

研究紹介

高性能算術演算回路の実装と性能評価

琉球大学 工学部 工学科 電子情報通信コース・准教授 島袋 勝彦

(E-mail : simabuku@tec.u-ryukyu.ac.jp)

1. はじめに

算術演算を行う数系として、情報処理で広く利用される重み数系とは異なる、数値を割った余り（剰余）を活用した剰余数系による算術演算方式が知られています。その剰余数系を用いると重み数系と比較して加減算・乗算剰余算が各剰余桁で並列に行えるため高速演算が期待できます（図 1）。また、乗算の演算処理方式の一種であるシリアル-パラレル演算方式においては、演算セルを効率よく利用することにより演算セルの稼働率が高く、パラレル演算方式と比較して性能比の向上が期待できます。

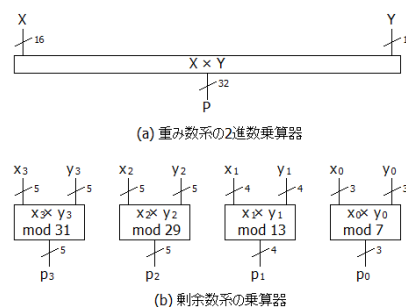


図 1. 重み数系の 2 進数乗算器と剰余数乗算器の比較

2. モンゴメリ法による乗算剰余算

剰余数系での各剰余桁内で必要となる乗算剰余算を行うためには、一般に除算が必要であるが、時間のかかる除算を実質的に行わず加減算・乗算・シフト演算のみで計算することができるモンゴメリ法が知られています。その法によって乗算剰余算を行う際、剰余の算出に利用される「割る数（モジュラス）」の値により計算完了までの時間（計算時間）の短縮が示唆されていましたが、その関係性の具体的な導出が未報告のため明らかにする必要がありました。またそれを踏まえて、パラレル演算方式より回路規模が縮小可能なシリアル-パラレル演算方式を組み合わせることにより、高速・高集積なモンゴメリ乗算器の実現が期待できます。

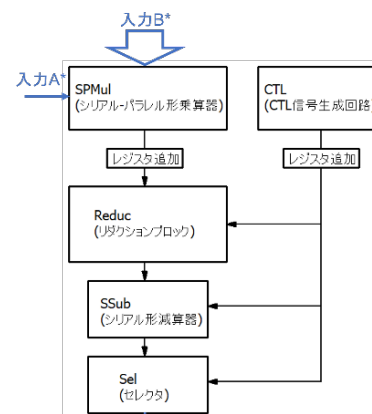


図 2. パイプライン化したシリアル-パラレル形モンゴメリ乗算器のブロック図

3. シリアル-パラレル形モンゴメリ乗算器の設計と評価 [1, 2]

計算時間が短縮可能なモジュラスの選択方法、シリアル-パラレル形およびパイプライン化技術を組み合わせたシリアル-パラレル形モンゴメリ乗算器（図 2）を提案し FPGA により実現しました。その結果、回路規模と計算時間を用いた評価（LT 積）においてパラレル形モンゴメリ乗算器より提案回路の方が約 6 分の 1（36 ビットでの評価）となり（図 3）、提案回路の性能が高いことを明らかにしました。

参考文献

- [1] 壺内博幸, 金城光永, 島袋勝彦, 信学技報, Vol.121, No.130, ICD2021-11, pp.54-57 (2021).
- [2] 壺内博幸, 琉球大学大学院理工学研究科電気電子工学専攻修士（工学）学位論文 (2022).

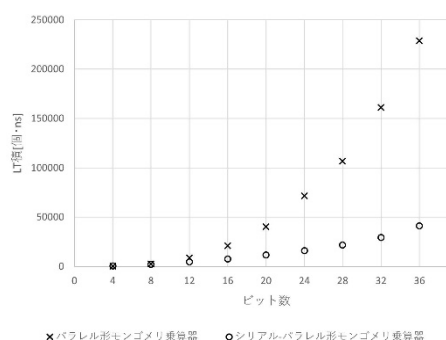


図 3. シリアル-パラレル形モンゴメリ乗算器（提案回路）とパラレル形モンゴメリ乗算器の各ビット数に対する LT 積