第５号様式

論文審査の要旨

博士の専攻分野の名称	博　士　（　工学　）	氏名	本田　巧
学位授与の要件	学位規則第４条第[1]・２項該当		

論　文　題　目

A Study of Multiple-length Multiplication on the GPU

(GPU における多倍長整数乗算に関する研究)

論文審査担当者

主　　査　　教　授　　中野　浩嗣　　印

審査委員　　教　授　　藤田　聡　　印

審査委員　　准教授　　伊藤　靖朗　　印

〔論文審査の要旨〕

GPU(Graphics Processing Unit)は，内部に多数のコアを搭載した画像処理に特化したハードウェアである．近年，GPU を汎用計算の高速化に利用する研究が活発に行われている．本研究では，GPU における多倍長整数乗算の並列計算手法の提案と実際の GPU を用いた性能評価を行っている．また，多倍長整数乗算を必要とするアプリケーションの GPU 実装も提案し，実際の GPU を用いて性能評価を行っている．本研究はこれらの研究をまとめたものである．

第 1 章では，研究背景と研究成果の概略について述べている．

第 2 章では，研究成果の理解に必要な GPU の構造と，GPU のための統合開発環境である CUDA(Compute Unified Device Architecture)について説明している．

第 3 章では，大量の多倍長整数乗算を効率的に並列計算する GPU 実装手法を提案している．一般的なプロセッサでは，32bit や 64bit の整数までしか直接的に扱うことができない．そのため，巨大な整数は 32bit や 64bit の固定長の整数型を複数用いて多倍長整数として表現する．多倍長整数演算は，プロセッサによって直接処理される 32bit や 64bit の整数演算に比べ非常に時間のかかる処理である．特に，多倍長整数乗算は加減算に比べ多くの時間を必要とする．しかし，暗号処理や科学技術計算の分野では，巨大な値の乗算が必要となるため，多倍長整数乗算の高速化への高い要求がある．本論文の提案実装では，ワープ同期プログラミングテクニックを導入し，32 個のスレッドで 1024bit の乗算の並列化を行っている．GPU での処理は，32 個のスレッドをまとめたワープと呼ばれる単位で行われる．ワープ内のスレッドは常に同期しながら処理を行う．そのため，ワープ内の 32 個のスレッドで処理を並列化することで，処理の遅延の原因となる同期操作を用いずに並列処理が可能となる．また，最新の GPU では，ワープ内のスレッドのデータ通信を，メモリを介さずに行う機能がある．これらの特徴に基づき，同

期操作とメモリアクセスを必要としない 1024bit 整数の並列乗算を実現している． また，1024bit より小さい， または， 大きな多倍長整数の乗算への適用方法も示している．1024bit より大きな多倍長整数の乗算については， 1024bit の並列乗算手法をサブルーチンとし， 乗算回数を低減できる乗算アルゴリズムである Toom-Cook 法を適用している．そして， 既存の CPU/GPU 実装との性能比較を行い高速に乗算できることを示している．

第 4 章では， コラッツ予想の網羅的検証のための GPU 実装手法を提案している． コラッツ予想では， 任意の自然数に対して次の 2 つの操作を考える． 偶数である場合はその値を 2 で割る． 奇数である場合はその値を 3 倍し 1 を加算する． コラッツ予想は， これらの 2 つの操作を繰り返すと全ての自然数は有限回で 1 に達するという予想であるが，証明は得られていない未解決の問題である． 現在， 検証が行われている自然数が 72bit で表現される値であるため検証は多倍長整数を用いて行われる．ルックアップテーブルと多倍長整数乗算を用いることで， 各自然数に対する複数回の操作を 1 回で行うことができ， 検証を高速化できることが知られている． しかし， GPU ではメモリアクセスはその他の命令よりも時間のかかる処理である． そのため， 各スレッドが効率よくメモリにアクセスができる GPU に適した自然数のスレッドへの割り当てを提案している． また，多倍長整数乗算の最適化を行っており， 結果として， CPU による網羅的検証に対して大幅な高速化が行えることを示している．

第 5 章では， 第 4 章までの成果を要約し結論としてまとめている．

以上，審査の結果，本論文の著者は博士（工学）の学位を授与される十分な資格があるものと認められる．

備考：審査の要旨は，1，500 字以内とする。