様式 C-19

科学研究費補助金研究成果報告書

平成２１年　５月　１８日現在

研究種目：基盤研究（Ｃ）
研究期間：2007～2008
課題番号：19500039
研究課題名（和文）　冗長な数表現による剰余数系演算回路および剰余数－重み数変換回路の研究
研究課題名（英文）　Research of residue arithmetic and number conversion circuits using redundant number representation

研究代表者
魏　書剛　（WEI SHUGANG）
群馬大学・大学院工学研究科・教授
研究者番号：10251125

研究成果の概要：　２進ＳＤ数表現を用いた剰余数系から従来の２進数系への変更を高速に実行できるハードウェアアルゴリズムを提案した。この方法では、ＳＤ数演算の並列処理特徴を生かした。変換に必要な演算をさらに高速に行うため、基本演算回路であるＳＤ数加算回路の高速化方法を考案した。変換回路および算術演算の回路設計およびシミュレーションを行い、高速な回路が得られることを明らかにした。また､そろばん数表現を剰余数系の演算に適用し、高性能の剰余回路の実現が期待できることを設計と回路評価により確認した。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	900,000	270,000	1,170,000
２００８年度	500,000	150,000	650,000
年度			
年度			
年度			
総　計	1,400,000	420,000	1,820,000

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：算術演算、剰余数系、剰余数演算、剰余数系―重み数系変換

１．研究開始当初の背景

剰余演算および剰余数系における算術演算は、現在信号処理、データ通信、暗号処理、情報セキュリティなどの分野において応用され、その高速化が、ますます重要な研究課題となってきている。

剰余数系は、各剰余桁の演算が独立に行われるため、算術演算が並列に実行できる特長を持つ。特に高速な実時間信号処理や多重化による高信頼情報処理システムなどの分野への応用が期待されている。しかし、剰余算術演算（例えば、剰余加算）システムでは従来の加算などの算術演算後、剰余演算を行う回路が必要となるため、２進数演算システムより構成される演算システムが複雑になってしまう。特に従来の方法では、剰余桁ごとにメモリを持つ剰余演算回路が複雑な構成となり、剰余数系の各剰余桁に２進数を用いたため演算速度は桁上げ伝播に制限されている。

我々は、剰余数系の冗長な数表現を定義することにより、符号桁付き（Signed-Digit, ＳＤ）数表現を剰余演算に導入するという新しい概念を提案した。ＳＤ数表現を用いた算術演算は、桁上げの伝搬を１桁に制限されるため、様々な長い語長の算術演算に活用されている。しかし、従来の非冗長な剰余数系には適用できない。我々は、ＳＤ数演算の優れた演算性質を冗長な剰余数系に適用できる概念に基づき、定数の剰余加算時間で語長に依存しない剰余加算アルゴリズムを提案した。従来の数系表現方法では、単純にＳＤ数表現を剰余数系演算に適用できない。我々は、冗長性を有する剰余数表現をすでに新しく定義してきている。この剰余数表現を利用することによりＳＤ数表現の演算を簡単に剰余演算に適用できるため、剰余数系における剰余演算が高速に実行される。結果として、剰余演算メモリが不用であること共に、剰余加算（減算）を桁上げ伝播が生じないＳＤ数加算器で行うことができる。さらに、剰余乗算器が剰余加算器を２分木構造に構築することにより実現でき、p 桁の剰余乗算器の場合、剰余乗算時間が log(p)に比例し、非常に高速である。このような算術演算システムが実時間信号処理などへ応用することにより、高速かつ高信頼性の信号処理システムの構築が期待できる。

剰余演算が高速に行われる算術演算アルゴリズムが検討されてきたが、従来の重み数系との数表現変換がまだ重要な課題となっている。２進数を用いた変換回路について、数多くの変換アルゴリズムが提案されているが、桁上げ伝搬の問題が依然に残されており、冗長な数系を用いた効率的な変換アルゴリズムが期待されている。

２．研究の目的

本研究では、剰余数系における算術演算の高速化方法、および従来の重み数系（例えば、２進数）への高速変換のハードウェアアルゴリズムの提案を研究の目的としている。例えば、算術演算システムは、従来の２進数の入出力データを持ち、内部ではＳＤ数表現を用いた高速剰余演算を行う。高速の剰余数系－重み数系の高速相互変換回路を使用すれば、従来の演算システムと同様に応用可能となる。

