研究会推薦論文

帰納法に基づく定理証明器によるシストリックアレイの検証

高橋和子[†,☆] 藤田博[††]

帰納法に基づく定理証明器によるシストリックアレイの検証において，帰納法を効果的に適用するための問題点を指摘しその解決策を示す．2次元シストリックアレイに対し，時刻や回路パラメータを陽に含む式で表される実装記述から入出力信号の関係式を導出する手続きを定式化し，行列の乗算回路に適用する．さらに，時刻や回路パラメータを陽に含まない値の関係式として表現された仕様と，それらの値が入出力ポートで観測されるべきタイミングが与えられたときに，実装記述から導出された入出力信号の関係式が仕様を満たすことを証明する際の技法についても述べる．

Verification of Systolic Arrays Using Induction-based Theorem Provers

KAZUKO TAKAHASHI[†,☆] and HIROSHI FUJITA[††]

This paper describes a verification method for systolic arrays using induction-based theorem provers. We pose the problems concerning effective application of induction and show the solutions. For a two-dimensional systolic array, we formalize the procedure for deriving the relation of input/output signals from the description of an implementation which is given as a time-parameterized formula. The procedure is applied to a systolic array for matrix multiplication. We also describe the techniques to verify that the derived relation satisfies a specification which is given not as the relation between signals, but that of input/output values together with their timing requirements.

1. はじめに

シストリックアレイ[11]は，規則正しく配列された複数のセルが同期的に動作しパイプライン処理を行って，高度の並列性を実現するアーキテクチャである．その検証は従来シミュレーションで行われてきたが，時間やコストがかかるうえ検証もれの問題があった．最近出始めた論理合成ツールもまだ技術的に洗練されたものではないため，シミュレーションに代わる検証技術の開発が望まれている．

一方，ハードウェア検証の分野ではBDD（Binary Decision Diagram）[3]を使った検証手法が有力なものとして近年注目をあびているが，この手法はパラメータを扱うのが苦手であり，特定のサイズに対してしか証明できないという欠点がある．したがって，シストリックアレイのような繰返し構造には，サイズをパラメータとして扱い，帰納法を使って証明する証明器の方が有利な場合が多い．本稿では，そのような証明器の1つとしてNQTHMを使う．

NQTHMは限量記号を含まない等号付き一階述語論理であるBoyer-Moore論理を機械化したBoyer-Moore型証明器[1]の実用向け改良版である．この証明器では基本関数や公理を初期データベースに持ち，ユーザによって定義された関数やすでに証明された補題がデータベースに追加されていく．このデータベースを使って与えられた式を書き換えることによって証明は進行し，trueが導出されると証明は成功して停止する．

我々は文献14)でNQTHMを使った同期順序回路の証明技法として時刻パラメータ関数方式を提案した．

† 三菱電機株式会社先端技術総合研究所
Advanced Technology R&D Center, Mitsubishi Electric Corporation
☆ 現在，ATR音声翻訳通信研究所
Presently with ATR Interpreting Telecommunications Research Laboratories
†† 九州大学大学院システム情報科学研究科
Department of Intelligent Systems, Kyushu University

本論文の内容は1996年11月のプログラミング研究会にて報告され，同研究会主査により情報処理学会論文誌への掲載が推薦された論文である．

同期順序回路の入出力データは，一般に時刻とともに変化する信号列になる．時刻パラメータ関数方式では，入力信号を瞬間的な値で表現し，入力信号も回路もともに時刻をパラメータとする関数として記述する．この方式では新たなデータ構造を導入する必要もなく，入力系列全体を引数として持ち回ることもないので記述，証明とも簡単なものになる[15]．また，この方式は時刻だけでなく回路内の位置もパラメータとして同様に扱うことができるので，シストリックアレイのような繰返し構造を持つ回路の検証にも有効である．帰納法をうまく適用するとNQTHMの能力が活かされるが，式のどの部分に対していつどのような帰納法が適用されるかはシステムが自動的に決定するため，しばしばユーザの意図と異なる部分に帰納法が適用され，その結果証明が複雑になったり失敗したりする．文献18)では，時刻パラメータ関数方式を使って1次元シストリックアレイを検証し，帰納法を適用させる際の問題点を明確にし，その解決策としてどのような中間補題を補えば証明をガイドできるかを示した．

