に対してその表現式が文法Ｇの生成する表現式かどうかをチェックする。文法Ｇはあいまいである可能性もあり、そのときは複数個存在する構文木のうち、どの構文木を採用するかについて書き手が選択できるようにする。構文解析終了後、各条件付き公理は、木構造の内部表現に変換される。このとき、項書き換えの高速化を図るために付ける同一演算子間のポインタなどの、付加的な情報も付け加えられる。この内部表現が、検証支援機能やその他のツールへの入力として用いられる。

5．おわりに

このシステムはＵＮＩＸ上で稼働するようにし、検証など大量の計算時間を要する機能についてはＵＮＩＸから高速の大型計算機を利用できるように構成する。

日頃御指導・御討論頂く嵩忠雄教授はじめ研究グループの諸氏に感謝する。

文　　献

(1) 嵩、谷口、杉山、関：“代数的言語ＡＳＬ／＊－意味定義を中心に－”，信学論(D),J69-D,7,pp.1066-1073(昭61-07).
(2) 東野、工藤、縄田、杉山、谷口：“代数的仕様検証支援系及びそれを用いた検証例”，信学論(D),J67-D,4,pp.472-479(昭59-04).
(3) 井上、関、谷口、嵩：“関数型言語ＡＳＬ／Ｆとその最適化コンパイラ”，信学論(D),J67-D,4,pp.458-465(昭59-04).