現在、ＳＤ数表現を用いた剰余加減算および剰余乗算アルゴリズムを提案し、従来の２進数による方法より高速性を有することを確認している。しかし、剰余除算アルゴリズムはまだ開発中であり、特に、法の選択により、より高速の演算ハードウェアアルゴリズムの構築が可能と予測している。また、ＳＤ数表現を用いた剰余演算を重み数系―剰余数系の相互変換に応用した場合、その高速性を引き出せる新しい原理に基づくアルゴリズムを構築するために、各種の法（modulus）について数表現の変換における数学的な性質を究明する必要がある。

具体的に次の目標を設けて、研究を進めてきている。

（１）ＳＤ数を用いた効率的な剰余数演算を行うための数学的な条件を明確し、異なる法を用いた演算処理のために必要となる基礎的な理論（定理など）を確立する。

（２）ＳＤ数により並列処理が行える高速の剰余数系算術演算アルゴリズムおよび通常の重み数系（例えば、２進数系）間の変換アルゴリズムを提案する。さらに、効率的な符号化を考察する。

（３）本提案の剰余演算システムをＶＬＳＩ化することにより性能評価および高速な実時間信号処理システムなどへの応用を実施する。

３．研究の方法

研究代表者が、研究の全般について、すなわち、研究の計画、実施および実験などを全般的に行った。大学院学生を指導し、関連の研究調査や実験などを実施した。数学的なモデリング方法および高速なVLSI演算アルゴリズムの提案をし、回路設計や回路性能評価などについて、学生の協力を得た。

（１）研究調査

効率的な演算を行うために、剰余数系の法の選択を含むいろいろな数学的な条件を満たさなければならない。特に、冗長なSD数表現を導入することにより、演算に使われている数表現が多様化となるため、多様な性質の存在が予測されている。研究調査を行うことにより、研究分野の研究成果を有効に取り入れ、本研究の数学的な方法および実験方法を効率に明らかにするため、調査を行った。

国内学会や研究会などに出席することにより、本研究の成果を発表するとともに関係する研究資料の収集などを行った。研究調査を申請の旅費で実施し、数値情報処理システムへの応用について、企業などの関係者から情報の収集を行った。

（２）実験および研究成果の評価

我々の提案したアルゴリズムをもっと一般的に展開し、剰余加算、減算、乗算などの基本演算アルゴリズムに加え、剰余除算および多項式などを計算する回路のアルゴリズムを考案してみた。実時間情報処理システムの構築を行う際に複合演算が必要となることを着目し、実際の２進数演算システムとのインターフェースを開発する必要がある。すなわち、冗長な剰余数表現を従来の重み数表現を高速に変換するアルゴリズムを研究してきた。冗長な数表現を用いた並列処理を行う統合的な演算アルゴリズムを重要な研究課題としていた。

数学的なモデリング手法を用いて、検討してきたアルゴリズムについて、従来の２進数法との比較を行い、数学的な解析を行った上、実際の回路設計による実験を実施した。

提案したハードウェアアルゴリズムのVLSI化評価のため、申請の計算機設備を用いて、東京大学大規模集積システム設計教育研究センターに提供されているVLSI設計ツールによりVLSI設計、動作シミュレーションを行った。もちろん、他の文献により提案された方法によるVLSI設計も同設備を使用して実験を行い、性能比較を実施した。すなわち、科研費で購入した高性能を持つ計算機（サンマイクロシステム社Blade1500）を用いて、数値情報処理システムの演算モデリングから、演算回路システムのVLSI設計、細かいタイミング動作の確認までを行った。具体的に、ハードウェア記述言語ＶＨＤＬなどの計算機言語を使用する設計開発ツールをこの計算機システム上で活用している。

さらに、VLSI設計評価の方法として、FPGA（Field Programmable Gate array）ICを用いることである。現在、Altera社の大学教育プログラムに参加し、無料に提供されているFPGA回路設計ライセンスを使用している。FPGAの評価ボードICを購入し、実機の実験によるシステム動作確認と評価を行った。

４．研究成果

本研究では、剰余数系における算術演算の高速化方法、および従来の重み数系（例えば、２進数）への高速変換のハードウェアアルゴリズムの提案を研究の目的としている。算術演算システムは、従来の２進数の入出力データを持ち、内部ではＳＤ数表現を用いた高速剰余演算を行う。高速の剰余数系－重み数系の高速相互変換回路を使用すれば、従来の演算システムと同様に応用可能となる。