本稿ではこれを2次元シストリックアレイの検証に拡張し，その検証手続きを定式化するとともに行列の乗算への応用を示す．また，文献18)では仕様が時刻や回路のサイズをパラメータとする入出力信号の関係式で与えられたときに，実装が仕様を満たすことを証明していたが，一般に仕様は回路に無関係なデータとそれらが入出力ポートで観測されるタイミングという形で与えられることが多い．この場合，証明すべき式は時刻や回路のサイズだけでなく，仕様に出現する数列や行列の位置を表すパラメータまで含むため，帰納法を適用するにはパラメータの数が多すぎて直接証明をしても失敗する．本稿では，パラメータの数を少なくするため証明を2段階に分ける．まず，中間補題を使って実装から入出力信号の関係式を導出し，得られた関係式をタイミングの要求に基づいて，仕様に出現する値の関係式にマッピングする．次に，それが与えられた仕様を満たすことを証明する．後半では，証明すべき式は時間的な要素を含まない式になっており，仕様に出現する数列や行列の位置を表すパラメータに関する帰納法が適用される．本稿では，後半部分で使った同一数列の異なる部分列の和の等価性を証明する技法を示す．

本稿の構成は以下のとおりである．2章で2次元シストリックアレイの検証方法を示す．3章ではこの方法を行列の乗算問題に応用する．4章で実験結果および考察を述べ，最後に5章で結論を述べる．

2. 2次元シストリックアレイの検証法

2.1 検証の概略

まず，1次元シストリックアレイの検証において仕様が入出力信号の関係で与えられたとき，実装が仕様を満たすことを証明する際に出現した問題点とその解決策を示す[16),18)]．

時刻パラメータ関数方式による検証では，まず単位セルの構成要素の論理関係を直截的に記述する．入力信号は隣のセルの出力信号であり，信号はすべて時刻，位置をパラメータとする関数で表される．この記述が仕様を満たすことを命題として証明すると，帰納法を適用する際以下の問題が生じる．

(1) 入力信号で定義にベースケースが2つあるものがある．

(2) 仕様と実装で帰納カウンタ，すなわち再帰呼び出しのたびに減少していき最後はベースケースにいたる変数の減少の割合が異なる．

これらは，シストリックアレイがループを持つ，すなわちあるセルの出力が将来自分自身の入力に影響を及ぼす構造を持つ場合に特有の問題点である．このようなシストリックアレイでは同一のセルが入力ポートと出力ポートを持つ．

(1)を解決するために，あらかじめ入力信号を表す関数を展開してベースケースを1つにしておく．(2)を解決するために，シストリックアレイ全体の入出力ポートをアレイの終端に位置するセルに関連づけるための新しい関数を導入し，展開/たたみ込み技法でそれを変換して再帰的な定義を得る．この変換を成功させるために，k 個のセルから成るシストリックアレイの $k-1$ 番目のセルの出力と $k-1$ 個のセルから成るシストリックアレイの $k-1$ 番目のセルの出力関係を示す命題を補題として証明する．得られた再帰的な定義は入出力ポートに対応するセルの入出力信号の関係式，すなわち外部からシストリックアレイ全体への入出力信号の関係式に相当する．

2.2 検証法の定式化

1次元の場合の検証結果をもとに，2次元の場合の検証方法を定式化する．**図1** のような $k \times k$ 個のセルから成る2次元6角シストリックアレイを考える．$\langle u, v\rangle$-座標をとり，各セルを座標 $\langle u, v\rangle$ で表す．

データは3方向に流れ，各方向の入力信号を G_1，G_2，G_3（ただし $G_3=0$）とすると，時刻 τ におけるポート $\langle u, v\rangle$ への入力信号は時刻とセルの位置をパラメータとする関数 $G_j(\tau, u, v)$ $(j = 1, 2, 3)$ で表される．

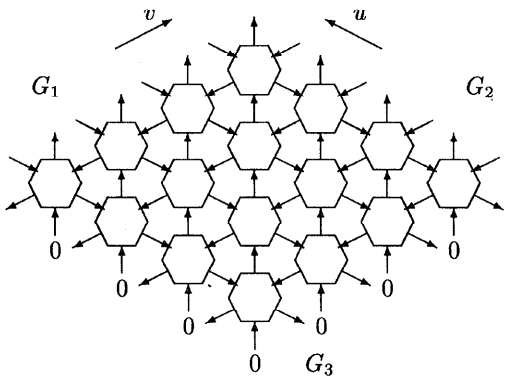


図1 2次元6角シストリックアレイ
Fig. 1 Two-dimensional hexagonal systolic array.

