

シストリックアレーによる回路設計の正しさの一証明法

1 K-2

竹中 崇 北道 淳司 西川 清史 谷口 健一

大阪大学 基礎工学部 情報工学科

1 まえがき

シストリックアレーの設計においては、シストリックアルゴリズムからの合成に関する研究が行われているが、そのアルゴリズム自体やアレーの構造が要求仕様を満たすことの検証に関する研究は少ない。文献[1]においては、時相論理を用いてシストリックアレーの正しさの検証に関する報告を行っているが、検証の自動化については行われていない。

本稿では、シストリックアレーの正しさを、ある制約された整数上の論理式の恒真性判定アルゴリズム[2]を利用して、自動的に証明する方法を提案し、いくつかの例題に適用した結果について報告する。

2 シストリックアレーの仕様と実現の記述

仕様および実現はプレスブルガー文の一つのサブクラス(以下P文)で記述する。P文は整数の集合上の変数、定数、整数の加減算、整数同士の比較演算、 \wedge 、 \vee 、 \neg に加えて、関数の出現を許すものとする。出現する変数は冠頭標準形の全称指定子で束縛される。記述の上では全称指定子を省略する。

シストリックアレーの仕様は、時刻を表す整数変数 t (または T)を引数とする関数によって入出力の値を表し、それらの関数間の関係で表される。本稿では、TPCD(2nd Conference on Theorem Proving in Circuit Design)[3]にて採用されたベンチマークの中から、シストリックアレーの設計検証のための例題である2次行列の乗算回路を取り上げることにする。

表1に、回路の仕様の記述例を示す。 a, b, c はそれぞれ $N \times N$ の整数行列とし、 a, b は入力、 c は出力を表す。なお、 $SQ \cdot MUL(a, b, N)$ は、 N 次の正方行列 a, b の積を表す関数であり、 N は回路の大きさ(この例では行列の大きさ)に関するパラメータである。

表1: 行列の乗算をするシストリックアレーの仕様の記述
 $c(T+1) = SQ \cdot MUL(a(T), b(T), N)$

回路の実現は、仕様と実現の入出力の対応、各機能要素の機能、各機能要素間の接続の記述からなる。

仕様では各時間毎に行われる動作が、実現では複数のステップで行われる場合がある。このような場合、仕様と実現において、入出力の対応関係を指定する。

本例では図2のような機能要素を図1に示すようにひし型状に配置したものを用いる。機能要素は3つの入力 $inputA, B, C$ 、3つの出力 $outputA, B, C$ をもつ。それぞれの値を表す関数の引数 x, y は、ひし型の下部頂点を $(0, 0)$ とし、左ななめ上を x 軸、右ななめ上を y 軸とした時の座標 (x, y) の機能要素のものであることを表している。機能は表2(b)で表される。これらを $(2N-1)^2$ 個用いてアレーを構成する。隣接する機能要素の接続関係を図3に示す。これらの関係は表2(c)で表される。

A Formal Verification Method for Systolic arrays.

Takashi TAKENAKA, Junji KITAMICHI,

Seishi NISHIKAWA and Kenichi TANIGUCHI

Department of Information and Computer Sciences,

Faculty of Engineering Science, Osaka University

Toyonaka-shi, Osaka 560 Japan

構成されたアレーに対し、図1のようにレイテンシを設定して入力 a, b を与えると、出力 c が得られる。これらの関係は表2(a)で表される。

表2: 行列の乗算を行うシストリックアレーの実現の記述*

(a) 仕様と実現の入出力の対応
$a(T)[i][j] =$
$inputA(2N-1, N-(i-1)+(j-1),$
$(5N-4)T+2(N-1)+(i-1)+2(j-1))$
$b(T)[i][j] = \dots$
$c(T)[i][j] =$
$if i >= j then$
$outputC(2N-1, 2N-1-(i-j),$
$(5N-4)T+2(N-1)+2N+(i-1)+2(j-1)-1)$
$else$
$outputC(2N-1-(j-1), 2N-1,$
$(5N-4)T+2(N-1)+2N+(j-1)+2(i-1)-1)$
(b) 機能要素の機能
$outputC(x, y, t) = inputC(x, y, t-1)$
$+ Mul(inputA(x, y, t-1), inputB(x, y, t-1))$
\dots
(c) 機能要素間の接続
$inputA(x, y, t) = outputA(x+1, y, t)$
$inputB(x, y, t) = outputB(x, y+1, t)$
$outputC(x, y, t) = inputC(x+1, y+1, t)$
$inputC(1, y, t) = 0 \quad inputC(x, 1, t) = 0$