研究成果として、２進ＳＤ数表現を用いた剰余数系から従来の２進数系への変更を高速に実行できるハードウェアアルゴリズムを提案した。この方法では、ＳＤ数演算の並列処理特徴を生かした。変換に必要なパラメータを演算に使いやすい形のＳＤ数表現にすることによって、変換の基本演算回路は演算量が極めて少ないＳＤ数加算回路と符号反転回路から構成される。また、得られたＳＤ数表現の重み数を２進数への変換アルゴリズムを工夫した。木構造の桁上げ回路を考案し、従来の２進数アルゴリズムより高速性を有することが、回路設計およびシミュレーションによって確認された。関連の研究成果を論文①にまとめて発表した。また、数系変換に使用している中国人剰余定理において、剰余逆数の計算が必要である。論文②では、ＳＤ数表現を用いた剰余乗算逆数演算の高速アルゴリズムを提案した。

剰余数系の法を2^p-1の形にしたとき、剰余演算の効率が一番効率よい回路構成が設計できることが、以前の研究成果から明らかにされている。しかし、効率的な変換アルゴリズムは提案されていない。変換手続きの中、剰余乗算逆数を求める方法が最も重要である。本研究では、ＳＤ数演算を用いた剰余乗算逆数を求める方法を提案した。

２進ＳＤ数表現を用いた剰余数系から従来の２進数系への変更を高速に実行できるハードウェアアルゴリズムを提案した。この方法では、ＳＤ数演算の並列処理特徴を生かした。変換に必要な演算をさたに高速に行うため、基本演算回路であるＳＤ数加算回路の高速化方法を考案した。剰余ＳＤ数加算回路の内部中間加算結果を２進数符号化にしたことにより、後続の加算入力数を減らし、回路全体の規模や遅延時間を小さくすることができた。変換回路および算術演算の回路設計およびシミュレーションを行い、高速な回路が得られることを確認した。新しい加算器を用いて新しい剰余乗算回路の設計を行った、設計ツールなどにより、提案した回路シミュレーションおよび性能評価をした。２進数表現を用いた演算回路との比較も行った。従来の方法より、高速の性能を大幅に向上させることを確認した。研究成果を論文④と⑥にまとめた。

また、本研究の目的で、異なった数表現である「そろばん」数表現を着目した。そろばんアーキテクチャを用いることにより、１０進数演算の遅延時間が従来のBCD符号を用いた演算より短いアルゴリズムを提案した。さらに、そろばん数表現を用いた剰余数系の演算に適用でき、剰余の法を使用しやすくなり、高性能の剰余回路の実現が期待できることを設計と回路評価により確認した。研究会で研究成果を公表し、今後、発展していきたい。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計６件）

1. 飯島唯仁、魏書剛、算盤アーキテクチャを用いた１０進加算器とその剰余演算への応用、電子情報通信学会技術研究報告、DC2008、19-23、2009、査読有

2. S.Wei, Modular Multipliers Using a Modified Residue Addition Algorithm with Signed-Digit Number Representation, Lectures Notes in Engineering and Computer Science, Vol.1, 494-499, 2009, 査読有

3. 長澤　俊介、魏　書剛、算盤アーキテクチャに基づく算術演算回路、電子情報通信学会技術究報告、ICD2007-148、53-58、2008、
査読無

4. S.Wei, A New Residue Adder with Redundant Binary Number Representation, Proceedings of the 6th Annual IEEE Northeast Workshop on Circuits and Systems,Vol.1, 157-160, 2008, 査読有

5. S. Chen and S. Wei, A fast algorithm for
RNS-to-binary conversion, WSEAS Transactions on Computers, Vol. 6, 733 - 740, 2007, 査読有

6. S. Wei 、A multiplicative inverse algorithm based on modulo (2^p -1) signed-digit arithmetic for residue to weighted number conversion, Proceedings of 2007 IEEE international Symposium on integrated Circuits, Vol.1,25-28, 2007, 査読有

６．研究組織
(1)研究代表者

魏　書剛（WEI SHUGANG）
群馬大学・大学院工学研究科・教授
研究者番号：10251125