(1) **単位セルの直截的な記述**

$x_j(u,v,\tau,k)$ を時刻 τ におけるセル $\langle u,v\rangle$ の G_j と同方向の出力信号とする．セル $\langle u,v\rangle$ の構成要素の論理関係を記述する．

$$x_j(u,v,\tau,k) = \begin{cases} 0 \ (\tau < \beta_j \text{ or } \tau-\beta_j < k-u \text{ or} \\ \quad \tau-\beta_j < k-v \text{ or } u=0 \text{ or} \\ \quad u>k \text{ or } v=0 \text{ or } v>k \text{ or } k=0) \\ G_j(\tau,u,v) \ (else, u=k+1 \text{ or } v=k+1) \\ \mathcal{C}_j[\, x_1(u+1,v,\tau-\beta_1,k), \\ \quad x_2(u,v+1,\tau-\beta_2,k), \\ \quad x_3(u-1,v-1,\tau-\beta_3,k), E(u,v)\,] \\ \qquad\qquad (\text{otherwise}) \end{cases}$$

ここで，$\mathcal{C}_j$ は単位セルの行う計算に対応する関数，β_j は信号 G_j が単位セル内で通過するレジスタの数，$E(u,v)$ は時間に依存しない要素である．パラメータが定義領域を越える場合や，まだ入力値が入ってこない時刻における出力信号は0である．また，入力ポートにあたるセル $\langle k,v\rangle$, $\langle u,k\rangle$ の入力は外部入力 G_j になるが，この定義では仮想セル $\langle k+1,v\rangle$, $\langle u,k+1\rangle$ の出力を G_j と定義し，入力はあくまでも隣接セルからの出力としている．

(2) **展開**

$\mathcal{C}_j[x_1(u+1,v,\tau-\beta_1,k), x_2(u,v+1,\tau-\beta_2,k), x_3(u-1,v-1,\tau-\beta_3,k), E(u,v)\,]$ に出現する x_1 および x_2 を展開する．その結果得られる式が再び x_1, x_2 を含めば，再びそれらを展開する．そして可能な限り展開を続け，展開できなくなったとすると☆，$x_j(u,v,\tau,k)$ は最終的に以下のように，$E(u,v)$ を除けばたかだか G_1, G_2 と自分自身のみによって定義される関数の形に変換される．

$$x_j(u,v,\tau,k) = \begin{cases} 0 \ (\tau < \beta_j \text{ or } \tau-\beta_j < k-u \text{ or} \\ \quad \tau-\beta_j < k-v \text{ or } u=0 \text{ or} \\ \quad u>k \text{ or } v=0 \text{ or } v>k \text{ or } k=0) \\ \mathcal{C}_j[\, G_1(\tau-\beta_1-(k-u),v), \\ \quad G_2(\tau-\beta_2-(k-v),u), \\ \quad x_j(u-1,v-1,\tau-\beta_3,k), \\ \quad E(u,v)\,] \qquad (\text{otherwise}) \end{cases}$$

(3) **出力に関する補題の証明**

$k\times k$ 個のセルから成るシストリックアレイと $(k-1)\times(k-1)$ 個のセルから成るシストリックアレイのセル $\langle u,k-1\rangle$ の出力 x_3 の関係式を補題として証明する．

$$x_3(u,k-1,\tau,k) = x_3(u,k-1,\tau-\beta_2,k-1)$$

(4) **新しい関数の導入と変換**

シストリックアレイ全体の入出力ポートを，アレイの終端に位置するセルに関連づけるための関数を導入し，展開/たたみ込み技法を使った変換により入出力信号の関係式を導出する．回路の対称性から $u\le v$ の場合のみを証明すれば十分である．したがって，$u\le v$ と仮定し，出力としてはポート $\langle u,k\rangle$ $(u=1,\ldots,k)$ のみを調べる．

$$z(u,k,\tau) \stackrel{\text{def}}{=} \underline{x_3(u,k,\tau,k)}$$

⇓ 展開

$$\mathcal{C}_j[\, G_1(\tau-\beta_1-(k-u),k), G_2(\tau-\beta_2,u), \underline{x_3(u-1,k-1,\tau-\beta_3,k)}, E(u,v)\,]$$

⇓ 補題

$$\mathcal{C}_j[\, G_1(\tau-\beta_1-(k-u),k), G_2(\tau-\beta_2,u), \underline{x_3(u-1,k-1,\tau-\beta_3-\beta_2,k-1)}, E(u,v)\,]$$

⇓ たたみ込み

$$\mathcal{C}_j[\, G_1(\tau-\beta_1-(k-u),k), G_2(\tau-\beta_2,u), z(u-1,k-1,\tau-\beta_3-\beta_2), E(u,v)\,]$$

この変換は $\mathcal{C}_j$ によらないことに注意．

最終的に以下のような形を得る．

$$z(u,k,\tau) = \mathcal{C}_j[\, G_1(\tau-\beta_1-(k-u),k), G_2(\tau-\beta_2,u), z(u-1,k-1,\tau-\beta_3-\beta_2), E(u,v)\,] \cdots (*)$$

☆ 停止性に関する議論は本稿の主題の範囲外である．

これは，出力ポート $\langle u,k\rangle$ からの出力信号の再帰的な定義になる．

2.3 信号のマッピング

仕様が入出力信号の関係式で与えられているときは，それが前節で得られた式 (*) と一致すれば証明は終了する．ところが，シストリックアレイの場合，その性格から仕様は行列や数列で与えられることが多く，行列や数列内の位置をパラメータとして含むことが多い．このとき，仕様として与えられるのは信号の関係式ではなく，時刻や回路内の位置という要素を含まない値の関係式と，その値がいつどの入出力ポートで観測されるかを示すタイミングの要求である．したがって，前節で得られた信号の関係式をタイミングの要求に基づいて，仕様に出現する値の関係式にマッピングする必要がある．