3 実現の正しさ

実現が仕様を満たしているとは、仕様と実現に対してもう一度同じ入力系列をあたえた時に同じ出力系列が得られるということである。このことは、実現の各式および基本演算・述語のもとで、仕様の各式が定理として成立つということである。

実現が仕様を満たしていることを、表3の手順で証明する。以下では、本例における証明において、式 $P(L+1, T)$ の証明の場合における、帰納法の仮定の選択、追加した補題、補題において変数に代入された値について説明する。

$P(L, T)$ を表4にしめす。 L はアレーの一辺に並べられた機能要素の数である。ひし型状に配置されているシストリックアレーの上部方向への出力 $outputC$ において左側部分($x=L$)と右側部分($y=L$)ではその表記方法が異なるので、 $P(L, T)$ が2つの式より表されている。右側と左側の証明は同様であるので以下では左側について説明する。左側の $P(L, T)$ と $P(L+1, T)$ との間の関係を図4に示す。次に、証明のために追加する補題をしめす。

- 帰納法の仮定 $P(L, T-1)$ を選択した。このとき、 y を $y-1$ に置き換えた $(P'(L, T-1):\alpha)$ 。
- 追加する機能要素群の機能(表5、計6個)の $outputC(L+1, y, t) = \dots$ なる式における t を T に置き換えた式を補題に追加した (β) 。他の式についても同様に t を置き換えて補題に追加した。ただし、この式の正しさは本例と同様帰納法で証明する。

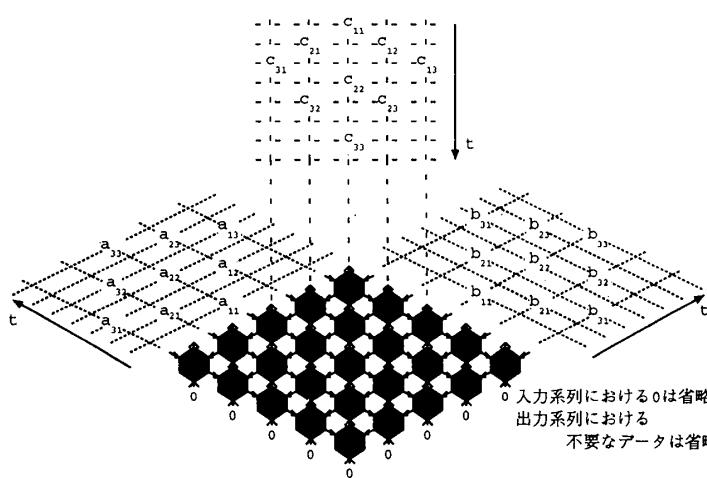


図 1: 仕様と実現の入出力の対応 (N=3 の場合)

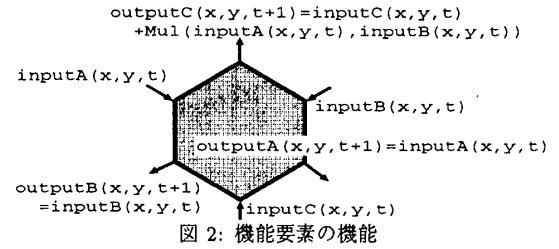


図 2: 機能要素の機能

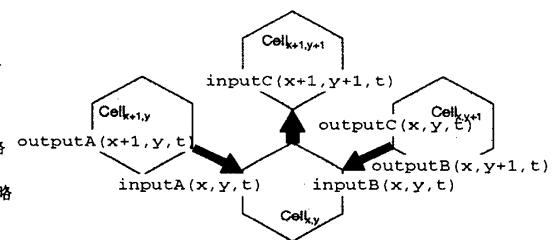


図 3: 機能要素間の接続

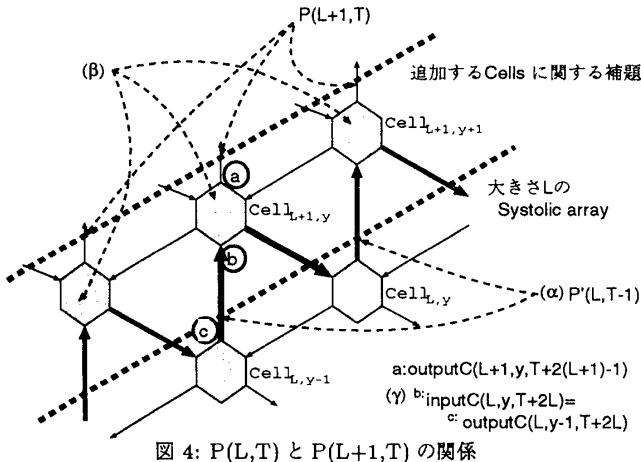


図 4: P(L,T) と P(L+1,T) の関係

- 表 2(c) の inputA,C の式における t を T-1 に, x を L に置き換えた式を補題に追加した (γ)
- 加算を表すマクロ \sum の性質には

