

2 値による情報の表現方法だけでなく多値も活用した 高速・高集積な演算回路の実現

工学科電子情報通信コース・准教授 島袋 勝彦

1. 研究背景

パソコンの中のマザーボード上には、様々な集積回路が搭載されています。この集積回路では、情報を 0 と 1 の 2 値で表現し処理を行っています。その情報表現において、2 値ではなく 3 つ以上の値を基本とした多値による表現方法（多値符号化）と処理方式も存在します。実際、情報を記憶するメモリは 0 と 1 の 2 状態ですが、例えば、最近の USB メモリなどでは、多値（マルチレベルセル（MLC）型）が利用されています。また、多値符号化を用いた情報処理において、多値に適した様々な算術演算方式の有用性が確認されています。例えば、2 値の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並列に加減算、乗算剰余算が行えるため高速演算が期待できます（図 1）。

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、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。そのモンゴメリ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す。また、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用いたモンゴメリ乗算器は開発途中であり、その完成が求められていました。これらを組み合わせることにより、高速で高集積なモンゴメリ乗算器の実現が期待できます。

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、回路規模と計算完了の時間を用いた評価（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。

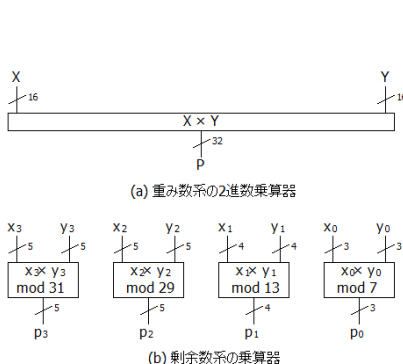


図 1 重み数系の 2 進数乗算器と剰余数乗算器の比較。

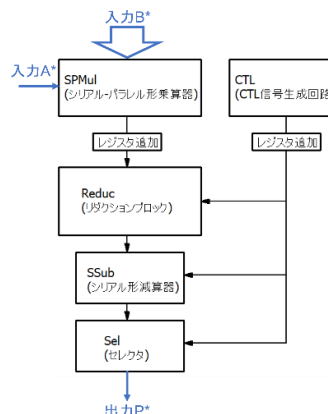


図 2 パイプライン化したシリアル-パラレル形モンゴメリ乗算器のブロック図。

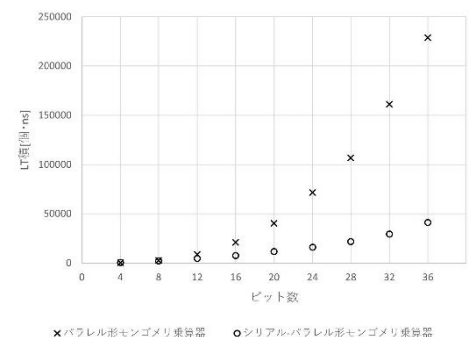


図 3 シリアル-パラレル形モンゴメリ乗算器（提案回路）とパラレル形モンゴメリ乗算器の各ビット数に対する LT 積