まず，与えられたタイミングの要求を以下のように公理として記述する．

$$D_1(\sigma)=G_1(f_1(\sigma),g_1(\sigma),h_1(\sigma))$$
$$D_2(\sigma)=G_2(f_2(\sigma),g_2(\sigma),h_2(\sigma))$$
$$D_3(\sigma)=z(f_3(\sigma),g_3(\sigma),h_3(\sigma))$$

ここで $D_1(\sigma),D_2(\sigma)$ は入力値，$D_3(\sigma)$ は出力値をそれぞれ表す．σ は仕様に出現するパラメータで行列や数列内の位置を示すもの，f_j，g_j，h_j は与えられた関数を表す．

これに従って前節の式 (*) を書き換え，以下の式を得る．

$$D_3(\sigma)=C_j[\,D_1(f'(\sigma)),D_2(g'(\sigma)),D_3(h'(\sigma))\,]$$

ただし，f'，g'，h' は対応する関数である．

この式が与えられた仕様と同一の式であれば証明は終了である．同一でなければ，仕様として与えられた式との等価性を証明する必要がある．2 つの式は時間的な要素を含まないので，σ に関する帰納法が適用される☆．

3. 行列の乗算への応用

前章で示した手続きを行列の乗算を行う 2 次元シストリックアレイ[10]に応用する．

3.1 仕　　様

$C=(c_{ij})$ を $k\times k$ 行列 $A=(a_{ij}),B=(b_{ij})$ の乗算の結果得られる行列とすると，以下の関係が成り立つ．

$$c_{ij}=\sum_{n=1}^{k}a_{in}b_{nj}$$

A を上三角行列，B を下三角行列とする．すなわち，$i>j$ ならば $a_{ij}=0$ であり，$j>i$ ならば $b_{ij}=0$ である．

すると，仕様は以下のような Boyer-Moore 論理で記述することができる．

$$c(i,j,k)=\begin{cases}0 & (k=0 \text{ or } i>k \text{ or } j>k)\\ a(i,k)*b(k,j)+c(i,j,k-1) & (\text{otherwise})\end{cases}$$

図 1 の 2 次元 6 角シストリックアレイにおいて，A の要素は入力ポート $\langle k,v\rangle$ $(v=1,\ldots,k)$ から，B の要素は入力ポート $\langle u,k\rangle$ $(u=1,\ldots,k)$ からそれぞれ 3 時刻ごとに与えられ，C の要素は出力ポート $\langle k,v\rangle$, $\langle u,k\rangle$ $(u,v=1,\ldots,k)$ から 3 時刻ごとに得られる．

3.2 実　　装

3.2.1 単位セルの直截的な記述

x,y をそれぞれ入力ポート $\langle k,v\rangle$ $(v=1,\ldots,k)$, $\langle u,k\rangle$ $(u=1,\ldots,k)$ で観測される信号，z を出力ポート $\langle k,v\rangle$, $\langle u,k\rangle$ $(u,v=1,\ldots,k)$ で観測される信号とする．すると，時刻 τ における入力ポート $\langle k,v\rangle$, $\langle u,k\rangle$ における入力信号はそれぞれ $x(\tau,v)$, $y(\tau,u)$ と，出力ポート $\langle k,v\rangle$, $\langle u,k\rangle$ における出力信号はそれぞれ $z(u,k,\tau)$, $z(k,v,\tau)$ と表される．

単位セルの構造を**図 2** に示す．この図で R_1，R_2 および R_3 は初期値 0 のレジスタを表す．Ain は R_1 に格納された後，$Aout$ としてセル $\langle u-1,v\rangle$ に送られる．同様に，Bin は R_2 に格納された後，$Bout$ としてセル $\langle u,v-1\rangle$ に送られる．Cin は Ain と Bin の積に加えられ，その結果は $Cout$ としてセル $\langle u+1,v+1\rangle$ に送られる．

$xout(u,v,\tau,k)$，$yout(u,v,\tau,k)$ および $zout(u,v,\tau,k)$ はそれぞれセル $\langle u,v\rangle$ の時刻 τ における出力信号 $Aout$，$Bout$ および $Cout$ の値を表す．すると，これらの関数は以下のように直截的に記述できる．

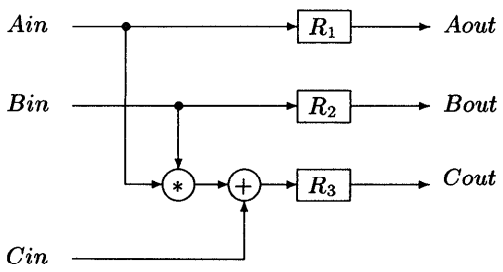


図 2 行列の乗算に対する単位セル
Fig. 2 A unit cell corresponding to the matrix multiplication.