$$\sum_{l=0}^m f(l) = \sum_{l=0}^n f(l) + \sum_{l=n+1}^m f(l)$$

$$\sum_{l=m}^m f(l) = f(m)$$
 なる関係がある。この関係における m を y-1 に, n を y-2 に, f(l) を $\text{Mul}(\text{inputA}(L+1, l+1, T-2y+2l+1), \text{inputB}(L-y+1+2, L+1, T-L-y+2l))$ に置き換えた式を補題として追加した。

本方法で, TPCD のベンチマークのうちシストリックアレーに関する一次元(ベクトルの内積を計算する)と二次元(本稿で例として用いた回路)の回路の検証を行った。仕様記述, スキームの考案などに試行錯誤を含み約1週間で行えた。プレスブルガー文恒真性判定ルーチンでの恒真性判定に要した時間は, それぞれ, 0.017秒, 0.14秒(Sony NEWS-5000, 100MIPS, 64MBメモリ使用)であった。

4 あとがき

今後, 検証者が行っている変数の置き換えを自動的に行う方法について考案する予定である。

参考文献

- [1] Ling N. and Bayoumi M.A.: "Systolic Temporal Arithmetic:A New Formalism for Specification and Verification of Systolic Arrays", IEEE Transactions on Computer-Aided Design, Vol.9, No.8, pp.804-820(August 1990).

[2] 森岡澄夫, 東野輝夫, 谷口健一: “全ての変数が存在記号で束縛された冠頭標準形プレスブルガー文の真偽判定プログラム”, 信学技報, SS95-18, pp.63-70(1995).

[3] Thomas Kropf: "Benchmark-Circuits for Hardware-Verification", T. Kropf and R. Kumar (eds.), Vol.901 of LNCS, pp.1-12, Springer Verlag(1995).

表 3: 実現の正しさの検証手順

- 実現の回路の入出力の関係を表した論理式 $P(L, T)$ (L は回路の大きさ, T は時刻を表す)を検証者が考案する。実現の各式および基本演算・述語のもとで, $P(L, T)$ が成り立つことを L 及び T に関する帰納法で証明し, さらに $P(L, T)$ が成り立てば仕様の各式 $Q(L, T)$ が成り立つことをしめす。帰納段階では $P(1, 1) \dots P(L-1, T), P(L, T-1), P(L, T)$ を仮定して用いる。 $P(1, 1), P(L+1, T), P(L, T+1), P(f(N), T) \rightarrow Q(N, T)$ の各式を P 文で記述する(式 A1)($f(N)$ は正整数)。
- 帰納法の仮定は, 実際に証明に必要なもののみを選択し変数に具体的な値を代入して補題として式 A1 に追加する(式 A2)。
- 仕様記述に用いた関数, 述語, 実現の記述, 実現の記述上で成り立つ性質を補題($R(L, T)$)として式 A2 に追加する(式 A3)。その際, 検証者が $R(L, T)$ における変数に具体的な値を代入する。
- 式 A3 をプレスブルガー文恒真性判定ルーチンによりその恒真性を判定する。ただし, 関数はその引数まで含めて変数として扱い, 2つの関数はその引数まで同一である時の同じ変数とみなす。

表 4: 例題で使用したスキーム $P(L, T)$

```

outputC(L, y, T)
=  $\sum_{l=0}^{y-1} \text{Mul}(\text{inputA}(L, l+1, T-2y+2l+1),$ 
   $\text{inputB}(L-y+1+2, L, T-L-y+2l+1))$ 
outputC(x, L, T)
=  $\sum_{l=0}^{x-1} \text{Mul}(\text{inputA}(L, L-x+1+1, T-L-x+2l+1),$ 
   $\text{inputB}(L+1, L, T-2x+2l+1))$ 

```

表 5: 追加する機能要素群の機能

```

outputC(L+1, y, t) = inputC(L+1, y, t-1)
+  $\text{Mul}(\text{inputA}(L+1, y, t-1),$ 
   $\text{inputB}(L+1, L+1, T-(L+1)+y-1))$ 
...

```