等式論理系における制約解消による証明支援環境構築の試み*

5X－2

井上 直§　石黒正揮◇　中川中§
情報処理振興事業協会 (IPA) §† 三菱総合研究所 ◇‡
e-mail: now@stc.ipa.go.jp, masa@mri.co.jp, nakagawa@sra.co.jp

1 はじめに

等式論理を基盤とする仕様記述言語では、仕様は項書換え系による操作的意味を持つため簡約手続きによる実行が可能であり、この実行機構を通して仕様の検証が行なわれる。私達は形式的記述 (仕様および検証記述) に自然言語等による説明を加えた拡張されたHTML: Forsdonnet (Formal specification document on network)[3] の文章を対象とし、形式的記述間の制約の記述と, 簡約手続き, 帰納的証明等の実行機能による制約解消を繰り返すことで, ユーザが対話的に仕様の検証を行う環境を構築した。以下でその説明を行う。

2 等式論理における証明

ここでは等式論理を基盤とする仕様記述言語としてCafeOBJ[2] で説明する。CafeOBJ で自然数の仕様を記述すると例えば以下のようになる。

```
mod! NAT { [ Nat ]
  op 0 : -> Nat
  op s : Nat -> Nat
  op _+_ : Nat Nat -> Nat
  vars N M : Nat
  eq N + 0 = N .
  eq N + s(M) = s(N + M) .
}
```

この仕様において次の定理

```
vars N M : Nat
eq N + M = M + N .
```

が成り立つ事の証明は、帰納法を用いて

```
eq [Base Step] M + 0 = 0 + M
eq [Ind. Step] M + s(N) = s(N) + M
```

を示すことでできる。

* A proof assistant system for equational logic based on constraint solving : Tadashi Inoue, Masaki Ishiguro, Ataru T. Nakagawa
†Infomation-technology Promotion Agency, Japan
‡Mitsubishi Research Institute, Inc.

3 Forsdonnet での証明記述

上記の例のような証明では、帰納法で示すべき等式の両辺を CafeOBJ の処理系で実行し、両辺の項が等しくなる事を確かめる必要がある。このような証明を記述する場合には、証明記述の途中で制約解消の支援が自然に行えると便利である。

このような制約解消支援を得るために Forsdonnet では<TARGET>,<CONSTRAINT>タグが存在する。簡単に役割を説明すると、<TARGET>,</TARGET>タグで囲まれた部分は制約を表し、<CONSTRAINT>タグのパラメータで解消すべき制約を指定する。そして制約解消のコマンドを実行する事で<CONSTRAINT>,</CONSTRAINT> タグで囲まれた部分に制約解消された結果が表示される。上記の例の M + 0 = 0 + M を示す場合は、<TARGET>タグで囲まれた部分が制約で、コマンドの実行で結果が<CONSTRAINT>タグの内側に表示される。

```
<TARGET NAME=BS>
  reduce M + 0 .
  reduce 0 + M .
</TARGET>
<CONSTRAINT CONTEXT=#NAT TARGET=#BS>
<CONSTRAINT>
```

4 証明編集支援環境

多言語エディタ Mule 上のパッケージ w3 を拡張してこのような証明作成支援環境が実現されている。現在この支援環境では主に次のような機能を持つ。

- Forsdonnet 文章のブラウズと編集
- <CONSTRAINT>タグの制約解消
- <MODULE>,<TARGET>等のタグ入力の補間
- ネットワーク上のリソースの参照

以下各機能について説明する。

4.1 Forsdonnet 文章のブラウズと編集

本環境では Forsdonnet 文章をブラウズした画面上で自由に文章の編集を行うという Netscape Navigator

gold と同様な事が出来る。ただしここで問題になるのはタグの編集である。Forsdonnet 固有のタグは HTML のタグと異なり、文章のレイアウト情報を記述した物ではない事もあり、本環境においては Forsdonnet 文章は<MODULE>,<TARGET>などの Forsdonnt タグを ¦、[のような2バイト文字で置き換えて表示される。

表示された ¦、[文字には Mule のテキスト属性機能によりタグのパラメター情報が保存されている。そのため、ブラウズした画面上で ¦、[などの文字での表示と<MODULE ...>,<TARGET ...>の表示の切替えができ、タグの編集を自由に行う事が出来る。

図 1: Forsdonnet 文章の表示例

4.2 <CONSTRAINT>タグの制約解消

<CONSTRAINT>タグで囲まれた部分の制約解消はユーザーがコマンドを実行する事で行われる。コマンドの実行はタグ上にカーソルを合わせて Ctrl-c,Ctrl-s とタイプする事で行われる。

制約解消の際には逐一外部の管理サーバ [5] を通して外部の証明エンジンを呼び出し、制約解消を対話的に実行する。

4.3 <MODULE>等のタグ入力の補間

Forsdonnet のタグは HTML タグに比べて複雑で入力する際に誤りを引き起こしやすい。よって本環境ではタグ入力の補間をサポートしている。また CafeOBJ スタイルで記述されたモジュールを Forsdonnet スタイルにするために自動的に <MODULE> タグを付け加える機能もある。

4.4 ネットワーク上のリソースの参照

CafeOBJ のモジュールでは外部で定義されたモジュールを輸入する事が許されている。そのため Forsdonnet 文章ではネットワーク上のファイルで定義されたモジュールの参照がサポートされている。その指定は以下のように、HTML の <A>タグに似た <MODREF> タグで行う。

```
<MODREF CONTEXT=fors://www.somewhere/a.fdn>
```

この<MODREF>タグは Forsdonnet リポジトリサーバ [4] 上の Forsdonnet 文章を HTML の<A>タグと同様の機能を持ち、証明の際にはモジュール間の関係を示す役割を持つ。

5 今後の課題

現在の支援環境はとりあえず必要と思われる機能が実装されている。実際に使用されれば、まだ新たな機能が必要になると思われる。

参考文献

[1] Nakagawa, A.T., "*Manipulating CafeOBJ on Networks*", in *Preprint for 12th Workshop on Algebraic Development Techniques*, Tarquinia, June 1997

[2] Nakagawa, A.T., Sawada, T., and Futatsugi, K. *CafeOBJ Manual*, SRA, 1997; available at `ftp://www.sra.co.jp/pub/lang/CafeOBJ/Manual/manual.ps`

[3] 瀬尾 明志, 中川中, "等式論理系における制約解消による証明記述の枠組", 情報処理学会第 55 回全国大会

[4] 山田 勉, 松島 英子, "HORB を用いた仕様記述文書の管理機構の構築", 情報処理学会第 55 回全国大会

[5] 石曽根 信, 澤田 寿実, "定理証明システムのための統合サーバの作成", 情報処理学会第 55 回全国大会