☆ ベースケース等に関しては個別に証明する必要がある．

$$xout(u,v,\tau,k)=\begin{cases}0 & ((1\le u\le k \text{ and } \tau=0) \text{ or}\\ & u=0 \text{ or } u>k+1 \text{ or } k=0)\\ x(\tau,u) & (else,\ u=k+1)\\ xout(u+1,v,\tau-1,k) & \\ & (\text{otherwise})\end{cases}$$

$$yout(u,v,\tau,k)=\begin{cases}0 & ((1\le v\le k \text{ and } \tau=0) \text{ or}\\ & v=0 \text{ or } v>k+1 \text{ or } k=0)\\ y(\tau,v) & (else,\ v=k+1)\\ yout(u,v+1,\tau-1,k) & \\ & (\text{otherwise})\end{cases}$$

$$zout(u,v,\tau,k)=\begin{cases}0 & (\tau<1 \text{ or } k=0 \text{ or}\\ & u=0 \text{ or } u>k \text{ or}\\ & \tau-1<k-u \text{ or}\\ & v=0 \text{ or } v>k \text{ or } \tau-1<k-v)\\ xout(u+1,v,\tau-1,k)* & \\ \quad yout(u,v+1,\tau-1,k)+ & \\ zout(u-1,v-1,\tau-1,k) & \\ & (\text{otherwise})\end{cases}$$

3.2.2 展　　開

$xout, yout$ を展開すると，以下のような $zout$ の定義が得られる．

$$zout(u,v,\tau,k)=\begin{cases}0 & (\tau<1 \text{ or } k=0 \text{ or}\\ & u=0 \text{ or } u>k \text{ or}\\ & \tau-1<k-u \text{ or}\\ & v=0 \text{ or } v>k \text{ or } \tau-1<k-v)\\ x((\tau-1)-(k-u),v)* & \\ \quad y((\tau-1)-(k-v),u)+ & \\ zout(u-1,v-1,\tau-1,k) & \\ & (\text{otherwise})\end{cases}$$

3.2.3 出力に関する補題の証明

続いて $k\times k$ 個のセルから成るシストリックアレイと $(k-1)\times(k-1)$ 個のセルから成るシストリックアレイのセル $\langle u,k-1\rangle$ の出力の関係を示す以下の補題を証明する．

$$zout(u,k-1,\tau,k)=zout(u,k-1,\tau-1,k-1)$$

3.2.4 新しい関数の導入と変換

シストリックアレイ全体の入出力ポートをアレイの終端に位置するセルに関連づけるための関数を導入する．

$$z(u,k,\tau)\stackrel{\text{def}}{=}\underline{zout(u,k,\tau,k)}$$

上の補題を用い，展開/たたみ込み技法を使ってこの式を変換し，入出力信号の関係式を導出する．

$$z(u,k,\tau)=\begin{cases}0 & (k=0 \text{ or } u<1 \text{ or } k<u \text{ or}\\ & \tau-1<k-u)\\ x(\tau-1-(k-u),k)*y(\tau-1,u) & \\ \quad +z(u-1,k-1,\tau-2) & \\ & (\text{otherwise})\end{cases}$$

ここで，$z(u,k,\tau)$ は $k\times k$ 個のセルから成るシストリックアレイの時刻 τ，出力ポート $\langle u,k\rangle$ における出力信号に対応する．

3.3 信号のマッピング

タイミングの要求が以下のように与えられたとする．

$$a(i,j)=x(i+2j-2,j-i+1)$$
$$b(i,j)=y(2i+j-2,i-j+1)$$
$$c'(i,j,k)=z(i-j+k,k,2i+j+2k-3)$$

ただし $1\le i\le j\le k$ である．最初の式は，データ $a(i,j)$ が時刻 $i+2j-2$ に入力ポート $\langle k,j-i+1\rangle$ に与えられることを表す．たとえば，$k=4$ のとき，a_{11}，a_{22}，a_{33}，a_{44} は入力ポート $\langle 4,1\rangle$ に時刻 1，4，7，10 にそれぞれ与えられることを表す．

前節で得られた入出力信号の関係式をタイミングの要求に従って以下のように書き換える．

$$\begin{aligned}&c'(i,j,k)\\ &\quad=z(i-j+k,k,2i+j+2k-3)\\ &\quad=x(3i+2k-4,k)*y(2i+j+2k-4,i-j+k)+\\ &\qquad z(i-j+k-1,k-1,2i+j+2k-3-2)\\ &\quad=a(i,i+k-1)*b(i+k-1,j)+c'(i,j,k-1)\end{aligned}$$

ベースケースを考慮すると，最終的に以下のような式が得られる．

$$c'(i,j,k)=\begin{cases}0 & (k=0 \text{ or } k-1<j-i)\\ a(i,i+k-1)*b(i+k-1,j)+ & \\ \quad c'(i,j,k-1) & (\text{otherwise})\end{cases}$$

これは 3.1 節で与えられた仕様と同一ではない．したがって c' と c の等価性，すなわち任意の i，j，k に対して $c'(i,j,k)=c(i,j,k)$ が成り立つことを証明する必要がある．定義を見ると，両者は引数も再帰呼び出しのパターンも同一であり，同一数列の異なる部分列の要素の和であることが分かる．

図 3 に $j\ge i$ の場合のこの 2 数列の関係を示す☆．図のように区間 I_1，I_2，I_3，I_4 を考える．$c'(i,j,k)$ は区間 I_1，I_2，I_3 の和，$c(i,j,k)$ は区間 I_2，I_3，I_4 の和である．I_1 では A，B とも行列の範囲外の要素

☆ $j<i$ の場合も同様に考えることができる．

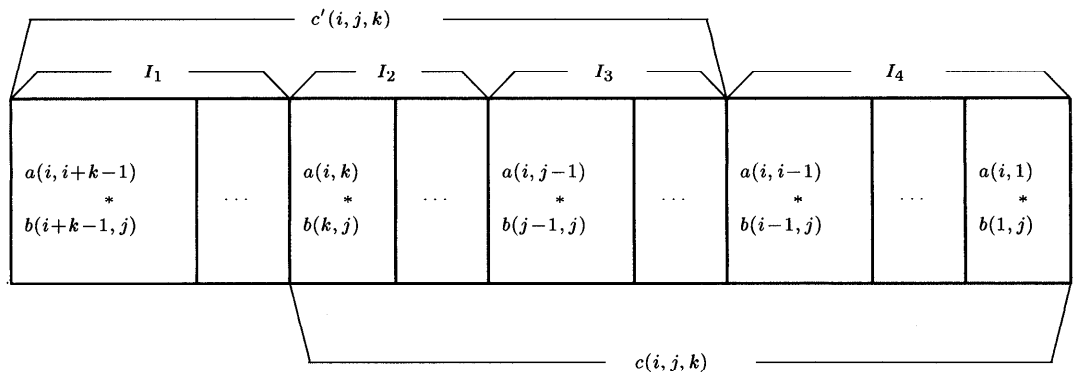


図3 2数列の関係
Fig. 3 The relation between the two sequences.

になっており，値は0である．I_4 では上三角行列 A の要素は0であり，I_3，I_4 では下三角行列 B の要素は0である．したがって，実質的な値が入っているのは区間 I_2 のみであり，問題の2数列はいずれもこの部分を部分列として持っていることから，総和として等しくなっている．

ここで，$c'(i,j,k) = c(i,j,k)$ を直接証明しようとすると失敗する．証明では k を帰納カウンタとした帰納法が適用され，左端から対応する値が調べられるが，両数列の左端の要素が一致しないため，対応する要素がすべてずれてしまうのが失敗の原因である．

以上の議論をもとに，証明を成功させるために，ここではまず I_1 を除いた部分における等価性を証明し，それから I_1 を含めた全体の等価性を証明する，という2段階に分けて証明を行う．

- **STEP1:** I_1 を除いた部分における等価性

$$\sum_{n=1}^{n=k-i+1} a(i,i+n-1)*b(i+n-1,j) = \sum_{n=1}^{n=k} a(i,n)*b(n,j)$$

左辺は c' の区間 I_2，I_3 部分の和，右辺は c 全体（I_2，I_3，I_4 部分）に相当する．帰納法がこの式に適用されると，数列の左端が一致するので，対応する要素は適切なものになる．そして三角行列の性質を使うと証明は成功する．

- **STEP2:** I_1 を含めた全体の等価性

$$\sum_{n=1}^{n=k} a(i,i+n-1)*b(i+n-1,j) = \sum_{n=1}^{n=k} a(i,n)*b(n,j)$$

表1 実験結果
Table 1 Experimental result.

段階	1次元		2次元	
	時間 (s)	補題数	時間 (s)	補題数
展開	76.8	11	184.3	16
出力関係	29.1	7	158.9	9
変換	1.5	1	1.8	1
マッピング	—	—	47.3	16
総和	107.4	19	392.3	42

これを証明するためにまず I_1 部分で定義される再帰関数を補助的に導入し，I_1 部分の要素の和が0であること，すなわち

$$\sum_{n=k-i+2}^{n=k} a(i,i+n-1)*b(i+n-1,j)=0$$

を証明する．次にこの関数を使って

$$\sum_{n=1}^{n=k} a(i,i+n-1)*b(i+n-1,j) = \sum_{n=1}^{n=k} a(i,n)*b(n,j)$$

を証明する．

4. 実験結果

表1 は1次元および2次元シストリックアレイの検証結果である．実験はSPARC Server 670MP 上で行った．

最初の2段階では，2次元の場合1次元に比べてパラメータの数が多いので，それだけ多くの時間がかかった．第3段階の証明は位置を表すパラメータに無関係なため，証明時間もほぼ同じとなった．最終段階は，数列の等価性を証明するのに必要な時間のみを示し，入出力関係をタイミングの要求に基づいてマッピ

ングする部分は含まない．この部分は今回は手作業で行ったが，もちろん自動証明が可能である．

5. おわりに

NQTHMを使ったハードウェア検証の研究開発は活発に行われているもの[2),5),7),9),17)]，シストリックアレイを扱ったものはほとんどなく，定式化もされていない．

GermanとWangは文献4)でBoole関数を計算する1次元シストリックアレイの証明を試みている．しかし，彼らはセルの数をパラメータ化して表現する効用として，毎回特定のサイズに対する検証をしなくても，1回で任意のサイズに対する検証ができるという点に重点をおいており，実際のBoyer-Moore論理を使った記述形式や証明の際に出現する問題点についてはいっさい触れていない．我々はNQTHMの帰納法を適切かつ効果的に利用してシストリックアレイの性質を証明する方法を定式化した．

PurushothamanとSubrahmanyanは文献13)でダイナミックプログラミングに対するシストリックアルゴリズムの証明を行い，証明の詳細や問題点を述べている．彼らは2つの異なる速さでセル間のデータ伝播が行われるような2次元シストリックアレイを対象とし，コンスタントに送られる外部入力は想定していない．我々は，データの速さは一定でコンスタントな外部入力のあるものを対象とした．決定的な違いは，我々がループのある構造を扱っていることであり，ループに起因して起こる帰納法に関する諸問題に解決策を与えたことである．

本稿では，NQTHMを使ったシストリックアレイの証明戦術として，パラメータの数の増大をおさえるために証明を2段階に分けた．まず実装から入出力信号の関係式を導出し，それをタイミングの要求に基づいてマッピングした式が与えられた仕様を満たすことを証明した．後半では，証明すべき式は時間的な要素を含まない式になっており，仕様に出現する数列や行列の位置を表すパラメータに関する帰納法が適用される．前半に関しては手続きを系統化できることを示し，後半に関してはゼロ要素を含む同一数列の異なる部分列の等価性の証明技法を示した．

最近，NQTHMの産業的な用途への適用を目的としたACL2が開発され，組込み補題集合，規則の自動適用機能，データベース利用ツール等がかなり強化された[8)]．これによれば，本稿での実験で用いた雑多な補題は不要となるかもしれないが，証明の大筋を構成する「知的な」補題をシステムが自動的に生成/示唆することは不可能であると考えられる．

本稿で提案した方法は他のシストリック構造に関しても適用可能であり，使った補題はシストリックアレイ検証用のライブラリとして提供することができる．また，本手法を証明戦術としてプログラム化することにより，HOL[6)]やPVS[12)]など戦略志向の証明器にも応用可能である．

参考文献

1) Boyer, R.S. and Moore, J.S.: *A Computational Logic Handbook*, Academic Press (1988).
2) Bronstein, A. and Talcott, C.L.: Formal Verification of Synchronous Circuits Based on String-Functional Semantics: The 7 Paillet Circuits in Boyer-Moore, *Automatic Verification Methods for Finite State Systems*, Sifakis, J. (Ed.), pp.317–333, Springer-Verlag (1989).
3) Bryant, R.E.: Graph-Based Algorithms for Boolean Function Manipulation, *IEEE Trans. Comput.*, Vol.C-35, No.8, pp.677–691 (1986).
4) German, S.M. and Wang, Y.: Formal Verification of Parameterized Hardware Designs, *Proc. International Conference on Computer Design*, pp.549–552, IEEE (1985).
5) Goldschlag, D.M.: Mechanically Verifying Safety and Livencss Property of Delay Insensitive Circuits, *Computer Aided Verification*, Larsen, K.G. and Skou, A. (Eds.), pp.354–364, Springer-Verlag (1991).
6) Gordon, M.J.C.: HOL: A Proof Generating System for Higher-Order Logic, *VLSI Specification, Verification and Synthesis*, Birtwistle, G. and Subramanyan, P.A. (Eds.), pp.73–128, Kluwer Academic Publishers (1988).
7) Hunt, Jr, W.A.: FM8501: A Verified Microprocessor, PhD Thesis, University of Texas at Austin (1985). Also available through Computational Logic Inc.
8) Kaufmann, M. and Moore, J.S.: ACL2: An Industrial Strength Version of Nqthm, *Proc. 11th Annual Conference on Computer Assurance (COMPASS96)*, pp.23–34, IEEE Computer Society Press (1996).
9) Kinniment, D.J. and Koelmans, A.M.: Modelling and Verification of Timing Conditions with Boyer Moore Prover, *Theorem Provers in Circuit Design*, Stavridou, V., Melham, T. and Boute, R.T. (Eds.), pp.111–127, Elsevier Science Publishers, North-Holland (1992).
10) Kropf, T.: Benchmark-Circuits for Hardware-Verification, *Theorem Provers in Circuit Design*, pp.1–12 (1995). TPCD Benchmarks,

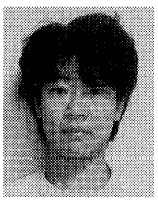
http://goete.ira.uka.de/benchmarks (1996).
11) Kung, H.T.: Why Systolic Architectures?, *IEEE Computer*, Vol.X, No.1, pp.37–46 (1982).
12) Owre, S., Rushby, J.M. and Shankar, N.: PVS: A Prototype Verification System, *11th International Conference on Automated Deduction*, pp.748–752, Springer-Verlag (1992).
13) Purushothaman, S. and Subrahmanyam, P.A.: Mechanical Certification of Systolic Algorithms, *Journal of Automated Reasoning*, Vol.5, No.1, pp.67–91 (1989).
14) Takahashi, K. and Fujita, H.: Time Parameterized Function Method: A New Method for Hardware Verification with the Boyer-Moore Theorem Prover, *Proc. CHDL '95* (*IFIP Conference on Hardware Description Languages and Their Applications*), pp.545–552 (1995).
15) Takahashi, K. and Fujita, H.: TPF: An Effective Method for Verifying Synchronous Circuits with Induction-Based Provers, *IEICE Trans. Information and Systems*, Vol.E81-D, No.1, pp.12–18 (1998).
16) Takahashi, K. and Fujita, H.: A Verification Method for Systolic Arrays Using Induction-Based Theorem Provers, *Artificial Intelligence in Engineering* (1998). To appear.
17) Verkest, D., Vandenbergh, J., Claesen, L. and de Man, H.: A Description Methodology for Parameterized Modules in the Boyer-Moore Logic, *Theorem Provers in Circuit Design*, Stavridou, V., Melham, T.F. and Boute, R.T. (Eds.), pp.37–57, Elsevier Science Publishers, North-Holland (1992).
18) 高橋和子，藤田 博：NQTHMを用いたシストリックアレイの検証，情報処理学会研究報告，95-PRO-4, pp.45–50 (1995).
19) 高橋和子，藤田 博：帰納法に基づく定理証明器によるシストリックアレイの検証，情報処理学会研究報告，96-PRO-10, pp.61–66 (1996).

(平成10年2月23日受付)
(平成10年5月 8 日採録)

推 薦 文

本論文は，帰納法に基づく定理証明系NQTHMを用いてシストリックアレイの検証を行った研究に関するものである．近年，ハードウェア検証の重要性がソフトウェア検証にも増して認識されている．その中でも，シストリックアレイは，繰返しパターンを持つため，検証に帰納法を必要とし，通常のハードウェアの検証とは違った難しさを持っている（普通のハードウェアならば組合せ的手法によって検証できる）．この論文は，シストリックアレイの検証を帰納法によって定式化したうえで，現実的な例に対する検証が証明系を使って現実に行えることを示したものであり，証明技法，応用事例の両面での貢献が大きい．プログラミング研究会からの推薦論文とするに値する十分な成果を含んでいる．

（プログラミング研究会主査 石畑 清）



高橋 和子（正会員）

1958年生．1982年京都大学理学部卒業．同年三菱電機（株）入社．同社中央研究所（1995年より先端技術総合研究所）勤務．知識表現，並列論理型言語を用いた問題解決手法，ハードウェア論理検証の研究に従事．1997年4月からATR音声翻訳通信研究所に出向．対話処理の研究に従事．1994年京都大学工学博士．1997年本会研究賞受賞．電子情報通信学会，日本ソフトウェア科学会各会員．

藤田 博（正会員）

1955年生．1980年東京大学大学院工学系研究科情報工学専攻修士課程修了．同年三菱電機（株）入社．同社中央研究所勤務．1986～1990年（財）新世代コンピュータ技術開発機構に出向．1996年九州大学大学院システム情報科学研究科助教授．工学博士．自動推論システム，知識表現，形式的検証等の教育・研究に従事．1989年本会研究賞受賞．電子情報通信学会，日本ソフトウェア科学会，人工知能学会，ACM，IEEE-CS各会員．